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 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. 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. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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, or hardware provided by Avaya. All content on this site, the documentation 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

Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Avaya channel partner would like to install two of the same type of vAppliances, then two vAppliances of that type must be ordered.
Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that 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”). 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 Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

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. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, 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 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.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.
# Contents

**Chapter 1: Introduction**

- Purpose................................................................. 9
- Intended audience.................................................. 9
- Document changes since last issue......................... 9
- Related resources.................................................... 9
  - Documentation...................................................... 9
  - Training............................................................... 12
  - Avaya Mentor videos............................................ 12
  - Support................................................................. 13

**Chapter 2: Verifying secure communication with client applications**

- Verifying secure communication between Avaya ACE™ and client applications................................................. 15
- Enabling weak ciphers............................................. 16
- Logging in to Avaya ACE host.................................... 17

**Chapter 3: Communication port management**

- Enabling or disabling the HTTP port on ACE host......................... 19
- Enabling or disabling port for event notification channel on ACE host......................................................... 21
- Configuring HTTPS on WebSphere Application Server administration interface.................................................. 21
- Verifying secure communication with Avaya ACE.............. 23

**Chapter 4: Certificate management**

**Chapter 5: User management fundamentals**

- User management interfaces.................................... 28
  - Web-based graphical user interface........................ 29
  - User Profile web service interface.......................... 29
- User authentication.................................................. 30
- Authorization policies............................................. 30
- Role profile.......................................................... 30
  - Licenses............................................................... 31
  - Access control rules............................................. 31
- Predefined roles.................................................... 32
  - SystemAdminRole................................................ 32
  - FederationRole.................................................... 33
  - SystemMonitorRole............................................... 33
  - TrustedRole........................................................ 33
  - RfSC role............................................................. 34
  - MessagingAdminRole............................................ 34
- Global user authorization policies.............................. 34
  - Global account policy........................................... 34
  - Global password policy....................................... 35
- User profile.......................................................... 38
  - Mandatory user information.................................. 38
  - Role membership................................................ 39
  - User account policy............................................. 39
  - User preferences................................................ 40
- Predefined user profiles.......................................... 40
<table>
<thead>
<tr>
<th>Chapter 6: User authentication</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWA authentication</td>
<td>43</td>
</tr>
<tr>
<td>IWA configuration for single domain</td>
<td>44</td>
</tr>
<tr>
<td>IWA configuration for multiple domains</td>
<td>45</td>
</tr>
<tr>
<td>Creating a user in AD</td>
<td>45</td>
</tr>
<tr>
<td>Configuring a domain name server</td>
<td>47</td>
</tr>
<tr>
<td>Generating the keytab file</td>
<td>52</td>
</tr>
<tr>
<td>Configuring browsers to support IWA authentication</td>
<td>54</td>
</tr>
<tr>
<td>Merging keytab files</td>
<td>57</td>
</tr>
<tr>
<td>Editing Kerberos configuration file</td>
<td>58</td>
</tr>
<tr>
<td>Creating trust between realms</td>
<td>59</td>
</tr>
<tr>
<td>Validating trust between realms</td>
<td>62</td>
</tr>
<tr>
<td>HTTP Basic</td>
<td>64</td>
</tr>
<tr>
<td>LDAP authentication</td>
<td>64</td>
</tr>
<tr>
<td>LDAP configuration parameters</td>
<td>65</td>
</tr>
<tr>
<td>ACE database authentication</td>
<td>66</td>
</tr>
<tr>
<td>Adding an IP as trusted host</td>
<td>66</td>
</tr>
<tr>
<td>Configuring authentication post installation</td>
<td>67</td>
</tr>
<tr>
<td>Troubleshooting authentication issues</td>
<td>68</td>
</tr>
<tr>
<td>Checks to be performed before configuring authentication</td>
<td>68</td>
</tr>
<tr>
<td>Verify Kerberos settings</td>
<td>69</td>
</tr>
<tr>
<td>Service principal not found or set incorrectly</td>
<td>70</td>
</tr>
<tr>
<td>Duplicate service principal names found</td>
<td>71</td>
</tr>
<tr>
<td>Incorrect FQDN in SPN</td>
<td>72</td>
</tr>
<tr>
<td>Authentication falls back to NTLM</td>
<td>72</td>
</tr>
<tr>
<td>Incorrect keytab file generation</td>
<td>73</td>
</tr>
<tr>
<td>LDAP bind user password expires</td>
<td>74</td>
</tr>
<tr>
<td>Authentication fails when user belongs to many groups</td>
<td>75</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7: Global security policy management</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing global password policy settings</td>
<td>79</td>
</tr>
<tr>
<td>Changing global password policy settings</td>
<td>80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8: Role management</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a role profile</td>
<td>81</td>
</tr>
<tr>
<td>Modifying a role profile</td>
<td>83</td>
</tr>
<tr>
<td>Deleting a role profile</td>
<td>84</td>
</tr>
<tr>
<td>Job aid for counting licenses</td>
<td>85</td>
</tr>
<tr>
<td>Job aid for configuring access control rules</td>
<td>85</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9: User management</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing your password</td>
<td>87</td>
</tr>
<tr>
<td>Logging on to the Avaya ACE GUI</td>
<td>88</td>
</tr>
<tr>
<td>Creating a user</td>
<td>89</td>
</tr>
<tr>
<td>Adding contact information to a user configuration</td>
<td>91</td>
</tr>
<tr>
<td>Job aid for specifying contact identifiers</td>
<td>92</td>
</tr>
</tbody>
</table>
Modifying contact information................................................................................................................... 94
Enforcing a password change........................................................................................................................ 95
Modifying a user............................................................................................................................................... 96
Unlocking a user account............................................................................................................................... 97
Configuring a user account policy.................................................................................................................. 97
Deleting contact information from a user configuration............................................................................... 98
Deleting user profiles.................................................................................................................................... 99
Viewing security audit logs............................................................................................................................. 100
Listing ACE users......................................................................................................................................... 101
Chapter 10: Managing Websphere security................................................................................................. 103
Chapter 11: Database administration........................................................................................................... 105
Changing the database password.................................................................................................................. 105
Appendix A: Kerberos terminology................................................................................................................ 107
Index............................................................................................................................................................... 109
Chapter 1: Introduction

Purpose

This document provides information on how Avaya Agile Communication Environment™ performs user and security management.

The Avaya ACE™ host supports a Web based OAMP GUI that administrators can use to perform tasks related to system administration, configuration, fault management, performance management, and user management.

Intended audience

The primary audience for this document is anyone who must configure, troubleshoot, maintain, or verify Avaya ACE at a customer site. The audience includes implementation engineers, field technicians, business partners, and customers.

Document changes since last issue

- *Introduction* chapter now includes the purpose, audience, help resources, and support information.
- *Configure secure communications* chapter includes procedures to set up secure communication with client applications through certificate exchange.

Related resources

Documentation

This document is a part of the Avaya ACE documentation suite. Avaya ACE documents provide information on Avaya ACE fundamentals and planning, ordering ACE software, and ACE
Installation and administration. The documents also contain information on Avaya and third-party system solution integration, Web service application programming interfaces (APIs), security, fault, and performance management, and troubleshooting.

You can also find information on core applications or APIs delivered with the base software, for example, Message Drop, and Message Blast API.

**Avaya ACE Release 6.2.1 documents**

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Overview and Specification</td>
<td>Provides a description of ACE including solution architecture, services, features, hardware, and software.</td>
<td>Sales engineers, Solution architects, Implementation engineers, and Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Documentation Roadmap (NN10850–002)</td>
<td>Provides a list of documents in the Avaya ACE documentation suite for the release.</td>
<td>Sales engineers, Solution architects, Implementation engineers, and Support personnel</td>
</tr>
<tr>
<td><strong>Installation, upgrades, migrations, and configurations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Planning and Installation (NN10850–004)</td>
<td>Describes network planning when integrating Avaya ACE with other applications. The document also contains information and procedures for installing and upgrading Avaya ACE software components.</td>
<td>Sales engineers, Solution architects, Implementation engineers, and Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ using VMware in the Virtualized Environment Deployment Guide (NN10850-065)</td>
<td>Describes the procedures for deploying the Avaya ACE vAppliance on VMware.</td>
<td>Sales engineers, Solution architects, Implementation engineers, Support personnel</td>
</tr>
<tr>
<td><strong>Maintenance and Troubleshooting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Troubleshooting</td>
<td>Contains troubleshooting information and procedures for Avaya ACE.</td>
<td>Solution architects, Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Fault and Performance Management</td>
<td>Describes how the fault and performance management system collects alarms and events generated by Avaya ACE. The document also describes how to monitor Avaya ACE.</td>
<td>Solution architects, Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>Audience</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Administration and system programming</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration and system programming</td>
<td>Provides information about the initial configuration, administration, and ongoing management of Avaya ACE service providers. The Avaya ACE host supports a Web-based GUI that administrators can use to perform the tasks.</td>
<td>Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Service Provider Administration</td>
<td>Provides information on how Avaya ACE uses certificates for secure communication. The document also contains procedures that describe how to manage certificates using OpenSSL, IBM certificate management tools, and Avaya Aura® System Manager.</td>
<td>Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Secure Communication Fundamentals</td>
<td>Provides information about user management on Avaya ACE. The Avaya ACE host supports a Web-based GUI that administrators can use to perform system administration, configuration, fault management, performance management, and user management.</td>
<td>Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Message Drop and Message Blast Administration</td>
<td>Provides information about the administration of the Avaya ACE Message Drop and Message Blast service.</td>
<td>Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Administering Avaya WebLM (stand-alone)</td>
<td>Provides administration, configuration, and troubleshooting information for the Web-based license manager (WebLM).</td>
<td>Implementation engineers, Support personnel</td>
</tr>
<tr>
<td>Application developer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Agile Communication Environment™ Web Services</td>
<td>Describes the Web services supported by Avaya ACE.</td>
<td>Solution architects, Implementation engineers, Support personnel, Application developer</td>
</tr>
</tbody>
</table>
## Training

<table>
<thead>
<tr>
<th>Course code</th>
<th>Course title</th>
<th>Activity type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10U00010 E</td>
<td>Avaya Agile Communication Environment(TM) (ACE) Core Implementation Virtual Campus Offering</td>
<td>On demand</td>
</tr>
</tbody>
</table>

## Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.
Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

**Support**

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.
Chapter 2: Verifying secure communication with client applications

Avaya Agile Communication Environment™ supports secure connections to Web services and applications using the Transport Layer Security (TLS) protocol or the Secure Socket Layer (SSL) protocol. TLS and SSL protocols encrypt data sent over TCP connections using X.509 certificates to establish trust and authentication.

Note:
Avaya ACE uses different ports for web services and ACE OAMP. The secure port for Web services is 9443 and the secure port for OAMP is 9449.

When communication occurs over SSL, traffic is encrypted. To ensure that this traffic is best protected, use strong cryptographic ciphers to encrypt. A cipher suite is a set of algorithms that provide authentication, encryption, and data integrity. Some cipher suites provide stronger level of security than others. During an SSL handshake, the client and server negotiate which cipher suite to use to exchange data.

Avaya ACE strengthens communication with client applications by removing support for weak, medium, and anonymous cipher suites. However, you can override this security feature and enable some of the weak ciphers. For more information, see Enabling weak ciphers on page 16.

Note:
For information on configuring client applications to communicate with Avaya ACE, see specific application documents.

Verifying secure communication between Avaya ACE™ and client applications

About this task
After you successfully upgrade Avaya ACE™ and client applications to support SSL connectivity, you must verify secure communication between them.

Client applications commonly interact with Avaya ACE to consume web services. To verify secure communication, you can invoke a web service request from a client application, on the default secure (HTTPS) port 9443.
For example, to configure your client application to invoke a Third Party Call Control (v2) web service request on the secure port, set the SOAP message service endpoint to: https://<ace_server>:9443/RaptorWeb/services/ThirdPartyCall where <ace_server> is the IP address of the ACE server hosting the web service. Avaya ACE successfully handles this request, thus verifying secure communication.

As an additional check, you can verify that the same web service request fails on the default unsecure port 9080. Set the SOAP message service endpoint to: http://<ace_server>:9080/RaptorWeb/services/ThirdPartyCall.

---

### Enabling weak ciphers

To secure communications between Avaya ACE and its client applications, Avaya ACE uses strong SSL ciphers to encrypt and authenticate data.

If your application does not support for strong ciphers, you can use this procedure to enable weak SSL ciphers. Avaya ACE defines weak ciphers as ciphers with a key size less than 128 bits.

**Important:**

Using weak ciphers compromises the level of security of your communications.

**Before you begin**

- You must be able to log in to the ACE host. See Logging in to the Avaya ACE host on page 17.

**About this task**

You can use this procedure on standalone and high availability (HA) deployments of Avaya ACE.

For HA deployments, run the procedure on HostA.

**Procedure**

1. Log in to ACE host.
2. Change directories. Enter:
   
   ```
   cd /opt/avaya/ace/bin
   ```
3. Run the procedure. Enter:
   
   ```
   ./enableWeakCipher.sh
   ```
   
   When you receive the following prompt:
   
   This script will enable weak cipher suites for SSL communication. Do you want to continue (Yes/No)?
4. Enter Yes.

Result
The `enableWeakCipher.sh` procedure stores the logs in `/var/avaya/ace/logs/install/ACE_cipherSuites.log`.

**Logging in to Avaya ACE host**

Avaya ACE does not support logging in to the server remotely with `root` user credentials. However, most of the administrative tasks need root credentials. To obtain `root` credentials, log in as `sysadmin` user and change to `root` user.

**Before you begin**

You must know the `sysadmin` and `root` credentials.

**Procedure**

1. Log in to the Avaya ACE host as `sysadmin` user.
   For HA deployments, log in to the active host.

2. Change to `root` user. Type `su - root` and press Enter.
   When changing to the root user, always use the command syntax `su - root`. Using a dash ensures that you have the correct environment when entering commands as the root user.

3. Enter the `root` password when prompted for it.
Verifying secure communication with client applications
Chapter 3: Communication port management

The Avaya ACE supports secure Web service communication, including notifications, by default. Avaya ACE™ supports secure communications including notifications, on port 9443. For a few client applications, Avaya ACE enables ports for event notification channels.

Avaya ACE disables the unsecure communication on ports 9080 and 9081 by default. However, you can enable the unsecure ports by performing the procedures listed in this chapter.

You must configure HTTPS on the IBM WebSphere Application Server to secure communication between Avaya ACE and Web service interfaces.

To enable HTTPS:

1. Create an IBM WebSphere Application Server SSL configuration
2. Assign that SSL configuration to the endpoint that you want to secure.

⚠️ Warning:
Enabling or disabling ports causes a server restart which leads to disruption of traffic. Perform such actions in a maintenance window.

⚠️ Note:
For HA deployments, you must enable (or disable) the unsecured ports on the active ACE host.

Enabling or disabling the HTTP port on ACE host

Avaya ACE supports secure Web communication by default. However, Avaya ACE also provides a means to enable the unsecure ports for unsecure communication and notifications. You can revert back to the default configuration of secure only communication by disabling the enabled unsecure ports.

Before you begin

- Ensure that you can log in to the Avaya ACE host.
- Ensure that you know the following:
  - Websphere application server (WebSphere) username with administrator privileges.
About this task

Use the following procedure to enable or disable the HTTP port (9080/9081) on an ACE host.

Note:

For high availability deployments, perform this task on the active host.

Procedure

1. Log in to the ACE host. See Logging in to the Avaya ACE host on page 17.

2. Change directories. Enter:
   ```
   cd /opt/avaya/ace/bin
   ```

3. Run the script. Enter:
   ```
   ./configureHttp.sh WASuser WASpswd [ enable | disable ]
   AppUtilities http port
   ```
   where,

   • WASuser: user name with administrative privileges on WebSphere.
   
   • WASpswd: password of WASuser.
   
   • [enable | disable]: parameter that indicates whether the port is to be enabled or disabled. Enter enable, to enable the HTTP port, and disable, to disable the HTTP port.
   
   • AppUtilities http port: optional parameter. If not provided, the tool uses the existing HTTP port for AppUtilities.

   The script enables, or disables, the HTTP port, and all servers on WebSphere are restarted.
Enabling or disabling port for event notification channel on ACE host

Before you begin

• You must obtain the sysadmin and root user passwords.

About this task

Use this procedure to enable or disable the unsecured port for the event notification channel on a ACE host. This procedure is optional because Avaya ACE enables ports for event notification channels only for specific client applications.

Procedure

1. Log in to the ACE host. For more information, see Logging in to the Avaya ACE host on page 17.
2. Change directories. Enter
cd /opt/avaya/ace/bin
3. To change the state of the event notification channel on the ACE host. Enter
./insecureChannel.sh [enable|disable]
The system returns a success or failure message.
4. Restart the ACE servers for the change to take effect. Enter
./RestartAllServer.sh

Configuring HTTPS on WebSphere Application Server administration interface

Before you begin

• Ensure that you have created the required key store and you know the path and name of the key store file.

• If you requested a CA signed certificate, ensure that you received and installed the certificate as per the instructions provided by the third party certificate authority.

About this task

Configure HTTPS on IBM WebSphere Application Server administration interface to secure management traffic between the Avaya ACE™ Web services and your management station.
**Procedure**

1. From the IBM Integrated Solutions Console left pane, select Security, SSL certificate and key management then SSL Configurations.

2. Create a new SSL configuration. Click **New**.
   A Configuration window opens

   Fill in General Properties for the new SSL configuration as follows.

   **Table 1: Properties for the new SSL configuration**

<table>
<thead>
<tr>
<th>Supported properties</th>
<th>Required values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of the Secure Sockets Layer (SSL) configuration within the management scope in which it resides.</td>
</tr>
<tr>
<td>Trust store name</td>
<td>A reference to a specific trust store used by Java (TM) Secure Sockets Extension (JSSE). The trust store holds signer certificates that validate the trust of certificates sent by remote connections during an Secure Sockets Layer (SSL) handshake.</td>
</tr>
<tr>
<td>Key store name</td>
<td>A reference to a specific key store. The key store holds personal certificates that represent the identity of one side of a connection. The public key of this personal certificate is sent to the other side of the connection to establish trust during the handshake. The remote side of the connection needs the root certificate authority (CA) certificate or self-signed public key (signer) to be in the trust store to validate this personal certificate.</td>
</tr>
<tr>
<td>Default server certificate alias</td>
<td>The certificate alias that is used as the identity for this Secure Sockets Layer (SSL) configuration if one has not been specified elsewhere.</td>
</tr>
<tr>
<td>Default client certificate alias</td>
<td>The description for a client certificate alias.</td>
</tr>
<tr>
<td>Management scope</td>
<td>The scope where this Secure Sockets Layer (SSL) configuration applies. For example, if you choose a specific node, then the configuration is only visible on that node and any servers that are part of that node. Only node-level SSL is applied.</td>
</tr>
</tbody>
</table>

3. Click **Get Certificate Alias**.

4. Click **OK**.
   The new SSL configuration is added to the list of available configurations

5. A message dialog indicates that you have you made changes to your local configuration. Click **Save** to save the changes directly to the master configuration.
6. From the IBM Integrated Solutions Console left pane, specify the server you want to configure. Select Servers, Application servers, and then <name of server>.

7. From the Configuration tab, in the Container Settings, expand Web Container.

8. Assign an SSL configuration to the inbound administration channel. From the list of transport chains, click WCInboundAdminSecure, and then SSL inbound channel (SSL_1).

9. Assign the desired SSL configuration to the endpoint. In the SSL Configuration section, use the Select SSL Configuration drop down list to choose the configuration you want to assign to the SSL inbound channel (SSL_1.)

10. Click OK and then Save to save your changes directly to the master configuration.

11. Restart the server.

12. From the IBM Integrated Solutions Console left pane, select Security and then SSL certificate and key management.

13. Click Manage endpoint security configurations and expand the tree structure.

14. Click the links which use the default SSL configurations and change them to the SSL configuration created in 2 on page 22.

15. After each change, click OK and save your changes.

---

**Verifying secure communication with Avaya ACE**

**About this task**

Use this procedure to verify communication with Avaya ACE.

The default secure or HTTPS port on Avaya ACE is 9449.

**Procedure**

To check if the secure port is enabled for communication,

Open a web browser and enter the following URL:

https://<ACE_IP_Address>:9449/oamp

If the Avaya ACE GUI login web page is displayed, the secure port is enabled for communication.

If an error message is displayed, the port is disabled.
Communication port management
Chapter 4: Certificate management

When you install Avaya Agile Communication Environment™, you have HTTPS Web access to Avaya ACE™ using an auto-generated self signed certificate.

However, there are situations where you must manage certificates. For example:

• A certificate is required that is not auto-generated; for example, when you add an Avaya Aura TR/87 service provider or a trust relationship between WebSphere Application Server (Websphere) nodes.

• A self-signed certificate expires.

• You have a requirement to use a CA-signed certificate.

• You have reason to believe that a private key is compromised.

Several tools are available for creating and managing certificates. For an overview of how certificates work to create a trust relationship between a client and server as well as some procedures for managing certificates, refer to Avaya Agile Communication Environment™ Secure Communication Fundamentals, (NN10850-006).
Chapter 5: User management fundamentals

The following sections provide conceptual information to help you manage the Avaya Agile Communication Environment™ (ACE) security policies and users.

The information in these sections are intended for Avaya ACE™ users that have system administrator privileges (assigned system administrator roles) who manage users and control user access to the Avaya ACE system. The information is also intended for developers of applications making use of operations provided by the Avaya ACE User Profile Web service. The chapter introduces key concepts required to understand the Avaya ACE user model and policy management.

Prerequisites for user management

- You must be familiar with the Avaya ACE user authorization model.
- You must be able to log in with system administrator access privileges.

Note:
A system administrator is a user who is assigned the SystemAdminRole. See SystemAdminRole on page 32.

User management tasks
The following work flow shows you the sequence of tasks you perform to configure and manage security policies and users to control access to the ACE system and to applications or Web services.
Figure 1: User management

User management interfaces

Avaya ACE supports the following interfaces for managing users and access policies:

- Web-based graphical user interface on page 29
- User Profile web service interface on page 29
Web-based graphical user interface

The Avaya ACE host supports a Web-based graphical user interface (GUI) that allows administrators to perform all tasks related to system administration, configuration, and user and license management.

The Avaya ACE GUI is available after you install Avaya ACE and is accessible as soon as the Avaya ACE application is started. The Avaya ACE GUI provides in context online help information which describes supported configuration attributes. You launch context help by clicking the question mark icon located at the top right corner of each GUI window.

To access the Avaya ACE GUI over a secure connection (HTTPS), point your browser to your ACE host by specifying the following URL:

https://<ACE IP address>:9449/oamp/

The Avaya ACE Web-based graphical user interface is supported on the following browsers:

- Microsoft Internet Explorer 7
- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 9
- Mozilla Firefox 3.x

Note:
The first time you log in to the Avaya ACE GUI, you will be prompted to change the access password.

User Profile web service interface

The Avaya ACE User Profile web service supports operations to perform activities related to user management and policy management using a programmatic interface. It also supports operations which allow regular users to update their personal data (such as password or contact information).

Client applications sending User Profile service requests to Avaya ACE are subject to the same security policies as Avaya ACE users.

The current version of Avaya ACE supports a newer version of the User Profile Web service (version 1.6) with new and updated operations to support role based authorization of Web services and packaged applications. The User Profile Web service version 1.5 is deprecated. It is therefore recommended that you familiarize yourself with the User Profile Web service version 1.6. For more information, see *Avaya Agile Communication Environment™ Web Services* (NN10850-007).
User authentication

Authentication enables clients and applications to use Avaya ACE™ regardless of whether they are inside or outside the Enterprise and without having to build specific software.

For more details on authentication mechanisms used in Avaya ACE, see User authentication on page 43.

Authorization policies

Authorization policies enforce rules to restrict and control user access to the system.

Avaya ACE supports two levels of authorization policies: individually defined role policies, and global system level policies.

Avaya ACE user authorization is performed through the configuration and management of individual role profiles which define licenses and corresponding access privileges to resources, for users that are assigned these roles. Resources can be Avaya ACE Web services and applications. The access privileges or authorization policies in turn depend on the licenses assigned to the role profile. For more information, see Role profile on page 30.

Global security settings provide system-level authorization policies which apply to all configured users. These policies act as system default security policies. See Global user authorization policies on page 34 for more information.

All successfully authenticated users are subject to Avaya ACE authorization policies.

Role profile

A role profile is a configured profile that defines licenses to resources (Avaya ACE Web services and applications). Access to resources is through licenses. An individual user or a group of users needing access to a resource is assigned a role profile which has the license to that resource.

Avaya ACE establishes the following relation between users, roles and licenses:

- Licenses define access control to a resource.
- Roles are assigned to users.
- Roles pull in licenses from a common pool. The number of licenses pulled by the role depends on the number of users assigned to that role.
Roles can be either predefined or user defined.

User defined roles are created by the administrator using the Avaya ACE GUI. For information on user defined roles, see Role management on page 81.

For a list of pre defined roles on Avaya ACE, see Predefined roles on page 32.

The Avaya ACE authorization model allows system administrators (users assigned SystemAdminRole) to customize each role profile to meet the specific needs of users.

A user can be assigned multiple roles. A user that is assigned multiple roles benefits from the union of all licenses and access privileges brought by each role.

A valid role profile contains the following elements to define licenses and the type and level of access privileges to users that are assigned this role profile:

- Licenses on page 31
- Access control rules on page 31

**Note:**
All users that require access privileges to resources must be assigned a role profile that has the appropriate licenses to these resources.

---

**Licenses**

Configure a role profile to manage licenses to resources (Avaya ACE Web services and applications) for Avaya ACE users based on the requirements of an individual user or a group of users.

You can configure a role profile with one or multiple licenses.

**Important:**
Licenses to Avaya ACE resources can be assigned only to a role profile. Users that need licenses must explicitly be assigned the role profile that has the required licenses configured.

For more information on Avaya ACE license management, see Avaya Agile Communication Environment™ Planning and Installation (NN10850–004).

---

**Access control rules**

Role profiles specify a role policy in the form of access control rules. Access control rules determine which Avaya ACE resource (application or Web service) can be accessed by users that are assigned this role profile.
Access control rules are displayed based on the licenses assigned to the role profile. For each configured role profile, the system administrator selectively enables the required resources.

Role hierarchy is not supported. Role profiles, and correspondingly the licenses and access control rules cannot be inherited.

---

Predefined roles

Avaya ACE creates the following predefined roles during ACE installation:

- **SystemAdminRole** on page 32
- **FederationRole** on page 33
- **SystemMonitorRole** on page 33
- **TrustedRole** on page 33
- **RESTful Session Control** on page 34
- **MessagingAdminRole** on page 34

⚠️ **Important:**

To be able to access the Avaya ACE GUI, users must be assigned the **SystemAdminRole** role and the users’ authentication type must be INTERNAL.

Non administrator users who cannot log into the ACE GUI can contact the ACE system administrator to reset their passwords. If user interaction with ACE is through a third-party application integration with ACE, the application must invoke the ACE User Profile Web service to change the password.

For more information on the User Profile Web service, see *Avaya Agile Communication Environment™ Web Services*, (NN10850–007).

---

**SystemAdminRole**

Users assigned the **SystemAdminRole** can perform all tasks related to ACE system configuration, user management, and user authorization management. Such users have system administrator privileges and are the only users that can access the Avaya ACE GUI.

Over a User Profile web service interface (programmatic interface), users with system administrator privileges can perform all tasks related to user management, including authorization policy management.

A default **admin** user profile is created and assigned this role.
Avaya ACE users that are assigned the system administrator role (role name = SystemAdminRole) have sufficient privileges to:

- Create, modify and delete user profiles.

  ! Important:
  A user profile that is already assigned a role cannot be deleted.

- Create roles
- View, create, and delete existing roles
- Modify access control rules of roles
- Modify global security settings
- Modify role membership (add/remove the assignment of roles to users) of roles
- Modify license membership (add/remove available licenses) of roles.

FederationRole

FederationRole supports user profiles that allow inter-region communication in a federated ACE deployment.

You cannot add or remove users from this role. Avaya ACE creates a default user who is assigned this role. For more information, see Predefined federation user profile on page 41.

SystemMonitorRole

SystemMonitorRole is an internal role created to monitor the health of the system.

Users assigned this role can monitor the health of an Avaya ACE system using the System Monitoring Web service interface.

You cannot modify the SystemMonitorRole.

TrustedRole

The TrustedRole is an internal role created to allow communication between Avaya ACE and packaged applications that need Avaya ACE services.

You cannot add or remove users from this role. Avaya ACE creates a default user who is assigned this role. For more information, see Predefined Trusted user profile on page 42.
RfSC role

The **RESTful_Session_Control** (RfSC) role is created to allow the RfSC application to monitor the users registered with it.

**RESTful_Session_Control** is a middleware between Avaya ACE services and an external client, providing Remote Call Control (RCC) features through a simple programmatic RESTful interface. The RfSC role is required for applications or users that need access to the RfSC API.

MessagingAdminRole

The **MessagingAdminRole** is a predefined role created during Avaya ACE installation.

Users assigned the **MessagingAdminRole** can:

- access not only their own mailboxes but also the mailboxes of all the enterprise users.
- access Messaging-specific logs
- control the amount of detail captured in Messaging logs

Global user authorization policies

Avaya ACE enforces system-wide, global user authorization policies. Global policies are applied to every user requesting access to supported web services. Avaya ACE enforces the following global authorization policies:

- **Global account policy** on page 34
- **Global password policy** on page 35

Only users that have administrator privileges (assigned the **SystemAdminRole** role) can modify the global security settings.

Global security settings can be changed using the Avaya ACE GUI or through a programmatic interface using the User Profile web service.

Global account policy

The ACE server is preconfigured with default global account policy settings. The global account policy settings specify parameter values that apply to all configured user accounts. The system administrator can customize these global settings to meet specific security requirements.
Global account policy settings

- apply to all configured user profiles
- are optionally overridden at the individual user profile level

⚠️ Important:
Inactive accounts that exceed the **Dormant Period** are disabled.

⚠️ Note:
Account policy settings are only available using the Avaya ACE GUI. They are not available from the User Profile web service interface.

**Figure 2: Global account policy settings: default values** on page 35 shows the default values of predefined global account policy settings.

---

Global password policy

Avaya ACE supports a global password policy. The default policy is preconfigured with default password rules. Some of the rules are implicitly defined and cannot be modified while others are explicitly defined through configuration. The goal of password rules is to strengthen passwords to make them less vulnerable to attacks. When a user configures a new password, the system always validates the new password against the set of predefined rules. If the password does not meet the password rule values, the password is rejected.

Avaya ACE administrators have control over explicitly defined password rules, but not over implicit rules. Implicit rules cannot be disabled and apply to all ACE users.

- **Implicit global password rules** on page 36
- **Explicitly defined global password rules** on page 36
Passwords are case sensitive.

**Implicit global password rules**

Avaya ACE enforces implicit password rules every time a user password is defined or changed. Implicit password rules are enforced by default and can neither be modified nor disabled.

The following implicit password rules apply:

The password must

- Not contain the string defined as the user ID.
- Not contain the string defined as the user ID in its inverted form (for example, if the user ID is "John", the password cannot contain the string "nhoJ" nor "nhoj").

**Important:**
The check on the inverted form does not consider upper or lower case.

- Not contain more than three consecutive characters from the previous password (the password being changed).
- Contain at least 6 characters, up to a maximum of 20 characters.
- Contain at least 1 special character. Permitted special characters are ! # $ % ( ) * + - . / = < > @ [ ] ^ { | } ~ and _ .

When an implicit password rule is broken, the password change fails. The Avaya ACE GUI displays an error message specifying the rule that was broken. If you break a password rule while changing a password using a User Profile web service interface, the corresponding operation fails and returns an error code accordingly. For more information about the User Profile Web service, see *Avaya Agile Communication Environment™ Web Services (NN10850-007).*

**Explicitly defined global password rules**

The ACE global password policy allows the administrator to explicitly define password rules by configuration. An ACE administrator can change global password policy settings to meet specific security requirements.

The Global password policy settings can be changed from the Avaya ACE OAM at: **Security > Global Security Settings > Internal Account Policy > Password Policy.**

Global password policy settings always apply to all users.
Important:

When an ACE administrator changes a user's password, the Avaya ACE does not perform a check on the Minimum Different Character rule. This rule is based on the comparison of the user's old and new passwords. However an administrator is not expected to provide the old password. Therefore, this rule does not apply.

Password history size

Avaya ACE supports a password history size attribute as part of the global password policy settings. This security setting determines the number of unique passwords that are associated with a user profile. The purpose of this feature is to enhance security by preventing users from continuously reusing the same user passwords. Passwords stored in a user's password history list cannot be reused. Every time a password is changed, the old password is added to the history list. When the number of passwords in the list reaches the number configured as the password history size, the oldest password in the list is removed and that password becomes available for use again.

The value of the password history size attribute must be between 10 and 32 passwords. The default value is 12. The password history size feature is always enforced. You cannot disable it.

Global password policy defaults

Figure 3: Global password policy settings: default values on page 38 shows the default values of predefined global password policy settings.
The online help accessible from the Avaya ACE GUI provides a description of all password policy attributes.

User profile

A user profile is the container which stores user-specific information. A user profile stores user data required for authentication and authorization and any other type of user data (such as user's contact URI) that may be required and used by web services.

For a complete list and description of each user profile parameter, see the online help which is accessible in context, from each window of the Avaya ACE GUI.

For a list of parameters supported by the User Profile service, see *Avaya Agile Communication Environment™ Web Services* (NN10850-007).

Mandatory user information

A valid user profile must contain at least a user name and a user password. Without a user name and password, the creation of a user profile fails.

In addition to user authentication data, this tab provides control over the user account using the *Account State* attribute. The user account can be enabled or disabled. By default, the *Account State* attribute is set to *Enabled*. 
Role membership

The user profile container is used to associate a user with roles. The level of access privileges and licenses to Avaya ACE resources, Web services and applications, associated with a user profile is determined by the role policies that are explicitly assigned to the user.

If a user profile is not linked to a configured role policy, the default global user group policy applies.

A user can be assigned multiple roles. In such cases, the user benefits from the union of all licenses and access privileges provided by each role.

For licenses to be assigned to a user, the user must explicitly be assigned a role that has the required licenses configured.

For more information on roles, see Role management on page 81.

User account policy

The user account policy defined within a user profile enforces rules to control a user login session. The user account policy defined at the user profile level is optional and, when defined, overrides the global user account policy defined in global security settings.

Figure 4: User account policy example on page 39 shows the settings defined in a user account policy.

![User account policy example](image)
Important:
Blank attribute value fields in the User account policy tab (accessed from the Create User window) indicate that settings are inherited from the global account policy (in Global Security Settings).

For a description of Avaya ACE configuration attributes, refer to the online help that is accessible directly from any Avaya ACE GUI window.

User preferences

An ACE user profile supports the provisioning of a user's preferred time zone. The time zone is specified in GMT format. During a GUI login session, time stamps are displayed using the user’s preferred time zone.

Predefined user profiles

Avaya ACE provides the following predefined user profiles.

Navigation

• Predefined admin user profile on page 40
• Predefined federation user profile on page 41
• Predefined sysmonitor user profile on page 42
• Predefined Trusted user profile on page 42

admin user profile

Avaya ACE provides a predefined system administrator (admin) user profile. This admin user profile is required to initially log into the Avaya ACE GUI. The admin user profile is preconfigured with the credentials: user name: admin, default password: agile. For security reasons, the admin user is prompted to change the default admin password during the initial login session.

Use the admin user profile or its equivalent to perform ACE administration.
For additional security, use the user management procedures in this document to create a new system administrator user ID and delete the default admin user. Perform the following procedures:

- Perform the procedure Creating a user on page 89 to create a new system administrator level user.
- Perform the procedure Modifying a user on page 96 to remove the admin user from the SystemAdminGroup user policy.
- Perform the procedure Deleting user profiles on page 99 to delete the admin user.

The predefined admin account has an account policy defined with the values shown in Figure 5: Admin user account policy on page 41. You can customize the admin user account policy settings to meet your requirements.

![Figure 5: Admin user account policy](image)

---

**Federation user profile**

The Avaya ACE software installation process creates a user profile with the user ID federation. Internal ACE processes use the predefined federation user for inter-region communications in a federated deployment.

The password for the federation user must be the same on all ACE systems in the federation. An ACE system with a different password cannot communicate with other regions in the federation. The federation user password follows the same validation rules as other ACE user passwords. You must manage the password based on network password policies.

When the user exceeds the configured maximum number of login attempts, the system locks the user out. By default, the federation user is never locked out. If the default setting is
changed, the federation user may become locked during password change activity. If this occurs, see Unlocking a user account on page 97.

To avoid a security risk, in non federated ACE systems, change the password after installation and then manage the account based on network password policies or disable the password for the federation user.

sysmonitor user profile

Avaya ACE creates a predefined sysmonitor user during ACE installation for internal processing.

You cannot delete or modify the default sysmonitor user profile.

Trusted user profile

Avaya ACE creates a predefined trustedUser during ACE installation for internal processing.

You cannot delete or modify the default trustedUser.
Chapter 6: User authentication

Avaya ACE Release 6.2.x supports the following authentication mechanisms:

- IWA authentication on page 43
- HTTP Basic on page 64

You can classify users as internal and external based on their authentication type. Users whose authentication type is set to internal are authenticated against their Avaya ACE database credentials and users whose authentication type is set to external are authenticated against their enterprise credentials.

By default, predefined users are considered internal. For information on predefined users, see Predefined user profiles on page 40.

Note:

Ensure that you set the authentication type to external for users using the IWA and LDAP authentication mechanisms. Set the authentication type to internal for users using the Avaya ACE database credentials for authentication.

IWA authentication

Integrated Windows Authentication (IWA) uses the security features of Windows clients and servers. Unlike Basic or Digest authentication, initially, it does not prompt users for a user name and password. The current Windows user information on the client computer is supplied to the Web server. If the user information is not authenticated, it prompts the user for a user name and password.

Avaya ACE uses Kerberos and Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) to provide IWA authentication.

Kerberos is a standard network authentication protocol used in providing a proof of identity between a client and server or between two servers.

Kerberos uses the concept of tickets. A ticket is small amount of encrypted, session specific data issued by the domain controller. When a client needs to access a server on the network, it first obtains a ticket from the domain controller for that server. The ticket and other data supplied by the client vouches for the clients identity and provides a way for the client to authenticate the server as well, which means Kerberos provides mutual authentication of both client and server.

Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) is a standard protocol that is used to negotiate the authentication protocol used when a client application wants to
authenticate to a remote server. Using Kerberos authentication and SPNEGO implementation you can design an Single Sign On (SSO) solution for Web applications.

See Kerberos terminology on page 107 for a detailed description of Kerberos terms.

Implementing a Kerberos and SPNEGO solution requires the following environment:

• A Windows domain controller with the KDC enabled, and one client system connected on a domain.
• A client application supported by Kerberos, such as Firefox, that use service tickets so that the user is not prompted to re-authenticate.
• In multiple domains scenarios, you need to use Kerberos to connect to all domains.
• Microsoft Active Directory 2003 R2 or Microsoft Active Directory 2008 R2 configured as a user registry.

Avaya ACE supports IWA authentication in single and multiple domains.

Points to note:

• All enterprise users must be present in the Active Directory. Both Microsoft Active Directory 2003 R2, Active Directory 2008 R2 are supported.
• LDAP configuration to establish connection between Avaya ACE and the Active Directory is done as part IWA configurations.
• To prevent replay attacks, Kerberos tickets presented to domain controllers by clients are time-stamped. The authenticating domain controller checks to make sure the timestamp is unique and falls within an allowable skew before accepting the ticket and authenticating the client. Ensure that the system clocks on the ACE machine and the machine on which Active Directory is installed, are synchronized to within 5 minutes.
• In multiple domain environments, ensure that the user you select for logging into the Active Directory domain (Kerberos User) is present in only one Active Directory.
• In standalone deployments, register the IP address of the ACE machine in the DNS server and in HA deployments, register the floating IP with the DNS server.
• If an enterprise user belongs to a group, ensure that the group does not have a null objectGUID. A null objectGUID causes IWA authentication to fail.

IWA configuration for single domain

The following are the main steps to configure IWA authentication on a single domain :

• Create a user in Active Directory.
• Register Avaya ACE IP address in the DNS server.
• Assign the service principal name and create the keytab file.
• Run the Avaya ACE installation tool.
• Configure the web browsers to enable SPNEGO authentication.

**Note:**
Procedures for setting up Microsoft Active Directory and the KDC are beyond the scope of this document.

---

### IWA configuration for multiple domains

The following are the main steps to configure IWA authentication on multiple domains:

- Create a user in Active Directory.
- Register the Avaya ACE IP address in the DNS server.
- Create a key tab file for each domain.
- Run the Avaya ACE installation tool.
- Merge the keytab files.
- Edit the Kerberos configuration file.
- Create trust between the realms.
- Configure the web browsers to enable SPNEGO authentication.

**Note:**
Procedures for setting up Microsoft Active Directory and the KDC are beyond the scope of this document.

---

### Creating a user in AD

**Before you begin**

Ensure that:

- Active Directory (AD) including a domain controller and a client workstation is installed.
- you know the username and password of a user in AD with administrator privileges.

**About this task**

Use this procedure to create a user in Active Directory. This user account will be used to create a mapping between the Kerberos service principal name (SPN) and the Websphere application server. This user account will connect with the Kerberos Domain Controller and authenticate users.
Procedure

1. Log in to the Active Directory Administration Center using administrator credentials.

2. Select **Users** from the left hand navigation tree.

3. On the User page, from the right pane, select **New > User**.

4. In the create User page, enter:
   a. Enter a name in the **First name** field.
   b. Enter the same name in the **User UPN logon name** field.
   c. Enter a password for this user in the **Password** field and reenter it in the **Confirm Password** field.
   d. Under password options, select **Other password options**, and **Password never expires** checkbox.
Important:

This user is created only to generate the keytab file.

The following rules apply only to this user. Regular Avaya ACE users do not have these restrictions.

- Do not use spaces in the user account name.
- Leave the Last name and Middle initials fields empty.
- Ensure that the password for this user does not expire. If the password expires, you must reset the password, generate the keytab file again in the Active Directory domain and copy the keytab file to the Avaya ACE domain.

Figure 6: Creating a user in AD

5. Click OK to create a user.

Configuring a domain name server

A domain name system (DNS) service is required for Active Directory to work properly. Use this procedure to create the DNS configuration that the Active Directory domain uses. When creating a realm (domain), the wizard verifies that the DNS is running. If the DNS is not running, the wizard provides the option to create the DNS service in the same machine where you create the realm.
**Note:**
The DNS service does not need to run in the same machine where you create the KDC realm. You can execute these services in different machines.

**Before you begin**

- Install DNS.
- Update the IP address for Preferred DNS Server to be the IP address of the DNS server. See following figure:

![TCP/IP configuration for DNS](image)

**Note:**
IP address in the **Use the following IP address** field and Preferred DNS server in the **Use the following DNS Server addresses** field are the same in situations where the DNS server and KDC realm are on the same machine.

- Update the `/etc/resolve.conf` file on the ACE machine with the DNS Server IP address. See [Editing resolv.conf file](#) on page 51

**About this task**
For Avaya ACE in a standalone deployment, register the ACE machine IP in the DNS server.
For Avaya ACE in HA deployment, register the floating IP in the DNS server.

**Procedure**

1. Start the DNS console:
a. Click **Start > Run.**

b. Enter `dnsmgmt.msc`.

c. Click **OK.**

**Figure 8: dnsmgmt.msc command**

The DNS window opens.

2. **In the DNS window:**

a. Right-click **Forward Lookup Zones**

b. Select **New Zone.**

**Figure 9: Creating a new zone**

3. When the Wizard opens, click **Next.**

4. In the Zone Type window:

a. Select **Primary Zone.**

b. Enable **Store the zone in Active Directory** because the DNS server and the KDC will run in the same machine.

c. Click **Next.**
5. Provide the zone name, for example, acedomain.mydomain.com, and click **Next**.

6. In the Dynamic Update window:
   a. Select **Allow both nonsecure and secure dynamic updates**.
   b. Click **Next**.

![Figure 10: Selecting the type of zone](image)

![Figure 11: Allowing dynamic updates](image)

7. Click **Finish** to create the DNS Forward Zone.

8. Test the new DNS configuration:
   a. Open a command prompt window.
b. Type the command, `ipconfig /registerdns`.

A sample output is shown below

```bash
c:\>ipconfig /registerdns
Windows Ip Configuration
Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.
```

9. Check the DNS console to make sure that the host was registered. An entry displays with the host name and the IP address of your host, as shown in the following figure:

![DNS Console Screenshot](image)

**Figure 12: Checking if host entry has been created on DNS server**

**Editing resolv.conf file**

The resolver is a set of routines that provide access to the Internet Domain Name System (DNS).

The resolver `resolv.conf` must exist in the `/etc` directory.

One of the configuration options of the `resolv.conf` file is `nameserver`. You can list the Internet addresses, in dot notation, which the resolver must query using the `nameserver` option. If multiple servers exist, the resolver library queries the servers in the order the servers are listed. Thus, list the `DNS IP` as the first IP.

*Note:*

For HA deployments, perform this procedure on both hosts.

**Before you begin**

Obtain `sysadmin` and `root` user passwords.

**Procedure**

1. Log in to the ACE host. See [Logging in to the Avaya ACE host](#) on page 17.
2. Open the /etc/resolv.conf file in an editor.

3. Add the following line as the first nameserver line:
   
   ```
   nameserver <DNSip>
   ```

   Where, DNSip is the IP of the DNS server.

---

**Example**

A sample resolv.conf file:

```
search mydomain.com
nameserver 9.152.233.23
nameserver 9.134.170.141
nameserver 23.143.233.61
```

---

**Generating the keytab file**

A keytab file is used to

- register the fully qualified domain name (FQDN) of Websphere for Kerberos authentication
- configure the Active Directory that is running the domain controller, to the associated Key Distribution Center (KDC).

**Before you begin**

- Install Active Directory
- Ensure that you have administrator privileges
- Add the ACE FQDN in DNS Server.
- You must know the values for the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Name and actual path of the keytab file to generate.</td>
</tr>
<tr>
<td></td>
<td>✪ Note: This is the .keytab file that you transfer to a computer that is running Avaya ACE.</td>
</tr>
<tr>
<td></td>
<td>For example, C: \users.myKeytabFile.keytab</td>
</tr>
<tr>
<td>FQDN of ACE machine</td>
<td>Fully qualified domain name of the machine running Avaya ACE.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> In HA deployments, it is the floating IP of the Avaya ACE HA system.</td>
<td></td>
</tr>
<tr>
<td>Hostname of ACE machine</td>
<td>host name of the machine running Avaya ACE.</td>
</tr>
<tr>
<td><strong>Note:</strong> To get the host name, on your ACE machine, at the command prompt, enter <code>/bin/hostname</code> FQDN will be in the form <code>myhost.mydomain.com</code> while hostname is the shortened version, <code>myhost</code>.</td>
<td></td>
</tr>
<tr>
<td>Realm</td>
<td>Realm is the Active Directory domain specified in UPPERCASE letters.</td>
</tr>
<tr>
<td>KerberosUser</td>
<td>user account you set up in <a href="#">Creating a user in AD</a> on page 45.</td>
</tr>
<tr>
<td><strong>Note:</strong> KerberosUser must match the sAMAccountName and the User logon name in Active Directory.</td>
<td></td>
</tr>
<tr>
<td>KerberosUserPswd</td>
<td>Password associated with KerberosUser.</td>
</tr>
</tbody>
</table>

#### Procedure

1. Log in to your Active Directory.
2. Generate the keytab file. At the command prompt, enter the following command:
   ```bash
   ktpass -out <Filename> -princ HTTP/<FQDN of ACE machine>@<realm> -mapUser <KerberosUser> -pass <KerberosUserPswd> -mapOp set -crypto RC4–HMAC-NT
   ```
3. Verify the new SPN list using the `setspn` command. Enter:
   ```bash
   setspn -l <KerberosUser>
   ```

#### Example

For the following parameters,
<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KerberosUser</td>
<td>User created in AD for keytab generation</td>
<td>server1</td>
</tr>
<tr>
<td>File Name</td>
<td>Full path and name of keytab file</td>
<td>C:\Users\server1.keytab</td>
</tr>
<tr>
<td>AD domain</td>
<td></td>
<td>mydomain.com</td>
</tr>
<tr>
<td>Realm</td>
<td></td>
<td>MYDOMAIN.COM</td>
</tr>
<tr>
<td>FQDN of ACE machine</td>
<td></td>
<td>server1.mydomain.com</td>
</tr>
<tr>
<td>hostname of ACE machine</td>
<td></td>
<td>server1</td>
</tr>
<tr>
<td>Password</td>
<td>Password for Kerberos User</td>
<td>pas$w0rd</td>
</tr>
</tbody>
</table>

A sample output of the command:

Targeting domain controller: <domaincontroller>
Successfully mapped HTTP/server1 to server1.
Password succesfully set!
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to C:\Users\server1.keytab:
Keytab version: 0x502
keysize 64 HTTP/server1@MYDOMAIN.COM ptype 0 (KRBCNT_LNKNOWN) vno 5 etype 0 x17 (RC4-HMAC) keylength 16 (0x7facdc498ed1680c4fd1448319a8c04f)

Next steps

Copy the keytab file generated to the /opt/avaya directory on the Avaya ACE host.

Configuring browsers to support IWA authentication

Configuring IE for SPNEGO

Use this procedure to configure Microsoft Internet Explorer on the user workstation for IWA authentication.

Procedure

1. Log in to your Active Directory domain.
2. Open Microsoft Internet Explorer.
4. Select the Local intranet icon and click Sites.
5. In the Local intranet window, select Include all local (intranet) sites not listed in other zones.
6. Click Advanced.
7. Enter the host names of the Web sites for which IWA is enabled, for example, myUser.myDomain.com, in **Add this Web site to the zone**.

8. On the Internet Options window, click the Advanced tab, and scroll to **Settings**. Select **Enable Integrated Windows Authentication (requires restart)**.

9. Click **OK**.

10. Restart Microsoft Internet Explorer to activate the settings.

---

**Example**

![Example](image_url)

**Figure 13: Configuring IE for IWA authentication — part 1**
Configuring Firefox for SPNEGO

Complete the following steps to ensure that the Mozilla Firefox web browser is enabled to perform IWA authentication.

Procedure

1. Log in to your Active Directory domain.
2. Open Mozilla Firefox.
3. In the browser address field, enter about:config.
4. In the Search field, enter network.n.
5. Double-click network.negotiate-auth.trusted-uris to list the sites that are permitted to engage in SPNEGO authentication with the browser.
6. Enter a comma-delimited list of trusted domains or URLs, such as myUser.myDomain.com. The separator is a comma.
7. If the deployed SPNEGO solution uses the advanced Kerberos feature of credential delegation, double-click network.negotiate-auth.delegation-uris to list the sites for which the browser can delegate user authorization to the server.
8. Click OK and the configuration displays as updated.
9. Restart the Firefox browser to activate this configuration.

---

**Example**

![Firefox configuration interface](image)

**Figure 15: Configuring Firefox**

---

**Merging keytab files**

To use Kerberos authentication in multiple domains, you need to create a separate keytab for each domain. After Avaya ACE has been installed, as part of the post installation configurations, merge these keytab files into one file.

**Before you begin**

- Ensure that the primary and secondary keytab files are in the same location.
- Ensure that you obtain the *sysadmin* and *root* user passwords.
About this task

Use this procedure to merge `secondary.keytab` and `primary.keytab` and store the result in `primary.keytab`.

Procedure

1. Log in to Avaya ACE host. See Logging in to the Avaya ACE host on page 17.
2. Enter:
   - `export PATH=/opt/IBM/WebSphere/AppServer/java/jre/bin:$PATH`
   - `ktab -m secondary.keytab primary.keytab`
   
   Where, `secondary.keytab`, `primary.keytab` specify the name and location of the keytab files of each domain.

Result

The merged keytab file is the `primary.keytab`.

Editing Kerberos configuration file

Kerberos configuration file `krb5.conf` must exist in the `/etc` directory. The file has several stanzas, each stanza controls certain aspects of kerberos installation.

To configure Kerberos in multiple domains, you must edit the section that maps domains to `realms`, `domain_realm`, and the section that specifies the location of the KDC for each realm, `realms`.

Before you begin

You must obtain the `sysadmin` and `root` user passwords.

About this task

Kerberos configurations are stored in the `/etc/krb5.conf` file. Edit the `realms` and `domain_realm` sections as shown:

Procedure

1. Log in to the Avaya ACE host. See Logging in to the Avaya ACE host on page 17.
2. Open the `/etc/krb5.conf` file in an editor.
3. Navigate to the `[realms]` section and enter:

```plaintext
[realms]
firstActiveDirectory Realm = {
  kdc = <kdcHost1>:88
}
default_domain=<firstactiveDirectoryDomain>
```
secondActiveDirectory Realm = {
    kdc = <kdcHost2>:88
    default_domain = <secondaryactiveDirectoryDomain>
}

4. Navigate to the [domain_realms] section and enter:
   [domain_realms]
   .firstActiveDirectory Realm = <firstactiveDirectory Realm>
   .secondActiveDirectory Realm = <secondaryactiveDirectory Realm>

5. Save the file.

Example

[realms]
  DOMAIN1.COM = {
    kdc = server1.domain1.com:88
    default_domain = domain1.com
  }
  DOMAIN2.COM = {
    kdc = server2.domain2.com:88
    default_domain = domain2.com
  }
  [domain_realms]
  .domain1.com = DOMAIN1.COM
  .domain2.com = DOMAIN2.COM

Creating trust between realms

You can create a trust relationship between two domains, which enables clients who are authenticated in one of the trusted domains to access the resources that are hosted in the other domain. As an example, consider a company that has two Microsoft Active Directory administrative domains (domain1.com and domain2.com) that have a trust relationship established. Clients registered and authenticated in the domain1.com domain can access an application running in a WebSphere Application Server that is hosted in the domain2.com domain.

Before you begin

- Ensure that the Active Directory domains, for example, domain1.com and domain2.com, are configured and working properly.
- Ensure that you have administrative access for each realm.
- Ensure that the two realms are pingable from each other.
Procedure

1. Log into the server containing one of the realms. For example, DOMAIN1.COM
2. Click Start > Run. Enter mstsc in the Open field and click OK.
3. Enter the computer name and the user credentials to log in. Click Connect.
4. Click Start > Run. Enter domain.misc in the Open field and click OK.
5. In the Active Directory Domain and Trusts console, right click the domain and select Properties.


7. The Welcome to the new trust Wizard window opens up. In the Welcome window, click Next.

8. In the Name field, enter the name of the domain with which you want to create the trust relationship, for example, domain2.com. Click Next.
9. In the Trust Type window, select **External trust**. Click **Next**.

10. The trust relationship is being established between the realms, thus, select **Two-way** in the Direction of Trust window. Click **Next**.

11. Select **This domain only** in the Sides of Trust window. Click **Next**.

12. Select **Domain-wide authentication** in the Outgoing Trust Authentication Level window and click **Next**.
13. Review the configuration summary and click **Next** to create the trust.

14. The trust relationship is created and the status is displayed. Click **Next**.

15. Confirm the trust relationship. Select **Yes, conform the outgoing trust** in the Confirm Outgoing Trust page. Click **Next**.

16. Click **Finish**.

---

**Validating trust between realms**

Use this procedure to validate the trust created between two realms in a multiple domain environment.

**About this task**

You can use the Active Directory Domain and Trusts console to validate the trusted environment. Using this window, you can validate both outgoing and incoming trusts.

**Procedure**

1. To open the console, select **Start > Run**.
2. Enter `domain.msc`, and click **OK**.
3. In the Active Directory Domain and Trusts console, right-click the domain, and select Properties.

4. Select the type of trust that you want to validate, incoming or outgoing. Click Properties to the right of the selection.

5. In the next window, select Yes, validate the incoming trust. Provide the administrative credentials for the target realm. Click OK.

6. A message displays with the information about the status of the trust relationship. If everything is working correctly, you see the message as shown in the following figure. Click OK.
HTTP Basic

In basic access authentication the user provides the user name or contact identifier and the corresponding password in the request.

Avaya ACE then compares the user ID and password to the user profiles stored on Avaya ACE. If the user ID and password provided are valid, authentication is successful and access is granted.

Avaya ACE provides the following types of Basic authentication:

- LDAP
- MySQL

LDAP authentication

Lightweight Directory Access Protocol (LDAP) an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

In Avaya ACE, a generic LDAP abstraction is supported as the authentication back-end. It is assumed that all Enterprise user credentials are present in these Active Directories. Avaya ACE will verify the user credentials present in the authentication request against LDAP registry.

You can choose either secure and non secure means of communication between Avaya ACE and Active Directory. You will be prompted to enter the means of communication and the port number for communication during the Avaya ACE installation procedure.

LDAP authentication can be configured for any of the following Active Directories:

- Microsoft Active Directory 2003 R2
- Microsoft Active Directory 2008 R2
- Sun(Oracle) Directory
**Note:**

Avaya ACE supports only one directory setup per organization.

---

**LDAP configuration parameters**

A LDAP server services client request by interfacing between client programs and directory services. To connect to an LDAP server, you must perform the binding operation. The Avaya ACE installation procedure performs the binding.

The installer prompts for the parameters values needed for the binding.

- **IP address or FQDN of LDAP server**

  IP address or FQDN of the machine on which the repository is installed.

- **Base Distinguished Name (DN)**

  LDAP stores user details in a tree structure. A Base DN specifies the search base for user lookup while authenticating. A DN has attribute=value pairs, separated by commas. For example, in Active Directory, if the domain is mydomain.com, the base DN is `dc=mydomain,dc=com`.

  **Note:**

  Ensure that the Base Distinguished Name does not contain any of the special UTF-8 characters other than the space character.

- **Binding user name**

  The bind DN is the user on the LDAP server permitted to search the LDAP directory within the defined search base. The role of the bind DN is to query the directory for authenticating users. When the LDAP directory returns the DN, the system uses the DN and password to authenticate the user.

- **Bind user password**

  Password associated with the binding user name.

  **Note:**

  - Ensure that the binding user name does not contain any of the special UTF-8 characters other than the space character.
  
  - Ensure that this password does not expire. You can do this by selecting the **Password never expires** option when creating the user in the Active Directory server.
ACE database authentication

MySQL is the database used in Avaya ACE. User credentials provided in the request are authenticated against the user credentials stored in the MySQL database.

**Trusted host authentication**

For requests using the trusted host authentication mechanism, password check will not be done, only the username will be verified against the ACE database. To enable this, the client or application must add the IP address of the client or application that they trust in the Avaya ACE GUI.

Trusted host authentication is supported only for all Web services running on Avaya ACE. It is not supported for the OAMP.

To add an IP address as a trusted host, See [Adding an IP as trusted host](#) on page 66

**Device ID authentication**

With this authentication mechanism, the client or application can login using their handle (contact-id), which is stored as personal contact information of a user in ACE database.

This authentication scheme is supported only for Blackberry devices, including Blackberry endpoints.

Add the source IP address as a trusted host. If you have not added IP as a trusted host, you must provide a valid password for authentication.

---

**Adding an IP as trusted host**

**Before you begin**

Ensure that:

- An Avaya ACE GUI session is open.
- You have system administrator privileges.
- You are familiar with the attributes provided in account policy settings.

**About this task**

Requests coming from an IP added as a trusted host in Avaya ACE do not need a password check during the authentication process.

**Procedure**

1. On the main menu bar, navigate to **Security > Global Security Settings**. The Global Security Settings window opens.
2. Select the **Trusted IPs** tab.
3. In the **Add Trusted IPs** section, add the IP address of the client you want to trust.
4. Click **Add** and then **Submit**.

---

**Configuring authentication post installation**

Use this procedure to configure or alter the authentication mechanism after Avaya ACE is installed.

**Before you begin**

- Ensure that Avaya ACE is installed.
- Get **sysadmin** and **root** user passwords.
- Get the values for the following parameters:
  - Websphere administrator credentials.
  - If installing in IWA mode,
    - Location of the keytab file

**Note:**
You can generate the keytab file using the `generateKeyTab.bat` file. You can download the `generateKeyTab.bat` file the ACE GUI at the Help > Software Downloads. For more information, see Generating the keytab file on page 52.

- Kerberos realm name, For example, MYDOMAIN.COM
- Active Directory host name, For example, acedc.mydomain.com
- Domain name, For example, mydomain.com

**Note:**
If you have multiple domains, you must know the domain names of all the domains.

- Base Distinguished Name (DN) of Active Directory, For example, DC=mydomain,DC=com
- LDAP user name and password

- If installing in LDAP mode,
  - Base Distinguished Name (DN) of Active Directory, For example, DC=mydomain,DC=com
  - LDAP user name and password
  - Type of communication, secure or unsecure, between Avaya ACE and LDAP user registry.
• port number for communication.

**Procedure**

1. Log in to the Avaya ACE. See [Logging in to the Avaya ACE host](#) on page 17.
2. Change directories. Enter:
   ```bash
   cd /opt/avaya/ace/bin
   ```
3. Run the configuration script. Enter:
   ```bash
   ./reconfigureACE.sh
   ```
4. Follow the prompts.

**Result**

The configuration script displays an appropriate message on conclusion. The script stores the logs at `/var/avaya/ace/log/install` in the file `configuration.log`.

---

**Troubleshooting authentication issues**

An authentication problem with console logon, network logon, access to network resources, or remote access might indicate a Kerberos error if Integrated Windows Authentication (IWA) is the default authentication protocol.

To determine whether a problem is occurring with the Kerberos part of the authentication mechanism, check the System event log for errors from any services such as Kerberos, kdc, LsaSrv, or Netlogon that provide authentication. If any such errors exist, there might be errors associated with the Kerberos protocol. In addition, failure audits in the Security event log might show that the Kerberos protocol was being used when a logon failure occurred.

---

**Checks to be performed before configuring authentication**

• Make sure that the network infrastructure is functioning properly and that all computers and services can communicate.

• Make sure that a domain controller is accessible.

• Make sure that DNS is configured properly and resolving host names and services appropriately.

• Make sure that the clocks are synchronized across the domain.

• Make sure you have administrative rights on the Active Directory you are troubleshooting.

• Make sure you have installed all the necessary support tools and configured the tools.
Install the support tools from the \Support\Tools folder of the Windows operating system CD.

Install the following support tools:

- Ldifde

  Ldifde.exe is present on domain controllers but can be copied and used on client computers running Windows XP and Windows Server 2003. Ldifde provides a method to quickly extract and display certain Service Principal Names (SPNs) in a forest or domain.

- LDP

  The Ldp GUI tool is included when you install Windows Server 2003 Support Tools. This GUI tool is a Lightweight Directory Access Protocol (LDAP) client that allows users to perform operations (such as connect, bind, search, modify, add, delete) against any LDAP-compatible directory, such as Active Directory. LDP is used to view objects stored in Active Directory.

- Setspn

  Setspn.exe is included in the Windows support tools. Setspn provides means to manually view and configure service principal names.

---

**Verify Kerberos settings**

**Verifying encryption used in keytab file**

Use this procedure to verify that the Kerberos keytab file is valid with the correct encryption.

**Before you begin**

- You must able to log into Active Directory with administrator privileges.

**Procedure**

1. Log into Active Directory.

2. At the command prompt, enter the following command:

   ```
   <JAVA_HOME>/jre/bin/java com.ibm.security.krb5.internal.tools.Klist -e -k <keytab file>
   ```

**Example**

The following is a sample output showing the usage of the correct encryption protocol in the keytab file:

```
./java com.ibm.security.krb5.internal.tools.Klist -e -k /tmp/krb5.keytab
Key table: /tmp/krb5.keytab
Number of entries: 1
```
Enabling traces in Websphere

If you encounter problems enabling SPNEGO or Kerberos in WebSphere Application Server, you can diagnose the failure by enabling traces as described in this section.

Before you begin
You must be able to log into the Websphere console with administrator privileges.

About this task
To enable the Java Generic Security Services (JGSS) and Kerberos (KRB) traces, follow these steps:

Procedure

1. Log into the Websphere administrative console.

   **Note:**
   You can access the Websphere console using the following URL:
   HTTPS://<ACE_IP>:9043/admin

2. Navigate to **System administration > Deployment manager**.


4. Set the following properties:
   - com.ibm.security.jgss.debug to all
   - com.ibm.security.krb5.Krb5Debug to all

5. Click **OK**, and click **Save changes**.

6. Ensure that the nodes are synchronized and restart the environment including all the servers, deployment manager and node agents.

Service principal not found or set incorrectly

Kerberos authentication is not possible for services without properly set Service Principal Names (SPNs). Only one SPN should be set for each service. If an SPN is not set for a service, then clients have no way to locate that service.

Possible error messages:
• 0x6 - KDC_ERR_C_PRINCIPAL_UNKNOWN: Client not found in Kerberos database
• 0x7 - KDC_ERR_S_PRINCIPAL_UNKNOWN: Server not found in Kerberos database
• 0x29 - KRB_AP_ERR_MODIFIED: Message stream modified
• 0x1B - KDC_ERR_MUST_USE_USER2USER: Server principal valid for user2user only

Resolution

Procedure

Generate the keytab file with correct values for its parameters. See Generating the keytab file on page 52 for more details.

Duplicate service principal names found

Kerberos authentication is not possible for services without properly set Service Principal Names (SPNs). Only one SPN should be set for each service. If an SPN is not set for a service, then clients have no way to locate that service. Multiple SPNs can cause clients to connect to the wrong system or the ticket may be encrypted with the wrong key.

Possible error messages:
• 0x8 - KDC_ERR_PRINCIPAL_NOT_UNIQUE: Multiple principal entries in database
• 0x1F - KRB_AP_ERR_BAD_INTEGRITY: Integrity check on decrypted field failed
• You are prompted for username and password. This implies that the authentication has fallen back to NTLM.

Resolution

Before you begin

• You must able to log into Active Directory with administrator privileges.

Procedure

1. Log into Active Directory.
2. To list all the service principal names, enter:
   
   setspn -l <userID>
3. To remove duplicates, enter:

   `setspn -D <SPN> <userID>`

   , where

   • `<SPN>` is the service principal name that is duplicated.
   • `<userID>` is the username associated with the duplicated SPN.

---

**Example**

To remove the duplicate SPN, `http/user1.mydomain.com` for the user, `user1`, enter:

   `setspn -d http/user1.mydomain.com user1`

A sample output:

   Unregistering ServicePrincipalNames for
   CN=user1,CN=Users,DC=mydomain,DC=com
   http/user1.mydomain.com
   Updated object

---

**Incorrect FQDN in SPN**

The principal service must be in the following format:

   `<Service>/<FQDN host name>@<Realm>`

The exception happens when the fully qualified host name is not specified and it was not found from the `/etc/hosts` file or the DNS server.

On UNIX or Linux systems, if the hosts line in the `/etc/nsswitch.conf` file is configured to first look in the hosts file before it looks in DNS, the Kerberos configuration might fail if the hosts file contains an entry for the system that is not the fully qualified host name.

---

**Resolution**

**Procedure**

Update the `/etc/hosts` file to contain a fully qualified host name for the system.

---

**Authentication falls back to NTLM**

The system attempts authentication by using the Kerberos protocol but it fails. As a result, the system attempts to authenticate by using NTLM.
Fallback to NTLM could occur due to:
  • Duplicate service principal names.
  • The web browser has not been configured to support IWA authentication.

Resolution

Use this procedure to resolve scenarios where the system is using NTLM authentication although it has been configured for IWA authentication.

Procedure

1. Check the IWA configurations of client.
2. Ensure that the browsers are configured to support IWA. See Configuring IE for SPNEGO on page 54
3. Delete duplicate SPNs. See Duplicate service principal names found on page 71.
4. Generate keytab file with the appropriate parameters. See Generating the keytab file on page 52

Incorrect keytab file generation

Generating the correct keytab file is an essential for Kerberos authentication to work correctly.

See Generating the keytab file on page 52.

The ktpass command is used to generate the keytab file.

The command can fail due to the following reasons:
  • Support tools needed for running the ktpass command are not installed. If you are using Windows Server 2003, you must install the support tools separately.
  • /mapUser and /pass parameters do not match that of the user created in AD.
  • The domain controller is not configured properly.

Resolution

Procedure

1. Enter the user credentials used while creating the user in Active Directory.
2. To ensure the domain controller is configured properly, do the following:
At the command prompt, enter:

```bash
netdiag.
```

To ensure that you have registered the domain controller, enter:

```bash
ipconfig/registerdns.
```

---

**LDAP bind user password expires**

In LDAP authentication, the user credentials of a user on the LDAP server are used to query the directory for authenticating users. This user is referred to as the bind user. When a username is returned as the result of such a query, the name and password are used to authenticate the user.

For LDAP authentication to work successfully, you must ensure that the binding user credentials are valid, that is, the username and password exists in LDAP and that the password has not expired. If the associated password expires, you will not be able to connect to the LDAP directory.

**Resolution**

**Before you begin**

You must obtain the *sysadmin* and *root* user passwords.

You must have administrator privileges to Websphere administrator console.

**About this task**

Use this procedure to reset LDAP bind user password when it expires.

**Procedure**

1. Log in to the Websphere console. Enter:
   ```bash
   https://<ACE_IP>:9043/admin
   ```
2. Navigate to **Security > Security domains**.
3. Click **ACE_SECURITY_DOMAIN**.
4. In the resultant window, click **User Realm**, click **Configure**.
5. In the Federated repositories window, click **manage repositories**.
6. In the Manage repositories window, click **LDAP Repo**.

**Note:**
If you have configured multiple domains, this page displays as many LDAP Repo links as there are domains.

7. In the resultant window, under Security, change Bind password and click Save.

8. Restart the servers.
   a. Log in to the Avaya ACE host. See Logging in to the Avaya ACE host on page 17.
   b. Change directories. Enter
cd /opt/avaya/ace/bin
c. Run the following script:
   ./RestartAllServer.sh

---

Authentication fails when user belongs to many groups

Authentication fails for users belonging to multiple groups in AD.

Probable causes:
- User belongs to a group which has a null objectGUID.
- Kerberos token generated exceeds the maximum size limit.

Resolution

- Perform one of the following:
  - If the objectGUID of any of the groups that the user belongs to is null, assign a valid objectGUID to the group.
  - Update the MaxTokenSize parameter in the Windows registry. For more information, see
    - [http://support.microsoft.com/kb/327825](http://support.microsoft.com/kb/327825)
    - [http://support.microsoft.com/kb/269643](http://support.microsoft.com/kb/269643)
User authentication
Chapter 7: Global security policy management

Manage Avaya Agile Communication Environment™ (ACE) global security policy to control Avaya ACE™ GUI session parameters and define and enforce user password rules. Global security policies apply to all users.

Prerequisites to global security policy management

• You are familiar with the security policy requirements specific to your ACE deployment.
• You are familiar with the ACE user authorization model. See User management fundamentals on page 27.
• You are a user with system administrative access privileges.

Note:
A system administrator is a user who is assigned the SystemAdmin role. See SystemAdmin role on page 32.

Global security policy management procedures

This task flow shows the sequence of procedures you perform to manage ACE global security policies.
Global security policy management

Figure 16: Global security policy management

Global security policy management navigation

- Adding an IP as trusted host on page 66
- Changing global password policy settings on page 79
Changing global password policy settings

Before you begin

• An Avaya ACE™ GUI session is open.
• You have system administrator privileges.
• You are familiar with the password rules requirements specific to your ACE deployment.
• You are familiar with the implicit password rules in addition to password rules that are explicitly configured. See Implicit global password rules on page 36

About this task

Change global password policy settings when you want to enforce customized user password rules and other password related settings. Global security settings define ACE global authentication policies applicable to all configured users.

By default, the global Password Expiry Period is set to 0, which means password expiry is set to "never". Leaving the field blank also sets the value to "never".

Important:

Changes to the Password Expiry Period or to the Password Expiration Notification require a password reset to take effect. After the policy has been updated, the value of those attributes apply to each user as they change their user password. If you want the new settings to take effect immediately, reset user passwords.

Procedure

2. Select the Internal Account Policy tab, and then the Password Policy tab.
3. Make the desired changes to existing password policy and password rules attributes. For a description of the supported attributes, click online help button located at the top of the GUI window.

Important:

Password rules are a set of rules to which all user passwords must comply. A zero (0) value in the numeric field of a rule disables the rule (rule is not applied). Password rules are defined globally and apply to all users. They cannot be overridden.

4. Click Submit.
Changing global password policy settings

Use the Account Policy tab to change global user login session attributes. Global Account Policy settings can be overridden by individual user profile configurations.

Before you begin

* Open an Avaya ACE™ GUI session.
* Ensure you have system administrator privileges.

About this task

Global security settings define ACE global authentication policies applicable to all configured users.

Procedure

2. Select the Internal Account Policy tab, and then the Account Policy tab.
3. Make the desired changes to existing account policy and account rules attributes. For a description of the supported attributes, click online help button located at the top of the GUI window.

**Important:**

You must log out of the current Avaya ACE GUI session and log back in for changes to Inactivity Period to take effect.

4. Click Submit.
Chapter 8: Role management

Avaya Agile Communication Environment™ (ACE) supports a role-based access control of resources such as Avaya ACE™ Web services or applications. Roles encompass licenses and the corresponding access privileges (role policies) to these resources.

On Avaya ACE, roles exist as role profiles. Role profiles are typically assigned to users that require access privileges to resources. The following sections describe procedures to create and update role profiles to manage licenses and corresponding access privileges for Avaya ACE users.

Prerequisites to role management

- You are familiar with the Avaya ACE user authorization model. See User management fundamentals on page 27.
- You are a user with system administrative access privileges.

*Note:* A system administrator is a user who is assigned the SystemAdmin role. See SystemAdmin role on page 32.

Navigation

- Creating a role profile on page 81
- Modifying a role profile on page 83
- Deleting a role profile on page 84

Creating a role profile

Create a role profile to define licenses and corresponding role policies. A role policy defines the access privileges to resources such as Avaya ACE Web services and applications. After you create a role profile you can assign it to one or multiple users.

Only users that have system administrator privileges can configure new role profiles.

**Before you begin**

Ensure that:

- You have system administrator privileges.
- You know the licensing requirements of the role profile. However, this is optional at the time of role profile creation.
• You know the list of configured ACE users who will be assigned this role profile. See Listing ACE users on page 101. However, this is optional at the time of role profile creation.
• An Avaya ACE GUI session is open.

About this task
Configuring a role profile consists of defining role information properties, and optionally user membership and license membership information.

Procedure
1. Log in to the Avaya ACE GUI.
2. On the main menu bar, choose Security > Role Management > Create Role. The Create Role window appears.
3. In the Role Information window, specify the name of the role profile. This is a mandatory parameter.
4. (Optional) Assign this role profile to configured users. To do this at a later time, see Modifying a role profile on page 83.
   a. In the Membership Information window, click the Users tab.
   b. Select the users to which you want to assign this role profile from the Available Users list and move them to the Member Users list.
5. (Optional) Configure license membership and role policy information. To do this at a later time, see Modifying a role profile on page 83.
   a. In the Membership Information window, click the Licenses tab.
   b. Select the licenses to add to the role from the Available Licenses list and move them to the Member Licenses list.
   The Role Policy window dynamically displays the services/applications and their default access level permissions, based on the licenses assigned to this role. For each service/application, the access level is displayed as On/Off. Modify the access level as required.
6. Click Submit to save the configuration.
Modifying a role profile

Before you begin

Ensure that:

• you have system administrator privileges.
• you know and understand the impact of the changes on the users that are assigned this role.
• An Avaya ACE™ GUI session is open.

About this task

Modify a role to update user, license membership details or role policy details to meet new requirements.

Important:

Changes you make do not impact users that are currently logged on the system or are currently using services. Changes to role configuration come into effect the next time the user assigned that role logs on to the system or sends a service request.

Procedure

1. On the menu bar, navigate to Security > Role Management > List/Edit Roles. The system displays the List Roles window.

2. In the Search Criteria window, click Search by All Roles and then click Submit.

3. Click the name of the role profile you want to modify. The system displays the Role Details window. The Role Details window contains the role profile configuration information. Make the required modifications to license membership, user membership, or role policy information.

4. To modify user membership information:
   a. In the Membership Information window, click the Users tab.
   b. Select the users you want to assign this role from the Available Users list, and move them to the Member Users list.

   Important:

   If you remove a user from a role configuration when the user is logged in to the ACE GUI, the GUI displays a message about a change in user permissions. The system automatically logs off the user and prompts the user to log in again.

5. To modify license membership and role policy information:
   a. In the Membership Information window, click the Licenses tab.
b. Select the licenses to add to the role from the **Available Licenses** list, and move them to the **Member Licenses** list.

The **Role Policy** window dynamically displays the services and the default access level permissions for each of those services. The default access permissions are based on the licenses assigned to this role. For each service, the access level is displayed as **On/Off**. Modify the access level if required.

6. Click **Submit**.

---

**Deleting a role profile**

**Before you begin**

- You have system administrator privileges.
- You know and understand the impact of deleting the role profile on the users that were assigned this role. If applicable, assign those users to another role with appropriate access privileges.
- An Avaya ACE™ GUI session is open.

**About this task**

Delete a role profile when the role profile no longer meets the licensing and access requirements. Deleting a role profile removes the licensing and role policy information configured on the role profile.

**Important:**

If you remove a user from a role configuration and the user is logged in to the ACE GUI, the GUI displays a message to that user warning him of a change in user permissions. That user is automatically logged off the GUI and prompted to log in again.

**Procedure**

1. On the menu bar, choose **Security, Role Management**, and then **List/Edit Roles**.
   The **List Roles** window appears.
2. In the **Search Criteria** dialog box, select **Search by All Roles**.
3. Click **Submit**.
   The list of all configured Role profiles are displayed.
4. Click the delete button beside the name of the role profile you want to delete.
5. When prompted to proceed, click **Yes** to delete the role profile.
Job aid for counting licenses

In Avaya ACE Release 6.2.x, the following relationship is established between licenses, roles, and users:

- Licenses define access control to Avaya ACE resources such as Web services.
- A license manager such as WebLM installs and manages the licenses. Roles use licenses from the license manager.
- Roles are assigned to users.

To use a license, assign the associated role to at least one user. Thus, the number of licenses a role uses depends on the number of users with that role.

For example, consider a customer with several API Integration Suite licenses.

Assign the API Integration Suite licenses to roles MessagingRole1 and MessagingRole2.

- Assign MessagingRole1 to User1: One API Integration Suite license is used.
- Assign MessagingRole1 to User1 and MessagingRole2 to User2: Two API Integration Suite licenses are used.
- Assign MessagingRole1 to User1 and MessagingRole2 to User2 and User1: Only two API Integration Suite licenses are used. Although User1 has two roles, the user needs only one license.

*Note:*
In Avaya ACE, you can associate a user with more than one role.

- Assign MessagingRole1 to User1 and MessagingRole2 to User2 and User3: Three API Integration Suite licenses are used.

You can assign MessagingRole1 and MessagingRole2 to users until all API Integration Suite licenses the customer bought are used. If you assign the Messaging role to a user after all the licenses are used, the system displays an error message.

Job aid for configuring access control rules

About this task
In order for Avaya ACE™ to respond to a client application making a web service request, the role assigned to the client application must be configured with the right level of service access control. The following table shows the minimum access level required for the Avaya ACE Web service subject to licensing.
### Important:

Your licensing agreement determines which service is listed. The Avaya ACE GUI only displays services for which you have acquired a license.

#### Table 2: Minimum access level required for service access control

<table>
<thead>
<tr>
<th>Service name</th>
<th>Minimum access level required</th>
</tr>
</thead>
<tbody>
<tr>
<td>AudioCallService Required for Avaya ACE Audio Call Web service</td>
<td>OFF</td>
</tr>
<tr>
<td>CallForwardingService Required for Avaya Avaya ACE Call Forwarding Web service</td>
<td>ON</td>
</tr>
<tr>
<td>CallHistoryService Required for Avaya ACE Call History Web service</td>
<td>ON</td>
</tr>
<tr>
<td>CallNotificationService Required for Avaya ACE Call Notification Web service</td>
<td>ON</td>
</tr>
<tr>
<td>LocationSupplierService Required for Avaya ACE Location Supplier Web service</td>
<td>ON</td>
</tr>
<tr>
<td>PresenceConsumerService Required for Avaya ACE Presence Web service</td>
<td>ON</td>
</tr>
<tr>
<td>PresenceSupplierService Required for Avaya ACE Presence Web service</td>
<td>ON</td>
</tr>
<tr>
<td>TerminalLocationService Required for Avaya ACE Terminal Location Web service</td>
<td>ON</td>
</tr>
<tr>
<td>ThirdPartyCallService Required for Avaya ACE Third Party Call Web service</td>
<td>ON</td>
</tr>
</tbody>
</table>
Chapter 9: User management

Manage users of Avaya Agile Communication Environment™ (ACE).

For a complete list and description of supported configuration parameters and attributes, see the online help which is accessible in context, from each window of the Avaya ACE™ GUI.

Prerequisites

• You must be familiar with the User management fundamentals on page 27.
• You must be able to log in with system administrator access privileges (assigned the SystemAdmin role).

Changing your password

Before you begin

• Open an Avaya ACE GUI session.
• Ensure that you are familiar with the enforced password rules.

About this task

Change your own user password before it expires or when you have any reason to believe that the security of your password has been compromised.

You cannot use this procedure to change another user's password. To change another user's password, use the procedure Modifying a user on page 96.

Important:

This GUI-based procedure applies only to users with system administrator privileges. Users who do not have system administrator privileges do not have access to the Avaya ACE GUI. Such users can change their own user password over a programmatic interface using the changePassword operation provided by the User Profile web service.

Always change your password when you log on the system for the first time. For information on how to log on to the system, see Logging on to the Avaya ACE GUI on page 88.

When you define a new user password, the new password must comply with a set of password rules. If your password does not comply with the defined rules, an appropriate error message displays the rules that are currently in effect. This message will help you define a valid password.
Consider the following when changing your password. A valid user password must not contain

• the string defined as the user ID
• the string defined as the user ID in its inverted form (for example, if the user ID is "John", the password cannot contain the strings "nhoJ".
• a sequence of three or more characters present in the previous password

⚠️ Important:
Passwords are case sensitive.

Procedure

1. On the menu bar, choose Security and then Change Password.
2. In the appropriate fields, enter your old password and then your new password.
3. Confirm your new password.
4. Click Submit.

Logging on to the Avaya ACE GUI

Before you begin

• You must know the IP address of the Avaya ACE host.

🌟 Note:
For HA deployments, you must know the floating IP of the Avaya ACE HA system.

• If you log in to Avaya ACE as a system administrator for the first time, you must know the default user name and password. If you log in for the first time as a user other than the administrator, you must know the login credentials associated with your user account. Otherwise, contact your system administrator.

• Your browser must be enabled for cookies and Javascript.

About this task

Use this procedure to log on the Avaya ACE Web-based graphical user interface (GUI). Initial login credentials for the root system administrator are:

• username: admin
• password: agile

⚠️ Important:
You cannot log on to the Avaya ACE GUI if the /tmp/ partition is full. There must be a minimum 1 MB of free space.
Important:
After you install Avaya ACE, you may receive a certificate error the first time you log on to the GUI. The error format depends on your web browser. Select the appropriate option to continue to the ACE GUI web page.

Important:
For security, Avaya ACE enforces a password change on the root user's initial login.

Procedure

1. Open an instance of a web browser and connect to the Avaya ACE GUI at the following address:
   https://<ACE_host_IP>:9449/oamp
   The ACE GUI User Authentication page appears.
2. Log on to Avaya ACE. Enter your user ID in the Username field.
3. Enter your ACE user password in the Password field. Click Reset if you need to clear both fields.
4. After you enter the user name and password, click Login.

   Important:
   On initial login as the root administrator user, you will be prompted to change the default password to a new password.
   The Avaya ACE GUI displays the Login Information page.

Creating a user

Before you begin

• You have system administrator privileges.
• An Avaya ACE™ GUI session is open.

About this task

Create a user configuration on the ACE system to allow a user or web service client with valid credentials to access the Avaya ACE. A user configuration also allows you to optionally configure and control security settings specific to that user.

Use this procedure to configure a valid ACE user account.

You create a user profile on Avaya ACE by defining, at a minimum, a user ID and user password. The user ID must be unique locally and across the federation, if ACE is part of a
federated deployment. The system then uses these credentials to authenticate a user or application requesting access.

For information on how to configure a user account policy, see Configuring a user account policy on page 97.

If contact information is required in the user configuration, see Adding contact information to a user configuration on page 91.

Procedure


2. Select the User tab. At a minimum, provide values for the following fields: User ID, User Password, and Confirm User Password.

   By default, Account State is set to Disabled. Optionally disable the account by setting the account state to Disabled.

   By default, Authentication Type is set to INTERNAL. Authentication Type determines the type of authentication used to authenticate the user. INTERNAL users are authenticated using mySQL authentication and EXTERNAL users are authenticated using IWA or LDAP authentication mechanisms.

3. Optionally, assign this user a role. If you do not want to assign a role at this point, go to the next step.

   Select the Role Membership tab. From the list of Available Roles, select the role that you want to assign to the user. Click the arrow to add the role to the list of Member Roles. Repeat this step for each required role.

4. Optionally, enforce a password change on the user. The user is then prompted for a password change during the next Avaya ACE GUI login session. If you do not want to enforce the password change, go to the next step.

   To enforce a password change, check the User must change password at next logon box.

5. Click Submit.

   The User Creation Success window opens and displays a message confirming that the new user was created successfully.

Important:

At this point, you have the option to modify the user account or create another user account. To modify/update the newly created user account, click Edit User. For more information about editing an existing user profile, see Modifying a user on page 96. To create another user account, click Create Another User.
Adding contact information to a user configuration

Before you begin

- An Avaya ACE™ GUI session is open.
- The Edit User window is open and the user profile configuration is displayed.
- You are familiar with the service provider requirements for specifying contact information.

About this task

Use this procedure to add contact information to an existing user configuration when this user data is required by a web service implementation.

Contact information such as the Contact Name associates a name with a specific contact information entry.

Contact information such as, contact identifier, must comply to an expected syntax and dial plan of the connected PBX elements in order to be recognized by some service providers.

For information about the expected syntax based on the service provider and type of contact information, see Job aid for specifying contact identifiers on page 92 at the end of this procedure.

If you have system administrator privileges you can modify any user configuration.

Procedure

1. From the Edit User window, select the Personal Data tab.
2. In the Contact Information dialog, select the required Contact Type from the list, to specify the type of communication media used by this user.

   If you select Conference as the type, the PIN field is activated. If your service provider supports a PIN, add a personal identification number (PIN) and then repeat in the Confirm PIN field.

   Note:
   Configuring a PIN is optional.
3. In the **Contact Name** field, enter a meaningful name for the user's communication device that will help the user, or Avaya ACE client applications identify it easily. Standardize contact names across multiple users. For example, all mobile phones can have a contact name of *mobile* and all office desk phones can have the name *deskphone*.

**Important:**
Contact names are sometimes used by Avaya ACE client applications such as Hot Desking or Mobility to, for example, distinguish a user’s mobile phone from a regular desk phone.

For more information on the contact name requirements for ACE client applications, see the respective application documentation.

4. In the **Contact Identifier** field, enter the number or address, such as, a telephone number, SIP, or IP address, associated with the contact type. Make sure to use the correct syntax and prefix when specifying this information. See [Job aid for specifying contact identifiers](#) on page 92.

5. Assign the desired priority level for this contact. This information is used for priority routing. In the **Priority** field, enter a number between 0 and 1, such as 0.1, where 0 is the lowest priority and 1 is the highest.

6. If applicable, make this contact the default calling line identifier (CLI) for this user. Enable the **Default CLI** check box.

**Note:**
The Default CLI feature is only supported for SIP calls.

7. Click **Save Contact Information**.
When you click **Save Contact Information**, the new information is displayed in the table, along with existing contacts configured for this user information.

8. Repeat 2 on page 91 to 7 on page 92 to configure additional contacts as required.

9. Click **Submit** to save the changes to the user configuration in the user database.

---

**Job aid for specifying contact identifiers**

When you define contact information in an ACE user profile, the service provider determines which syntax or prefix must be used in the **contact identifier** field.

Avaya ACE supports ITU-T Recommendation E.123 (Notation for national and international telephone numbers, e-mail addresses and Web addresses) for the definition of the
**contactIdentifier** parameter value when the **type** is set to **Telephone**. For example, the following URIs are valid values for a telephone contact identifier:

- tel:+31421234567
- tel:(042) 123 3456
- tel:+31 42 1234567

⚠️ **Important:**

Ensure that you do not use square brackets ([ ]), when defining contact identifiers.

⚠️ **Important:**

For **Telephone** contact types, use the full international number, for example, tel: +31421234567, to ensure that the number is globally unique for that device. This facilitates inter-working among multiple service providers. Using the full international number in a federated ACE deployment scenario facilitates Avaya ACE to contact the user's (telephone) device using the optimum provider.

The following table shows how to specify contact information for specific service provider network elements.

<table>
<thead>
<tr>
<th>Service provider</th>
<th>Contact type</th>
<th>Contact identifier</th>
<th>Contact identifier example</th>
<th>PIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Communication Server 1000</td>
<td>Telephone</td>
<td><strong>tel:&lt;number&gt;</strong></td>
<td>tel:+1 (613) 12345</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>sip:</strong></td>
<td>sip:jane@acme .com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The format of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>tel:&lt;number&gt; and/or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sip:&lt;address&gt; depends on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>dial plan provisioning of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the connected PBX.</td>
<td></td>
</tr>
<tr>
<td>Avaya Communication Server 2000</td>
<td>Telephone</td>
<td><strong>tel:&lt;number&gt;</strong></td>
<td>tel:88501</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sip:jane@acme .com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The format of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>tel:&lt;number&gt; and/or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sip:&lt;address&gt; depends on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>dial plan</td>
<td></td>
</tr>
<tr>
<td>Service provider</td>
<td>Contact type</td>
<td>Contact identifier example</td>
<td>PIN</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------</td>
<td>----------------------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>Cisco Call Manager</td>
<td>Telephone</td>
<td>tel:&lt;number&gt; sip:&lt;address&gt;</td>
<td>tel:88501 sip:<a href="mailto:jane@acme.com">jane@acme.com</a></td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tandberg</td>
<td>Video</td>
<td>sip:&lt;address&gt;</td>
<td>sip:<a href="mailto:tandberg-10@acme.com">tandberg-10@acme.com</a></td>
<td>Not supported</td>
</tr>
<tr>
<td>Avaya Aura Application Server 5300</td>
<td>Telephone</td>
<td>sip:&lt;address&gt;</td>
<td>sip:<a href="mailto:jane@acme.com">jane@acme.com</a></td>
<td>Not supported</td>
</tr>
</tbody>
</table>

### Modifying contact information

**Before you begin**

- An Avaya ACE™ GUI session is open.
- The Edit User window is open for the user whose contact information you want to modify.

**About this task**

Use this procedure to edit existing contact information. You can change the value of any of the contact information parameters with the exception of the contact type value. If a change to the contact type is required, you must configure a new contact specifying the required type.

**Procedure**

1. From the Edit User window, select the Personal Data tab.
2. In the Contact Information area, see the table that lists all the configured contact names and the corresponding contact information.
3. Click the **Edit** icon next to the contact you want to change.

4. For all contact types, clicking **Edit** provides an editable view of the contact parameters values. You can edit any of the following field values: **Contact Identifier**, **Contact Name**, **Priority**, **Default CLI** and, if the contact type is Conference, you can also edit the **PIN**. To create a new PIN, enter a new **PIN** value and then repeat in the **Confirm PIN** field.

   When you modify the **Contact Name** field, enter an appropriate name (or string) for the user (or the user’s communication devices), depending on the contact type. For example, for a contact type of telephone, you can specify the user’s telephone device to be either a mobile or an office desk phone. For a contact type of chat, specify a friendly name by which the user can be known.

   ⚠ **Important:**

   When editing a PIN, leaving the **PIN** and **Confirm PIN** fields blank or clearing these fields sets the PIN to a blank value which is equivalent to "no PIN configured".

5. Click **Save Contact Information** to save your configuration changes.

   The contact information table shows the new value.

---

### Enforcing a password change

**Before you begin**

* An Avaya ACE™ GUI session is open.
* The **Edit User** window is open for the user whose password you want to change.

**About this task**

Enforce a password change on an existing user by making the current user password temporary. This forces the current password to expire. As a result, the user is prompted to change password at the next GUI login session. You can only enforce a password change on Avaya ACE GUI users. Over a web service interface, when a password has expired, authentication fails.

**Procedure**

1. From the main menu, select **Security**, **User Management** and then **List/Edit Users**. The configured user configurations are listed.

2. Click the User ID corresponding to the user configuration you want to modify. The **Edit User** window opens giving you access to the user configuration.
3. To enforce a password change, you must change the current user password. In the User Password, enter a user password. Re-enter the password in the Confirm Password field.

4. Check the User must change password at next logon box.

5. Click Submit to save your configuration changes.

---

**Modifying a user**

**Before you begin**

- You have system administrator privileges.
- An Avaya ACE™ GUI session is open.

**About this task**

Modify a user configuration when you want to add or change user authentication credentials or other user configuration data like, for example, role membership.

⚠️ **Important:**

Changing the role membership of a user logged on the ACE GUI automatically logs off that user, warning him that the user permission has changed. The user is then prompted to logon again.

You cannot use this procedure to change your own user password. For information about how to change your own user password, see Changing your password on page 87.

**Procedure**

1. From the main menu, select Security, User Management, then List/Edit Users. The user configurations are listed.

2. Click the User ID corresponding to the user configuration you want to modify. The Edit User window opens and gives you access to the user configuration.

3. Make the required modifications.

4. Click Submit to save your configuration.
Unlocking a user account

Unlock a user account when you want to provide immediate login access to a user who's account has been locked.

A user is locked out of his account when he has exceeded the configured maximum number of login attempts.

Unless the system administrator unlocks the account, a locked account remains inaccessible until the configured amount of time as specified by the Lockout Period attribute has elapsed.

Before you begin

An Avaya ACE™ GUI session is open.
You have system administrator privileges.

Procedure

1. From the main menu, select Security, User Management, then List/Edit Users. The List Users window appears.
2. Using the Search Criteria dialog box, specify the search criteria to search for the user whose account you want to unlock. Alternatively, click Submit to display all Avaya ACE configured users.
3. Click the User ID corresponding to the user account you want to unlock. The Edit User window opens and gives you access to the user configuration.
4. Select the Account Policy tab.
5. In the Account Policy window, click Unlock Account. A message appears asking you to confirm if you want to unlock the user account.
6. Click OK to unlock the account. The account Lockout Status changes to Unlocked.

Configuring a user account policy

Before you begin

• An Avaya ACE™ GUI session is open.
• You have system administrator privileges.
About this task

Configure a user account policy when you want to enforce user login session settings or change attribute values related to password expiry period and password expiry notification.

When a user account does not specify account policy settings, the global account policy defined in Global Security Settings applies.

Procedure

1. From the main menu, select Security, User Management, then List/Edit Users. The List Users window appears.

2. Using the Search Criteria dialog box, specify the search criteria to search for the user whose account policy you want to modify. Alternatively, click Submit to display all Avaya ACE configured users.

3. Click the User ID corresponding to the user configuration you want to modify. The Edit User window opens and gives you access to the user configuration.

4. Select the Account Policy tab.

5. Make the required changes. For information about each available attributes in the Account Policy window, launch the online help from the GUI by clicking on the help icon located in the top right of the Edit User window.

   Important:
   Changes to the Password Expiry Period or to the Password Expiration Notification in the user account policy require a password reset to take effect. If you want the new settings to take effect immediately, reset the user password.

6. Click Submit to save your changes.

Deleting contact information from a user configuration

Before you begin

• An Avaya ACE GUI session is open.
• You have system administrator privileges.
• The Edit User window is open for the user whose contact information you want to delete.

About this task

Delete contact information from an existing user configuration when a contact number is no longer needed.
Procedure

1. From the Edit User window, select the Personal Data tab.
2. In the Contact Information dialog, look in the table that lists all the configured contact names or types and corresponding number or IP address.
3. Click the icon in the Delete column next to delete the unwanted entry.
   A dialog box appears asking you if you want to delete the contact details.
4. Click Yes to proceed.
5. Click Submit to save the changes to the user configuration in the user database.

Deleting user profiles

Before you begin

Ensure that:

- You have system administrator privileges.
- An Avaya ACE GUI session is open.
- Remove all roles from the user profiles you want to delete.

About this task

Delete one or multiple user profile configurations when the user profiles are no longer required and you want to permanently remove the user profiles.

⚠️ Note:

You cannot delete predefined users.

Procedure

1. From the main menu, select Security > User Management > List/Edit Users.
2. In the Search Criteria, select All Users.
   Click Submit.
   The GUI displays a list of configured user profiles.
3. Select the users you want to delete using the check boxes. You can select one or multiple users. To select all users, use the top most check box.
4. Click Delete to delete the selected users.
   A prompt lists the selected user profiles and asks you to confirm.
5. Click OK to delete the user profiles.
The GUI displays a message listing the user profiles who were successfully deleted, and user profiles which were not. The message specifies why Avaya ACE did not delete the user profiles.

---

**Viewing security audit logs**

**Before you begin**

- An Avaya ACE™ GUI session is open.
- You have system administrator privileges.

**About this task**

View security audit logs to monitor events such as configuration changes affecting user data or security policies.

**Procedure**

1. From the menu bar, select **Fault**, and then **Event Browser**. The **Event Browser** window opens.
2. In the **Start Time** field, set the start date and time of the period for which to collect data.
   
   If you do not want to specify a time period, go to 4 on page 100.
3. In the **End Time** field, set the end date and time of the period for which to collect data.
4. In the **System ID** field, select the system for which you want to collect data.
5. In the **Event Class** list, select **Audit**.
6. In the **Severity** list, select the desired severity criteria.
7. Click **Query**.
   
   The generated logs are listed.
Listing ACE users

Before you begin

• An Avaya ACE™ GUI session is open.

About this task
List users to display users configured on the Avaya ACE.

The Avaya ACE GUI allows you to search and display a list of ACE users based on selected criteria. You can list all users, or search by filtering on one of the following criteria: user ID, surname, given name, common name, nickname, contact identifier, postal address and description.

Procedure

1. On the menu bar, select Security, User Management, and then List/Edit Users. The List Users window appears.

2. Using the Search by list, select the search criteria. In the Search for field, define the search criteria value. Avaya ACE supports searches using a wildcard character where you substitute the asterisk (*) sign for a single or a string of characters. By default, Avaya ACE lists all users

3. Click Submit. The List Users Result window displays the users matching the selected criteria.
User management
Chapter 10: Managing Websphere security

About this task
After installation, you can add WebSphere user IDs and define the access privileges for each user ID. The default password for the WebSphere primary administrative account password is set during installation. After installation, you can use this user ID to log in to the WebSphere administrative console.

For more information on WebSphere security, see the [http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp](http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp), at the IBM Information Center.

⚠️ Important:
Do not change the WebSphere user ID ClusterAdm default password.

The Avaya ACE™ installation process creates the default user ID ClusterAdm. This user ID is assigned only operational privileges for use during a high availability switchover. In order to maintain the capability to perform a switchover, do not change the default password for the ClusterAdm user ID.

Procedure

1. Open a Web browser and enter the following URL for the administrative console:
   
   https://<hostname>:9043/admin
   
   The administrative console loads and a window opens for your user ID and password.

2. In the navigation pane on the left, select Security, and then Global security.
   
   Use the security screen to manage WebSphere security.
Managing Websphere security
Chapter 11: Database administration

This section contains procedures for administering the Avaya Agile Communication Environment™ (ACE) database. ACE 6.2.x installs MySQL5.5.30-1. For information on managing the database, see the http://dev.mysql.com/doc/refman/5.5/en/.

The Avaya ACE™ installation process installs and configures a MySQL database with the database name profile. The following user IDs are created.

<table>
<thead>
<tr>
<th>User ID</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>Top level user ID with all privileges. The password is set during installation.</td>
</tr>
<tr>
<td>aceDBuser</td>
<td>select insert update delete</td>
</tr>
<tr>
<td>replication</td>
<td>select insert update delete</td>
</tr>
</tbody>
</table>

⚠️ Important:
The aceDBuser and replication user IDs are used by Avaya ACE for system tasks. Do not change the passwords for these user IDs.

Changing the database password

About this task
To change the database user name password, you must connect to the database and change the password

⚠️ Important:
You must not use the ! character for MySQL passwords.

Procedure

1. On the ACE host, open a console window, and connect to the database. Enter
   mysql -u root -p
2. At the command prompt, enter the password for root user. Enter
3. Change the password. Enter
   SET PASSWORD = PASSWORD(''<new_password>'');
4. Disconnect from the database. Enter QUIT.
Appendix A: Kerberos terminology

Key Distribution Center (KDC)
Kerberos uses symmetric key cryptography and requires a trusted third party, the KDC.

The KDC has three logical components:

• Authentication server
  The authentication server handles requests from a client that wants to obtain a Kerberos ticket representing proof of identity. The authentication server authenticates the client, for example, with a user ID and password verification. If the authentication is successful, the authentication server returns a Kerberos ticket called the ticket-granting ticket (TGT) that represents proof of identity.

• Ticket granting server
  The ticket-granting server (TGS) handles requests for a service ticket, which the client uses to access a TGT application or service. The TGS validates the client’s TGT and returns a service ticket.

• User repository
  The user registry (sometimes refer to as the user database) holds Kerberos user information, such as the user ID, password, and the shared secret information.

Kerberos realm and principal
A Kerberos realm consists of members, which can be users, servers, services, or network resources, that are registered in the KDC. Each member has a unique principal.

The principal is a unique identifier to which the KDC can assign tickets.

A service principal name (SPN) is associated with the security principal (user or groups) in whose security context the service executes. SPNs are used to support mutual authentication between a client application and a service. A service principal name is associated with an account and an account can have many service principal names.

A principal name has the form:

\[
\text{service/\{instance\ name\}@\{realm\}}
\]

where,

• The service type name can be the user’s name, the host, or the name of the service. For example, HTTP.
• The REALM name is the name of the Kerberos realm, which is usually the domain name in uppercase letters. For example, MYDOMAIN.COM
• The instance name is optional. It is used to further define the primary name.

Thus, the SPN would be, HTTP/admin@MYDOMAIN.COM
Kerberos terminology

**Kerberos ticket**
Tickets are essentially an encrypted data structure that uses shared keys that are issued by the KDC to communicate in a secure fashion.

**Kerberos token**
A Kerberos token is created when the client authenticates with WebSphere. The token includes the Kerberos principal and the realm name that the client is using to authenticate. In Avaya ACE, authentication requests from the intranet are first intercepted by the Kerberos module, which checks the kerberos tokens presented against the Active Directory.
# Index

## A
- Account policy .......................................................... 39
- ACE documents .......................................................... 10
- Administrator role .................................................. 32, 34
  - Messaging ............................................................ 34
  - System .................................................................. 32
- authentication ............................................................ 52
- Authentication .......................................................... 54, 56, 67, 70, 71, 73, 75
- authentication failure .................................................. 68
- Authentications falls back to Basic ................................ 75
- Avaya ACE ............................................................... 30
  - Roles .................................................................... 30
- Avaya Mentor videos .................................................. 13

## B
- Basic Authentication .................................................. 64, 66

## C
- Configuring DNS ......................................................... 48, 51
- creating trust ............................................................. 59

## D
- Device ID authentication ............................................. 66
- DNS, .......................................................................... 48, 51
- configuring ................................................................. 48, 51
- Document Intent .......................................................... 9
- Document suite ........................................................... 10

## F
- fallback NTLM ........................................................... 73
  - Kerberos ................................................................ 73
  - Federation role ...................................................... 33
  - Firefox .................................................................... 56

## G
- Global passwords; ....................................................... 36
  - rules ....................................................................... 36

## I
- IE .............................................................................. 54

## K
- Kerberos .................................................................... 52, 68
- Keytab file ................................................................. 52

## L
- LDAP ......................................................................... 64, 65
  - LDAP Authentication ............................................. 64, 65
  - LDAP password ...................................................... 74
  - LDAP server configuration ...................................... 65
- Log in to ACE ............................................................. 17
- Login to ACE host ...................................................... 17

## M
- Membership ................................................................. 39
  - Roles ..................................................................... 39
- Messaging Admin role ................................................ 34
- multiple domain Authentication .................................. 59
- MySQL ...................................................................... 64, 66

## N
- New in this release ..................................................... 9

## P
- Password rules ........................................................... 36
- post installation ........................................................ 67
- Pre defined roles ....................................................... 32–34
- predefined profiles .................................................... 42
- Predefined roles ....................................................... 33
- Predefined users ....................................................... 40

## R
- related resources ........................................................ 13
  - Avaya Mentor videos .............................................. 13
- resolve SPN errors .................................................... 71
- Roles on ACE ........................................................... 30
### S

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPN</td>
<td>70–72</td>
</tr>
<tr>
<td>Duplicates</td>
<td>71</td>
</tr>
<tr>
<td>Incorrect SPN</td>
<td>72</td>
</tr>
<tr>
<td>Incorrect, Missing SPN</td>
<td>70</td>
</tr>
<tr>
<td>SPNEGO, Kerberos</td>
<td>70</td>
</tr>
<tr>
<td>support</td>
<td>13</td>
</tr>
<tr>
<td>contact</td>
<td>13</td>
</tr>
<tr>
<td>sysmonitor user</td>
<td>42</td>
</tr>
<tr>
<td>System Admin role</td>
<td>32</td>
</tr>
<tr>
<td>System defined users</td>
<td>40</td>
</tr>
<tr>
<td>System monitor role</td>
<td>33</td>
</tr>
</tbody>
</table>

### T

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshoot</td>
<td>75</td>
</tr>
<tr>
<td>Authentication</td>
<td>75</td>
</tr>
<tr>
<td>troubleshooting IWA</td>
<td>68</td>
</tr>
</tbody>
</table>

### U

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>User accounts</td>
<td>39</td>
</tr>
<tr>
<td>User management</td>
<td>39</td>
</tr>
<tr>
<td>user profiles</td>
<td>42</td>
</tr>
</tbody>
</table>

### V

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>videos</td>
<td>13</td>
</tr>
<tr>
<td>Avaya Mentor</td>
<td>13</td>
</tr>
</tbody>
</table>

### W

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Websphere</td>
<td>70</td>
</tr>
</tbody>
</table>