Configuring and Managing Avaya Identity Engines Single-Sign-On

Release 9.0
NN47280-502
Issue 1.04
December 2014

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

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

License types

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

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” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document guides you through a first-time configuration of the Avaya Identity Engines (IDE) Ignition Server to set up Avaya Aura Single-Sign-On (SSO). This guide also explains how to monitor SSO, provides use cases to demonstrate how to use SSO, and explains how to troubleshoot common problems. This guide is written for network administrators who need to configure SSO. This guide assumes you have installed the Avaya IDE Ignition Server virtual appliance as shown in the *Avaya Identity Engines Ignition Server Getting Started* guide.

Related resources

Documentation

See the following related documents.

Title	Purpose	Document number
Avaya Identity Engines Ignition Server Getting Started	Installation and simple configuration	NN47280–300
Avaya Identity Engines Ignition Server Administration	All configuration options	NN47280–600
Avaya Identity Engines Ignition Server Release Notes	Reference	NN47280–400

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to 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 website.

Note:

Videos are not available for all products.

Subscribing to e-notifications

Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

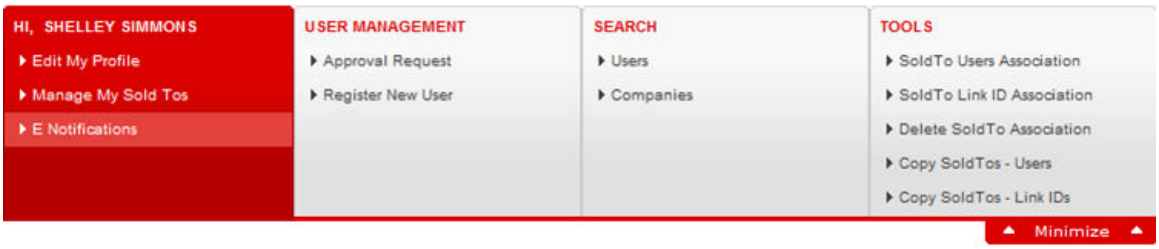
About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing Switch 8800.

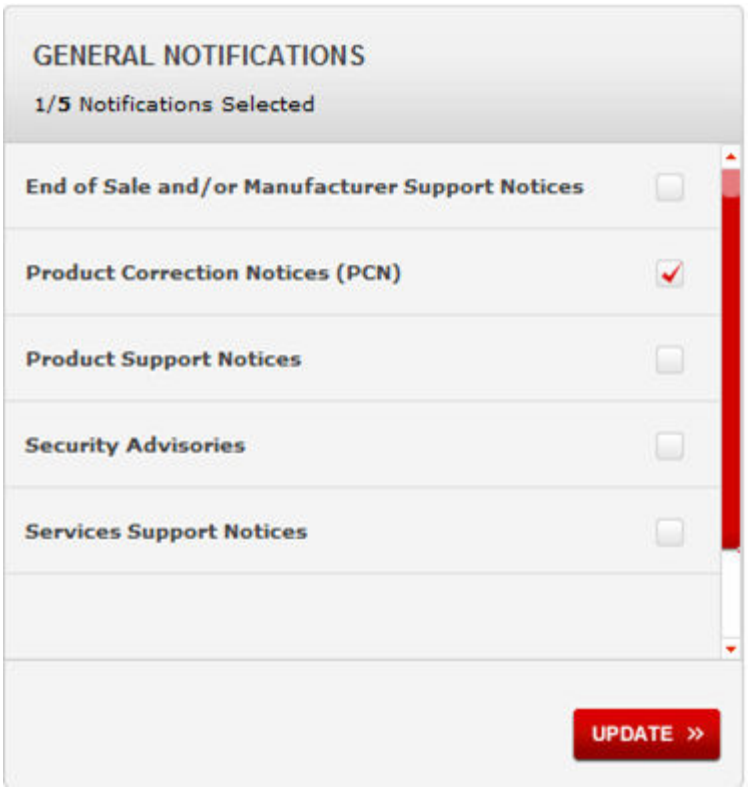
Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **LOG IN**.
3. Click **MY PROFILE**.

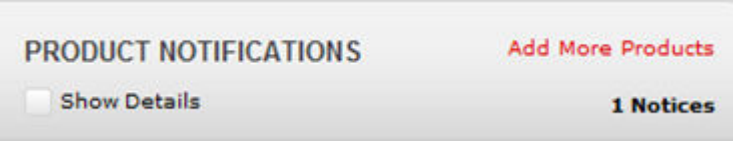
4. On the site toolbar, click your name, and then click **E Notifications**.



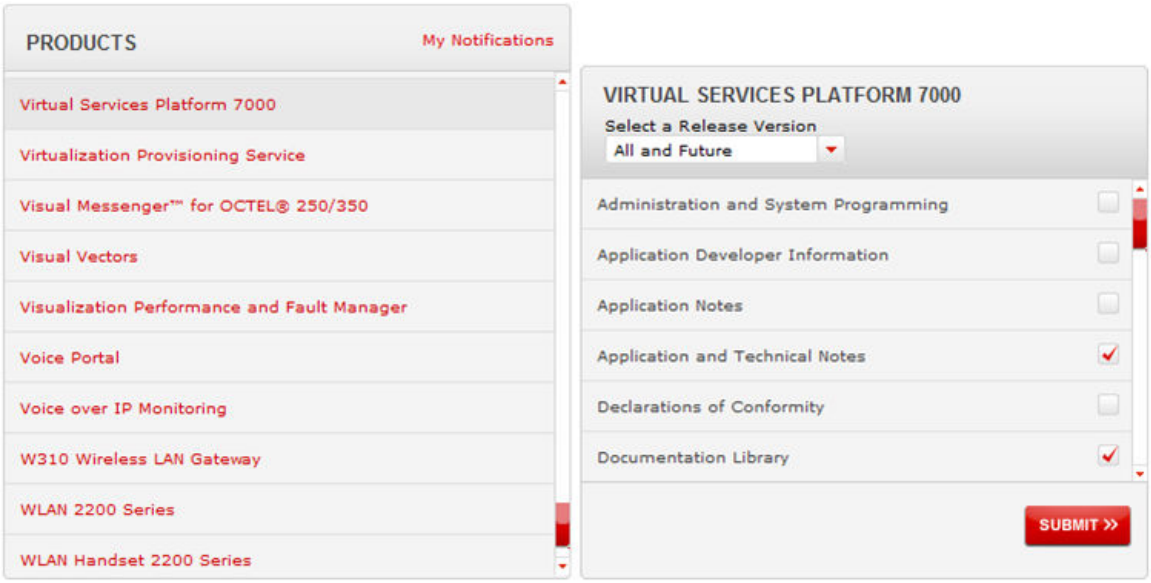
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.



8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.



11. Click **Submit**.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.

3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments
6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Support

Go to 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: New in this release

Configuring and Managing Avaya Identity Engines Single-Sign-On is a new document for Release 9.0. All content is new.

Chapter 3: Identity Engines Single-Sign-On fundamentals

Today's enterprises must deal with multiple user IDs and passwords, a situation that adds cost and complexity as well as potential security risks.

Identity Engines Single-Sign-On (SSO) mitigates this by allowing network administrators to centrally configure, assign, securely store, and change access credentials.

Users do not need to log in separately to individual resources. Instead, they get:

- Consistent, efficient, secure, and easy access to critical resources from any location
- One password to remember

Enterprises benefit from:

- Simplified administration
- Reduced support costs
- Improved enterprise security
- Greater user experience and productivity
- Ability to achieve regulatory compliance

Related Links

Identity Engines as a solution on page 13
Architecture on page 14
Architectural component overview on page 16
Benefits of IDE SSO on page 18

Identity Engines as a solution

The Identity Engines (IDE) portfolio is a powerful and flexible enterprise identity management system. Identity Engines:

- Is designed from the ground up to manage user access privileges across all of a company's networks and resources contained within a network (such as wired and wireless network access).

- Easily handles the most uncompromising and rigorous IT and business requirements for secure access.

With the Identity Engines Single-Sign-On (SSO) feature, in addition to controlling the network access for a user, IDE provides granular policy-based access control to the resources (applications) contained within an enterprise network

Identity Engines SSO provides standards-based SSO capabilities. It allows various Web applications to make informed authorization decisions for individual access to protected online resources in a privacy- preserving manner.

The Security Assertion Markup Language (SAML) 2.0 is used for the purpose of identity authentication. Proper use of this SAMLv2 ensures that implementations:

- Meet open standards
- Maximize interoperability
- Provide end users with a consistent context for credential use in Enterprises

Related Links

Identity Engines Single-Sign-On fundamentals on page 13
Applicability for IDE Release 9.0 on page 14

Applicability for IDE Release 9.0

IDE SSO support is limited to Avaya Aura® applications for IDE Release 9.0.

As of General Availability of IDE Release 9.0, Aura® Flare Experience 1.2 for iPad supports IDE SSO capabilities.

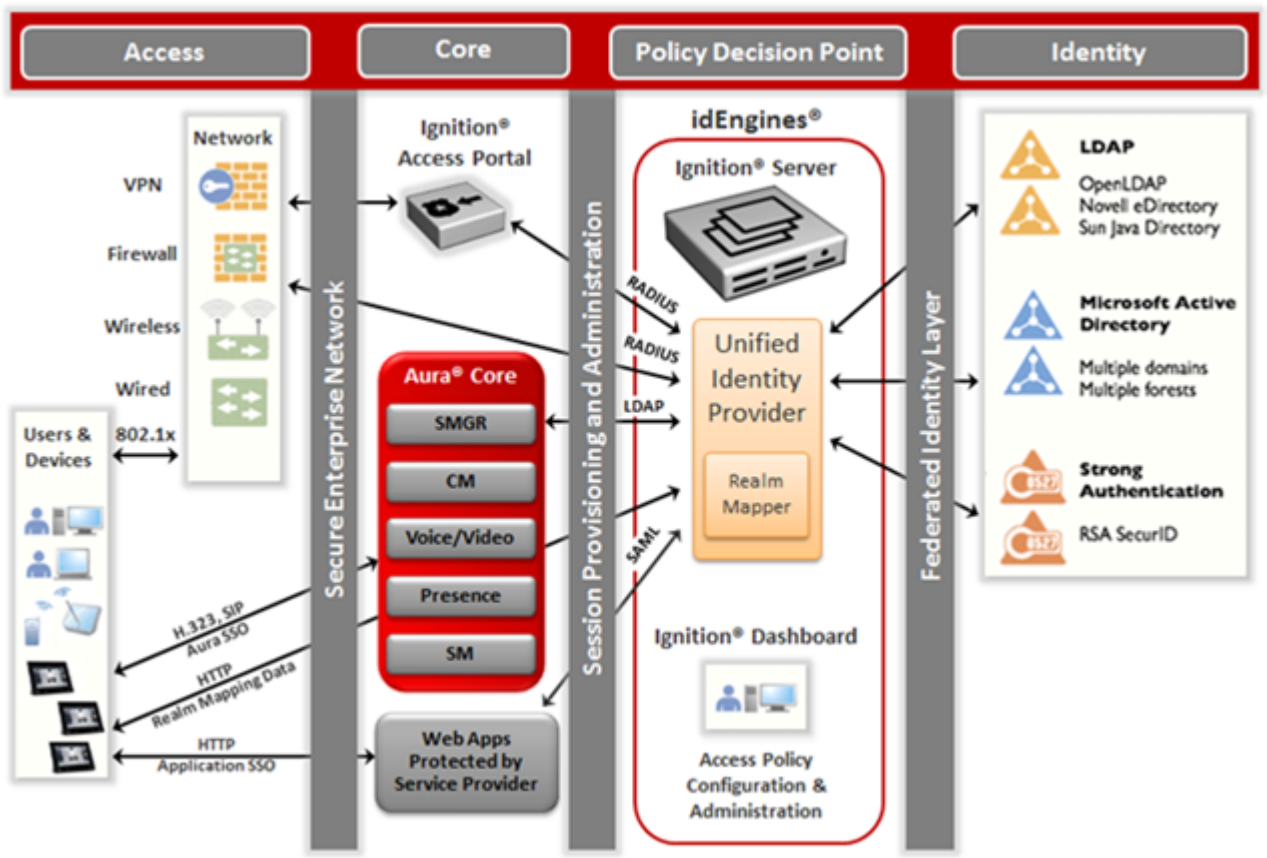
Related Links

Identity Engines as a solution on page 13

Architecture

With the Identity Engines (IDE) Single-Sign-On (SSO) architecture, the Ignition Server acts as a Unified Identity Provider and supports multiple interfaces to accept authentication requests. The Ignition Server runs different types of Services such as RADIUS, TACACS, SOAP, and SAML.

On the back end, it continues to utilize the existing directory virtualization to provide federation of Identity information. This model allows Ignition Server to play a role of Network Access Controller as well as Application Access Controller and provide enforcement of highly granular Access Policies.



The XACM-based Policy Engine has been extended to utilize the Web application specific policies.

With IDE's data store virtualization, identities are already integrated to create a clean global list of all users for the identification phase of authentication, while delegating the credential checking back to the authoritative sources.

The Unified Identity Provider allows enterprises to consolidate AAA functionality across network and application layer.

The Avaya Aura architecture for SSO consists of:

- IDE acting as an Identity Provider (IdP) that integrates with the enterprise Directory Services
- The Service Provider (SP) agent protecting the Aura services by validating the assertions from IdP
- The Realm Mapper, a Web-based service to map a user's enterprise credentials to their Aura identity

With this architecture, the end user is only asked for credentials once, through an interaction with the enterprise's SSO solution. After signing on, the user is able to access to all of the services needed for various applications to operate.

The IDE SSO architecture provides two SSO work flows to take into account different modes of client access:

1. Web-based SSO targeted for browser-based client access or thin clients
2. ECP-based SSO targeted for thick clients or intelligent clients

Web-based SSO

When a user tries to access application services using a browser, the SP agent on the application server intercepts the client request, checks for the required authentication token and, if not present, redirects the client to authenticate to the enterprise.

If the token is present, the SP agent validates the token with the IdP on Ignition Server, which returns a SAML assertion to the SP agent. The SP Agent parses the SAML assertion and asserts the user's identity and any authorization policy required for the service.

ECP-based SSO

When thick clients (such as Avaya SIP) that do not run in the context of a browser try to access the applications, they use the ECP-based architecture.

ECP is a SAML standard acronym that stands for "Enhanced Client or Proxy". The ECP profile is an adaptation of the SAML profile used for Browser SSO with the parts that were designed around the limitations of a browser removed.

The ECP-based Single-Sign-On provides Avaya SIP clients with the capability to directly contact a user's IdP without requiring a redirection by the SP, as in the case of a browser.

The Realm Mapping service, hosted on Identity Engines Ignition Server, is required to perform the translation from the Enterprise domain to the Aura® domain. The Realm Mapping service on Identity Engines Ignition Server is protected by its own internal SP agent.

- The SP agent on Ignition Server intercepts the request for Realm Mapping data from the client and responds to the client with a SAMLv2 Authentication Request.
- The client takes this Authentication Request to IdP, which then performs the user authentication and authorization.
- As a part of the response from IdP, the client receives a SAMLv2 Authentication Response package containing the assertion.
- The client then requests the Realm Mapper URL using the Assertion in the response package.
- SP then returns the Realm Mapping data, which is used to authenticate to Aura® services such as SM and CM.

Related Links

Identity Engines Single-Sign-On fundamentals on page 13

Architectural component overview

This section provides an overview of the Identity Engines (IDE) Single-Sign-On (SSO) architectural components.

Identity Provider

In perimeter authentication, a user needs to be authorized and authenticated only once (Single-Sign-On).

The Identity Assertion Provider (IdP) is an authentication module that authenticates the user within a security realm and then issues a security token, which can by used by the client to get access to protected resources within that security realm without having to authenticate again.

An IdP is hosted on the IDE Ignition Server as a licensable service. This IdP uses all of the IDE Ignition Server's capabilities to enforce XACML-based policies and integration with various directory services.

Service provider

Service provider (SP) is the entity that provides services to users or other system entities. In simpler terms, a service provider is a Web application or a Web site.

Realm mapper

Avaya Aura® services do not directly support Web SSO for Single-Sign-On because the security realms are not identical, yet all VoIP requests must be authenticated. Avaya Enterprise SSO for SIP allows a client to:

- First authenticate to the enterprise infrastructure using standard Web-based SSO techniques
- Then automatically be granted user authentication privileges in the associated SIP realm without the user being prompted for SIP credentials

It relies on a one-way one-for-one trust mapping from a single Enterprise user to a single SIP Identity. The responsibility of the realm mapping service is to map an Enterprise identity for a particular user to an Aura® identity.

Beginning in Release 9.0, the realm mapping service is hosted on the IDE Ignition Server.

Aura® services

Aura® services are the Voice and Multimedia services to which the endpoints connect, once authenticated using Enterprise ID. The end points discover the Aura®-specific credentials from Realm Mapper.

VPN controller

A VPN controller is a part of remote access when a user has to gain access to the Enterprise network using VPN before they can access Aura® services. There is no change in terms in how users connect to wired or wireless connections.

Network access switch (wired and wireless)

Network access switches are a part of network edge access when the user has to gain access to the Enterprise network before they can access Aura® services. There is no change in terms of how users connect to wired or wireless connections.

Avaya Aura® System Manager

The Ignition Server communicates with the Avaya Aura® System Manager to receive the realm mapping information. This communication happens over a secure LDAP interface. Ignition Server maintains a local cache of the realm mapping information available from each System Manager acting as a Directory service.

Related Links

Identity Engines Single-Sign-On fundamentals on page 13

Benefits of IDE SSO

Identity Engines Single-Sign-On offers several important advantages to the enterprise:

- Gain access from any location to maximize productivity.
- Eliminate lost or forgotten passwords; users have one password to remember.
- Lower user support costs by eliminating password-related support calls.
- Securely store and manage all passwords; no more searching for lost passwords.
- Improve network security by preventing unauthorized users from accessing enterprise applications.
- Facilitate regulatory compliance.

Related Links

Identity Engines Single-Sign-On fundamentals on page 13

Chapter 4: Configuring SSO

Related Links

Overview

This section guides you through a first-time configuration of the Avaya Identity Engines (IDE) Ignition Server to set up Avaya Aura Single-Sign-On (SSO).

The basic steps to configure SSO using the Ignition Server are:

- Making settings on the Ignition Server virtual appliance
- Installing the Ignition Aura SSO license
- Configuring SAML Service
- Creating a SAML Access Policy
- Setting up the Realm Mapper service
- Setting up your connection to a directory service
- Creating a Directory Set

- Setting up your connection to an Avaya Aura System Manager
- Creating Virtual Groups
- Creating User Virtual Attributes
- Configuring Authentication Policy details
- Configuring Identity Routing Policy details
- Configuring Authorization Policy details
- Configuring Outbound Attribute Policy details
- Configuring Service Providers (optional)

Note: When using this guide, ensure that you have a copy of *Avaya Identity Engines Ignition Server Getting Started*, NN47280–300 available. *Avaya Identity Engines Ignition Server Getting Started* covers basic Ignition Server configuration tasks. For advanced configuration topics, see *Avaya Identity Engines Ignition Server Administration*, NN47280–600.

Related Links

Configuring SSO on page 19

Before you begin

Ensure that you have completed the following tasks before you begin configuring the Ignition Server.

- Setting up the Ignition Server
- Configuring the Avaya Aura System Manager
- Ensuring that the client device has the correct version of the software installed

Related Links

Configuring SSO on page 19
Setting up the Ignition Server on page 20
Configuring the Avaya Aura System Manager on page 21
Ensuring the client device has the correct software version installed on page 22

Setting up the Ignition Server

Complete the following Ignition Server tasks using the steps shown in *Avaya Identity Engines Ignition Server Getting Started*, NN47280–300.

- Install the Ignition Server virtual appliance.
- On the Virtual Machine’s console, perform administrative network configuration to allow access from Dashboard.
- Install the Base license. The Base license can be LITE, SMALL, or LARGE.

- Install Ignition Dashboard on your Windows-based laptop or PC.

Note:

Identity Engines is a suite of applications. For Avaya Aura SSO, only the Ignition Server and the Ignition Dashboard are required. Other Identity Engines applications such as the Ignition Guest Manager and the Ignition Access Portal are optional and may be needed for use in conjunction with network access.

Related Links

Before you begin on page 20

Configuring the Avaya Aura System Manager

This section covers the configuration required on the Avaya Aura System Manager to allow interaction with the Identity Engines (IDE) Ignition Server. For complete installation and configuration of Avaya Aura System Manager, refer to the appropriate documentation.

You must configure the Avaya Aura System Manager to allow the IDE Ignition Server to read the realm mapping data. The IDE Ignition Server requires an Administrative User Account on Avaya Aura System Manager to read the realm mapping data. You can use the existing Administrative Account on Avaya Aura System Manager or you can create a new account through the User Management screen or the Administrators' screen on the Avaya Aura System Manager.

After you configure an IDE Ignition Server Administrative User Account on the Avaya Aura System Manager, the realm mapping service on the IDE Ignition Server can use the realm mapping data to map an Enterprise ID for a particular user to an Aura ID and provide the credentials over secure exchange.

About this task

Use the following procedure to create a new Administrative User Account on Avaya Aura System Manager.

Procedure

1. Open a web browser.
2. Point the web browser to the Avaya Aura System Manager fully qualified domain name (FQDN) or IP address.

   The Log On page displays.
3. Enter your **User ID**.

   The default is **admin**.
4. Enter your **Password**.
5. Click **Log On**

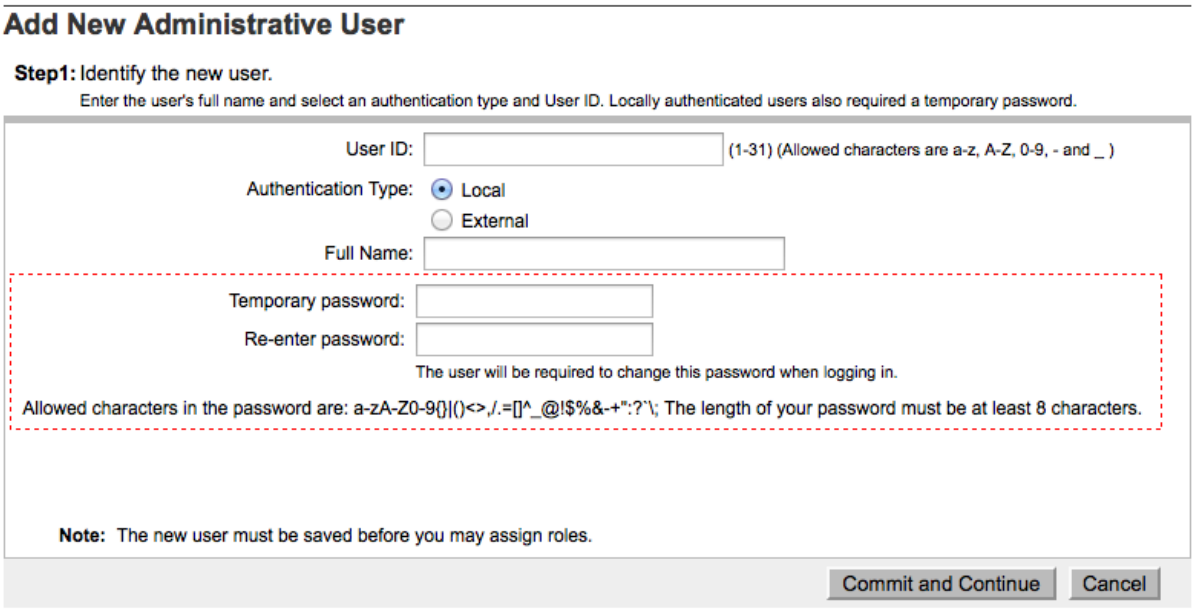
   The Home page appears and displays three columns: **Users**, **Elements**, and **Services**.

6. At the top of the **Users** column, click the **Administrators** link.

   The Administrative Users page displays.

7. Click **Add** to add a new Administrative User to be used by the IDE Ignition Server.

   The **Add New Administrative User** page displays.



8. On the **Add New Administrative User** page, perform the following actions:
   a. In the **User ID** field, enter the User ID for the Administrative User account.
   b. Select the **Authentication Type** that the user will undergo at runtime to obtain access to the system. The choices are: **Local** or **External**.
   c. In the **Password** field, enter a password for the Administrative User account.
   d. Click **Commit and Continue**.
9. From the **Roles** window, select **Network Administrator** and **System Administrator** and click **Commit**.

   This creates a new administrative user account that the IDE Ignition Server can use to sync realm mapper data.

Related Links

Before you begin on page 20

Ensuring the client device has the correct software version installed

About this task

Use the following procedure to ensure that the client device has the correct version of software installed.

Procedure

1. Launch Avaya Flare® Experience for iPad.
2. Click **Settings**.
3. Click **Support**.

   The release number should display as `Release 1.2.1` or higher.

Related Links

[Before you begin](#) on page 20

Making settings on the Ignition Server virtual appliance

You use Ignition Dashboard to make settings on the Ignition Server virtual appliance.

About this task

Use the following procedure to make settings on the Ignition Server virtual appliance.

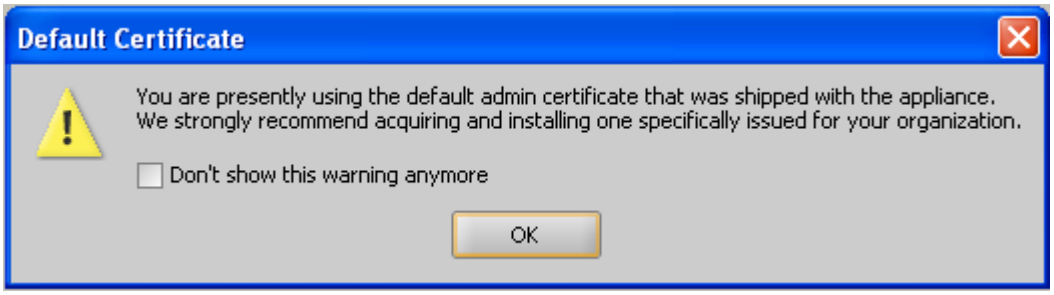
Procedure

1. Start Ignition Dashboard: Double-click Ignition Dashboard icon on your desktop, or, on the Windows task bar, select **Start** > **Programs** > **Ignition Dashboard** > **Ignition Dashboard**.

   The application displays its login window.

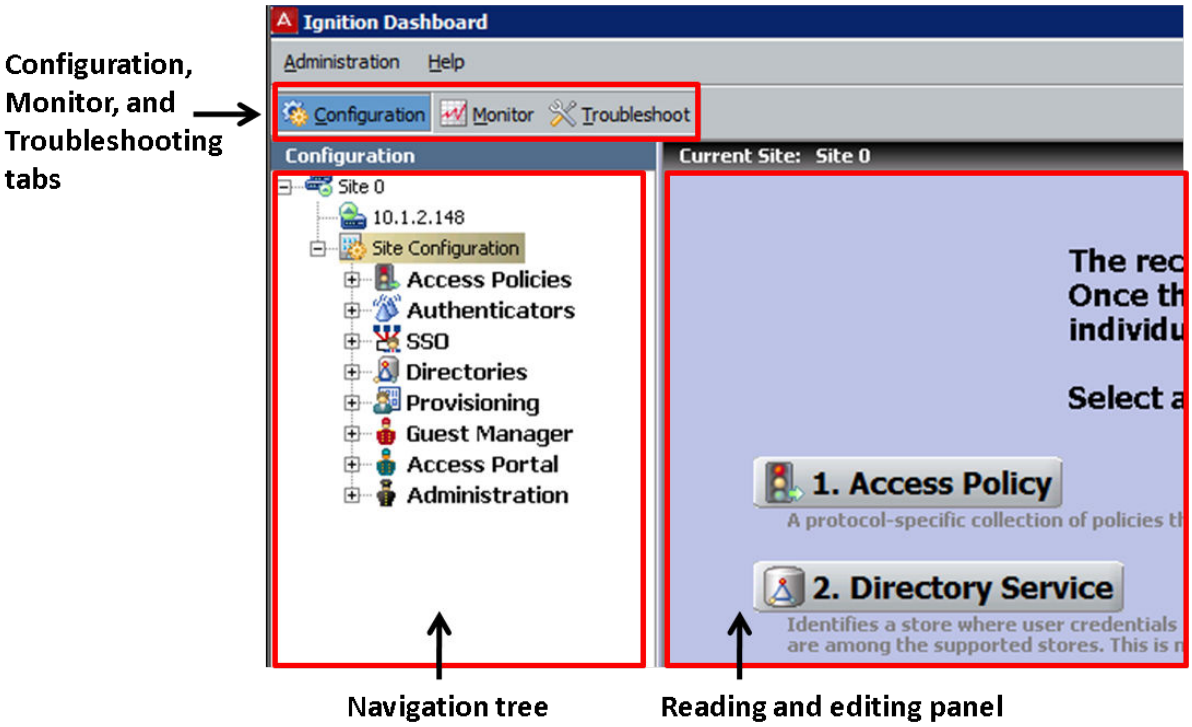
2. Type the Ignition administrator **User Name** and **Password**.

   The default login credentials are admin/admin. In the **Hostname** field, enter the hostname or IP address of your Ignition server's administrative network, and click **OK**.



   Initially, the **Default Certificate** window appears alerting you that you are using the default Ignition Dashboard-to-Ignition Server certificate ("admin certificate") that was shipped with Ignition Dashboard. Click **OK** to dismiss the window. (Avaya recommends that you later consult the "Certificates" chapter of the Avaya Identity Engines Ignition Server Administration Guide and replace the certificate as explained there.)

Dashboard displays its main window, which consists of three tabs, a navigation tree, and a reading and editing panel.



3. In the **Configuration** tree, click on *Site 0*, then right-click on *Site 0* and select the **Rename Site** command. In the **Rename Site** dialog, type a name for your site.
4. In the navigation tree, click on the machine name or IP address of the Ignition Server virtual appliance you want to configure.

   The application displays the **Nodes** panel, which allows you to manage network settings on the appliance, and check its current status.

   Hint: The **Actions** menu allows you to manage the appliance hardware (actions such as rebooting and shutting down). To use the **Actions** menu, right-click the IP address of your Ignition Server in the navigation tree, or, with the IP address selected, click the **Actions** menu at the upper right.

   Warning:

   Since your installation uses an Active Directory service, you must specify your DNS server address(es) before you connect Ignition Server to Active Directory.
5. Configure the DNS. DNS settings apply to each Ignition Server individually, even if the Ignition Server is part of an HA pair.

   Make your DNS settings as follows:

   a. In Dashboard's Configuration hierarchy tree, click the name or IP address of your node.

   b. In the **Node Configuration** panel, click the **System** tab and click the **DNS** tab.

c. In the **DNS** section of the **System** tab, click **Edit**.

d. In the **Primary IP Address** field, enter the unique IP address of your primary DNS Server using dotted decimal notation.

e. (Optional) In the **Secondary IP Address** field, enter the unique IP address of your secondary DNS Server using dotted decimal notation.

f. In the **Search Domain** field, enter the DNS search domains.

When entering more than one domain, separate the domain names with a space. When trying to resolve a host name, the Ignition Server searches these domains. Typically this is your organization's domain name, such as, for example, *Avaya.com*. Enter no more than six domains, and no more than 1024 characters in the **Search Domain** field.

g. Click **OK** to apply your changes.

Note:

If you will use an Active Directory (AD) data store, it is particularly important that you set the time correctly. If the time settings of the Ignition appliance and the AD server machine are more than five minutes out of sync, Ignition may not be able to log into AD.

6. Set the clock. Click on the **System** tab, click the **Date and Time** tab, and click **Edit**.

Make sure that the time and date set on the Ignition appliance are correct. If the current setting is incorrect, use the Edit Date and Time Configuration window to set the time in one of the following ways:

a. To set the time manually, click the **Manual Setting** radio button, click the clock and calendar icon, set the time in the dialog window that appears, and click **OK**.

b. To set the time to match the clock on your Dashboard management PC, click **Manual Setting** , click **Sync** , and click **OK**.

c. To set up automatic clock-setting using an NTP time server, click **NTP Server** , type the IP address of the NTP server in the **Primary IP Address** field (if you have a second NTP server, type its IP address in the **Secondary IP Address** field), and click **OK**.

7. (Optional) If you intend to separate your *authentication network* from your *management* network, perform the following actions.

Note:

For most installations, the following steps are not necessary. Only perform the following steps if your authentication network is separate from your management network.

a. Activate the Service Port ("SVC"): In the Dashboard **Configuration** tree, click the IP address or name of your site.

b. In the Nodes panel, click the **Ports** tab.

c. Click the **Service Port** row, and click **Edit**.

d. In the **Edit Port Configuration** window, select the **Enable Port** check box and in the **IP Address** field, assign an address to the port. In the adjacent field, enter the subnet mask.

e. Click **OK**.

Next steps

Installing the Ignition Aura® SSO license on page 26

Related Links

Configuring SSO on page 19

Installing the Ignition Aura® SSO license

Single-Sign-On (SSO) is a licensed feature of Identity Engines. You must install the Ignition Aura® SSO license (also known as the SAML license) to enable the Identity Engines (IDE) SSO feature support on the Ignition Server.

The Ignition Aura® SSO license requires, at a minimum, an Identity Engines Ignition Server Base license of any size (for example: Ignition Server Base LITE, SMALL or LARGE license). A single Identity Engines Aura® SSO license is required for either a standalone deployment of the Ignition Server or an High Availability (HA) deployment of a pair of Ignition Servers.

Before you begin

- Obtain the Ignition Aura® SSO license (also known as the SAML license).
- Ensure that your Ignition Server is running and accessible on the network.
- Run Dashboard.

About this task

Avaya Identity Engines currently supports the KeyCode Retrieval System (KRS)-based licensing model.

Beginning in Release 9.0, Identity Engines supports Avaya Product Licensing and Delivery System (PLDS) licensing model, in addition to the KRS. The Avaya PLDS provides customers, Business Partners, distributors and Avaya Associates with easy-to-use tools for managing asset entitlements and electronic delivery of software related licenses. Using PLDS, you can perform activities such as license activation, license de-activation, license re-host, and software downloads.

Important:

Note the following:

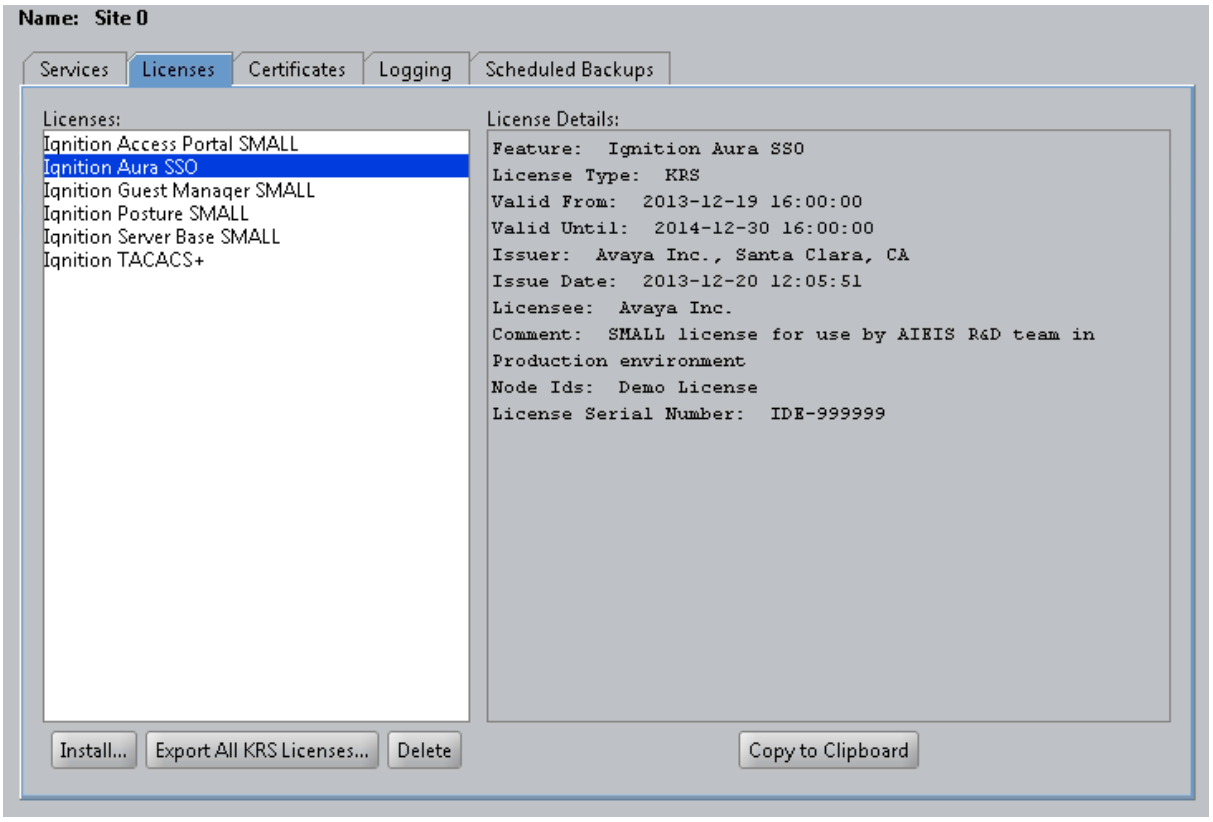
- An important difference between KRS licenses and PLDS licenses is that KRS licenses are individual licenses while a PLDS license file always includes all PLDS licenses within a single PLDS license file, which is in XML format.
- At the time of IDE Release 9.0, Ignition Server supports both KRS and PLDS licenses to accommodate customers who do not yet have access to Avaya PLDS. Over time, Identity Engines will transition to support a single licensing system, PLDS.

Use the following procedure to install the Ignition Aura® SSO license.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Click the **Licenses** tab.
3. Click **Install**.
4. Depending on your license type, perform one of the following actions:
   - For **KRS**: Browse to the Ignition Aura® SSO license and open it in your e-mail tool or text editor. Highlight and copy the entire contents of your license file. Return to the License Installation window of Dashboard and click **Paste** to paste the license text there.
   - For **PLDS**: Click **Browse**. Browse to and double-click the PLDS license file you downloaded from PLDS. The Ignition Server reads in the license file.
5. Click **OK**.

   The following figure shows a sample Ignition Aura® SSO PLDS license installed on the system.



   After you install the license, an SSO node appears under Site Configuration.

Next steps

After you install the Ignition Aura® SSO license, you can configure the various SAML parameters required to support SSO on the Ignition Server.

Related Links

Configuring SSO on page 19

Configuring SAML service

The Ignition Server SAML service handles user authentication requests from Avaya Aura Unified Communications (UC) soft clients. The first client supporting the Identity Engines (IDE) Single-Sign-On (SSO) Solution is Avaya Flare® Experience for iPad.

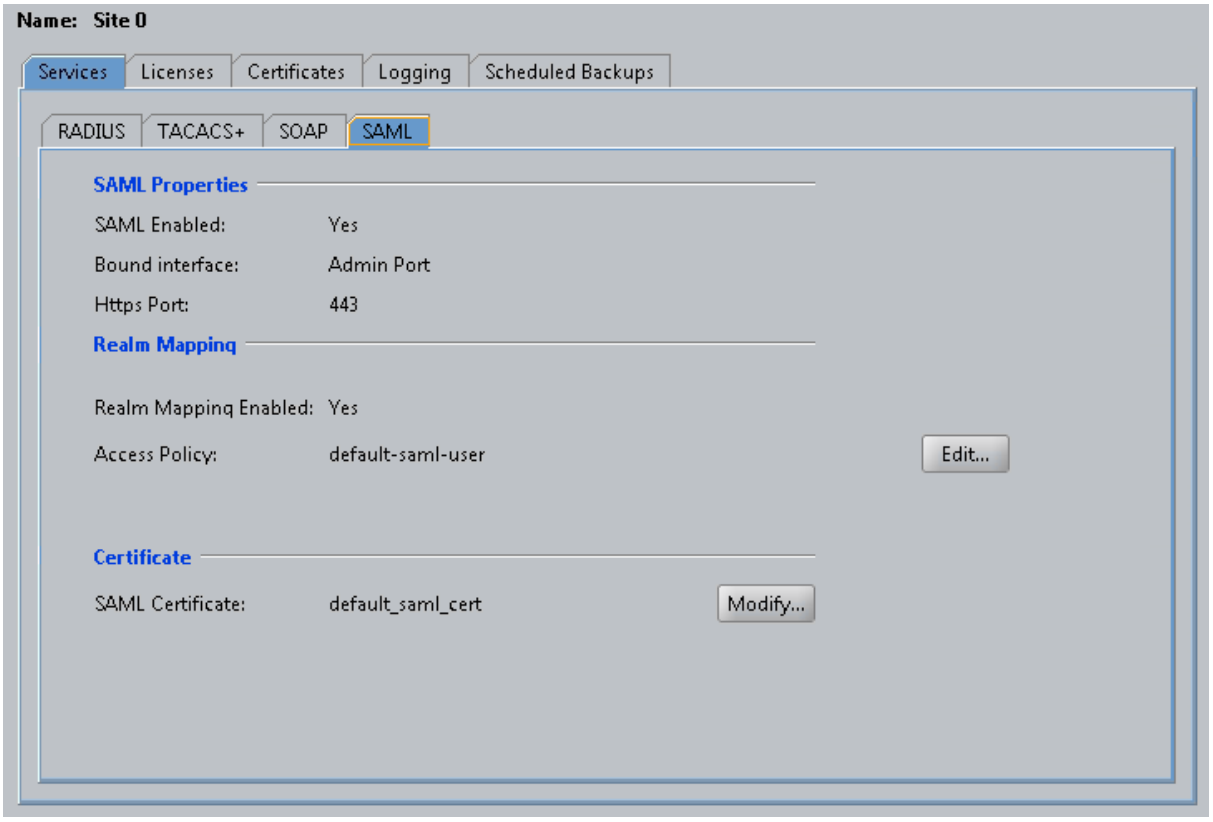
You can bind the Ignition Server SAML service to a physical Ethernet port on the Ignition Server (the Admin port). Use the SAML tab to enable SAML service, bind the SAML service, configure its port numbers, and select the certificate that the SAML service will use.

About this task

Use the following procedure to configure SAML service.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. In the Sites panel, click the **Services** tab and then click the **SAML** tab.



3. Click **Edit**.

The **Edit SAML Configuration** dialog box displays.

4. Edit as necessary.

   The following table describes the SAML service information.

Attribute	Description
SAML Enabled	Enables or disables SAML service. Ensure that this check box is selected.
Bound Interface	Specifies the Ignition Server Ethernet interface that handles the SAML authentication traffic. From the drop down list, choose the Ignition Server Ethernet interface that you want to handle the SAML authentication traffic. **Note:** You can bind SAML to any port on the Ignition Server. If you are running an HA pair of Ignition Servers, you can choose to bind SAML to a Virtual IP (VIP) interface. See “Managing Virtual Interfaces (VIPs)” in the *Avaya Identity Engines Ignition Server Administration* guide for information about using VIPs.
Https Port	Specifies the secure HTTP port number that should receive SAML authentication requests. The default SAML authentication port is 443. If you don’t want to use the default port, enter the secure HTTP port number to receive SAML authentication requests.
Realm Mapping Enabled	This specifies if the Realm Mapping Service is enabled. For now, leave it disabled.

5. Click **OK** to apply your changes.
6. Click **Modify** to select the certificate that the SAML service will use.

   The **Modify Certificate** dialog box displays.

7. You can upload your own certificate. For more information , see the “Managing certificates” section in the *Avaya Identity Engines Ignition Server Administration* guide.
8. Select the certificate that the SAML service will use.

   A default certificate (default-saml-cert) is used if you do not select a certificate.

9. Click **OK**.

Next steps

Creating a SAML Access Policy on page 30

Related Links

Configuring SSO on page 19

Creating a SAML Access Policy

Your SAML Access Policy contains the rules that determine how a user must authenticate and, based on the user's identity, which applications the user is allowed to use. Each Service Provider has one SAML Access Policy applied to it, meaning that all users trying to access an application protected through that Service Provider are governed by the same associated SAML Access Policy.

A default SAML Access Policy (default-saml-user) exists that you can edit to specify the authentication, identity routing, and authorization details.

Note:

You cannot delete the default-saml-user policy.

About this task

Use the following procedure to create a SAML Access Policy.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Access Policy**.
4. Expand **SAML**.
5. Perform one of the following actions:
   - If you want to edit the default SAML Access Policy, click **default-saml-user**, and click **Edit**.
   - If you want to create a new SAML Access Policy, click **New**.
6. In the **Access Policy Name** field, enter a name for your SAML Access Policy.

   The name typically offers a clue as to which Service Provider will use this policy. For example, the name may indicate the location of the application server.

   For now, we will create a SAML Access Policy to authorize the requests to the Realm Mapper service.

   Note:

   The Realm Mapper service is located on the Ignition Server.
7. Click **OK**.

   Your SAML Access Policy is saved. For now, we will leave the policy empty. Later, you can add rules to your SAML Access Policy, as shown in Configuring Authorization Policy details on page 57.

Next steps

Setting up the Realm Mapper service on page 31

Related Links

Configuring SSO on page 19

Setting up the Realm Mapper service

The Ignition Server Realm Mapper service handles the mapping of the Enterprise domain to the Avaya Aura domain, essentially tying together the user information in both the domains. Configuring the Realm Mapper service involves enabling the service and then associating your SAML Access Policy to this Realm Mapper Service. Your SAML Access Policy governs the rules to access the Realm Mapper service.

About this task

Use the following procedure to enable the Realm Mapper service on the Ignition Server.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. In the Sites panel, click the **Services** tab and then click the **SAML** tab.
3. Click **Edit**.

   The **Edit SAML Configuration** dialog box displays.
4. Edit as necessary.

   The following table describes the Realm Mapper service information.

Attribute	Description
Realm Mapping Enabled	Enables or disables realm mapping service. Ensure that this check box is selected.
Access Policy	Specifies the SAML Access Policy that will govern the rules to access. From the drop-down list, select the SAML Access Policy that will govern the rules to access the Realm Mapper service.

5. Click **OK** to apply your changes.

Next steps

Setting up your connection to a directory service on page 32

Related Links

Configuring SSO on page 19

Setting up your connection to a directory service

You can configure the Avaya Identity Engines Ignition Server to retrieve users from any combination of internal and external data stores, including external Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) stores, as well as the internal user store of the Ignition Server virtual appliance.

The set of connection settings for a data store is called a *directory service* in Ignition Server. This section shows you how to create a directory service. For each store you wish to use, you define one directory service. After you define your directory services, you place them in *Directory Sets* that tell the Ignition Server when to use which service.

Warning:

To configure Single-Sign-On for Avaya Aura services, you must configure at least one directory service to connect to an AD store. You also must configure another directory service to connect to an Avaya Aura System Manager data store, which is required for Realm Mapping.

This section explains how to configure a directory service to connect to an AD data store that contains your site's user accounts and groups. Once the Ignition Server has connected to an AD and joined the domain, it can authenticate users against the AD.

This section also explains how to configure a directory service to connect to an Avaya Aura System Manager data store, which is required for Realm Mapping. The Avaya Aura System Manager directory service is specifically used to map the Realm of two Domains: Enterprise Active Directory and Avaya Aura. This service must not be used to authenticate any user.

This section consists of the following related topics.

Related Links

Configuring SSO on page 19
Gathering Active Directory connection settings on page 32
Preparing to connect to your Active Directory on page 34
Connecting Ignition Server to your Active Directory on page 37
Troubleshooting AD and LDAP connections on page 40
Creating a Directory Set on page 45
Connecting Ignition Server to your Avaya Aura® System Manager on page 46

Gathering Active Directory connection settings

Use the AD connection settings that you used, or talk to your AD administrator to obtain the connection settings for your AD data store. Record them in the following table.

Setting name	Description
AD Domain Name	The **AD Domain Name** specifies the Active Directory domain that holds your user accounts. Domain names typically carry a domain suffix like ".COM" as in,for example, "COMPANY.COM".

Setting name	Description
Service Account Name	If you want to perform Kerberos-based Single Sign-On authentication, the service account must have permission to create and delete user accounts (the Create User object and Delete User Object permissions) in the Netlogon account root in Active Directory. See “Netlogon account root DN,” in this table. If you have not specified a Netlogon account root DN in Ignition Server, then the service account must have these permissions in the Users container of your AD service. Ignition Server uses the service account to join the Active Directory domain. Joining the domain requires creating a user account in the Netlogon account root and periodically resetting the password on that account for security. The user account itself is necessary to perform Kerberos-based SSO authentication. The service account must also have permission to create and delete computer accounts (the Create Computer Object and Delete Computer Object permission) for RADIUS authentication. See “Netlogon account root DN,” in this table. If you have not specified a Netlogon account root DN in Ignition Server, then the service account must have these permissions in the Computers container of your AD service. Ignition Server uses the service account to join the Active Directory domain. Joining the domain requires creating a machine account in the Netlogon account root and periodically resetting the password on that account for security. The machine account itself is necessary to perform Netlogon authentication requests for MSCHAPv2 traffic to Active Directory.
Service Account Password	The **Service Account Password** is the password for the AD service account. **Do not record the password here**.
Security Protocol: Simple or SSL	The Security Protocol setting specifies whether Ignition Server should SSL-encrypt traffic to the directory service. Avaya Identity Engines recommends that you use an SSL connection.
IP Address (Primary)	The **IP Address** of the primary AD data store.
Port (Primary)	The LDAP **Port** of the primary AD data store. For SSL enter 636. If SSL is not used, enter 389. You *cannot* use the global catalog port (3268).
Name	The **Name** is a name you use in Ignition Server to identify this AD data store. This can be any name.
NetBIOS Domain	The **NetBIOS Domain** name (pre-Windows 2000 domain name) of your AD data store. This setting is typically written in all uppercase letters, for example “COMPANY”. This setting applies only to *Active Directory* stores
NetBIOS Server Name	The **NETBIOS Server Name** is optional. It allows Ignition Server to find the NETBIOS server where Ignition Server will perform the Netlogon (a prerequisite to performing MSCHAPv2 authentication). If the **NETBIOS Server Name** is not specified, then Ignition Server relies on DNS to find the NETBIOS server. Avaya strongly recommends that you specify a **NETBIOS Server Name** to ensure that MSCHAPv2 authentication can continue when the DNS server is unavailable. The directory service set-up wizard will help you determine the NETBIOS server name by retrieving a list of domain controllers in the domain.

Setting name	Description
Directory Root DN	The **Directory Root DN** is the root of the AD tree containing your groups and schema, expressed using X.500 naming. For example, dc=company,dc=com. When you connect the directory service, the Ignition Server Create Service wizard attempts to choose a Directory Root DN for you.
User Root DN	The **User Root DN** specifies the AD container that holds your user records, expressed using X.500 naming. For example, cn=users,dc=company,dc=comorou=uswest,ou=americas,dc=company,dc=com. When you connect the directory service, the Ignition Server Create Service wizard attempts to choose a User Root DN for you.
Netlogon Account Root DN	The **Netlogon Account Root DN** is the container in AD where the Ignition Server creates its own user account and machine account when joining the AD domain. This setting is optional. If specified, Ignition Server only attempts to create its user account and machine account in the specified location. If left unspecified, Ignition Server obtains the Netlogon account root DN from the domain controller. Specifically, Ignition Server gets the DN of the well known computer root from the DC and uses that as the Netlogon account root DN.

Related Links

Setting up your connection to a directory service on page 32

Preparing to connect to your Active Directory

About this task

Check and, if needed, address the following before you try to connect to your Active Directory (AD).

Procedure

1. **Ensure that you have gathered your AD connection settings** as explained in Gathering Active Directory connection settings on page 32.
2. **Check your clock settings.** When the Ignition Server connects to an AD server, the Ignition Server clock must be in sync with the clock on the AD Server. If the clocks are out of sync, then the Ignition Server cannot connect to the AD store.
3. **Check your firewall settings.** If a firewall protects your AD server, ensure that it does not block the ports required by Ignition Server. Ignition Server needs access to the following ports: 88 (UDP), 389 (TCP), 445 (TCP), 464 (UDP), 636 (TCP).
4. **Find or create your service account.** Ensure that you have a user account in the AD that can act as the Ignition Server Service Account. See Creating your service account in AD on page 35.
5. **Set AD permissions on your service account.** If you want to perform Kerberos Ticket validation, ensure that your Ignition Server Service Account has, at a minimum, permission to create and delete **computer** and **user** accounts in the Netlogon account root of AD. See Setting AD permissions on your service account on page 36.

Next steps

Connecting Ignition Server to your Active Directory on page 37

Related Links

Setting up your connection to a directory service on page 32
Creating your service account in AD on page 35
Setting AD permissions on your service account on page 36

Creating your service account in AD

To connect to Active Directory, the Ignition Server virtual appliance requires a user account (which we call a *service account*) in Active Directory. If you want to perform SSO authentication, then this service account must have write and delete permissions in the Netlogon account root of your AD service. The location of the service account in AD does not matter.

If you have a suitable account already, you can skip this section and go to Setting AD permissions on your service account on page 36.

About this task

Use the following procedure to create your service account in AD.

Procedure

1. Log into your AD server machine as the Domain Administrator or as a user with sufficient privileges to create users.
2. Open the Active Directory Users and Computers snap-in from the Administrative Tools or the Windows Control Panel.
3. In the object tree on the left side, click on the container in which you will create the new user. For this example we'll use the **Users** container.
4. Select the **Action > New > User** command.
5. In the **New Object - User** window, create the Ignition Server service account.

   Avaya recommends creating an account that will be used exclusively by the Ignition Server virtual appliance. For this example, we use the account name, "ideadmin". Click **Next** after specifying the name.
6. Assign a secure password to the account.

   Follow your organization's password policies. If you wish to ensure the reliability of the service account, select the **User cannot change password** and **Password never expires** checkboxes.
7. Click **Finish** to save the new account.

Next steps

Setting AD permissions on your service account on page 36

Related Links

Preparing to connect to your Active Directory on page 34

Setting AD permissions on your service account

If you want to perform Kerberos Ticket validation, ensure that your Ignition Server Service Account has, at a minimum, permission to create and delete computer and user accounts in the Netlogon account root of AD.

About this task

Use the following procedure to configure AD permissions on your service account.

Procedure

1. Log into your AD server machine as the Domain Administrator.
2. Open the Active Directory Users and Computers snap-in from the Administrative Tools or the Windows Control Panel. Under **View**, enable **Advanced Features**.
3. In the object tree on the left side, click on the container that will serve as your Netlogon account root. You can configure the location Ignition Server will use as the Netlogon account root.

   Note:

   If you want to create a new container to serve as the Netlogon account root, click on the root domain in the tree and create the new *OU* there.
4. Right-click your *Netlogon account root container*, select the **Security** tab, and, under the **Permissions for Account Operators** list, click **Advanced** .
5. In the **Advanced Security Settings** window, click the **Permissions** tab and:
   a. Ensure that the **Allow inheritable permissions from the parent to propagate...** check box is selected.
   b. Click **Add**.
6. In the **Enter the object name** field, type the name or partial name of your Ignition Server service account and click **Check Names**.

   The window displays a list of names that match the name you typed.
7. Click the desired account name and click **OK**.
8. In the **Permission Entry** window, click the **Object** tab and:
   a. In the **Apply onto** field, choose **This object and all child objects**.
   b. In the **Permissions** table, scroll to find the rows **Create User Objects and Delete User Objects** and **Create Computer Objects and Delete Computer Objects**, and select the **Allow** check box for each.
   c. Click **OK**.

   Now that you have granted the Ignition Server service account the appropriate permissions, the Ignition Server can authenticate users against the AD service.
9. Click **OK** to dismiss the Advanced Security Settings window and again to close the snap-in.

Next steps

Connecting Ignition Server to your Active Directory on page 37

Related Links

Preparing to connect to your Active Directory on page 34

Connecting Ignition Server to your Active Directory

To connect Ignition Server to your Active Directory data store, you save the AD store as a *directory service* in Ignition Server. The directory service specifies the connection settings that Ignition Server uses to connect to the AD. You create one directory service for each AD domain you want to connect to, and you can search across multiple directory services by grouping them into a Directory Set. The following procedure assumes that your user data resides in the AD and that you have an AD user account that you can use as the Ignition Server service account. If you need to create a service account, see Creating your service account in AD on page 35.

About this task

Use the following procedure to connect Ignition Server to your Active Directory data store using Ignition Server's AD connection wizard in *automatic connection* mode.

Procedure

1. In the Dashboard **Configuration** tree, click **Site Configuration**.
2. In the main panel on the right, click **2. Directory Service**.
3. In the **Choose Service Type** window, click **Active Directory** and click **Next**.
4. In the **Configuration Options** window, click **Automatically configure** and click **Next**.

   The **Connect to Active Directory** window displays.
5. In the **Connect to Active Directory** window, perform the following actions:
   a. In the **AD Domain Name** field, enter the AD Domain Name.
   b. In the **Service Account Name** field, enter the AD service account name.
   c. In the **Service Account Password** field, enter the AD service account password.
   d. Click **Next**.
6. In the next window, perform the following actions:
   a. Select the **Security Protocol**. From the **Security Protocol** drop-down list, select **Simple** for unencrypted communication with AD, or select **SSL** for encrypted communication.
   b. In the **IP Address** field, type the address of your desired AD server.
   c. Check the **Port** setting and edit if necessary.

Note:

You *cannot* use the global catalog port (3268).

d. Click **Next**.

Ignition Server binds to the store, reads the schema, generates default settings, and displays the results in the **Configure Active Directory** window.

7. In the **Configure Active Directory** window, perform the following actions:

a. In the **Settings** section, type a **Name** for this directory service.

For this example, call it Enterprise-AD-1.

b. In the **Joined Domain As** section, the settings are already populated by the wizard. If you need to change a setting, click the lock/unlock button and edit the field.

c. The **Primary Server IP Address** and **Port** fields are populated by the wizard. If necessary, click to unlock and edit them.

d. (Optional) The **Secondary Server IP Address** and **Port** fields are optional. If you have a backup AD server, enter its address here.

e. The **DN Configuration** fields are populated by the wizard. If necessary, edit the fields.

The **Directory Root DN**, **User Root DN**, and **Netlogon Account Root DN** fields are explained in the Gathering Active Directory connection settings on page 32 section. You can type the DN in the fields or click the **Browse** button to browse your directory to find it.

Enabling the **Accept all users in the forest** check box allows Ignition Server to look up users in the global catalog of your AD.

Note:

The schema browser does not display auxiliary classes. You must type auxiliary classes in the appropriate fields.

f. The Ignition Server maintains an internal cache of the group hierarchies and attribute schemas of the directory services. If necessary, disable this caching by clearing the **Enable Group Caching** check box.

By default, Ignition Server looks for groups starting at the Directory Root DN. You can change this default behavior by specifying Group Search Base DNs. This is useful in case of huge AD deployments, where starting at the root DN can take up a substantial amount of time. In addition, you can restrict the types of groups that IDE caches by specifying a custom Group Search Filter. The filter follows the LDAP query syntax.

Enter the sync interval between Ignition Server and Active Directory, in hours, in **Resync Duration**.

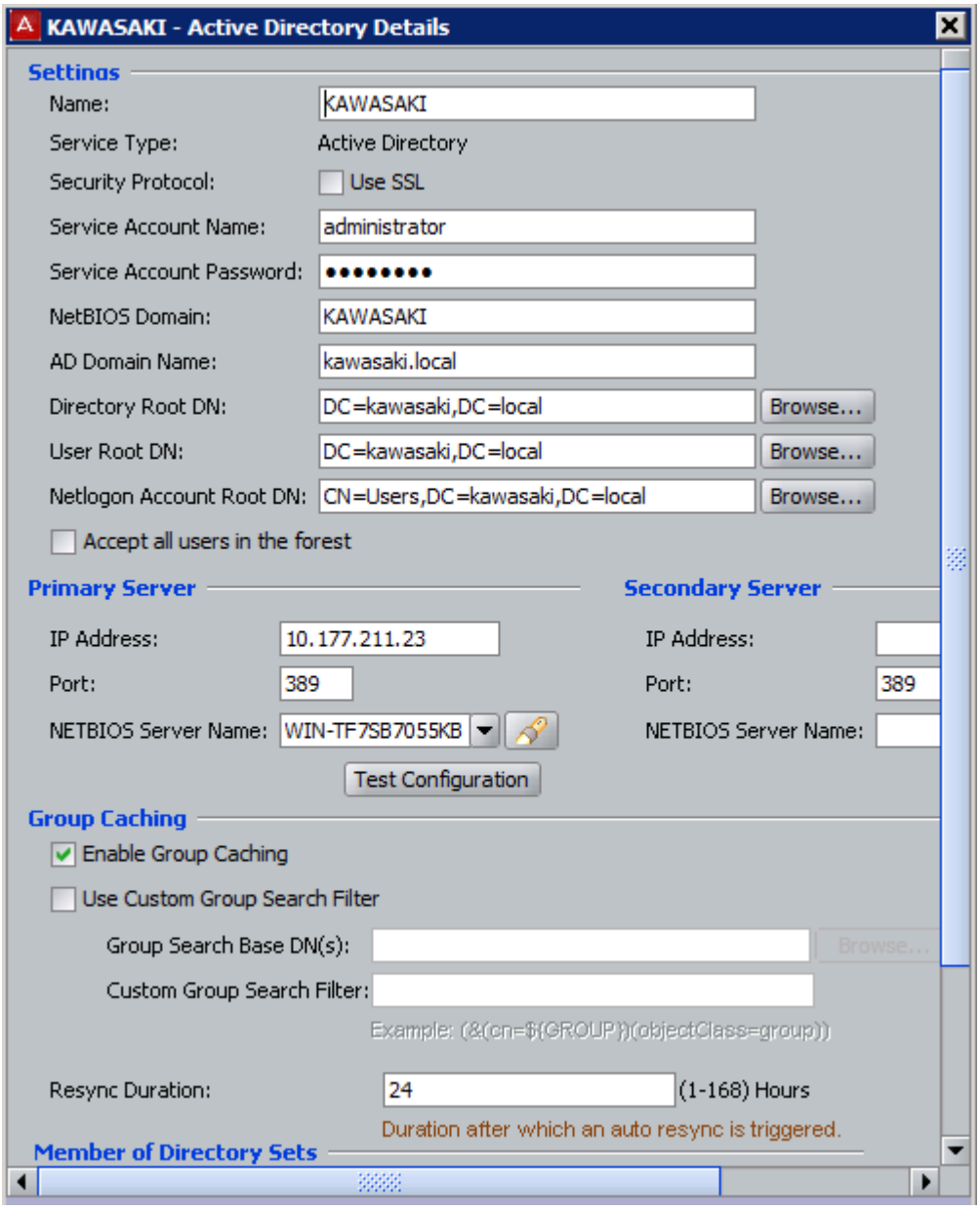
The range is 1 to 168 hours. The cache is automatically refreshed based on this setting.

g. Click **Next**.

The wizard applies your settings to create the directory service in Ignition Server and displays a confirmation page summarizing the connection settings of the service.

8. If the settings on the confirmation page are correct, click **Finish** to create the directory service.

   Your directory service is saved in Ignition Server.



Related Links

Setting up your connection to a directory service on page 32

Troubleshooting AD and LDAP connections

This section contains tips to troubleshoot AD and LDAP connections.

Related Links

Setting up your connection to a directory service on page 32
Checking a directory connection on page 40
Checking directory connections and cache status on page 40
Testing a directory in-depth on page 41
Looking up AD settings: Finding your Root DNs on page 42
Looking up AD settings: Finding Domain and NetBIOS names on page 43
Looking up AD settings: IP Address on page 44

Checking a directory connection

About this task

Use the following procedure to check that Ignition Server is connected to your directory service.

Procedure

1. In Dashboard's **Configuration** tab, in the navigation tree, click the plus sign (+) next to **Directories**.
2. Click the plus sign (+) next to **Directory Services**.
3. Click the name of your directory service.
4. Click **Test Configuration**.

   Ignition Server tests the connection to the primary server and, if configured, the secondary server. For each server, the connection test consists of an anonymous bind to the directory, retrieval of the directory's root DSE, a bind using the service account credentials, and a search for the user root.

   The **Test Connection Results** window displays the test outcome, displaying one success/failure line for the primary server and one line for the secondary server, if configured.

Related Links

Troubleshooting AD and LDAP connections on page 40

Checking directory connections and cache status

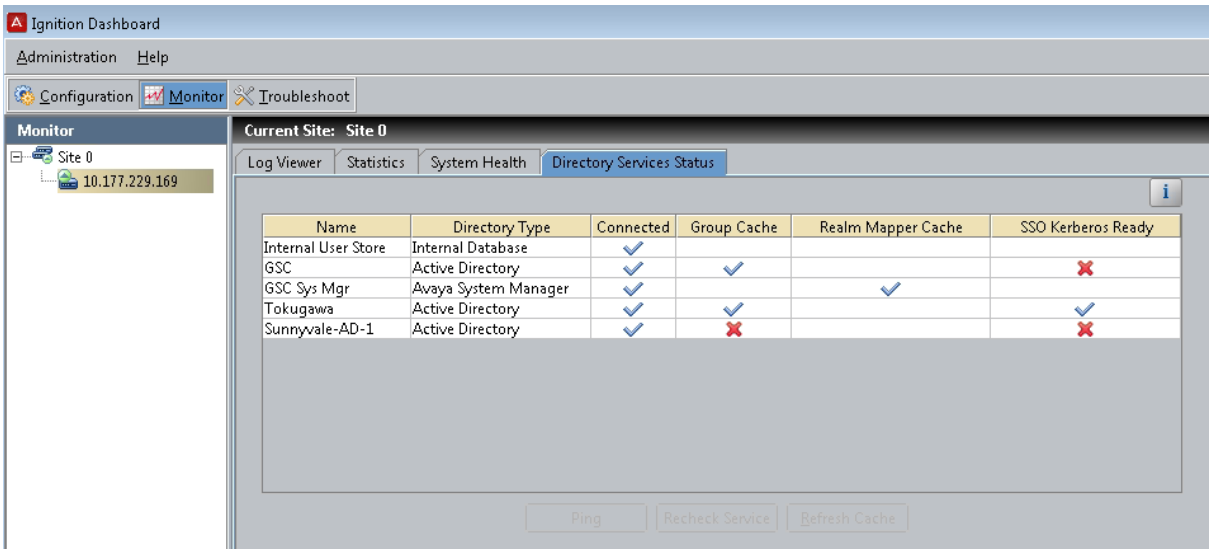
About this task

Use the following procedure to the connection status and cache status (Ignition Server caches user group memberships) of all of your directory services.

Procedure

1. Click on Dashboard's **Monitor** tab.

2. In the navigation tree, click the IP address of your node (your Ignition Server).
3. Click the **Directory Services Status** tab.



4. Click the name of your directory service.
5. Click **Recheck Service**.

   For each service, the Directory Services window displays a row indicating the connection status to that service. A blue check mark indicates Ignition Server succeeded in connecting to the server; a red **x** indicates it failed to connect.

   A blue check mark under **Group Cache** means group cache information was successfully retrieved. A red **x** means that group caching is disabled, it is still in progress, or there was an error in this operation.

   The **Realm Mapper Cache** column is only applicable for a Directory Service corresponding to a System Manager. A blue check mark in this column indicates the Realm Mapping data was successfully retrieved. A red **x** indicates that either caching is in progress or an error has occurred in this operation. Refer to Troubleshooting Flare for IPad specific issues on page 109 if the red **x** is due to an error condition.

   The **SSO Kerberos Ready** column is applicable only to Directory Services corresponding to an Active Directory. A blue check mark indicates Ignition Server succeeded in connecting to the server and created a user account and Kerberos authentication can be performed against that directory service. A red **x** indicates that the IDE failed to connect to AD or failed to create a user account. Refer to Kerberos authentication fails on page 99 for hints on fixing this issue.

Related Links

Troubleshooting AD and LDAP connections on page 40

Testing a directory in-depth

About this task

Use the following procedure to test a directory in-depth.

Procedure

1. In Dashboard's **Troubleshoot** tab, in the navigation tree, click the IP address of your Ignition Server.
2. Click the **Directory Service Debugger** tab.
3. Click the **Process Request**, **User Lookup**, **Device Lookup**, **Auth User** , or **Process Kerberos** tab to run your tests. For instructions, see "Advanced Troubleshooting for Directory Services and Sets" in *Avaya Identity Engines Ignition Server Administration*, NN47280–600.

   For instructions for the **Process Kerberos** tab, see Kerberos authentication fails on page 99.

Related Links

Troubleshooting AD and LDAP connections on page 40

Looking up AD settings: Finding your Root DNs

About this task

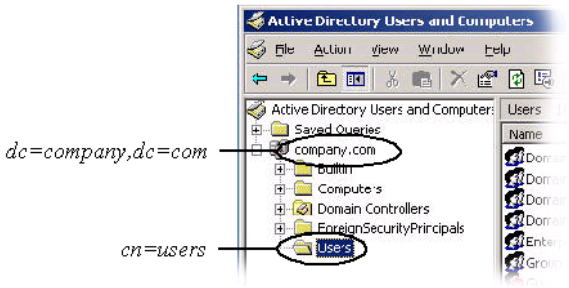
Use the following procedure to find your **User Root DN** and **Directory Root DN**.

Procedure

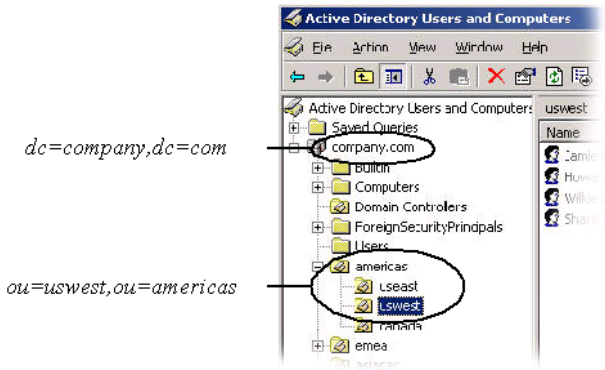
1. Enter the names of containers in your AD data store using X.500 naming.
   - **User Root DN** points to the AD container that stores your user records.
   - **Directory Root DN** points to the root of your AD tree and is used to obtain schema and group information.
2. To determine the X.500 names of your containers, open the **Active Directory Users and Computers** snap-in and check the tree panel on the left.

   At the root of the tree is the DNS name of your AD server. This provides the "dc=company,dc=com" portion of the name in the following example. For User Root DN, you must find the appropriate container ("CN") or organizational unit ("OU") and use its name as the "cn=" or "ou=" portion of the name. Note that an OU name can contain spaces, but that no space may directly follow a comma in the X.500 name.

***Example 1**: User Root DN is*
cn=users,dc=company,dc=com



***Example 2**: User Root DN is*
ou=uswest,ou=americas,dc=company,dc=com



Form the full User Root DN name by pre-pending the CN or OU portion of the name to the root portion of the name as shown in the preceding two examples. In the text that follows, we continue to use “cn=users,dc=company,dc=com” as our DN example.

Related Links

[Troubleshooting AD and LDAP connections](#) on page 40

Looking up AD settings: Finding Domain and NetBIOS names

About this task

Use the following procedure to find the **AD Domain Name** and **NetBIOS Name**.

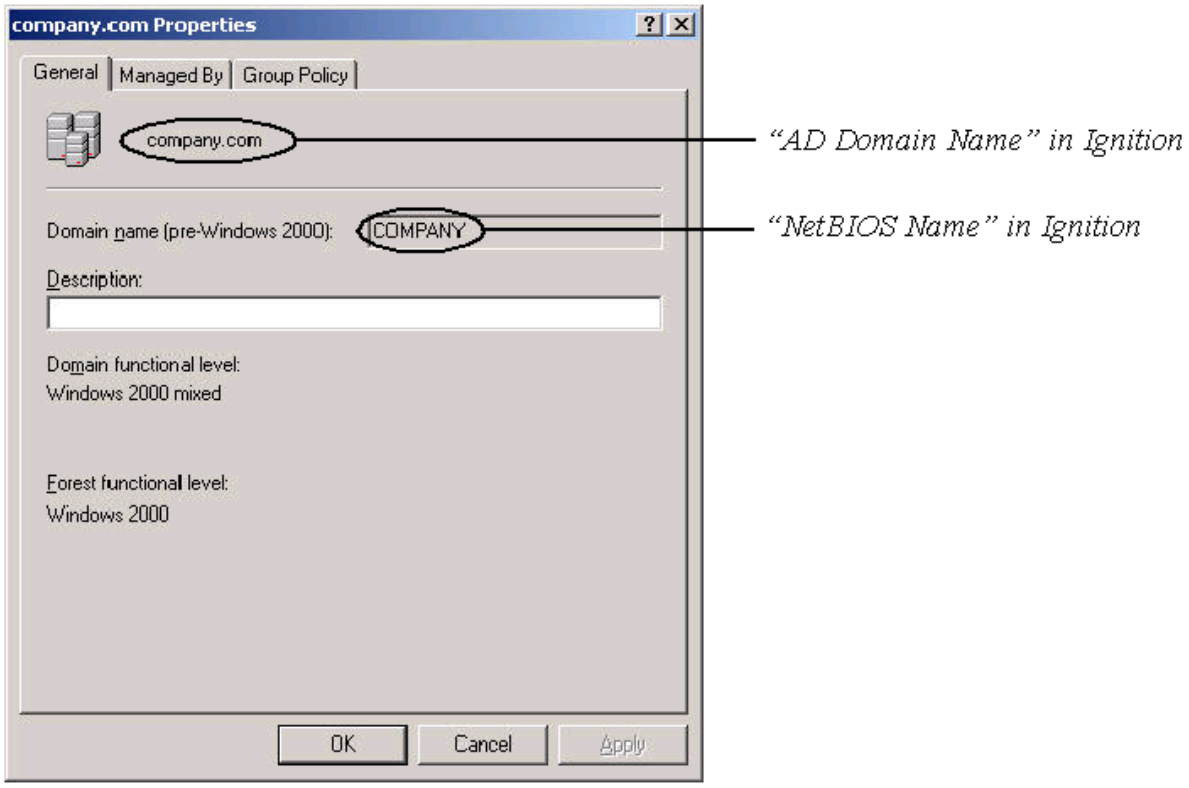
Procedure

1. Open the **Active Directory Users and Computers** snap-in and find your root domain in the tree panel on the left.

   In this example, the root domain is “company.com”.

2. Right-click the root domain name and select **Properties** to open the Properties window.

3. In the **General** tab of the **Properties** window, use the uppermost name as the “AD Domain Name” in Ignition Server, and use the Domain name (pre-Windows 2000) as the “NetBIOS Name” in Ignition Server.



Related Links

Troubleshooting AD and LDAP connections on page 40

Looking up AD settings: IP Address

About this task

Use the following procedure to find the IP address of your AD server.

Procedure

Log in to the machine that hosts your AD server and perform one of the following actions:

- Use the “ipconfig” tool from the command line.
- Open the Windows Control Panel and select **Network Connections > Local Area Connection**.

  In the Local Area Connection Status window, click **Properties**.

  In the Local Area Connection Properties window, click **TCP/IP** and then click **Properties**.

  Read the **IP address** from the TCP/IP Properties window.

Related Links

Troubleshooting AD and LDAP connections on page 40

Creating a Directory Set

A Directory Set is the mechanism Ignition Server uses to scan multiple directories for a user account. You define each user data store (that is, each AD data store, LDAP data store, and the embedded store) as a directory service in Ignition Server, and then you group those directory services into a Directory Set. To authenticate a user, Ignition Server searches all of the services in the set. For the purposes of this exercise, one Directory Set and one directory service will suffice.

About this task

Use the following procedure to create a Directory Set.

Procedure

1. In the Dashboard **Configuration** tree, click **Site Configuration**
2. In the main panel on the right, click **3. Directory Set**.
3. In the **Directory Set** window, type a **Name** for your Directory Set.

   The name should indicate that this set determines the search order for user lookups at your site or organization. We will use the name **Enterprise-Directory-Set**.
4. Click **Add** to start adding directory services to the set.
5. In the Directory Set Entry window, specify the directory that will provide user account data and group memberships (**User Lookup Service**) and the directory that will authenticate users (**Authentication Service**).

   Note:

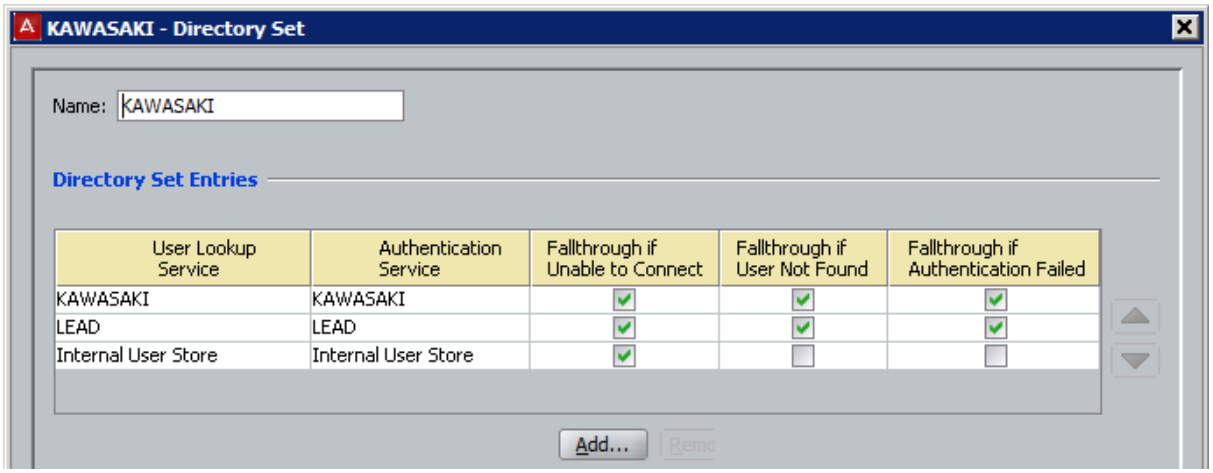
   Usually the directory that provides user account data and group memberships and the directory that authenticates users are the same directory. You can choose different directories in cases where you want to split your authentication from your user lookup, as you might when you couple RSA SecurID authentication with authorization based on AD group membership.

   a. From the **User Lookup Service** drop-down list, select *Enterprise-AD-1*.
   b. From the **Authentication Service** drop-down list, select *Enterprise-AD-1*.
   c. Click **OK**.
6. If you want to fallback to internal user store, perform the following actions:

   a. In the Directory Set window, click **Add**.
   b. From the **User Lookup Service** drop-down list, select **Internal User Store**.
   c. From the **Authentication Service** drop-down list, select **Internal User Store**.
   d. Click **OK**.
   e. In the **Directory Set** window, select the **Fallthrough** check boxes in the top row of the table to specify how you want Ignition Server to handle directory failover.

By checking these boxes, you can, for example, specify that Ignition Server will attempt authentication against internal user store if the user's lookup in the *Enterprise-AD-1* fails.

7. In the **Directory Set** window, click **Save** to save the set and close the window.



Next steps

Connecting Ignition Server to your Avaya Aura® System Manager on page 46

Related Links

Setting up your connection to a directory service on page 32

Connecting Ignition Server to your Avaya Aura® System Manager

To connect Ignition Server to your Avaya Aura® System Manager store, you save the store as a *directory service* in Ignition Server. The directory service specifies the connection settings that Ignition Server uses to connect to Avaya Aura® System Manager. You create one directory service for each Avaya Aura® System Manager server you want to connect to.

Warning:

To configure Single-Sign-On for Avaya Aura® Services, you must set up a directory service to connect to an Avaya Aura® System Manager data store, which is required for Realm Mapping. The Avaya Aura® System Manager directory service is specifically used to map the Realm of two Domains: Enterprise Active Directory and Avaya Aura®. This service must not be used to authenticate any user.

About this task

Use the following procedure to connect Ignition Server to your Avaya Aura® System Manager store.

Procedure

1. In the Dashboard **Configuration** tree, click **Site Configuration**.
2. In the main panel on the right, click **2. Directory Service**.

3. In the **Choose Service Type** window, click your type of Avaya Aura® System Manager store and click **Next**.
4. In the **Configuration Options** window, click **Automatically configure** and click **Next**.

   The **Connect to Directory Server** window displays.
5. In the **Connect to Directory Server** window, perform the following actions:
   a. In the **Service Account DN** field, enter the DN of the administrator account on Avaya Aura System Manager.

      Ignition Server will connect as this administrator. For example, uid=admin, ou=administrators, ou=smgr.
   b. In the **Service Account Password** field, enter the password of the administrator.
   c. The **Use SSL** check box is selected by default. Ignition Server uses SSL to encrypt traffic to the directory service. You cannot edit the **Use SSL** field.
   d. In the **IP Address** field, enter the IP address of the primary Avaya Aura® System Manager server.
   e. The **Port** field is populated by default. The default port number where the service can be reached when using SSL is 10636. You cannot edit the **Port** field.
   f. Click **Next**.

      The **Configure Directory Server** window displays.
6. In the **Settings** section, type a **Name** for this directory service. For this example, call it Sunnyvale-SystemManager.
7. In the **Settings** section, in the **Resync Duration** field, enter the sync interval between Ignition Server and System Manager in hours.

   The Ignition Server maintains an internal cache of the group hierarchies and attribute schemas of the directory services. The cache is automatically refreshed based on this setting.

   For System Manager, only the updated information on System Manager is retrieved by IDE every sync interval, which is different from other directories for which all the information is retrieved.
8. In the **Settings** section, the **DN** and **Username** fields are populated by the wizard. Edit them if necessary, or click **Browse** to set them. The fields are:
   - **Directory Root DN**: The DN where the schema containing your Aura users can be found. You must select **ou=smgr**. When you connect the directory service, the Ignition Server Create Service wizard attempts to choose a Directory Root DN for you.
   - **User Root DN**: The DN of the Ignition Server container that holds the user records. You must select **ou=people,ou=smgr**. When you connect the directory service, the Ignition Server Create Service wizard attempts to choose a User Root DN for you.
   - **Username Attribute**: An LDAP attribute that stores the user name. Typically, this is uid.

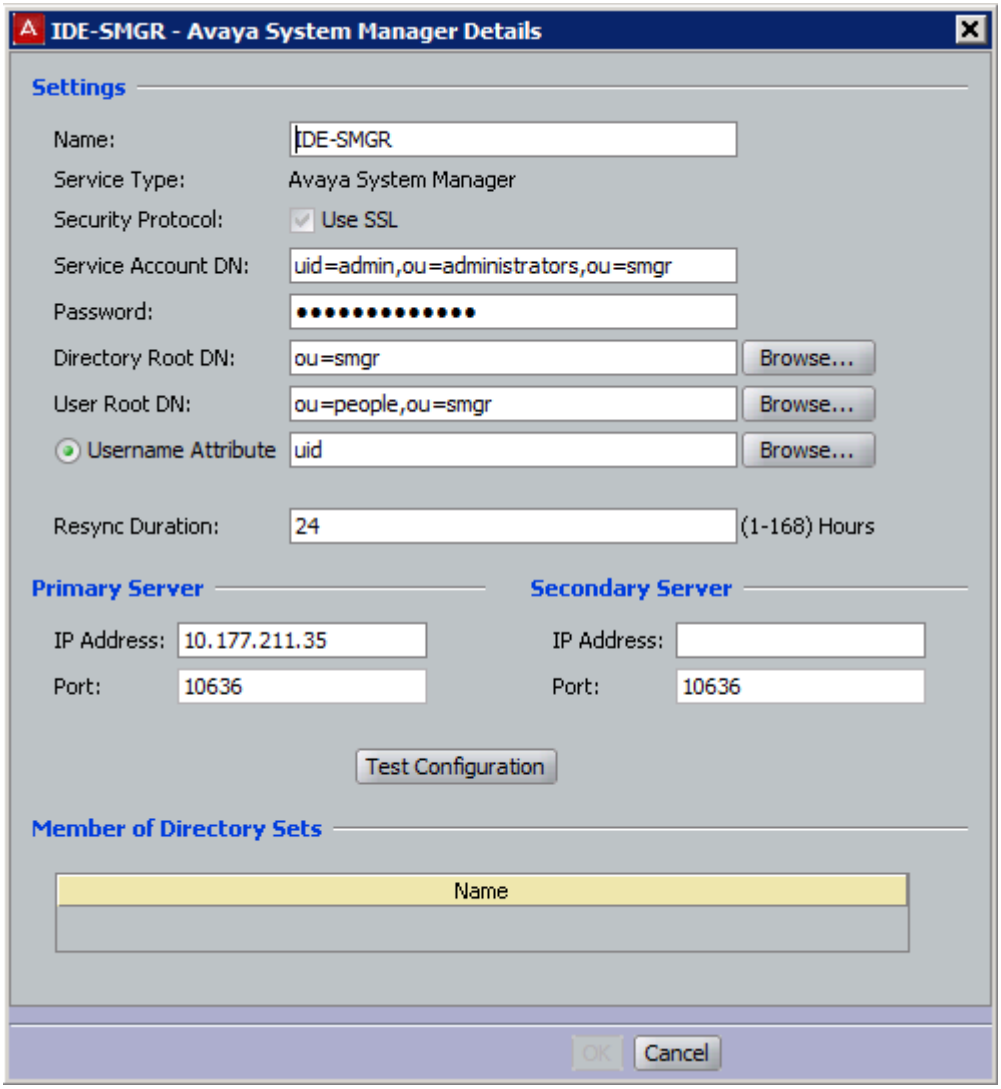
Note:

The schema browser does not display auxiliary classes. You must type auxiliary classes in the appropriate fields.

9. In the **Primary Server** section, the **IP Address** and **Port** fields are populated by the wizard. If necessary, click the padlock button to unlock and then click in the fields to edit them.
10. In the **Secondary Server** section, the **IP Address** and **Port** fields are populated by the wizard. If necessary, click the padlock button to unlock and then click in the fields to edit them.
11. Click **Next**.

    The wizard applies your settings to create the directory service in Ignition Server and displays a confirmation page summarizing the connection settings.
12. If the settings on the confirmation page are correct, click **Finish** to create the directory service.

    Your Avaya Aura® System Manager directory service is saved in Ignition Server.



Related Links

Setting up your connection to a directory service on page 32

Creating Virtual Groups

Virtual Groups are Ignition Server's mechanism for abstracting, or standardizing, group names across multiple user databases. You can map an Ignition Server Virtual Group to many groups in many databases, allowing you to treat these groups as a single group in your policies.

For example, you might create an Ignition Server Virtual Group called, "*Administrators*" and map it to the DN, "*ou=admin,ou=Users,dc=company,dc=com*" in the user database of your Fresno office, and also map it to the nsRole value "*AdminGroup*" in the user database in your Irvine office. Your Access Policies would refer to the group by the single name, "*Administrators*".

Virtual Groups are required if you wish to evaluate group membership in your policies. Ignition Server looks up group membership only by means of a Virtual Group, so even if you have only one data store, you must create a Virtual Group.

In this example, we create a Virtual Group that maps to the Domain Users group in the AD store.

About this task

Use the following procedure to create a Virtual Group.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Directories**.
4. Expand **Virtual Mapping**.
5. Click **Virtual Groups**.
6. In the **Virtual Groups** panel, click **Actions** and select the command, **Add New Virtual Group**.
7. In the **Add a New Virtual Group** window, type the Virtual Group name and click **OK**.

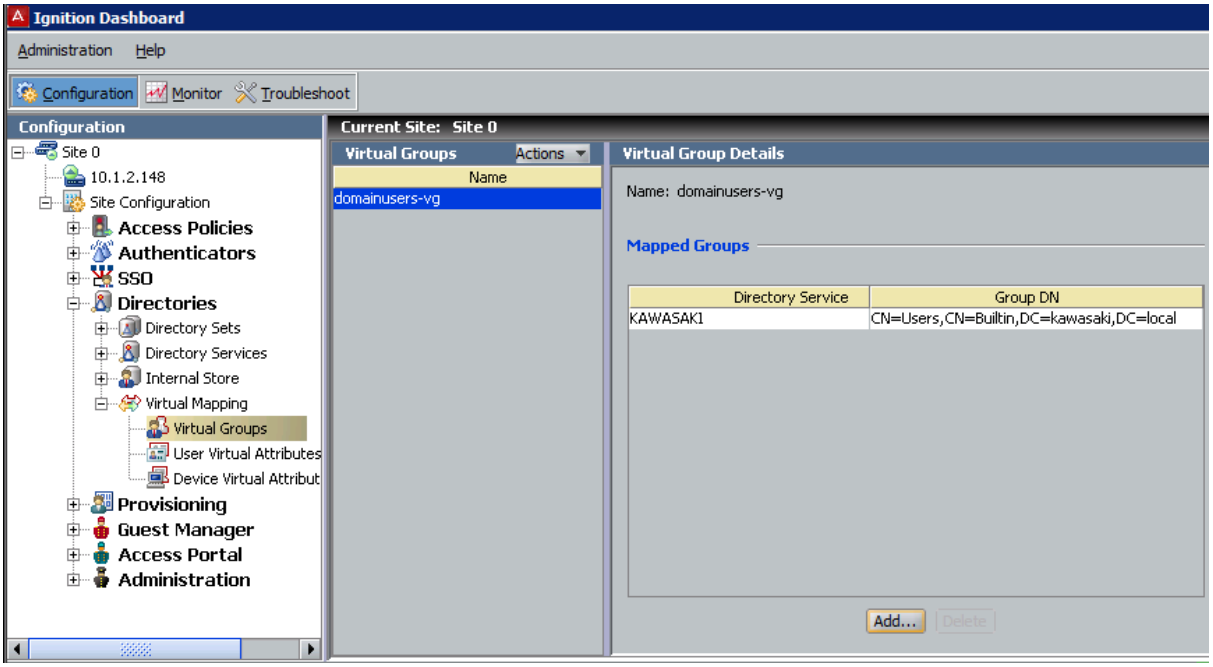
   In this example, we give the Virtual Group the name domainusers-vg. This group will contain the members of the “Domain Users” group of the AD server.
8. In the **Virtual Groups** list, select the group name you just created. At the bottom of the Virtual Group Details panel, click **Add**.
9. In the **Map Groups** window, click in the **Directory Service** drop-down list and select the name of your Directory Service.
10. Use the tree list to find the group (AD container) that you want to map.

    In this example, we will use the Active Directory group, “CN=Domain Users”. This allows us to create an Ignition Server authorization rule that grants access to any user who is a member of *Domain Users*.

    Note:

    If you are using the Embedded Store instead, you can create an embedded group and map your Virtual Group to that instead.
11. Click **OK** to close the Map Groups window.

    The new mapping appears in the Mapped Groups list.



Next steps

Setting up User Virtual Attributes on page 51

Related Links

Configuring SSO on page 19

Setting up User Virtual Attributes

User Virtual Attributes are the Ignition Server mechanism for abstracting, or standardizing, attribute names across multiple directory services. You must define a User Virtual Attribute for each directory service field whose value you want to use in:

- authorization rules or
- Outbound Values for sending return attributes to Service Providers

Group and attribute naming is often inconsistent across the various directories (directory services) that store users in an organization. For example, your local LDAP store may keep employee id numbers in the attribute, `employeeId`, while the LDAP store of your Atlanta office stores them in `employeeNumber`.

Ignition Server's User Virtual Attributes allow you to write authorization and policies that span users stored in disparate data stores, and handle them consistently, even if attributes are named inconsistently. To address the `employeeId` / `employeeNumber` problem shown above, you would use a User Virtual Attribute, "*Employee-ID*" and map it to `employeeId` in your local store and to `employeeNumber` in the Atlanta store.

The initial list of User Virtual Attributes includes mappings to the user fields in the internal data store only. You can add to these mappings.

Related Links

Configuring SSO on page 19
Viewing the existing list of User Virtual Attributes on page 52
Adding a new User Virtual Attribute on page 52

Viewing the existing list of User Virtual Attributes

About this task

Use the following procedure to view the existing list of User Virtual Attributes.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Directories**.
4. Expand **Virtual Mapping**.
5. Click **User Virtual Attributes**.

   The User Virtual Attributes panel displays.
6. In the **Attributes** list on the left, scroll to find the desired attribute and click the attribute name.

   The **User Virtual Attribute Details** pane displays the following information:

   - **Name**: The name of the attribute. This name is used in your authorization rules and Outbound Attribute mapping rules.
   - **Data Type**: The data type of the attribute. When you create the attribute, you set its data type to a type that is compatible with the directory fields you plan to map to it.
   - **Mapped Attributes** table: In this table, each row represents one mapping of this User Virtual Attribute to a field in a data store. The **Directory Service** column shows the name of the data store, and the **Attribute DN** column shows the mapped field in the data store.
7. To sort the **Directory Service** and **Attribute DN** lists in ascending or descending order, click the title bar of the column.

Related Links

Setting up User Virtual Attributes on page 51

Adding a new User Virtual Attribute

Use the following procedure to add a new User Virtual Attribute, for example, **email**.

Note: It is not necessary to create a virtual attribute, since all the virtual attributes needed for Avaya Aura® SSO are already created for you. This task shows you how to create a new virtual attribute, if needed.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Directories**.
4. Expand **Virtual Mapping**.
5. Click **User Virtual Attributes**.
6. At the top of the Attributes column, click **Actions > Add A New Virtual Attribute**. Ignition Server displays a dialog box requiring a name for the new User Virtual Attribute and its data type.
7. In the dialog box, enter the unique name **email** for the new User Virtual Attribute.
8. From the drop-down list, select the data type for the new User Virtual Attribute.

   For **email**, we will use: **String**: LDAP-standard format

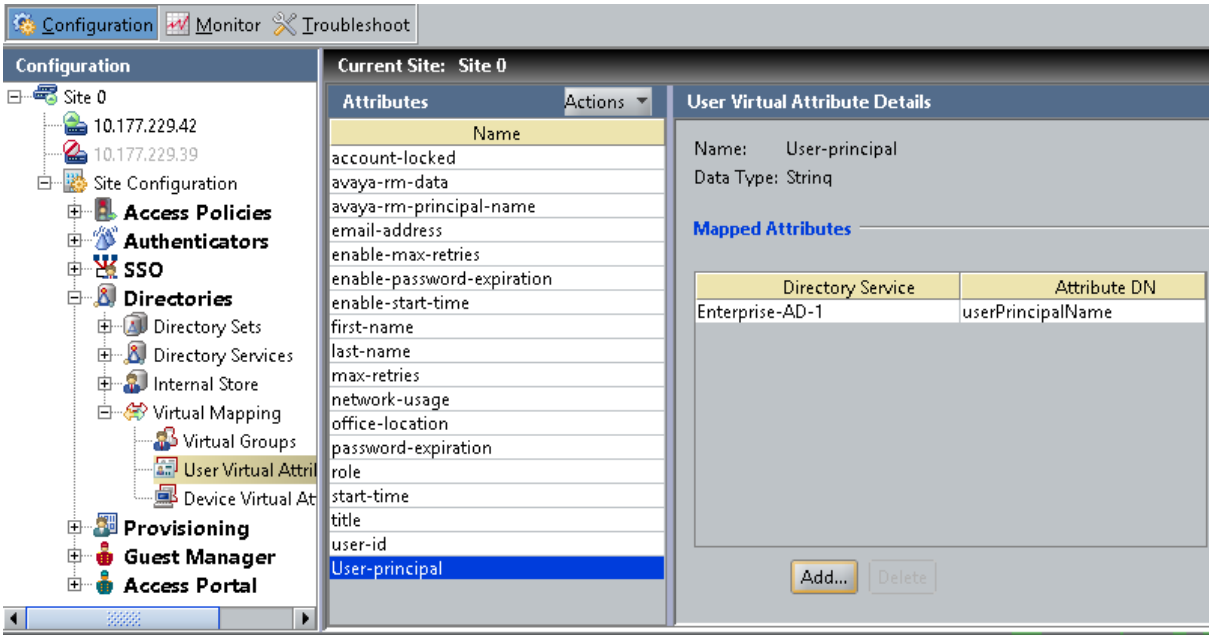
   Warning:

   After you create the attribute you cannot change its data type. You must delete the Virtual Attribute and then recreate it.
9. Click **OK**.

   Ignition Server displays the new User Virtual Attribute in the list.
10. To map attributes (Distinguished Names) from a directory service object to a User Virtual Attribute, perform the following actions:
    a. From the **Attributes** list in the **Attributes** column, click **email**.
    b. In the **User Virtual Attributes Details** panel, click **Add**.

       The **Map Attributes** window displays.
    c. From the drop-down list, select the Active Directory service **Enterprise-AD-1**.
    d. Select **Available attribute name** to pick the directory attribute from a list.

       Ignition Server displays the available attributes (distinguished names).
    e. Click **email**.
    f. Click **OK** to close the Map Attributes window.



Related Links

Setting up User Virtual Attributes on page 51

Configuring Authentication Policy details

An Authentication Policy determines how Ignition Server verifies the identity of a user. Each Access Policy has an Authentication Policy. Enforcement of the Authentication Policy is the first step in Ignition Server's handling of a user.

Ignition Server separates the Authentication Policy definition into two components: the **Authentication Protocol Policy** and the **Identity Routing Policy**.

The **Authentication Protocol Policy** contains the *Authentication Profile* and the *Login Handler*. The *Authentication Profile* specifies which type of SAML Profile to use when communicating SAML messages. There are two types of SAML Profiles that Ignition Server supports:

- Web based Single-Sign-On (WebSSO)
- Enhanced Client Proxy (ECP)

The *Login Handler Policy* specifies which method to use to accept user's credentials. There are two types of Login Handlers that Ignition Server supports:

- Form-Based
- Kerberos-Basic

The **Identity Routing Policy** specifies where Ignition Server can find user records and how it should handle user lookup failures.

To support Single-Sign-On for Aura clients using Realm Mapper Service on Ignition Server, we will select ECP as the Authentication Profile and Kerberos-Basic as the Login Handler.

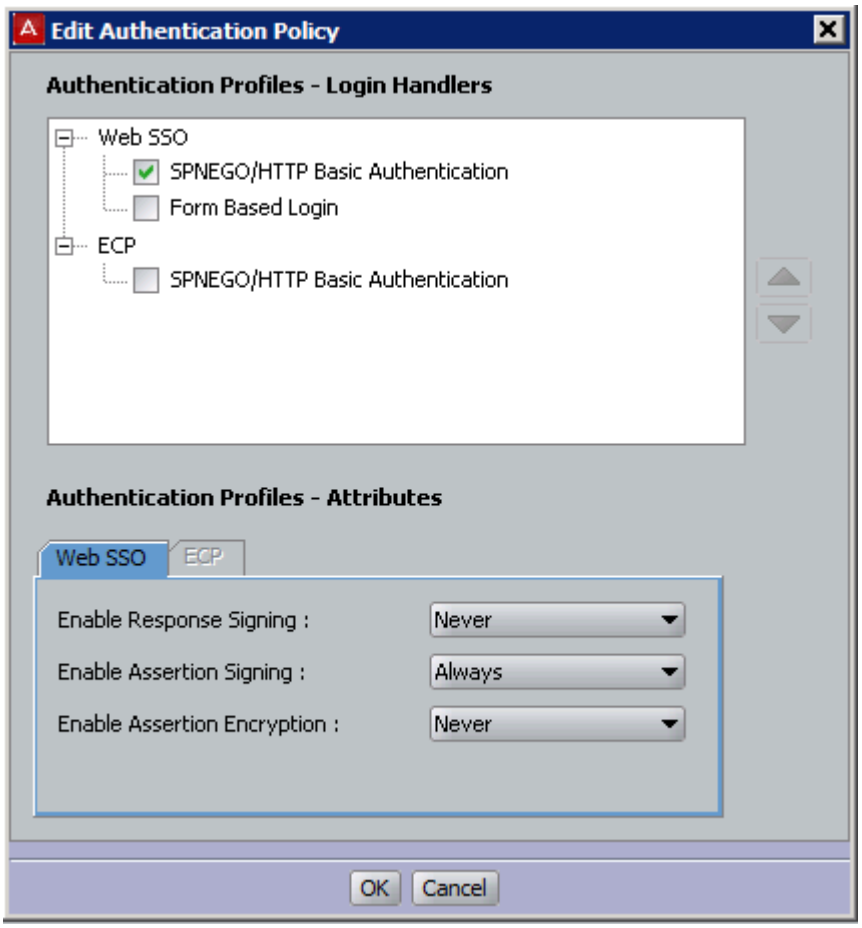
About this task

Use the following procedure to configure an Authentication Policy for Realm Mapper.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Access Policies**.
4. Expand **SAML**.
5. Click the name of your Access Policy.
6. Click the **Authentication Policy** tab.
7. Click **Edit**.

   The **Edit Authentication Policy** dialog box displays.



8. In the **Edit Authentication Policy** window, the **Authentication Profile – Login Handlers** section allows you to establish the set of Authentication Profiles and Login Handlers that your SAML Access Policy supports.

Next steps

Configuring Identity Routing Policy details on page 56

Related Links

Configuring SSO on page 19

Configuring Identity Routing Policy details

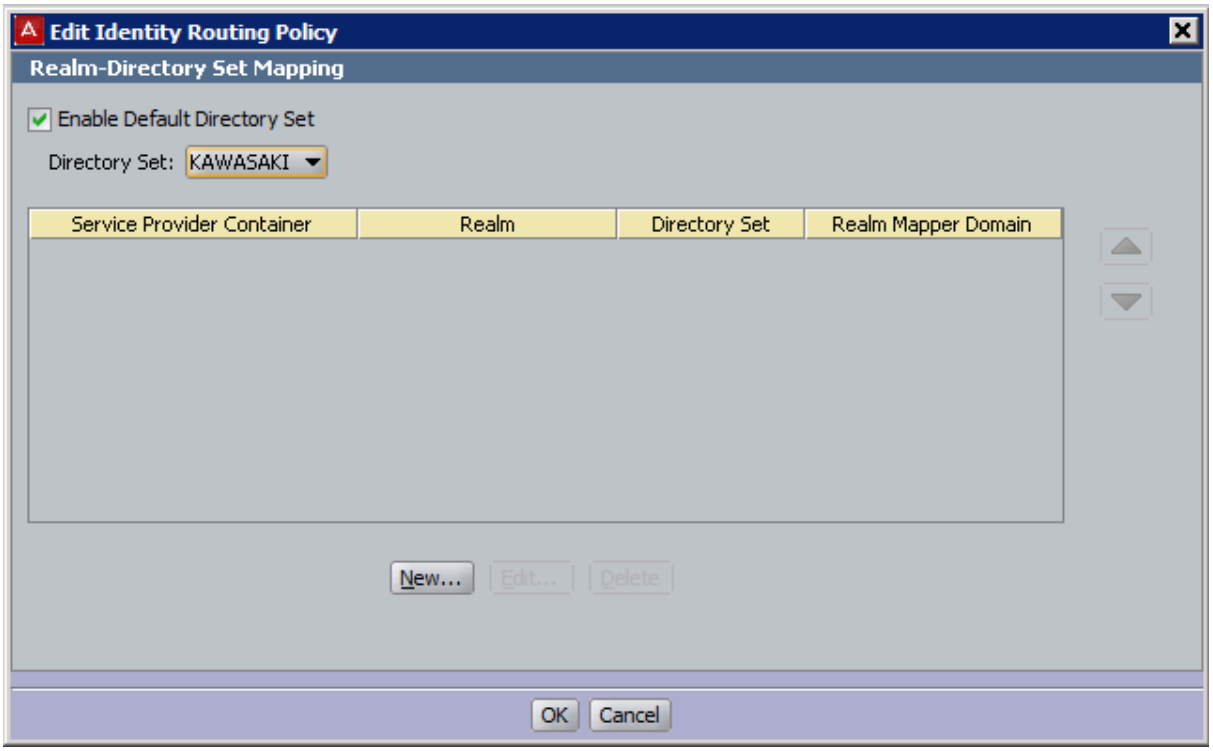
The next policy to configure in your Access Policy is the Identity Routing Policy. This is Ignition Server's prescribed sequence for searching a set of user stores to find a user account when attempting authentication. This example creates a catch-all policy that uses a single Directory Set for all users.

About this task

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Access Policies**.
4. Expand **SAML**.
5. Click the name of your Access Policy.
6. Click the **Identity Routing** tab.
7. Click **Edit**.

   The **Edit Identity Routing Policy** window displays.
8. In the **Edit Identity Routing Policy** window, click **New**.
9. In the **Realm-Directory Set Mapping** window, perform the following actions:
   a. From the **Directory Set** drop-down menu, select the Directory Set you created.
   b. Select the **Match All Realms** check box.
   c. Select the **Disable Service Provider Container Matching** check box.
   d. If this policy is to be associated with RealmMapper, you can specify a Domain Name that the Ignition Server can use to look up Realm mapping data instead of using the domain from the Active Directory or from the user request.
   e. Click **OK**.



Next steps

Configuring Authorization Policy details on page 57

Related Links

Configuring SSO on page 19

Configuring Authorization Policy details

The next policy to configure in your Access Policy is the Authorization Policy. This policy is a set of rules that govern which users are granted access to which applications. You can configure Ignition Server to evaluate user attributes and the context of the access request in order to decide whether to authorize the user.

The following procedure shows you how to create a policy that authorizes access for any user who has a user account on the AD domain (that is, if he or she has an account in the *Domain Users* group). Upon authentication, the user is provisioned based on his or her Virtual Group name.

Note:

The Virtual Group may map to a single AD workgroup or multiple workgroups on one or more domain controllers.

This is just an example of how to configure a rule. You can configure any kind of rule to meet your objective. For example, you can create an authorization policy to authorize only the users who are

supervisors. If supervisors in your organization are defined as being members of a particular group, for example, “Supervisor group”, then in AD you can create a policy to check for "Supervisor group" membership.

About this task

Use the following procedure to create a rule that checks AD domain membership. You can use this procedure as a guide to create similar rules for other authorization checks

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Access Policies**.
4. Expand **SAML**.
5. Click the name of your Access Policy.
6. Click the **Authorization Policy** tab.
7. Click **Edit** to edit the policy.
8. The top half of the **Authorization Policy** tab contains your SAML Authorization Policy. In the top half of the panel, click **Edit** .

   The **Edit Authorization Policy** window appears.
9. In the **Rules** section, in the lower left part of the window, click **Add**.

   The application displays the **New Rule** dialog, where you name the new rule.
10. Type **CheckHasADAccount** and click **OK**.

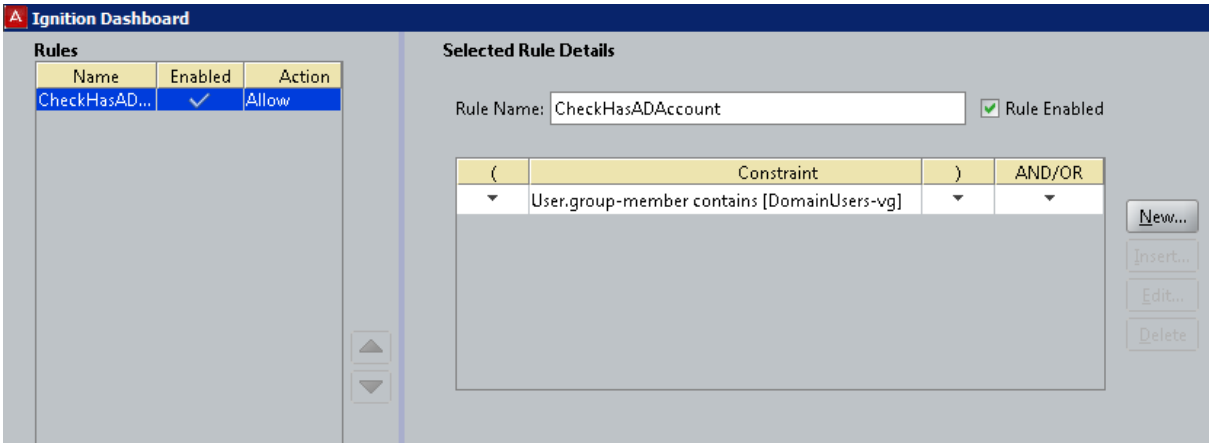
    The **New Rule** dialog closes. In the **Edit Authorization Policy** screen, the rule you just created appears in the **Rules** list that occupies the left side of the window.

    The **Rules** list of the Edit Authorization Policy window shows the rule sequence that forms your Authorization Policy. The right side of the window (the **Selected Rule Details** section) allows you to edit the rule you selected in the list.
11. With **CheckHasADAccount** selected in the **Rules** list, go to the buttons to the right of the **Constraint** list and click **New**.
12. In the **Constraint Details** window, perform the following actions to create your constraint:
    a. From the drop-down menu at the top of Constraint Details window, select the Attribute Category, **User**. The list just below this displays the names of attributes of type **User**.
    b. In the list, select the attribute named **group-member**.
    c. From the drop-down menu in the **Phrase** section, select **Contains Any** and select **Static Value** .
    d. Click **Add**.
    e. In the **Add Value** window, select the Virtual Group you created. If you are following the example, it is **domainusers-vg**.

Click **OK** to close the window.

f. Click **OK** to close the **Constraint Details** window and return to the **Edit Authorization Policy** window.

13. In the **Action** section of the **Edit Authorization Policy** window, click **Allow** . In the **Provisioning** section, make no changes. At runtime, this rule will check whether the user is a member of the AD group, “Domain Users.” If the user is a member, the rule records an ALLOW action. During evaluation, if at least one ALLOW is recorded and if Ignition Server finishes evaluating the rule sequence without triggering a REJECT, the user is authorized.
14. Click **Save** to close the **Edit Authorization Policy** window and return to the **Policy Management** window



Next steps

Setting up your Outbound Attribute Policy details on page 59

Related Links

Configuring SSO on page 19

Setting up your Outbound Attribute Policy details

When a user authenticates, the Ignition Server policy engine provisions the user’s session by sending return attributes to the Service Providers. Ignition Server sends these instructions in the form of SAML attributes.

SAML attributes carry important information from the Service Providers to Ignition Server, and you can configure Ignition Server to make authorization decisions based on that information. In addition, you can configure Ignition Server to return attributes as data.

Outbound Attributes are the data fields Ignition Server uses to carry provisioning data to Service Providers. In technical terms, Outbound Attributes are SAML attributes that Ignition Server can include in messages to Service Providers and to Clients.

The first task in setting up provisioning in Ignition Server is to ensure that you have an Outbound Attribute to carry each provisioning message. To provide Realm Mapping data to the clients, we will use pre-created global Outbound Attributes.

The second task in setting up provisioning in Ignition Server is to map the virtual attribute from a directory server object to a User Virtual Attribute.

The third task in setting up provisioning in Ignition Server is to associate the Outbound Attributes with the Authorization Policy.

Related Links

Configuring SSO on page 19
Mapping a Directory Attribute to a User Virtual Attribute on page 60
Associating Outbound Attributes with the Authorization Policy on page 62

Mapping a Directory Attribute to a User Virtual Attribute

Before you begin

Ensure that you have an appropriate directory service configured to map the virtual attribute that represents the authenticating principal to an attribute in the directory service. See Setting up your connection to a directory service on page 32 for more information.

We will use the following user Virtual Attribute:

- avaya-rm-principal-name

Note: There is no need to create a mapping for the **avaya-rm-data** attribute since it is automatically populated by Ignition Server.

About this task

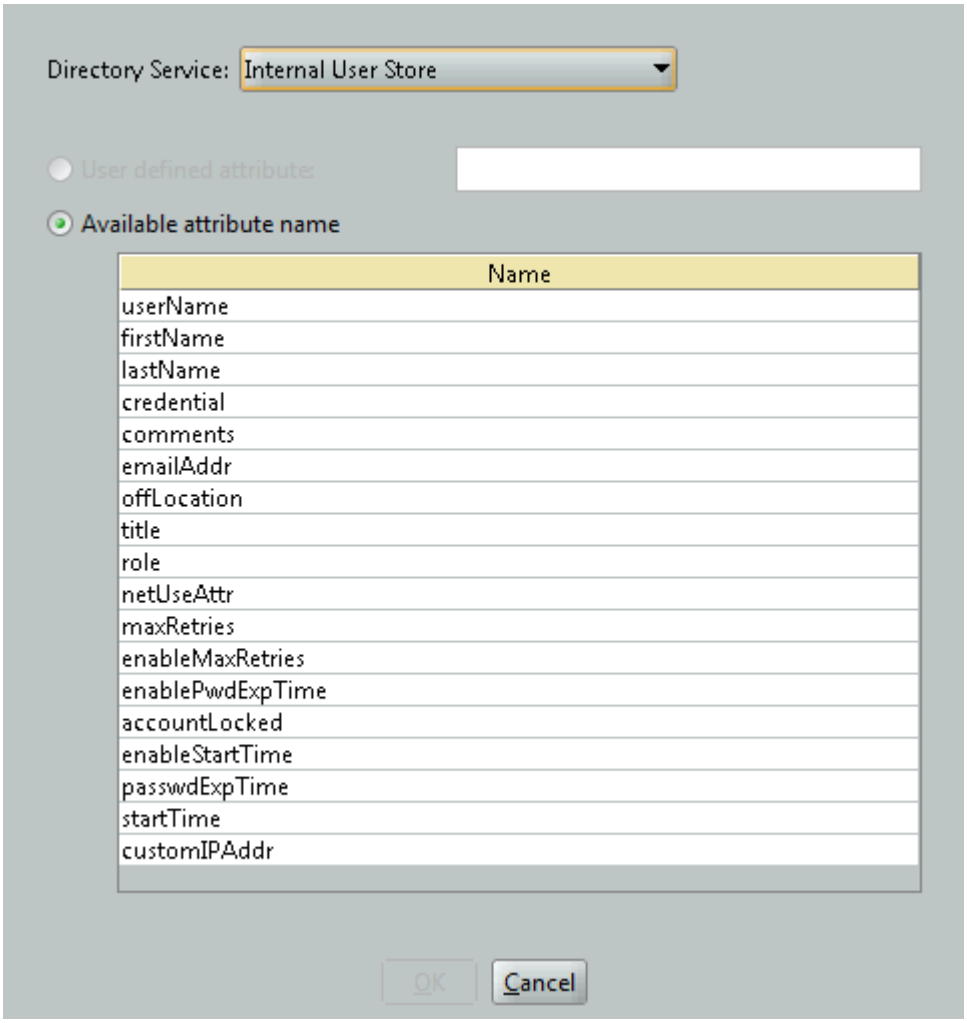
Use the following procedure to map the **userPrincipalName** attribute from a directory service object to the User Virtual Attribute **avaya-rm-principal-name**.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Directories**.
4. Click **Virtual Mapping**.
5. Click **User Virtual Attributes**.

   The virtual attribute Values panel lists all the sets of virtual attributes that have been defined in your Ignition Server.
6. Select the virtual attribute **avaya-rm-principal-name**.
7. Click **Add** in the User Virtual Attribute Details pane.

   The Map Attributes window opens.



8. Select the appropriate directory service from the drop down list.
9. Select **Available Attribute Name**. Choose the attribute you want from the directory whose values should be populated in **avaya-rm-principal-name**. For an active directory, it is normally **userPrincipalName**.
10. Click **OK**.

Next steps

Associating Outbound Attributes with the Authorization Policy on page 62

Related Links

Setting up your Outbound Attribute Policy details on page 59

Associating Outbound Attributes with the Authorization Policy

Ignition Server policies support session provisioning by allowing the administrator to return Outbound Values to Service Provider or Client. Your provisioning instructions are part of your user authorization and/or MAC authorization rules, as configured via the Access Policy panel of Dashboard. When a rule is triggered during user authorization, Ignition Server sends its provisioning value (or values) as attributes in the SAML Assertions.

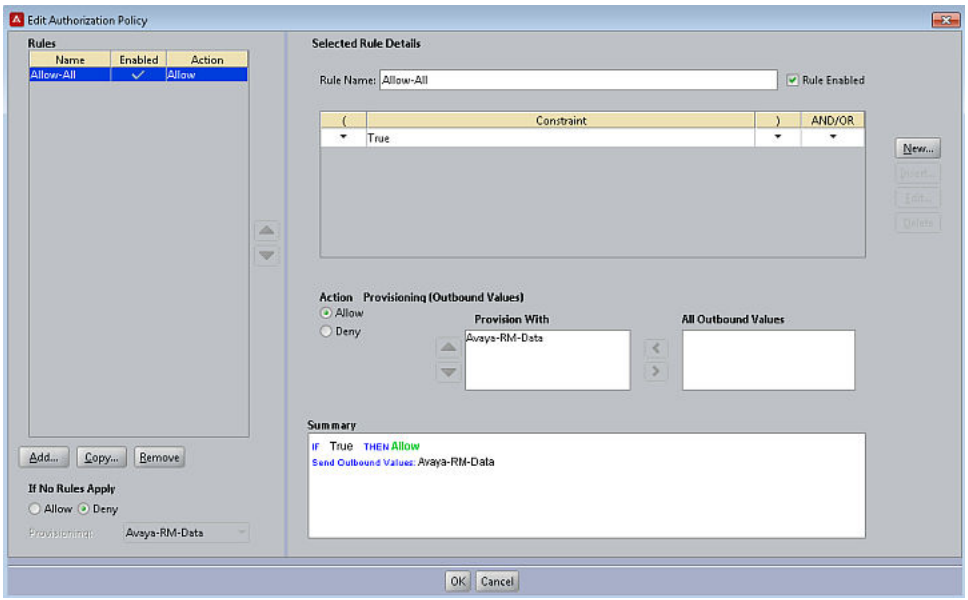
About this task

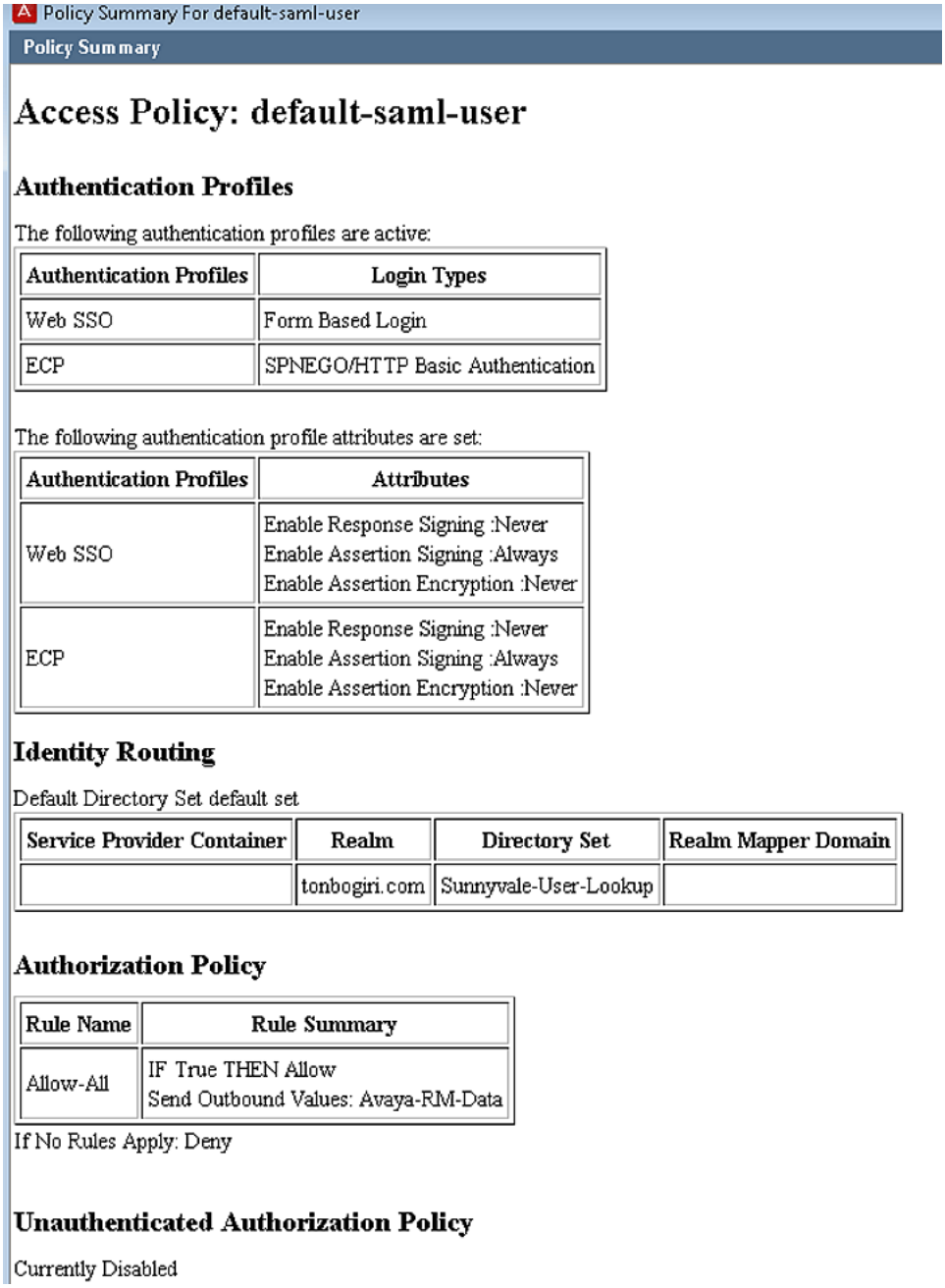
Use the following procedure to associate the Outbound Attributes with Authorization Policy.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand the **Access Policies** > **SAML** folders.
4. Click the name of your Access Policy.
5. Click the **Authorization policy** tab, and click **Edit**.
6. The top half of the **Authorization Policy** tab contains your SAML Authorization Policy. In the top half of the panel, click **Edit**.

   The **Edit Authorization Policy** window displays.
7. In the **Action** section of the **Edit Authorization Policy** window, select **Allow**.
8. In the **Provisioning** section, select the **Avaya-RM-DATA** Outbound Attribute.





Policy Summary For default-saml-user

Policy Summary

Access Policy: default-saml-user

Authentication Profiles

The following authentication profiles are active:

Authentication Profiles	Login Types
Web SSO	Form Based Login
ECP	SPNEGO/HTTP Basic Authentication

The following authentication profile attributes are set:

Authentication Profiles	Attributes
Web SSO	Enable Response Signing :Never Enable Assertion Signing :Always Enable Assertion Encryption :Never
ECP	Enable Response Signing :Never Enable Assertion Signing :Always Enable Assertion Encryption :Never

Identity Routing

Default Directory Set default set

Service Provider Container	Realm	Directory Set	Realm Mapper Domain
	tonbogiri.com	Sunnyvale-User-Lookup	

Authorization Policy

Rule Name	Rule Summary
Allow-All	IF True THEN Allow Send Outbound Values: Avaya-RM-Data

If No Rules Apply: Deny

Unauthenticated Authorization Policy

Currently Disabled

Related Links

Setting up your Outbound Attribute Policy details on page 59

Viewing the SAML Access Policy summary

After you configure the SAML Access Policy, you can view a summary of the information.

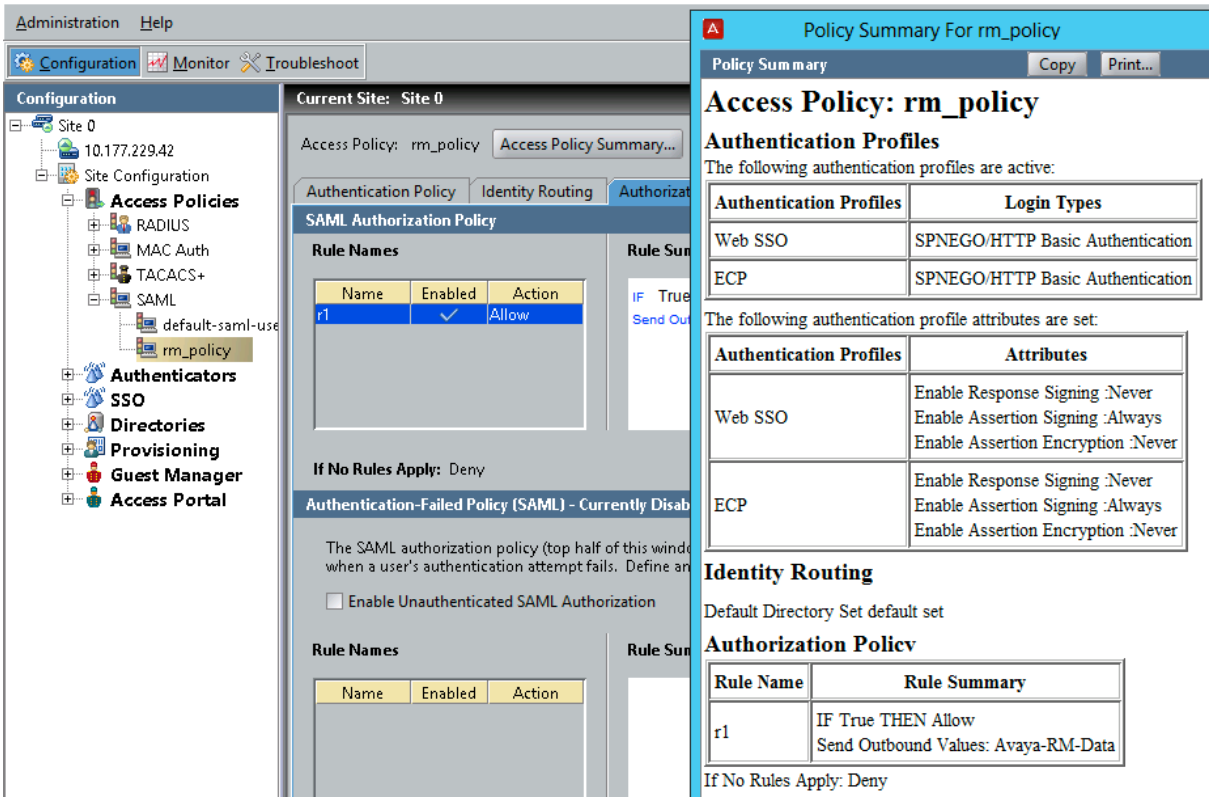
About this task

Use the following procedure to view the SAML Access Policy summary.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Access Policies**.
4. Expand **SAML**.
5. Click the name of your Access Policy.
6. Click **Access Policy Summary**.

   The **Policy Summary** window displays.



7. Click **OK** when you are finished viewing the SAML Access Policy summary.

Next steps

[Creating a Service Provider](#) on page 65

You do not need to add a Service Provider to perform SSO from Aura® clients for fetching Realm Mapping data. You can add a new Service Provider if you want to enable SSO for a web application such as Avaya Aura® Conferencing (AAC).

Related Links

Configuring SSO on page 19

Configuring Service Providers

You can create and delete different Service Providers that can federate with the Identity Provider.

Note: You do not need to add a Service Provider to perform SSO from Aura® clients for fetching Realm Mapping data. You can add a new Service Provider if you want to enable SSO for a web application like Avaya Aura® Conferencing (AAC).

Related Links

Configuring SSO on page 19
Creating a Service Provider on page 65
Deleting a Service Provider on page 67

Creating a Service Provider

About this task

Use the following procedure to create a Service Provider (SP).

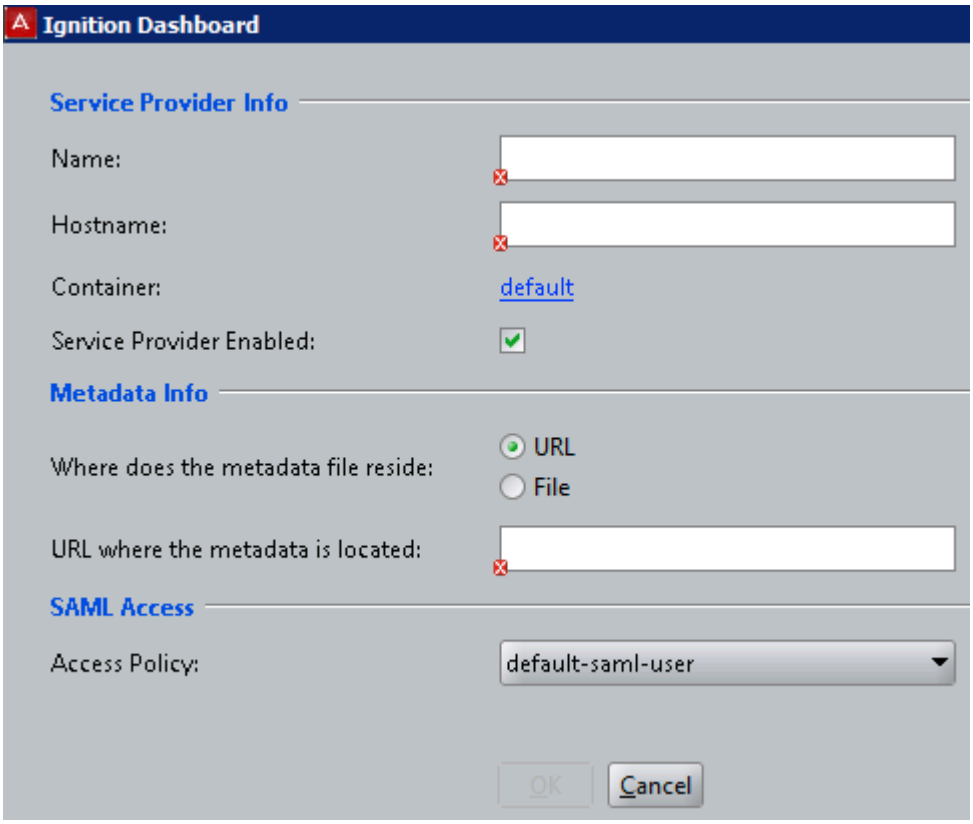
Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **SSO**.
4. Expand **Service Providers**.

   The Service Provider node contains a default container. Previously-created Service Providers are listed under this default container.

5. Click **default**.
6. Click **New**.

   The **Service Provider Details** dialog box displays.



7. Specify the Service Provider details.

   The following table describes the Service Provider details.

Attribute	Description
Name	Specifies the name of the Service Provider.
Hostname	This is the name of the host on which the Service Provider is deployed. The hostname you specify here must match the hostname specified in the Service Provider metadata. If the hostname you enter here does not match the hostname specified in the Service Provider metadata, the validation will fail and user will not be able to create or edit the Service Provider.
Container	Specifies the container hierarchy under which this Service Provider should be created.
Service Provider Enabled	Enables or disables a Service Provider.

Attribute	Description
	Note: If you disable a Service Provider, it does not accept any incoming authentication requests.
Metadata file location	Indicates where the Service Provider metadata is located. • If you select **URL**, you must enter the URL in the **URL where the metadata is located** text box. • If you select **File**, you must browse to the location in the local file system where the Service Provider metadata XML file resides.
Access Policy	Specifies the SAML Access Policy associated with this Service Provider.

8. Click **OK**.

Related Links

Configuring Service Providers on page 65

Deleting a Service Provider

About this task

Use the following procedure to delete a Service Provider.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **SSO**.
4. Click **Service Providers**.
5. In the **Service Providers Summary** panel, click the Service Provider that you want to delete.
6. Click **Delete**.

   A confirmation window displays.
7. Make sure you selected the appropriate Service Provider to delete, and click **OK**.

Related Links

Configuring Service Providers on page 65

Chapter 5: Monitoring SSO

Related Links

Monitoring SAML requests on page 68
Viewing SAML provisioning information on page 73
Viewing Realm Mapper Cache entries on page 79
Viewing Identity Provider Details on page 80
Monitoring Identity Provider logs on page 82

Monitoring SAML requests

You can use the SAML Access Summary tab to view a consolidated picture of the various SAML requests (succeeded and failed). You can also use the Access tab under the Log Viewer tab to view the various successful or failed SAML Authentication request and additional details.

Related Links

Monitoring SSO on page 68
Viewing SAML access summary information on page 68
Viewing SAML access logs on page 70

Viewing SAML access summary information

The SAML Access Summary information provides a consolidated picture of the various SAML requests (Successful and Failed) processed by the Ignition Server. The separate tabs to view Successful requests and Failed requests makes a clear distinction between how the SAML requests were processed and list the end outcome of each SAML request processing.

About this task

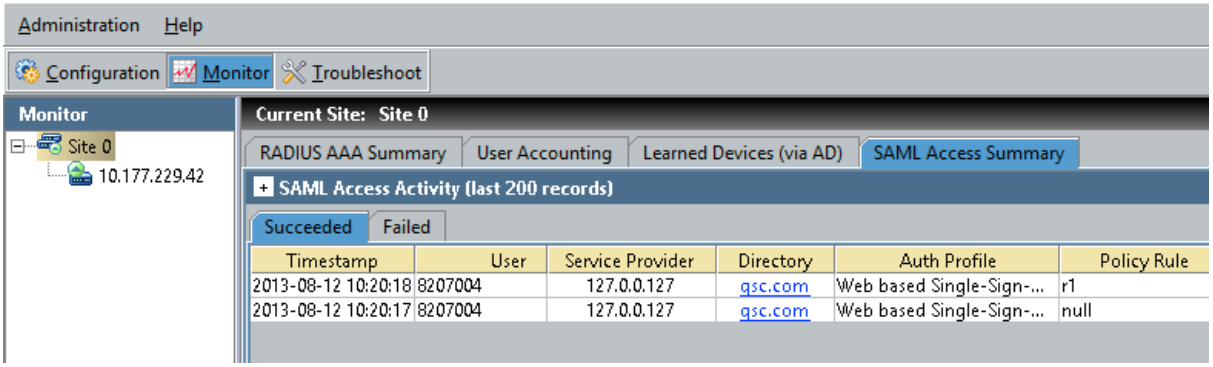
Use the following procedure to view SAML access summary information.

Procedure

1. At the top of the main Dashboard window, click **Monitor**.
2. In the **Monitor** hierarchy tree, click your site name.
3. Click the **SAML Access Summary** tab.

4. Click the **Succeeded** tab.

   The Succeeded SAML access summary screen lists information about successful SAML requests processed by the Ignition Server.

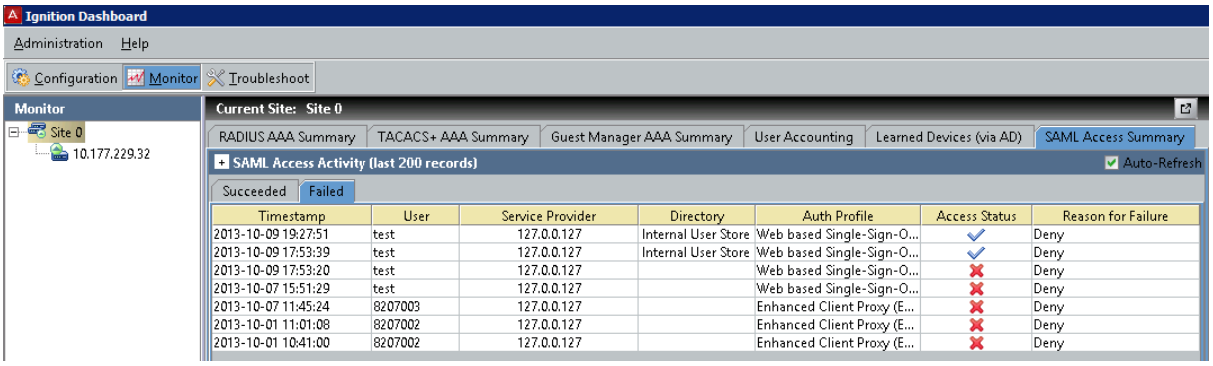


   The following table describes the successful SAML request information.

Column name	Description
Timestamp	The time when the Ignition Server received the SAML request.
User	The user name of the logged in user making the SAML request.
Service Provider	The name of the Service Provider.
Directory	The Directory Service against which this user was authenticated.
Auth Profile	The Authentication Profile used to validate this SAML request. The value can be Web SSO or ECP.
Policy Rule	The SAML Access Policy Rule that was evaluated to process this SAML request.

5. Click the **Failed** tab.

   The Failed SAML access summary screen lists information about failed SAML requests processed by the Ignition Server.



   The following table describes the failed SAML request information.

Column name	Description
Timestamp	The time when the Ignition Server received the SAML request.
User	The user name of the user trying to log in.
Service Provider	The name of the service provider. For a local service provider, this column displays the local IP address.
Directory	The Directory Service against which this user was authenticated. The value is empty if Authentication fails. The value is non-empty only if Authentication succeeds and Authorization fails.
Auth Profile	The Authentication Profile used to validate this SAML request. The value can be Web SSO or ECP.
Access Status	This indicates whether Authentication succeeded.
Reason for Failure	This indicates the reason why the SAML request was not processed.

Related Links

Monitoring SAML requests on page 68

Viewing SAML access logs

The Access Logs section lists the various successful or failed SAML Authentication requests and provides details for each request.

About this task

Use the following procedure to view SAML access logs.

Procedure

1. At the top of the main Dashboard window, click **Monitor**.
2. In the **Monitor** hierarchy tree, click the IP address or name of your node.
3. Click the **Log Viewer** tab.
4. Click the **Access** tab.
5. To filter the view to only show SAML access logs, click the plus sign (+) near under the **Access** tab.

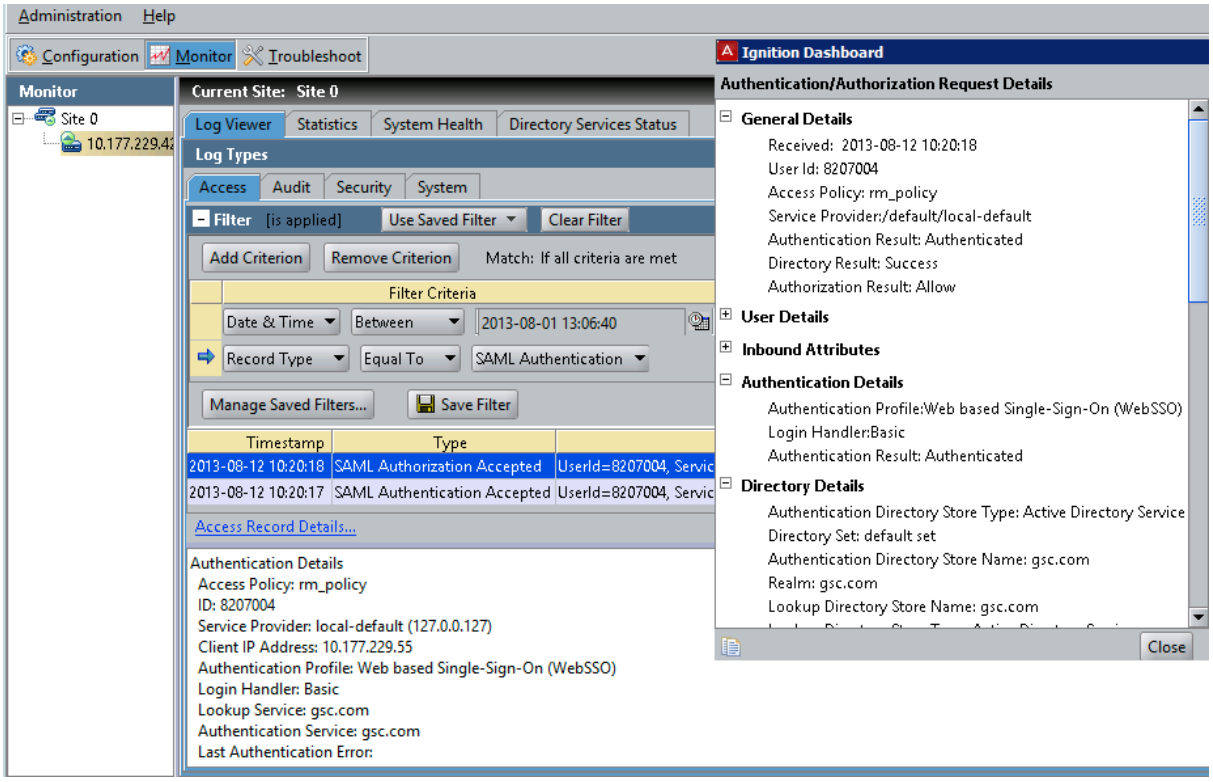
   The **Filter panel** displays.

   The SAML access logs are classified as two types: **SAML Authentication** and **SAML Authorization**.

6. To filter on a specific type of SAML access log, perform the following actions:
   a. Click **Add Criterion**.
   b. From the first drop-down list, select **Record Type** as the field you want to filter on.
   c. From the second drop-down list, select **Equals To**.
   d. From the third drop-down list, select either **SAML Authentication** or **SAML Authorization**.
7. Click **Apply**.

   Only SAML authentication access logs or SAML Authorization access logs appear in the list.
8. For a more detailed description of each access request, double-click the access record or click the **Access Records Details** link near the bottom of the window.

   Access Record Details window displays.



The following table describes the information in the **Access Record Details** window.

Attribute	Description
General Details	The General Details summarize the following results of the login attempt: • Received: Time of request • User Id: Submitted user name

Attribute	Description
	• Access Policy: Name of the Access Policy used • Service Provider: The name of the Service Provider that the user connected through • Authentication Result: Authenticated or Authentication failed • Directory Result: Success or failure of user lookup • Authorization Result: Allow or Deny result based on your authorization rules. Shown only if the Access Record Type is **SAML Authorization**.
User Details	The User Details show the values of the virtual attributes that have been configured for the directory service against which the user has authenticated. Also shown are all the virtual groups to which the user belongs for the directory service against which the user has authenticated.
Inbound Attributes	Inbound Attributes show the details of the user and the client that are trying to authenticate. The details include the following: • Avaya-Saml-Principal-Name: User ID of the user trying to authenticate • Avaya-Saml-SP-Entity-ID: Identity of the service provider that sent the authentication request • Avaya-Saml-SP-IP-Address: IP address of the service provider • Avaya-Saml-Client-IP-Address: IP address of the client machine from which the user is trying to authenticate • Avaya-Saml-Client-User-Agent: The user agent string from the browser or the application that the user is using to authenticate
Authentication Details	The Authentication Details show what type of authentication was attempted. The Authentication Details include the following: • Authentication Profile • Login Handler • Authentication Result

Attribute	Description
Directory Details	The Directory Details show which user store/ authentication server was used to authenticate the user, and which user store provided the user's account details. The Directory Details include the following: • Authentication Directory Store Type • Directory Set • Authentication Directory Store Name • Realm • Lookup Directory Store Name • Lookup Directory Store Type • Directory Result
Authorization Details	The Authorization Details show which rule in your Ignition Server Authorization Policy was used to make the Allow/Deny decision, and what the result was. This section is displayed only if the Access Record Type is **SAML Authorization**. The Authorization Details include the following: • Policy Rule Used • Authorization Result
Outbound Attributes	This section shows the outbound attributes that have been configured to be provisioned in the Access Policy. Only outbound attributes with non-empty values are displayed here. This section is displayed only if the Access Record Type is **SAML Authorization**.

Related Links

Monitoring SAML requests on page 68

Viewing SAML provisioning information

You can use the the SAML provisioning node to view the SAML Attribute definitions and the Inbound and Outbound Attributes defined by default for SAML.

Related Links

Monitoring SSO on page 68
Viewing SAML Attribute Definitions on page 74
Viewing SAML Inbound Attributes on page 75

Viewing SAML Outbound Attributes on page 76
Viewing SAML Outbound Values on page 77

Viewing SAML Attribute Definitions

About this task

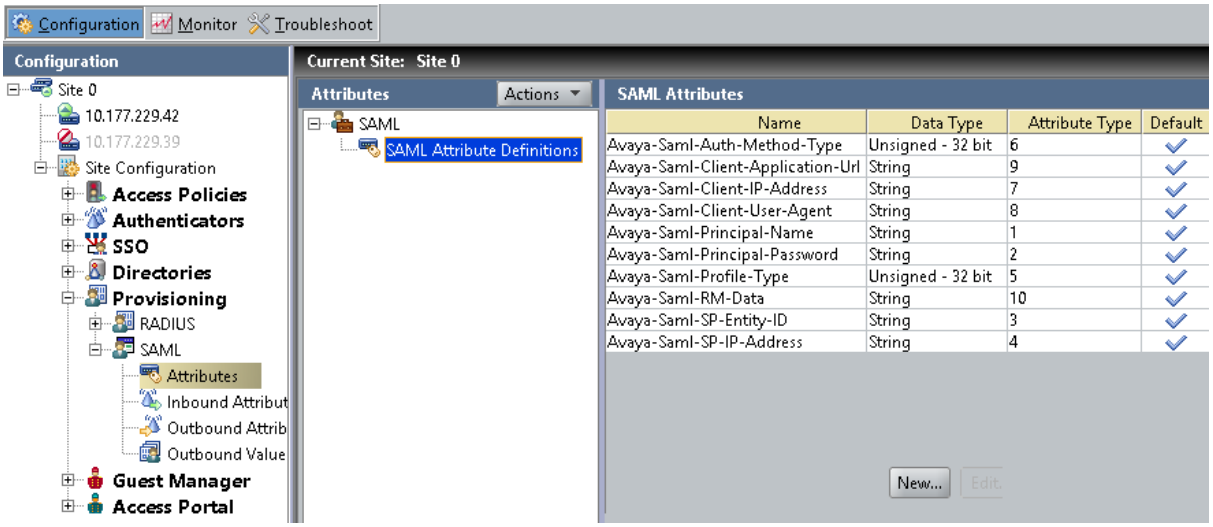
Use the following procedure to view SAML Attribute Definitions.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Provisioning**.
4. Expand **SAML**.
5. Click **Attributes**.
6. In the **Attributes** panel, expand **SAML**.
7. Click **SAML Attribute Definitions**.

   The SAML Attributes panel displays.

   The following figure shows the default SAML Attributes.



   The following table describes the SAML attribute information.

Column name	Description
Name	Indicates the name of the SAML attribute.
Data Type	Indicates the data type of the SAML attribute.
Attribute Type	Indicates the ID of the SAML attribute.

Column name	Description
Default	Indicates whether the SAML attribute is a system default.

Related Links

Viewing SAML provisioning information on page 73

Viewing SAML Inbound Attributes

A piece of data that Ignition Server receives from the Service Provider is called an *inbound value*, and is carried in an *inbound attribute*.

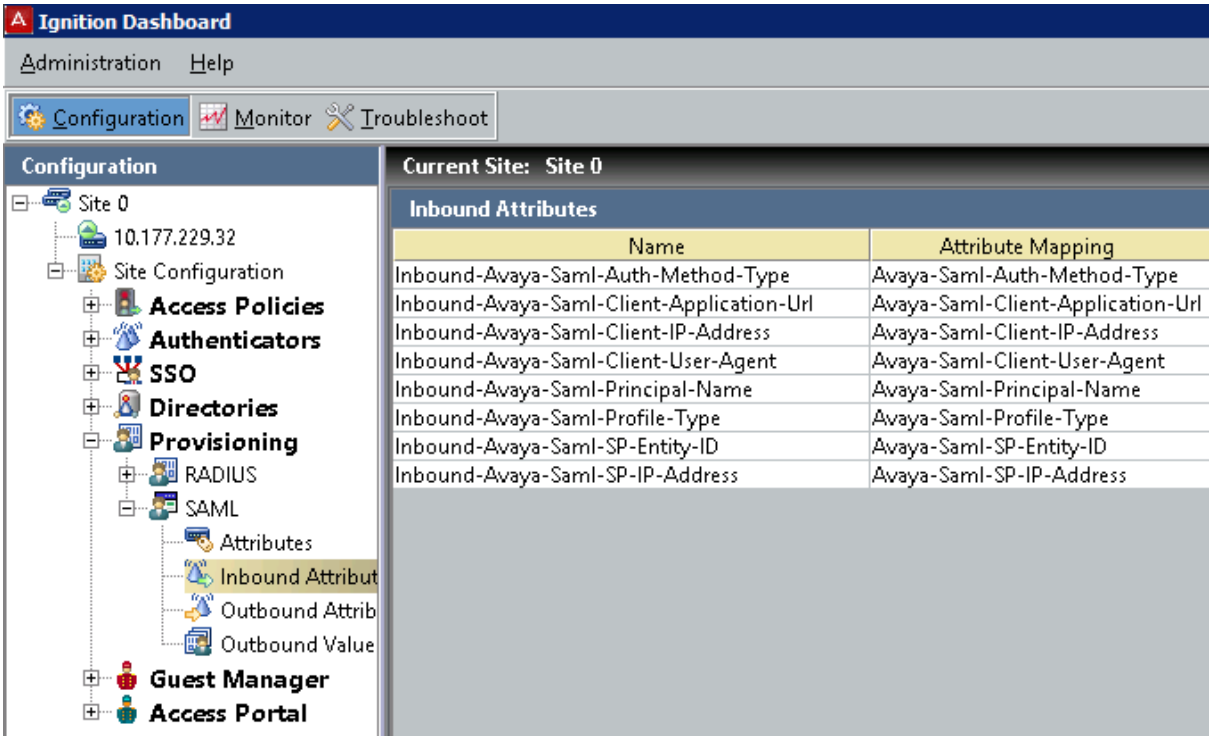
About this task

Use the following procedure to view SAML Inbound Attributes.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Provisioning**.
4. Expand **SAML**.
5. Click **Inbound Attributes**.

   The Inbound Attributes panel displays. The following figure shows the default SAML Inbound Attributes.



The following table describes the default SAML Inbound Attributes.

Column name	Description
Name	The name used to uniquely identify this attribute. When you create a new attribute, you can assign any name to identify it. The default inbound attributes that are already created for you begin with the prefix `Inbound-Avaya-Saml`.
Attribute mapping	The SAML attribute name.

Related Links

Viewing SAML provisioning information on page 73

Viewing SAML Outbound Attributes

Outbound Attributes are the data fields Ignition Server uses to carry provisioning data to Service Providers.

About this task

Use the following procedure to view SAML Outbound Attributes.

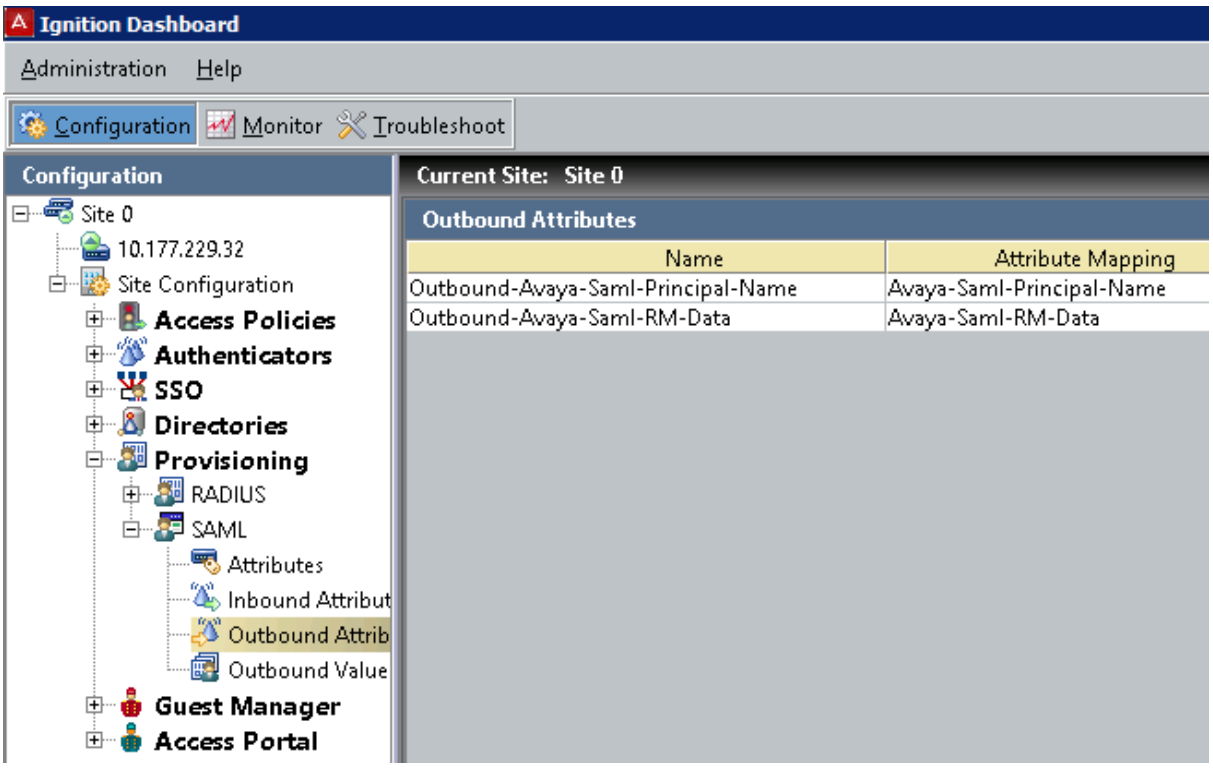
Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.

3. Expand **Provisioning**.
4. Expand **SAML**.
5. Click **Outbound Attributes**.

   The Outbound Attributes panel displays.

   The following figure shows the default SAML Outbound Attributes.



   The following table describes the default SAML Outbound Attributes.

Column name	Description
Name	The name used to uniquely identify this attribute. When you create a new attribute, you can assign any name to identify it. The default outbound attributes that are already created for you begin with the prefix `Outbound-Avaya-Saml`.
Attribute mapping	The SAML attribute name.

Related Links

Viewing SAML provisioning information on page 73

Viewing SAML Outbound Values

Outbound Values are the provisioning data that Ignition Server sends to Service Providers.

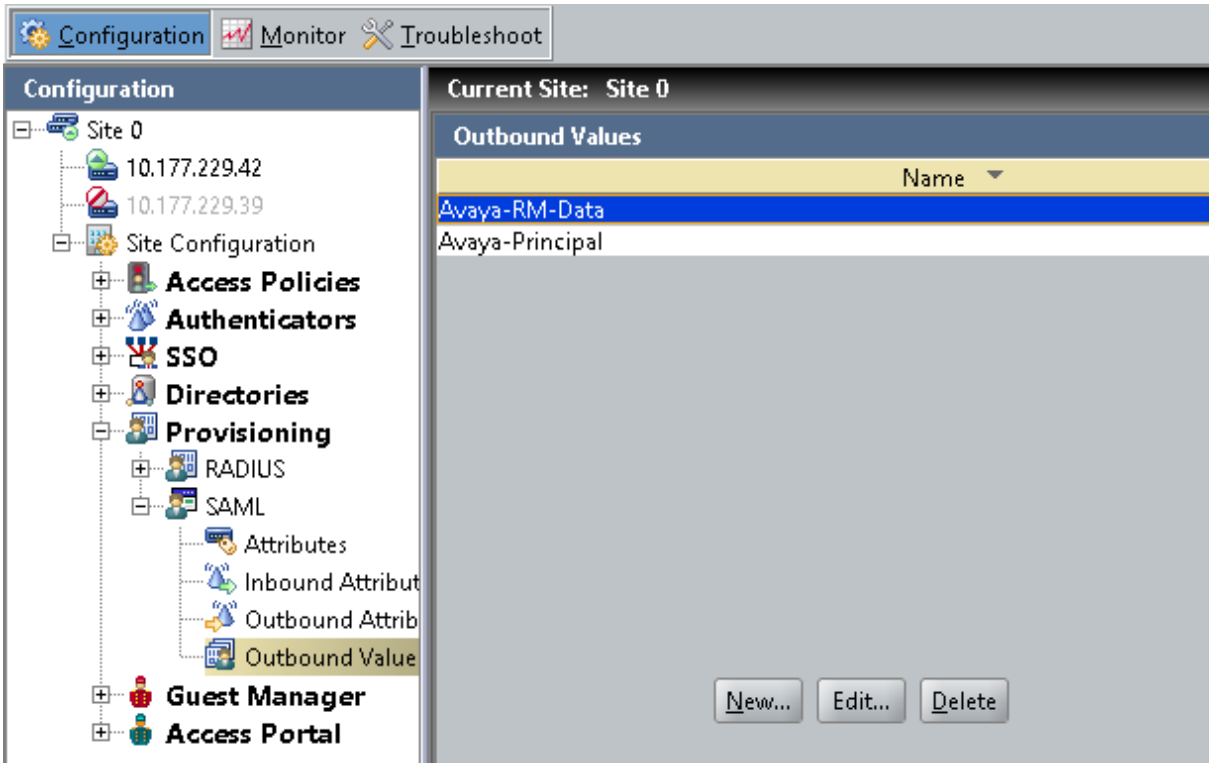
About this task

Use the following procedure to view SAML Outbound Values.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Provisioning**.
4. Expand **SAML**.
5. Click **Outbound Values**.

   The Outbound Values panel appears. The following figure shows the default SAML Outbound Values.



Related Links

Viewing SAML provisioning information on page 73

Viewing Realm Mapper Cache entries

You can use the Realm Mapper cache node under Internal Store, to view read-only Realm Mapper cache entries obtained when the sync occurs with the Avaya Aura System Manager. You can specify filter criteria to narrow down the entries displayed.

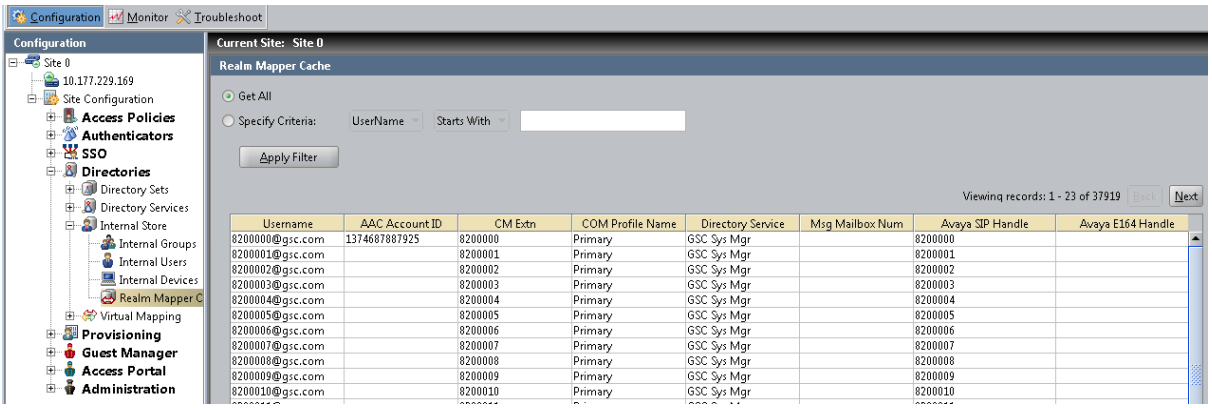
About this task

Use the following procedure to view Realm Mapper Cache entries.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **Directories**.
4. Expand **Internal Store**.
5. Click **Realm Mapper Cache**.

   The following figure shows a sample view of the Realm Mapper Cache entries.



The following table describes the Realm Mapper Cache entry information.

Column name	Description
Username	Login ID which represents the user in the customer's Directory Server (Enterprise ID)
AAC Account ID	Avaya Audio Conferencing Account Id
CM Extn	H.323 extension associated with this user
COM Profile Name	Name of the Communication Profile of the user in SMGR
Directory Service	Name of the SMGR Directory Service this user is associated with
Msg Mailbox Num	Messaging mailbox number of the user
Avaya SIP Handle	SIP handle associated with this user
Avaya E164 Handle	E.164 handle associated with this user

Column name	Description
Avaya MSO Handle	Microsoft OCS handle associated with this user
Avaya Other Handle	Any other handle associated with this user
SMTP Handle	SMTP Handle associated with this user
XMPP GTalk	XMPP Google Talk handle associated with this user
XMPP Jabber	XMPP Jabber handle associated with this user
XMPP Other	Any other XMPP handle associated with this user

6. (Optional) To filter the cache entries, in the Realm Mapper Cache window, select the **Specify Criteria** radio button.
7. Two drop-down lists are shown to the right of the **Specify Criteria** radio button. In the first drop-down list, select *UserName*.
8. In the next drop-down list, select the comparison to be performed. Choose *Starts With* or *Equals*.
9. In the text field, type the comparison value.
10. Click **Apply Filter**.

    Dashboard filters the list.

    To view all cache entries again, select **Get All** and click **Apply Filter**.

Related Links

Monitoring SSO on page 68

Viewing Identity Provider Details

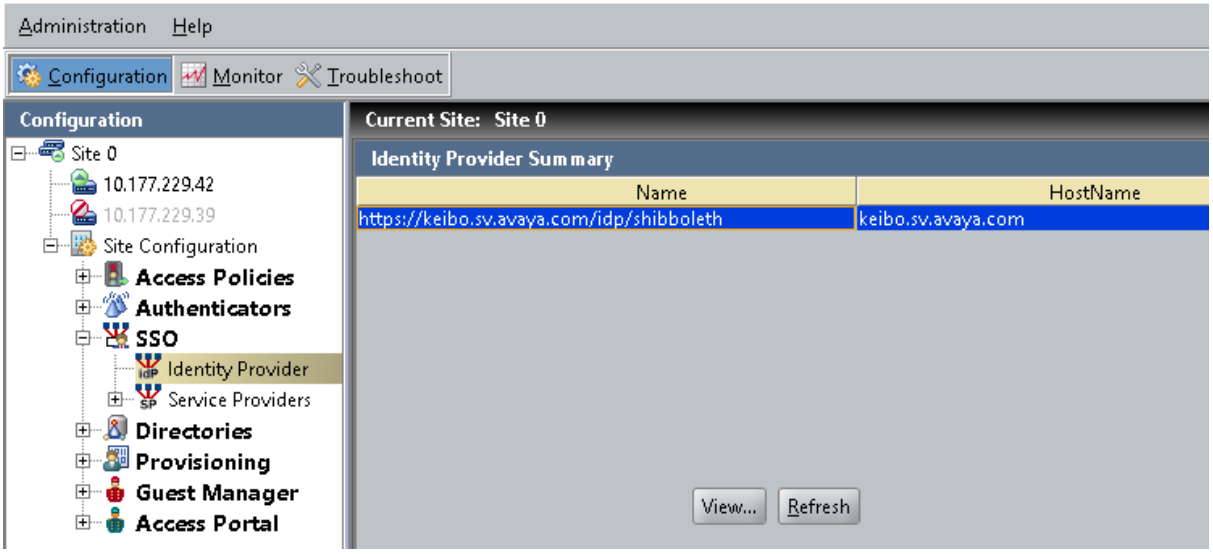
About this task

Use the following procedure to view Identity Provider information.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**.
3. Expand **SSO**.
4. Click **Identity Provider**.

   The default Identity Provider that is hosted on the Ignition Server appears in the Identity Provider Summary list.



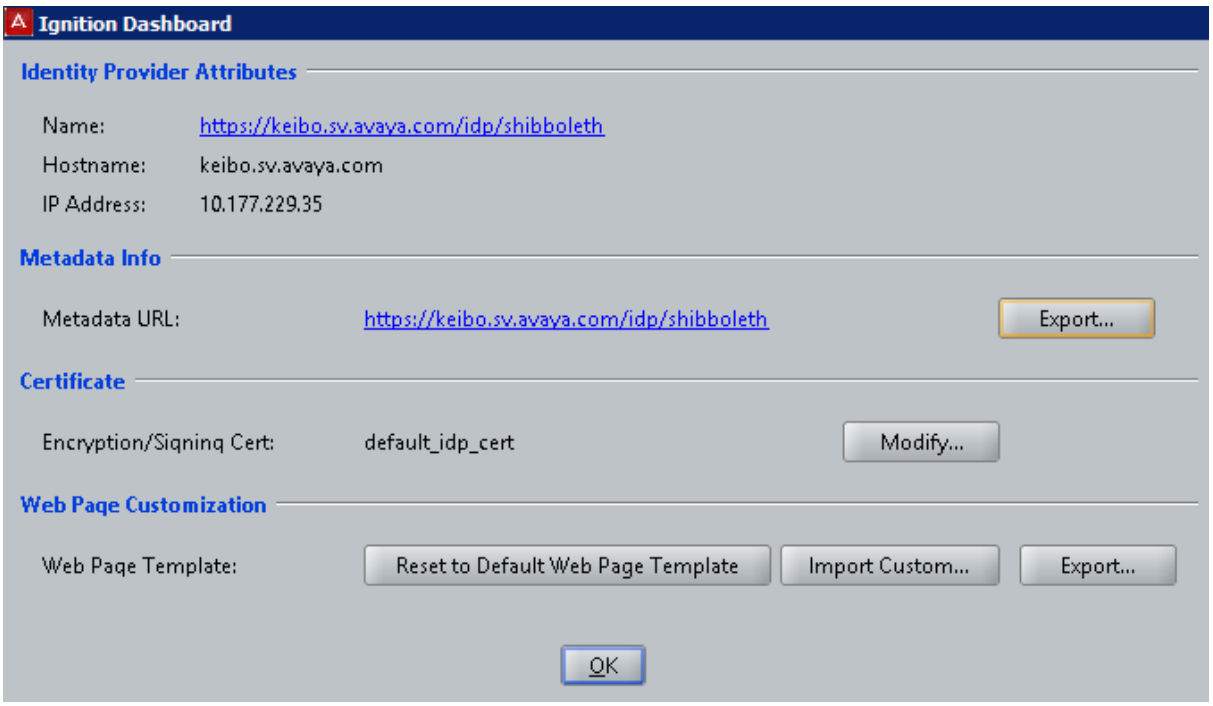
The **Name** corresponds to the entityId specified for this Identity Provider in the metadata.
The **HostName** corresponds to the machine on which this IDP is hosted.

Important:

You cannot add a new Identity Provider or delete the existing one.

5. Click **View**.

   The **Identity Provider Details** dialog box displays.



6. Edit as necessary.

The following table describes the Identity Provider information.

Attribute	Description
Name	Specifies the name of the Identity Provider.
Hostname	Specifies the Host Name of the host on which the Identity Provider is deployed.
IP Address	Specifies the IP address of the interface over which communication happens with the Identity Provider.
Metadata URL	Specifies the location at which the Identity Provider metadata is located.
Encryption/Signing Cert	Specifies the Encryption/Signing certificate used by the Identity Provider for securing the communication with the Service Provider.
Web Page Template	Specifies the Web page template to use when the authentication request is redirected to the Identity Provider for authentication. The following options are supported: • **Reset to Default Web Page Template** button: Click this button to specify that the default Identity Provider Web page template that is bundled with the Ignition Server will be used. • **Import Custom**: Allows you to import a custom Web page template to be used by the Identity Provider. • **Export**: Allows you to export the current Web page template present on the Identity Provider.

7. Click **OK**.

Related Links

Monitoring SSO on page 68

Monitoring Identity Provider logs

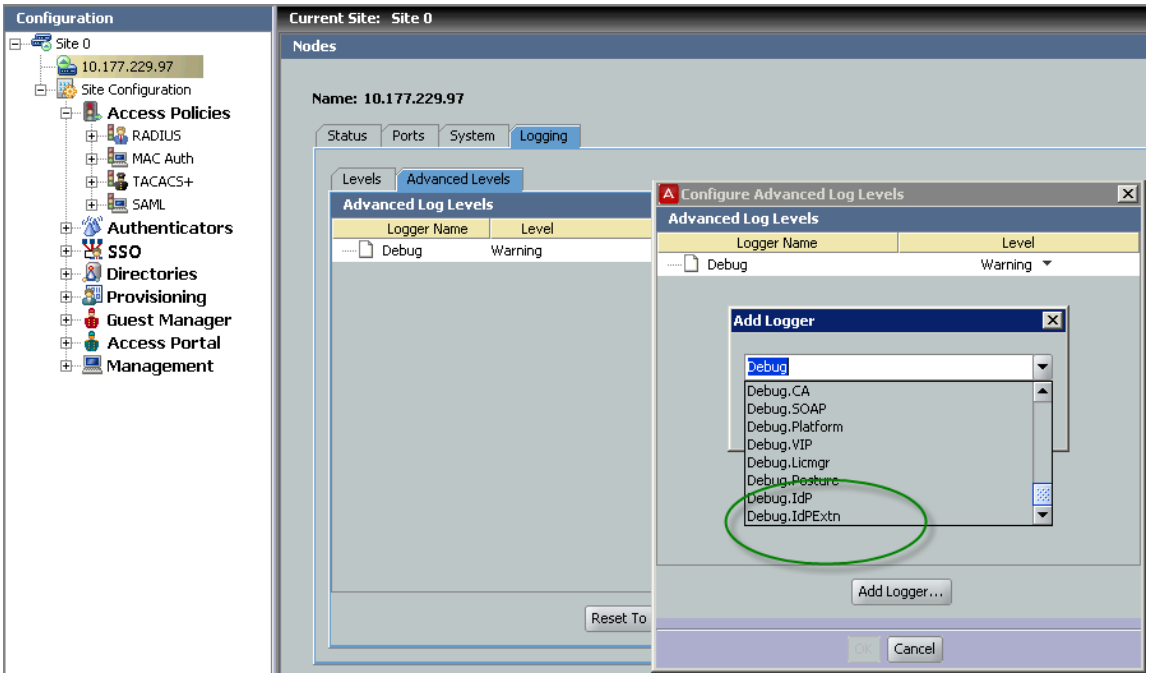
About this task

Use the following procedure to monitor Identity Provider (IdP) logs.

Procedure

1. At the top of the main Dashboard window, click **Monitor**
2. In the **Monitor** hierarchy tree, click the IP address or name of your node.
3. Click the **Log Viewer** tab. The default level for IdP loggers is set to **Warning**.

4. To change the logging level for IdP loggers, perform the following actions:
   a. In the Dashboard **Configuration** tree, click the IP address or name of your node.
   b. Click the **Logging** tab.
   c. Click the **Advanced Levels** tab. The Configure Advanced Log Levels window appears.



   d. Edit the logging levels as required. The loggers for the IdP are **Debug. IdP** and **Debug.IdPExtn**. Debug.IdP is used to configure the IdP framework logs and Debug.IdPExtn is used to debug the IdP framework extensions.

      Note: Avaya recommends that administrators lower the log level from **Warning** to **Info** or **Debug** for IdpExtn logger first and, if required, update the log level for Debug.IdP. Lowering the log level of IdP framework logger can greatly increase the volume of log messages captured.

   e. Click **OK**.

Related Links

Monitoring SSO on page 68

Chapter 6: Use cases

Beginning in Release 9.0, Avaya Identity Engines supports Single Sign On (SSO) for the following use cases:

- Flare for iPad from within the Enterprise on page 84
- Flare for iPad from outside the Enterprise using a VPN on page 88
- Flare for iPad from outside the Enterprise using SBC (VPN-less mode) on page 88

Refer to the preceding sections for design and configuration information.

Flare for iPad from within the Enterprise

The following diagram shows how the major components interact when using Flare for iPad from within the Enterprise.

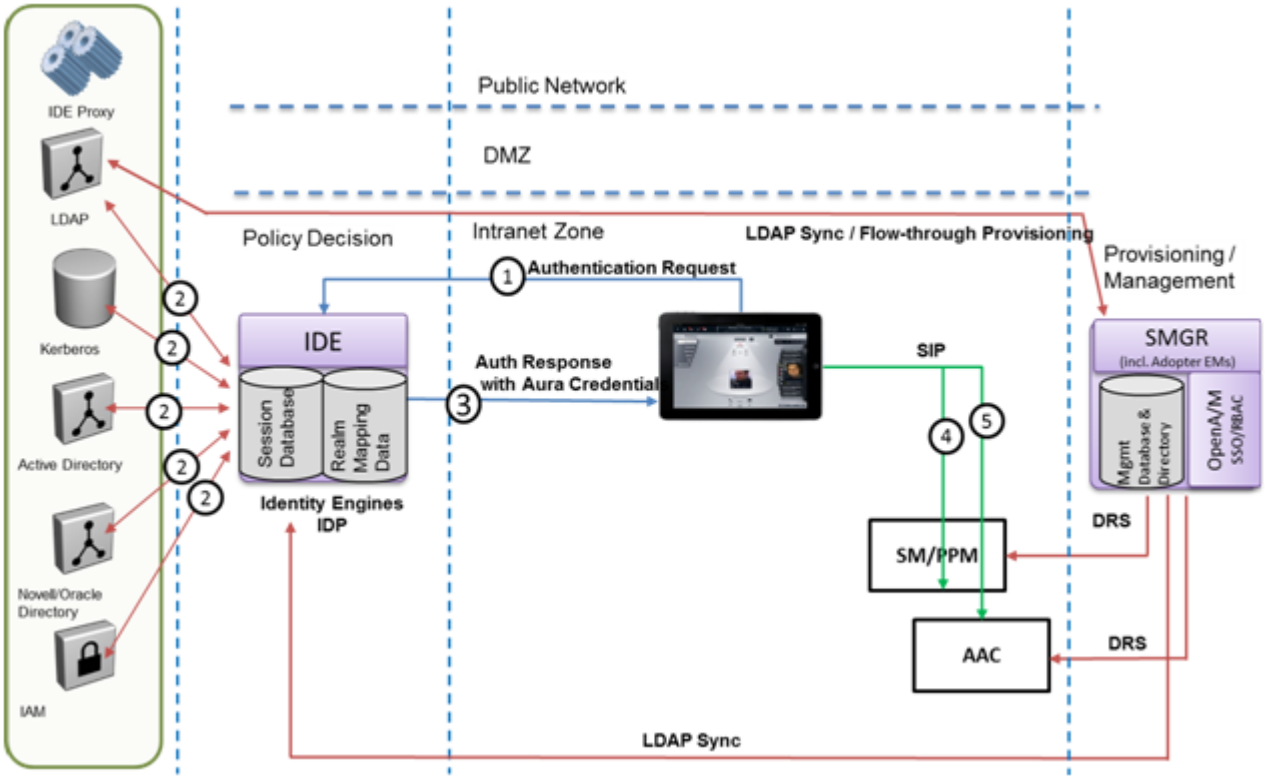


Figure 1: Component diagram of Flare for iPad within the Enterprise

You can either provision System Manager with user accounts or synchronize it with the user information from an Active Directory instance. IDE maintains a cache of Aura credentials for users in System Manager using LDAP sync with System Manager. IDE then uses the following process to authenticate users:

- Flare user requests IDE for authentication by providing enterprise credentials.
- IDE verifies the user identity against the directory.
- After a successful authentication, IDE returns an assertion to Flare, which it can use to authenticate other Aura services like SIP server, Presence and CM.

The result is that the end user is authenticated for all Aura services simply by providing their Enterprise credentials once. The user does not have to remember multiple sets of credentials for logging into different Aura Services such as phone number and password to log into the SIP server, Enterprise credentials for logging into Enterprise Search, and the credentials for Avaya Aura Conferencing to login to Conferencing.

Configuring Flare for iPad using Discover Services

Use this procedure to configure Unified Login.

You can select either **Discover Services** or **Manually Configure Services**. It is always easier to discover services if your deployment supports it rather than manually configuring them.

Before you begin

Install Flare 1.2 for iPad.

Note: Flare for iPad must be Release 1.2 build #50 or above.

Procedure

1. Click **Discover Services**.
2. Specify a URL for the profile file, for example, http://sand.sv.avaya.com:8080/SSO.txt.
3. Enter your email address.

   The rest of the fields are automatically populated and no other configuration is required. Flare is ready for use.

   Note: For more information on how to use **Discover Services** to provision your deployment, refer to Flare for iPad documentation.

Configuring Flare for iPad using Manually Configure Services

Use this procedure to configure Unified Login. You can select either **Discover Services** or **Manually Configure Services**. It is always easier to discover services if your deployment supports it rather than manually configuring them.

Before you begin

Install Flare 1.2 for iPad.

Note: Flare for iPad must be Release 1.2 build #50 or above.

Procedure

1. Click on the **Settings** icon to configure Unified Log In.
2. Click **Accounts and Services**
3. In the **Unified Log In** field, select `ON`.
4. In the **Identity Server** field, enter the URL for your specific environment such as `ide.avaya.com/RealmMapper/getCredentials`.
5. In the **User Name** field, enter your corporate handle or email address such as `user@avaya.com`.
6. In the **Password** field, enter your corporate password.
7. In the **Phone Service Address** field, enter the IP address for your specific environment.
8. In the **Phone Service Port** field, enter `5061` unless your environment uses a different port.
9. In the **Phone Service Domain** field, enter the URL for your environment.
10. In the **TLS** field, enter the setting for your environment.
11. In the **Use Unified Log In** field, select `ON`.

12. In the **Enterprise Directory** field, select `ON`.
13. In the **Directory Server Address** field, enter the address of the directory server in your environment.
14. In the **Use SSL** field, select `ON`.
15. In the **Search Root** field, enter the root for your environment such as `OU=Global Users, DC=global, DC=avaya, DC=com`.
16. In the **Use Unified Log In** field, select `ON`.
17. In the **Presence Service** field, select `ON`.
18. In the **Presence Server Address** field, enter the IP address of your Presence Server.

Configuring System Manager

The IDE Ignition Server requires an Administrative User Account on Avaya Aura System Manager to read the comm profiles for the users. Use either step in this procedure to configure an Administrative User Account.

Procedure

Use the existing Administrative Account on Avaya Aura System Manager or create a new account. To create a new account, use either the User Management screen or the Administrators' screen on the Avaya Aura System Manager.

Note: For information on creating a new Administrative Account, see Configuring the Avaya Aura System Manager on page 21.

Configuring Identity Engines

This procedure outlines the basic steps to configure IDE for SSO. For information on configuring each step, see Configuring SSO on page 19.

Procedure

1. Install the Avaya Aura SSO license.
2. Configure the SAML service.
3. Create a SAML Access Policy.
4. Configure the Realm Mapper service.
5. Create a Directory service to your enterprise directory service.
6. Create a Directory Set.
7. Connect Ignition Server to your Avaya Aura System Manager.
8. Configure User Virtual Attributes.

9. Configure Authentication Policy details.
10. Configure Identity Routing Policy details.
11. Configure Authorization Policy details.
12. Configure your Outbound Attribute Policy details.
13. Associate Outbound Attributes with the Authorization Policy.

Flare for iPad from outside the Enterprise using a VPN

This use case works exactly like the use case within the Enterprise. For information, see Flare for iPad from within the Enterprise on page 84.

The only additional step required on the iPad is to connect to the Enterprise VPN. No other configuration changes are needed on IDE, Flare, System Manage, or any other component.

Flare for iPad from outside the Enterprise using SBC (VPN-less mode)

This use case shows how to use Flare for iPad from outside the Enterprise such as when an employee works from home.

To support remote access, a Split DNS infrastructure is essential to enable the Identity Engines Ignition Server name resolution for external clients.

- The SBC masks as the Ignition Server for the external clients so the host name of Ignition Server resolves to SBC's external facing IP address from outside the Enterprise.
- Within the Enterprise, the Ignition Server host name resolves to the IP address of the Ignition Server.

Note: You must configure the TCP relay on the SBC to forward traffic associated with Ignition Server to the actual IP address on the internal network. For information, see Configuring SBC on page 91.

The following diagram shows the deployment in this scenario.

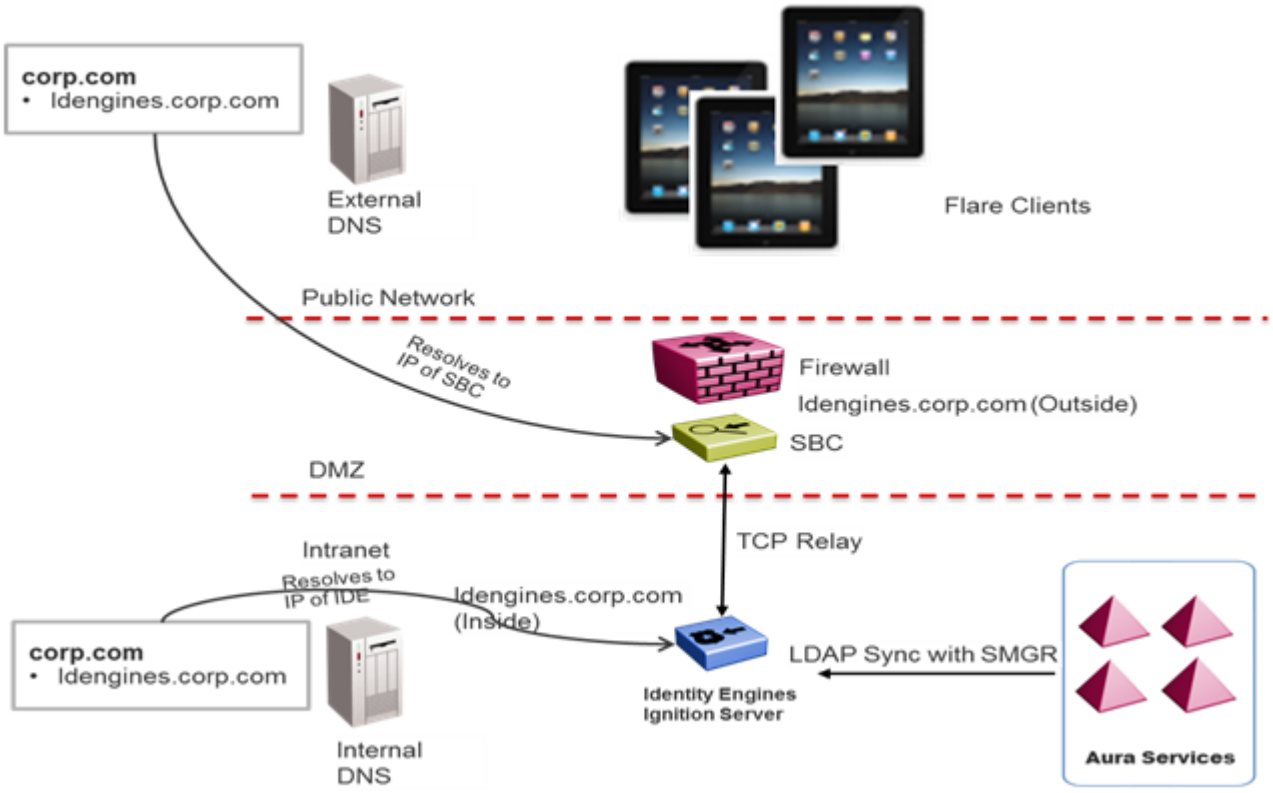


Figure 2: Architectural diagram of Flare for iPad using SBC

The following high-level diagram shows the interaction among the major components.

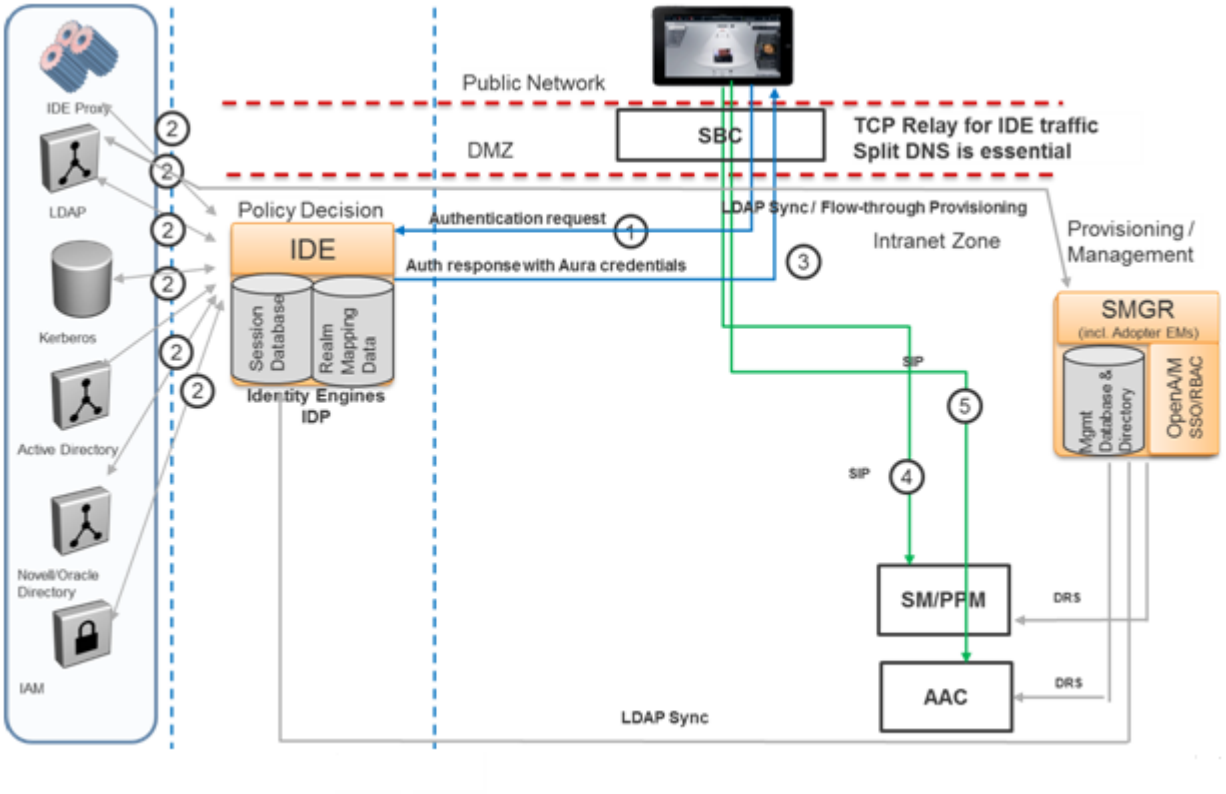


Figure 3: Component diagram of Flare for iPad using SBC

Configuring Flare for iPad using SBC

The procedure for configuring Flare for iPad using SBC is the same as it is within the Enterprise. For configuration information, see Configuring Flare for iPad on page 85.

Configuring System Manager using SBC

The procedure for configuring System Manager using SBC is the same as it is within the Enterprise. For configuration information, see Configuring System Manager on page 87.

Configuring Identity Engines using SBC

The procedure for configuring Identity Engines using SBC is the same as it is within the Enterprise. For configuration information, see Configuring Identity Engines on page 87.

Configuring SBC

You must configure the TCP relay on the SBC to forward traffic associated with Ignition Server to the actual IP address on the internal network.

Procedure

1. In the **Remote Domain** field, enter the Domain name of the Ignition Server interface hosting the SAML service.
2. In the **Remote IP** field, enter the IP address of the Ignition Server hosting the SAML service.
3. In the **Remote Port** field, enter the port on which the Ignition Server is listening for SAML. The default port is `443`.
4. In the **Remote Transport** field, enter the Relay type. (This example uses TCP relay.)
5. In the **Published Domain** field, enter the domain name of the Ignition Server exposed on the external network. It must be the same as the domain name in the internal network.
6. In the **Listen IP** field, enter the IP address on the SBC exposed to the external network for SSO.
7. In the **Listen Port** field, enter the port on which the SBC listens for SSO traffic. (This port must be the same as the **Remote Port**.)
8. In the **Connect IP** field, enter the IP address on the internal side of SBC that will be used to proxy SSO traffic to the Ignition Server.
9. In the **Listen Transport** field, enter the same relay type as **Remote Transport** (TCP).

Example

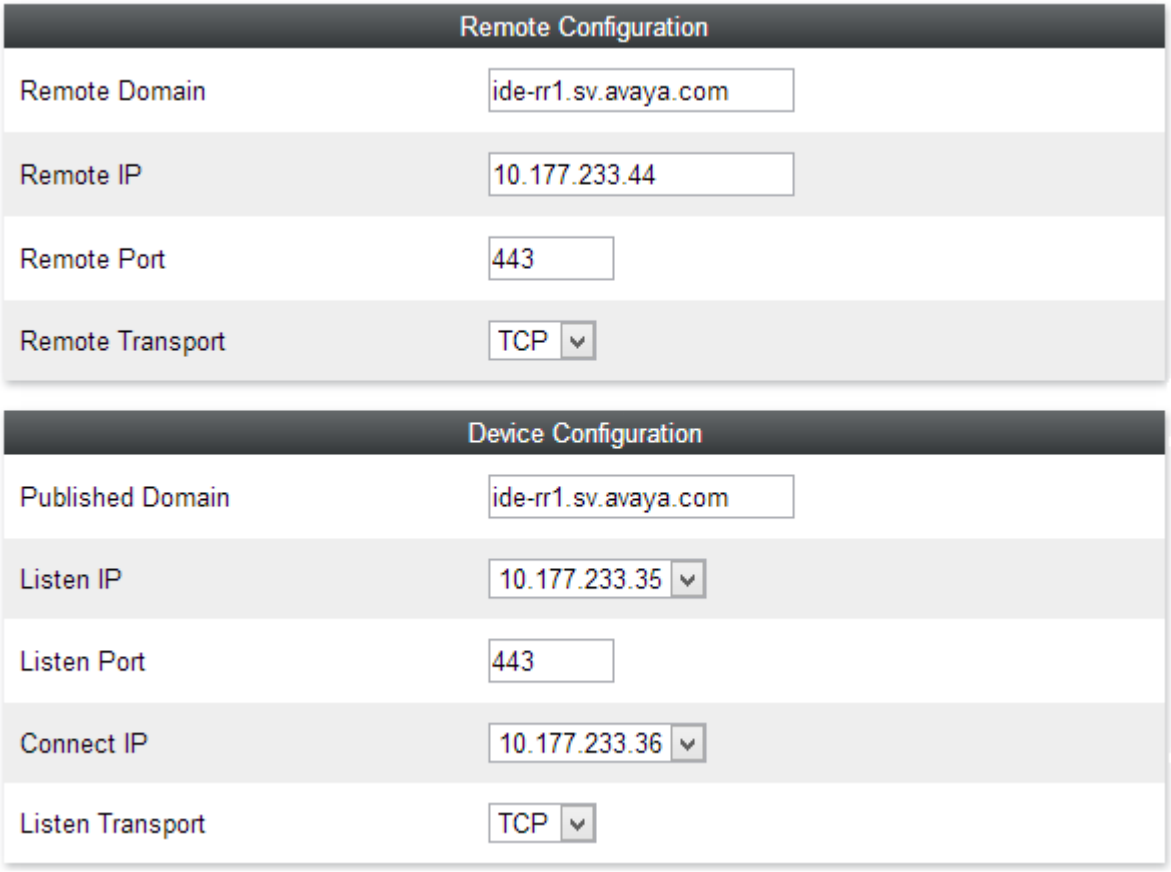


Figure 4: Example of an SBC remote configuration

Chapter 7: Troubleshooting

This section lists troubleshooting techniques and solutions for common Identity Engines (IDE) Single Sign-On (SSO) issues.

Related Links

General troubleshooting techniques on page 93
Troubleshooting specific issues on page 98
Troubleshooting Flare for IPad specific issues on page 109

General troubleshooting techniques

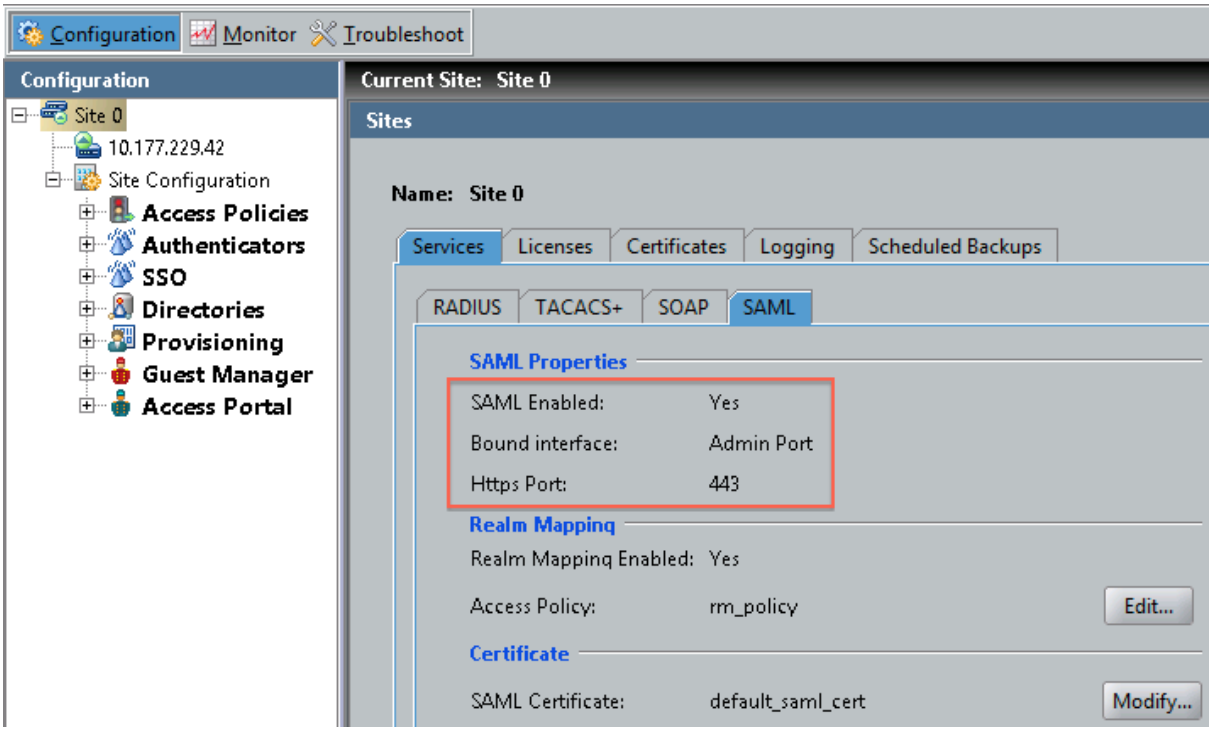
Single-Sign-On support in Identity Engines (IDE) is provided by several services and applications working together on Ignition Server. IDE comes with an extensive complement of diagnostics tools. To troubleshoot any kind of SSO issue, it is a good idea to first use these tools to verify that the basic services related to SAML are working correctly before attempting to debug any specific issue you have.

About this task

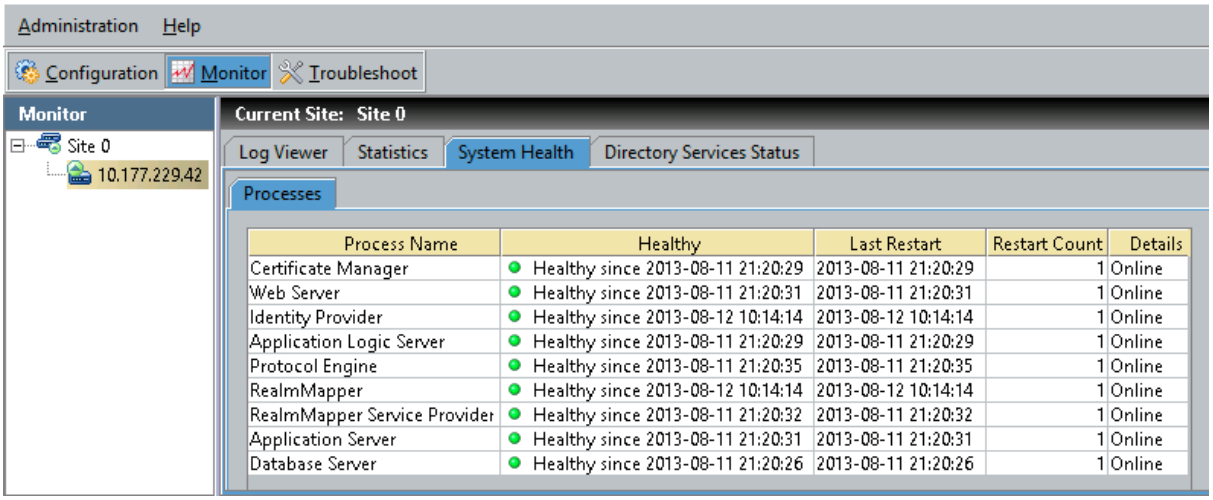
Use the following troubleshooting steps to verify the following on the server.

Procedure

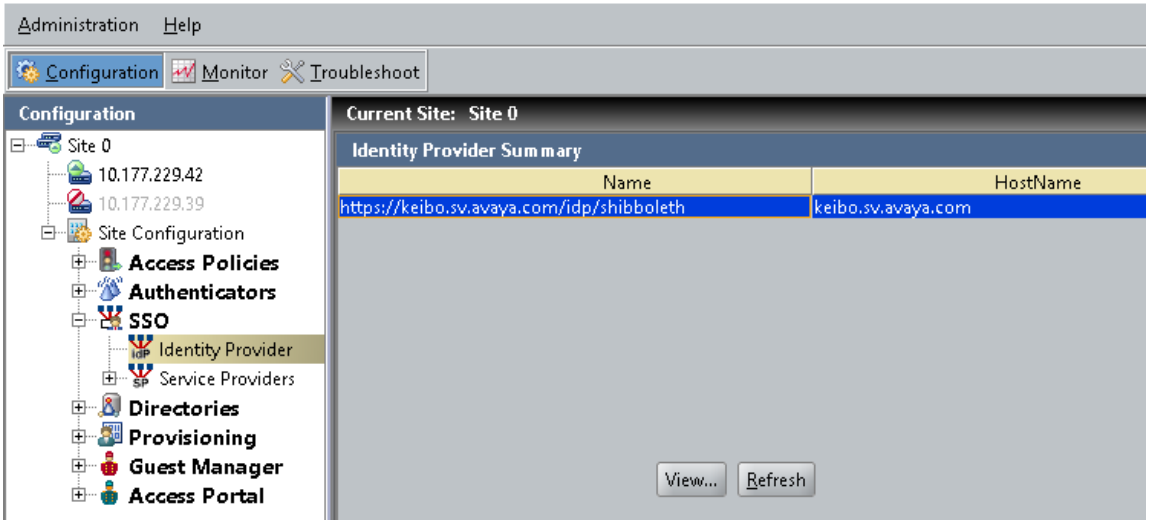
1. Verify SAML is enabled by going to **Configuration > Site > Services** tab **> SAML** tab. Ensure that SAML is bound to the correct port as per your network configuration. Make a note of the Https port if using anything other than the standard (443) port.



2. Perform a System Health Check. Go to **Monitor > IP address or name of your node > System Health** tab **> Processes** tab. Ensure that Apache, Tomcat, IdP, Protocol Engine, (and Realm Mapper if you will be using that) are up and running.

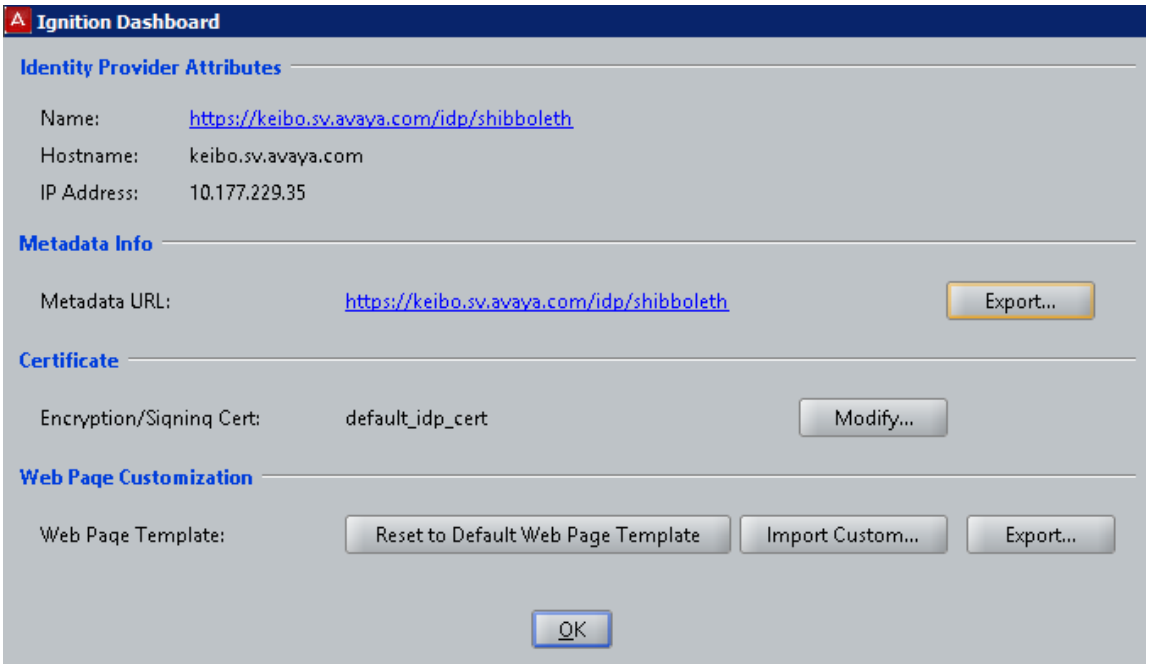


3. Verify that DNS configuration is correct and Identity Provider (IdP) is running properly.
   a. Go to **Configuration > Site > Site Configuration > SSO > Identity Provider**. The Name of the Identity Provider contains the host name instead of the IP address if DNS configuration has been correctly applied.



   b. Next, select the IdP and click **Edit**.

   c. Click the Metadata URL to verify that IdP metadata is correctly generated. Verify if the entity id in the metadata matches what is shown as the Name of the IdP.



   d. In your browser, go to `https://<FQDN of IDE>:port/idp/profile/Status`.

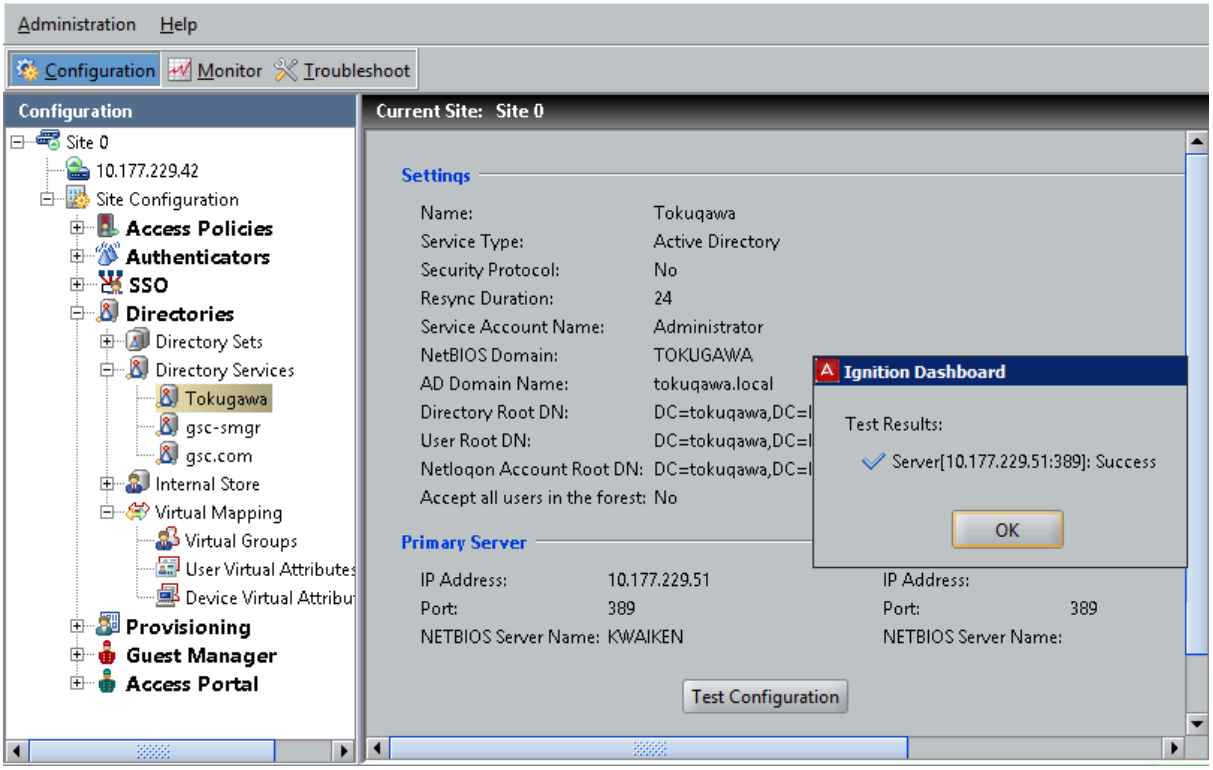
For the URL, the port is only needed if the SAML service has been configured with a port other than the default value of 443.

For example:

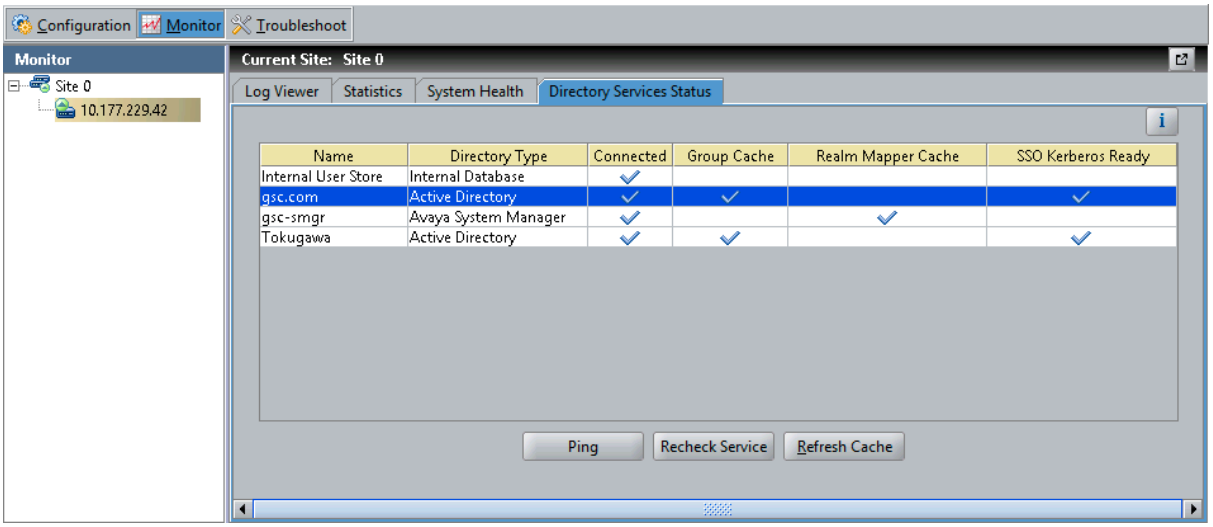
- `https://ide.exampleA.com/idp/profile/Status` if the SAML service is configured with the default port
- `https://ide.exampleB.com:5778/idp/profile/Status` if the SAML service is configured on a non-default port, 5778 in this example

4. If you are using an external Service Provider, verify that the Service Provider was added successfully, is enabled, and has the correct Access Policy associated with it by going to **Configuration > Site > Site Configuration > SSO > Service Providers > <Container Name or default>**. This step is not necessary if you are just accessing the Realm Mapping URL.

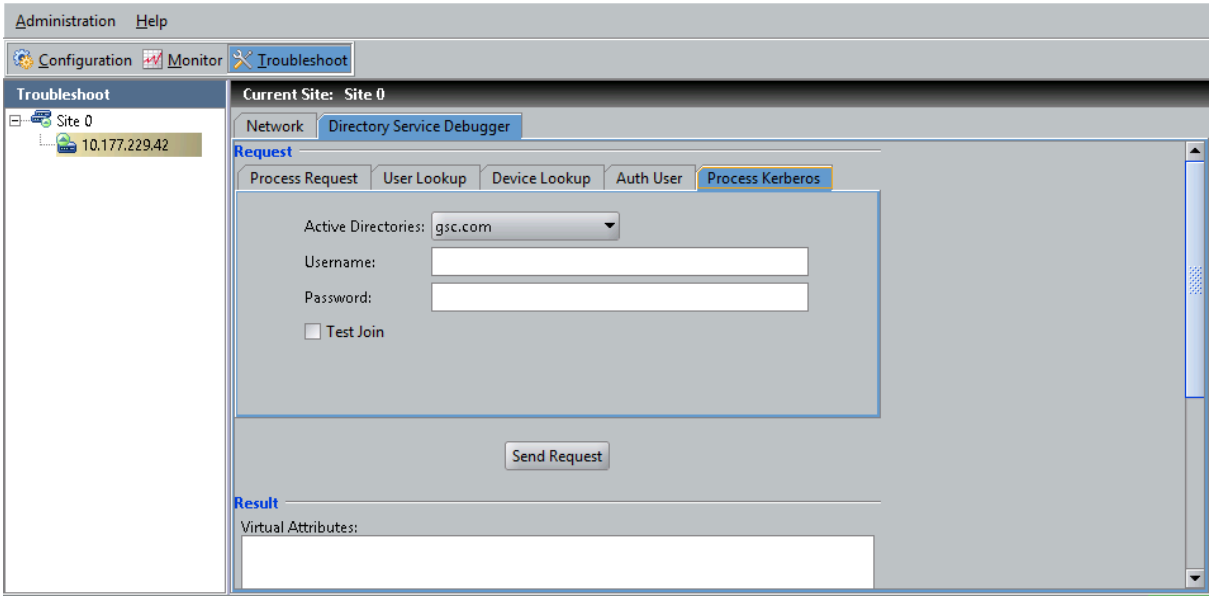
5. If you added an Active Directory, verify the configuration. Go to **Configuration > Site > Site Configuration > Directories > Directory Services > <Your Active Directory >** and click **Test Configuration**. Any issues are reported here.



6. Go to **Monitor > IP address or name of your node > Directory Service Status** tab, and verify that a check mark is shown for AD under the **SSO Kerberos Ready** column.



7. Go to **Troubleshoot > IP address or name of your node > Directory Service Debugger** tab **> Process Kerberos** tab. You can simulate Kerberos authentication for any user by providing user's credentials here.



8. Verify that the client browser supports the setting of cookies. Cookies play a central role in SSO and must be enabled for SSO to succeed. Refer to the following links for more information on enabling the setting of cookies:
   - **Internet Explorer:** http://windows.microsoft.com/en-us/windows-vista/block-or-allow-cookies
   - **Firefox:** http://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences
   - **Safari:** http://support.apple.com/kb/ph5042
   - **Chrome:** https://support.google.com/chrome/answer/95647?hl=en

Related Links

Troubleshooting on page 93

Troubleshooting specific issues

This section lists troubleshooting techniques and solutions for specific Identity Engines (IDE) Single-Sign-On (SSO) issues.

Related Links

Troubleshooting on page 93
Kerberos authentication fails on page 99
SSO authentication fails with external SP on page 104
Realm Mapping URL does not work on page 105
Accessing Realm Mapping URL prompts for a file download, but the file is empty on page 105
Accessing Realm Mapper URL from Internet Explorer prompts for a file download. However, instead of containing the JSON credentials, the file contains HTML error page on page 106

With Kerberos-Basic authentication turned on, accessing the protected URL from a computer not joined to any domain, user is prompted twice for credentials on page 106
My SSO was working fine, until I changed the bound interface / host name, now it no longer works on page 107
SSO works fine in a single node scenario, but fails in an HA scenario on page 108

Kerberos authentication fails

For Kerberos-based Single-Sign-On (SSO) authentication, Ignition Server must have necessary permissions to create a user account and an associated Service Principal Name (SPN) on the Active Directory. The user and SPN records are required to validate the Service tokens presented by the clients who are trying to log in using the Kerberos Tokens.

When configuring the Active Directory, administrators must provide a service account with necessary permissions to create and delete computer and user accounts. The machine account is required to perform MSCHAPv2 based network authentication using RADIUS service. The user account is required to perform Kerberos-based SSO and is created only if the administrator installs the Ignition Aura SSO license and enables SAML Service. The user account is created irrespective of whether you are using ‘Form Based Login’ or ‘SPNEGO/HTTP Basic Authentication Policies.

If there are any issues while creating the records on Active Directory, such as clock skew between Active Directory and Ignition Server, you can detect them by using the **Test Configuration** button in the Active Directory create/edit wizard.

The status field, **SSO Kerberos Ready**, allows you to determine if the Ignition Server is able to create the user account and SPN on the Active Directory and if it is ready to perform Kerberos-based SSO authentication. To access the **SSO Kerberos Ready** field, from the Dashboard, log in to the Ignition Server, go to **Monitor > IP address or name of your node > Directory Service Status** tab **> SSO Kerberos Ready**.

An additional test utility to check if the Ignition Server is able to create the user record and SPN for Kerberos is provided on the Dashboard. This utility is only applicable for the Active Directory type of Directory Services. From the Dashboard, log in to Ignition Server, go to **Troubleshoot > IP address or name of your node > Directory Service Debugger > Process Kerberos.** From the drop-down list, select the appropriate Active Directory, provide user details for which you are trying to perform Kerberos Authentication, and click **Send Request**. The utility tests if SAML is enabled, checks if the Ignition Server is able to communicate with the Active Directory, that a user record and an associated SPN are created on the Active Directory and, performs the Kerberos authentication using the supplied credentials. If any of the preceding conditions fail, an appropriate error message is displayed in the **Results** section.

If the failure occurs because the user record or the associated SPN has not been created, repeat the above test after selecting the **Test Join** check box. This ensures that a forced join is performed to create the user record and associated SPN. The rest of the test is performed as before.

Related Links

Troubleshooting specific issues on page 98
Client configuration issues on page 100

Client configuration issues

If you are using Internet Explorer (IE) or Firefox browsers, you must perform browser-specific configuration.

Fix: Perform browser-specific configuration as specified in the following section Browser-specific configurations on page 100. After performing the browser configuration, close all instances of the browser and restart it to ensure that the configuration changes are applied to the browser.

Fix: Restart browser.

Kerberos authentication may also fail if the client fails to get a service ticket. That could happen if the user password is changed from AD. If that is the case, logging out of the client and logging back in with the new password will fix this issue.

Fix: Logout off the client machine and log in again.

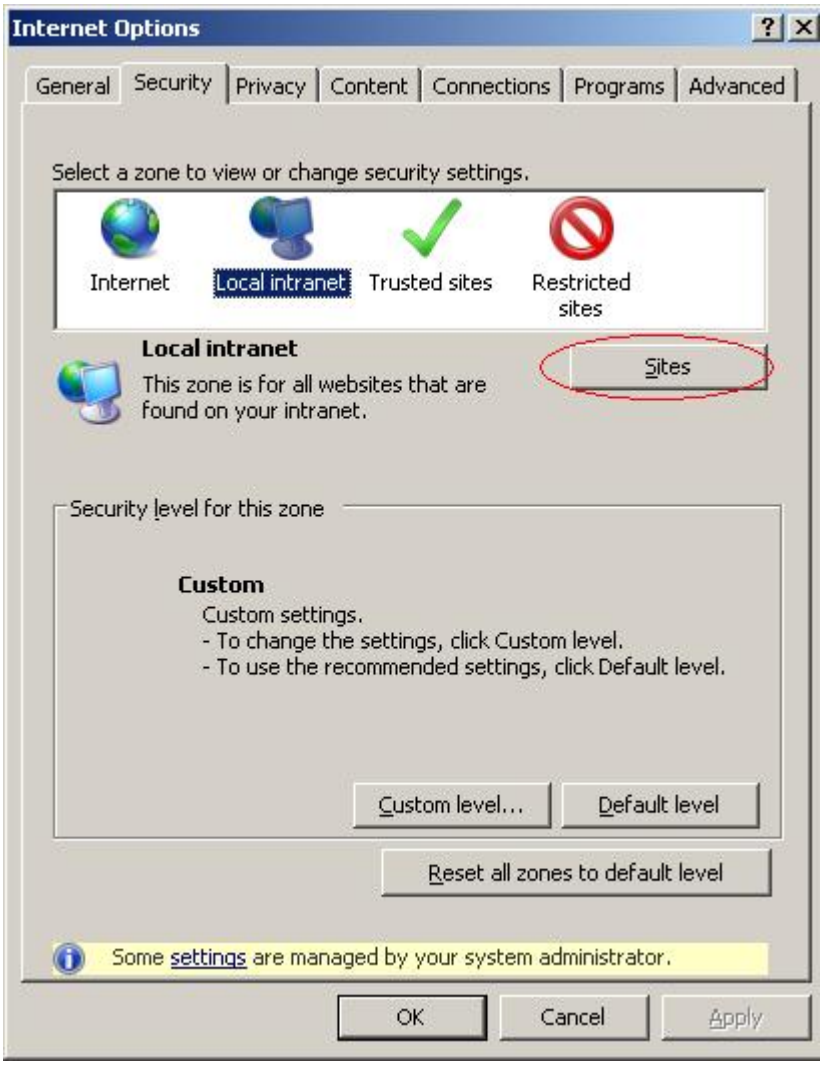
Browser-specific configurations

Internet Explorer:

You must add the Fully Qualified Domain Name (FQDN) of the Identity Provider (IdP) server. You must also ensure that Automatic Authentication Handling is enabled in the browser.

1. From the Internet Explorer menu, select **Tools > Internet Options**.
2. Click the **Security** tab, click **Local intranet**, and click **Sites**.

   The Local Intranet window displays.



3. In the **Local Intranet** window, click **Advanced**.

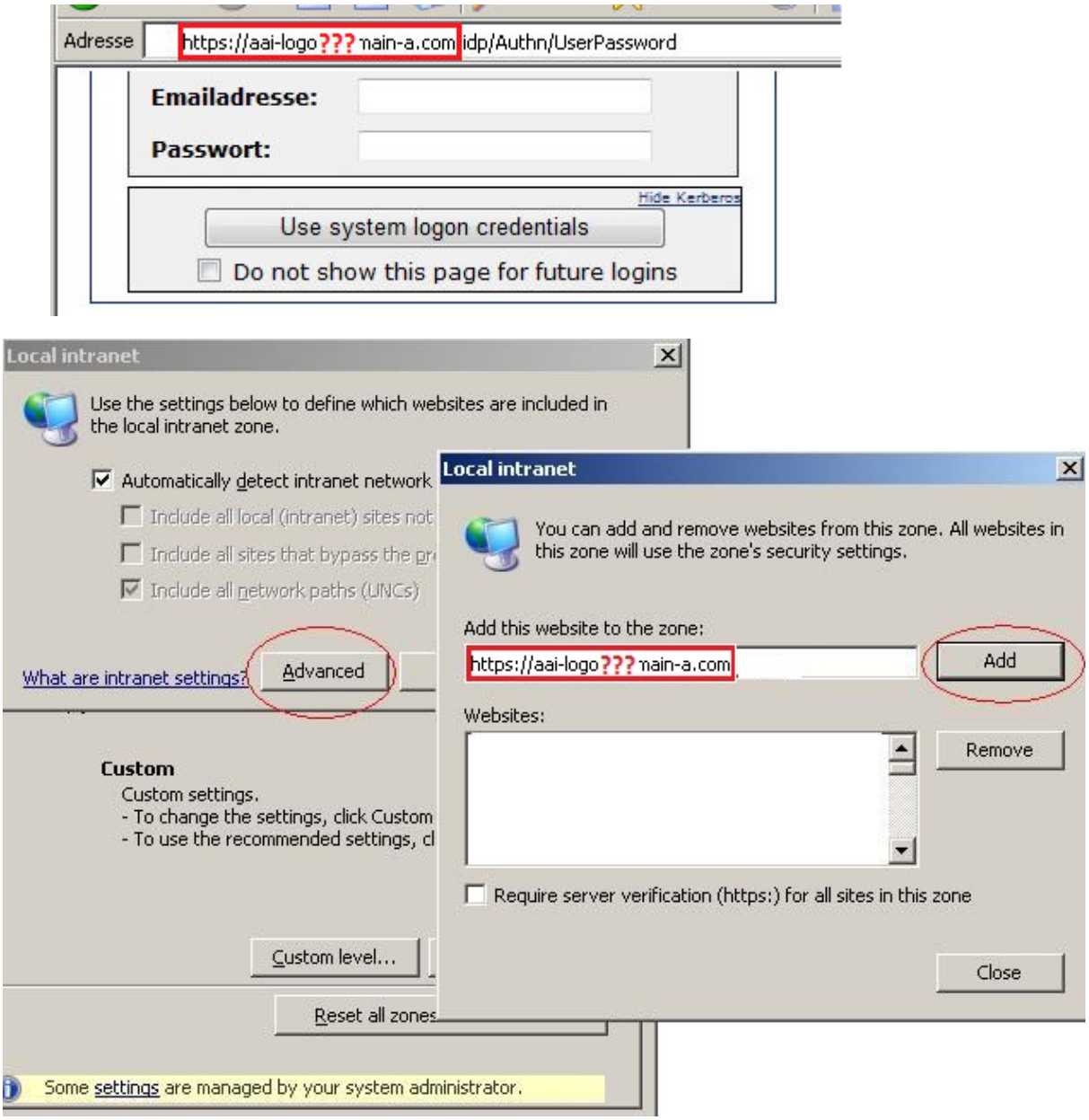
   A dialog box displays.

4. In the **Add this website to the zone** field, enter the FQDN of IdP server and click **Add**.

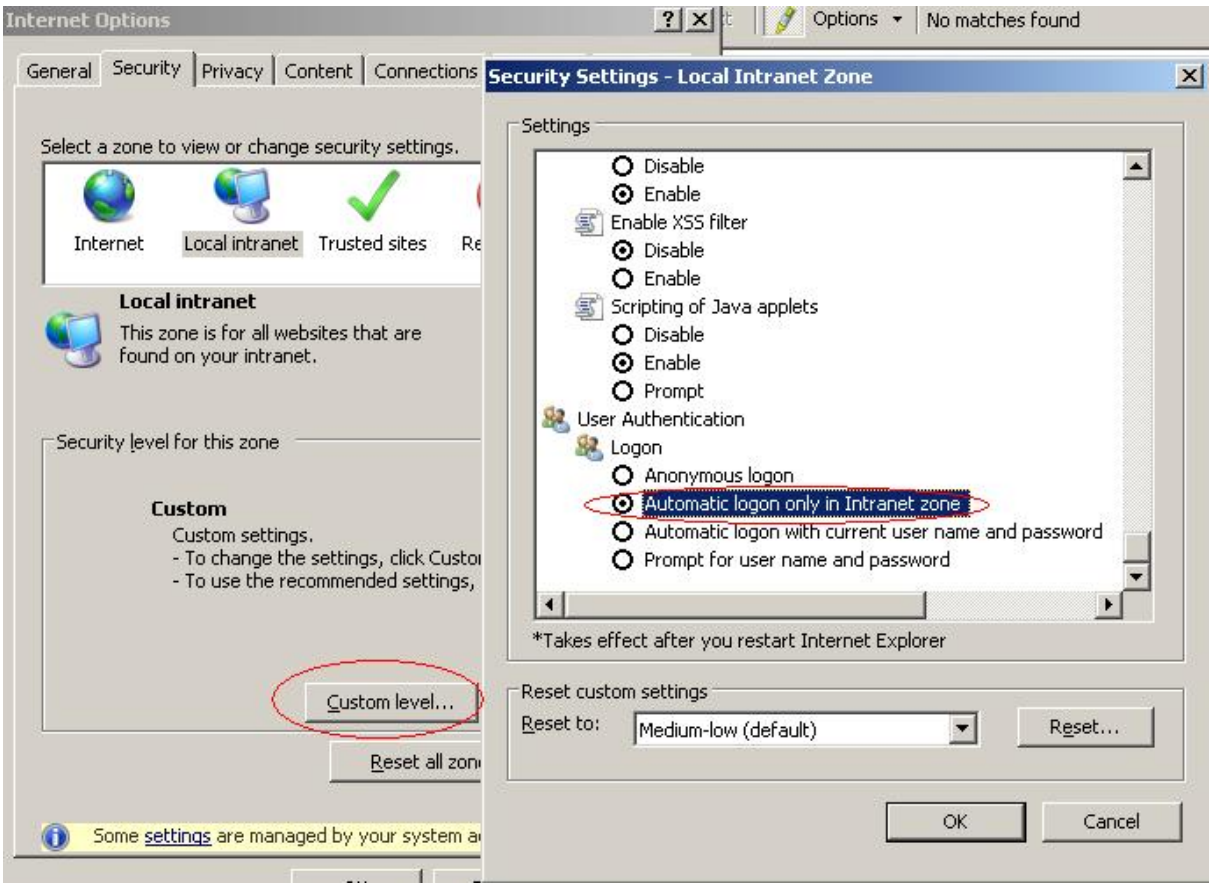
   Wildcards are supported; for example: *.host_b.com.

   Tip:

   You can find the FQDN of the IdP server on the login page.



5. To ensure that Automatic Authentication Handling is enabled in the browser, go to the **Security** tab and click **Custom level**.
6. In the **Settings** section, scroll down to the bottom and ensure that Logon is set to **Automatic logon only in Intranet zone**.



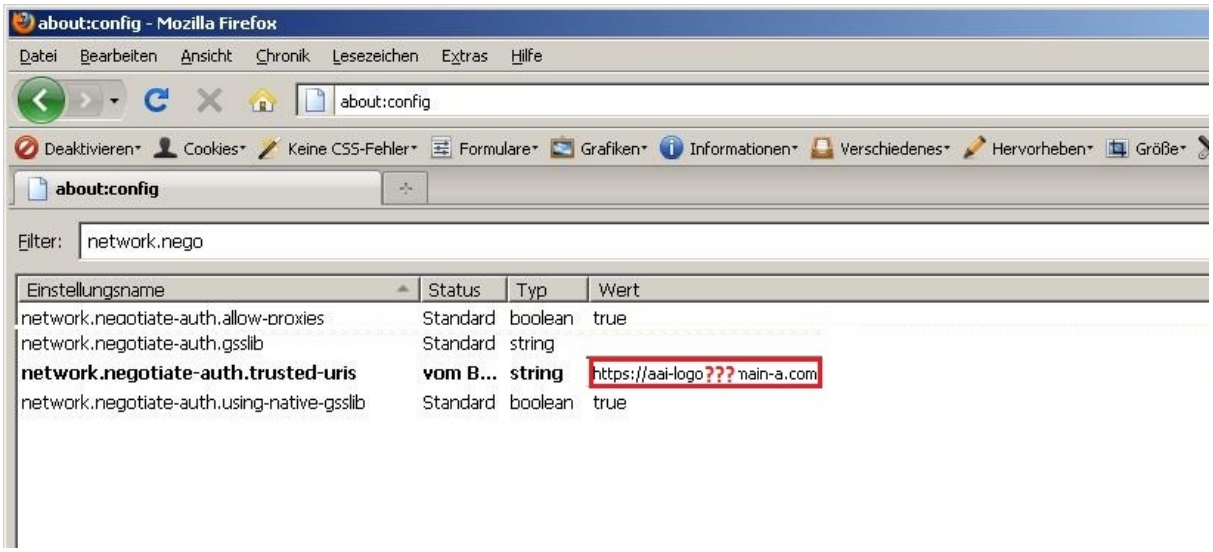
Firefox:

You must add the FQDN of the IdP server.

1. To access the Firefox settings, enter **about:config** in the Address bar and press **[Enter]**.

   A list of customizable preferences for the current installation of the browser displays.

2. Add the FQDN of the IdP server into the list of trusted URIs: **network.negotiate-auth.trusted-uris** - FQDN of the IdP Server (for example: https://idengines.sv.avaya.com).



Safari:

The Safari browser does not require any special configuration.

Chrome:

The Chrome browser does not require any special configuration.

Related Links

Kerberos authentication fails on page 99

SSO authentication fails with external SP

Use the following troubleshooting techniques to resolve this issue.

The clocks on Service Provider and Ignition Server must be in sync.

Fix: Adjust the clocks on Ignition Server and Service Provider to the same time or sync them to the same NTP server.

Make sure the Identity Provider (IdP) meta data file on the Service Provider is the latest. Also ensure that the SP meta data file on the IdP is the latest. Be sure to update the corresponding metadata files if any configuration changes have been made since the metadata files were last exchanged.

Fix: Update Identity Provider configuration with the latest Service Provider metadata and update Service Provider configuration with the latest Identity Provider metadata.

Confirm if the Authorization Policy allows the release of at least one Outbound Value. This will usually be user principal.

Fix: Configure release of at least one Outbound Value as explained in the following sections: Mapping a Directory Attribute to a User Virtual Attribute on page 60 and Associating Outbound Attributes with the Authorization Policy on page 62.

If SSO succeeds for a user in the local store, but fails for a user in the AD, ensure that the user principal Outbound Value is mapped to some attribute value of the AD like user id. You can perform this configuration in Dashboard under **Configuration > Site > Site Configuration > Directories >Virtual Mapping > User Virtual Attributes**.

Fix: Create mapping for the Outbound Value representing user principal to an attribute value of AD as explained in Mapping a Directory Attribute to a User Virtual Attribute on page 60.

Related Links

Troubleshooting specific issues on page 98

Realm Mapping URL does not work

If using a non-standard port for SAML (the default is 443), ensure when you are accessing the Realm Mapper URL, either through a browser or through a thick client like Avaya Flare, that the correct port number is being used. For example, if the SAML port is configured to be 5778, the Realm Mapper URL would be https://<FQDN of Ignition Server>>:5778/RealmMapper/getCredentials.

Fix: Use the correct Realm Mapper URL.

Related Links

Troubleshooting specific issues on page 98

Accessing Realm Mapping URL prompts for a file download, but the file is empty

This condition could occur if there is no Realm Mapping data available for the user attempting to log in. Use the following troubleshooting techniques to resolve this issue.

There is no System Manager added to Ignition Server.

Fix: Add a System Manager to Ignition Server as explained in Connecting Ignition Server to your Avaya Aura® System Manager on page 46 .

System Manager is not syncing to AD that has been added to IDE.

Fix: Do the following:

1. Go to the **Monitor** tab.
2. Select the node under **Site 0**.
3. Select the **Directory Services** status tab.
4. Select the directory service corresponding to the System Manager.
5. Click **Refresh Cache**.

The user was added to AD after the System Manager was added to Ignition Server. (**Hint:** If this is the case, it is possible that the System Manager cache has not been refreshed since the user was added to AD. By default, this refresh interval is 24 hours.)

Fix: Perform a manual refresh of the System Manager cache to fetch fresh data. To perform a manual refresh, go to **Monitor > IP address or name of your node > Directory Services Status**. Select the System Manager and click **Refresh Cache**. Verify that the realm mapping data for the user is present by going to **Configuration > Site > Site Configuration >Directories > Internal Store > Realm Mapper Cache** and search for the user.

Note: It could take up to a couple of minutes to fetch all of the data from System Manager.

Related Links

Troubleshooting specific issues on page 98

Accessing Realm Mapper URL from Internet Explorer prompts for a file download. However, instead of containing the JSON credentials, the file contains HTML error page

This problem is caused because the **download files automatically** option is disabled in Internet Explorer.

Fix: Enable the **download files automatically** option. To enable this option, from the Internet Explorer menu, select **Tools > Internet Options >Security >Local Intranet > Custom level**.

Related Links

Troubleshooting specific issues on page 98

With Kerberos-Basic authentication turned on, accessing the protected URL from a computer not joined to any domain, user is prompted twice for credentials

This problem occurs when using Internet Explorer (IE) and Chrome and from a non-domain joined PC. However, this problem does not occur when using Firefox as the browser. This problem occurs because the browser cannot find any Kerberos tickets when the Identity Provider (IdP) sends a SPNEGO challenge, so it prompts the user for the credentials. This first dialog for credentials is coming from the browser. This authentication fails (irrespective of the credentials used) as the browser is sending a password and not a Kerberos ticket. So the IdP challenges again, this time just for BASIC authentication. Then the browser prompts again (this time because IdP is asking for it. You can confirm that this time the dialog is because of IdP challenge by looking at the prompt string. The prompt string will contain the words “IDE realm”). When the user enters the correct credentials, the authentication succeeds.

Fix: To avoid getting prompted twice, perform the following browser-specific configuration.

Internet Explorer

To avoid getting prompted twice, perform the following browser configuration on Internet Explorer.

1. From the Internet Explorer menu, select **Tools > Internet Options**.
2. Click the **Security** tab, click **Local intranet**, and click **Custom level**.
3. Scroll all the way down to **User Authentication > Logon** and select **Automatic logon with current user name and password** and click **OK**. This ensures that you will get prompted only once when the IdP asks for it.

Firefox

Firefox does not need any configuration as it is intelligent enough to prompt only once on the IdP challenge.

Safari

Safari does not need any configuration as it is intelligent enough to prompt only once on the IdP challenge.

Chrome

To avoid getting prompted twice, perform the following browser configuration on Chrome.

1. From the Chrome menu, select **Settings**.
2. Click **Show advanced settings**.
3. Under **Network**, click **Change proxy settings**.
4. Click the **Security** tab, followed by **Local intranet**, **Sites**, and **Advanced**.
5. Add the URL to the zone and click **Close**.
6. Click **OK** and then click **OK** again.

   This ensures that you will get prompted only once when the IdP asks for it.

Related Links

Troubleshooting specific issues on page 98

My SSO was working fine, until I changed the bound interface / host name, now it no longer works

Use the following troubleshooting techniques to resolve this issue.

This issue could be caused because you forgot to update your Service Provider with the new Identity Provider (IdP) metadata file. Whenever there is a host name change or the bound interface for SAML service changes, Ignition Server regenerates the metadata file.

Fix: Update your Service Provider configuration with the most recent IdP metadata file.

Sometimes this regeneration of metadata on IdP can fail for some reason or can take a long time to happen. You can verify if the new metadata file has been generated after the configuration change by examining the name of the Identity Provider under **Configuration > Site > Site Configuration >**

SSO > Identity Provider. This name should correspond to the new name. If it has not been updated, restarting Ignition server should solve this issue.

Fix: Restart Ignition server.

Related Links

Troubleshooting specific issues on page 98

SSO works fine in a single node scenario, but fails in an HA scenario

Use the following troubleshooting techniques to resolve this issue.

First verify if the Identity Provider (IdP) is active on both the nodes by going to **Configuration > Site > Site Configuration > SSO > Identity Provider**. It should list two IdPs if it is a HA in a non-VIP mode. If it is HA in a VIP mode, there will be only one IdP listed here.

Verify by looking at the details of the IdPs to make sure that the entity ids are correct for them.

This issue could be caused because there is no route between your HA ports.

Fix:

1. Repair the network connection between the HA port on your first Ignition Server and the HA port your second Ignition Server.
2. Launch a new session of Dashboard and log in to the first Ignition Server. (Leave the existing Dashboard session running, but ignore it for now.)
3. In the new session of Dashboard, ping the HA port of the second Ignition Server. To do this, click the **Troubleshoot** button at the top of the Dashboard window; click on the *first* Ignition Server's node name or IP address in the hierarchy tree; click **Network** and go to **Ping Test**; type the IP address of the *second* Ignition Server's HA port, set the number of packets to send, and click **Start**. If the test fails, fix your network connection. If it succeeds, continue to the next step.
4. In the new session of Dashboard, log out from the *first* Ignition Server and log in to the *second* Ignition Server. Perform another ping test: Click the **Troubleshoot** button at the top of the Dashboard window; click on the *second* Ignition Server's node name or IP address in the hierarchy tree; click **Network** and go to **Ping Test**; type the IP address of the *first* Ignition Server's HA port, and click **Start**. If the test fails, fix your network connection. If it succeeds, continue to the next step.
5. Close the new session of Dashboard.

Related Links

Troubleshooting specific issues on page 98

Troubleshooting Flare for IPad specific issues

This section lists troubleshooting techniques and solutions for specific Flare for IPad Single-Sign-On (SSO) issues.

Related Links

[Troubleshooting](#) on page 93
[User provided correct user credentials but failed to perform unified login on iPad Flare](#) on page 109
[IM not working with Single-Sign-On](#) on page 116

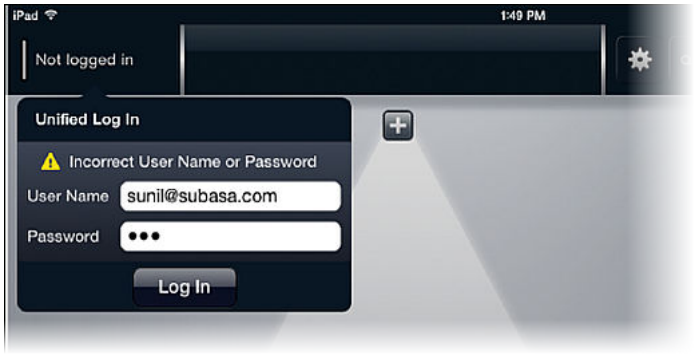
User provided correct user credentials but failed to perform unified login on iPad Flare

Condition

This condition can occur for one of two reasons:

- authentication or authorization failure
- authentication and authorization success, but Realm Mapping data is missing or incorrect

Look at the iPad to see which error message Flare displays:



If Flare displays the message “Incorrect User Name or Password”, an authentication or authorization failure has occurred. If Flare displays the message “Untitled log in error”, the Realm Mapping data is missing or incorrect.

Solution

Fix authentication or authorization failure

1. Check the Dashboard access logs. Click the **Monitor** tab and select the site name. Click the **Access** tab under **Log Types**.

   Each successful login request results in two operations: SAML authentication and SAML authorization. Each of these operations generate a log. If the SAML authentication fails, SAML authorization is not attempted, resulting in only one log corresponding to SAML authentication.

2. Double-click the authentication log and check the contents. The authentication log provides failure information. Take corrective action as necessary.

Confirm missing or incorrect Realm Mapping data

To confirm that the Realm Mapping data is missing or incorrect, double-click the authorization log and check the contents. If the authorization result is successful, the authorization log lists `Outbound-Avaya-Saml-RM-Data` under outbound attributes. If you do not see any outbound attributes, the user's corresponding Realm Mapping data is missing or incorrect.

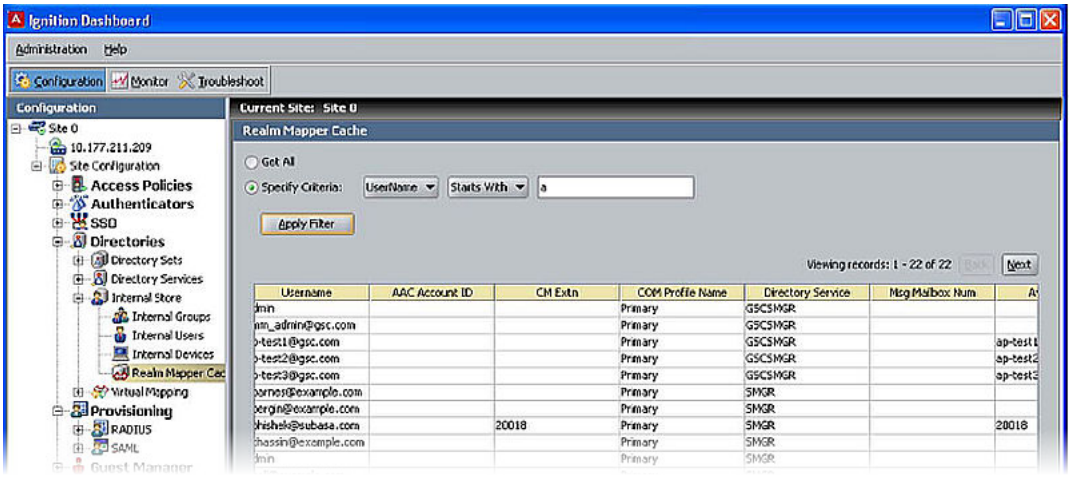
Obtain missing Realm Mapping data

1. Ensure that the Ignition Server is able to connect to SMGR and to read Realm Mapping data. From the Ignition Dashboard, click the **Monitor** tab, select the node, and click the **Directory Services Status** tab. The SMGR listed should have a blue check mark under **Connected** and **Realm Mapper Cache**.

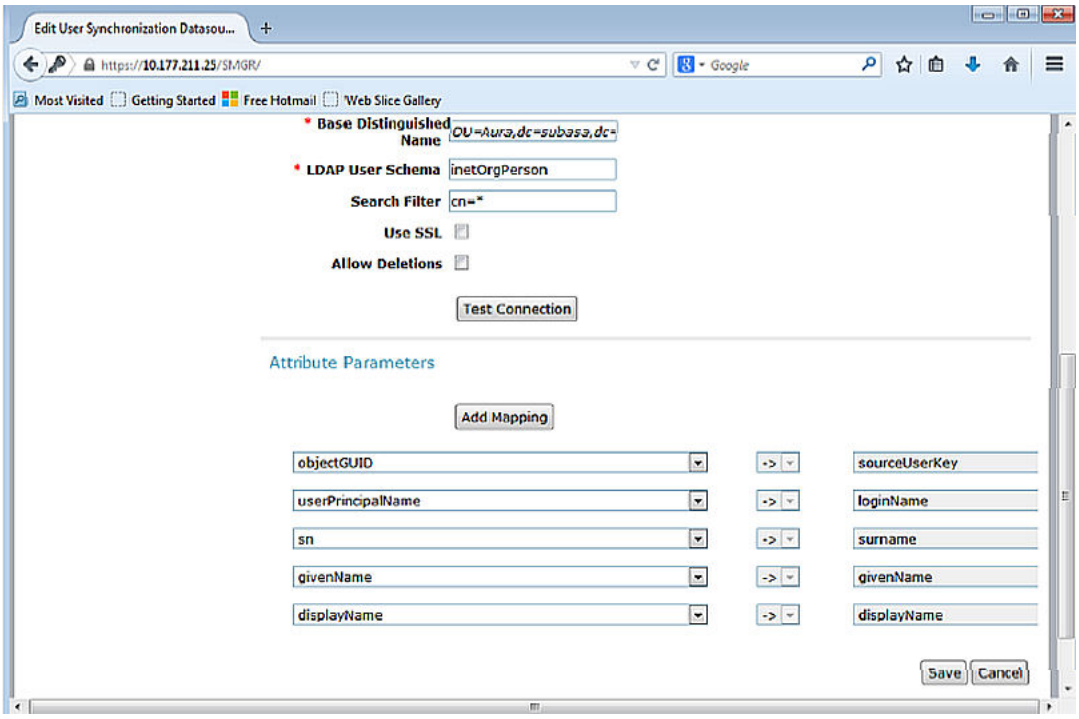
   If you do not see the check mark under **Realm Mapper Cache**, caching loading may be in progress. Wait for the cache load to complete, or, to retry the load, select the SMGR entry and click **Refresh Cache**. The refresh time depends on the size of the SMGR data; it takes approximately three to five minutes for 20,000 records.

2. Once the cache load is complete, check the user records. In the Dashboard **Configuration** tree, expand the **Site Configuration** > **Directories** > **Internal Store** > **Realm Mapper Cache** folders.

   You should see data that is similar to the following example. If the user records or Realm Mapping data are not present, there is likely a mismatch of attributes between System Manager and Active Directory (AD).



3. See the following example for the correct mapping between AD and System Manager attributes. Note that, in most cases, the userPrincipalName attribute of AD is mapped to the loginName attribute of System Manager. However, in some cases, the userPrincipalName in AD may not be populated. In these cases, the mail attribute of AD is used for mapping to the loginName attribute of System Manager.



Define correct Realm Mapping data

While replying to an authorization request, Ignition Server uses the incoming client user ID and finds the corresponding Realm Mapper entry. If the user record realm does not match the realm as configured on SMGR, the mapping fails.

This situation can happen when the users in System Manager are not synchronized up from AD but instead have been created manually in System Manager.

For example, consider a scenario where the users in System Manager have been created manually with a realm “domain.com” and the users in AD have the realm “global.domain.com”. Now there are two possibilities:

- the user logs in as <user>@domain.com
- the user logs in with userid <user>

In both the cases, Ignition Server is able to authenticate the user against the AD as follows:

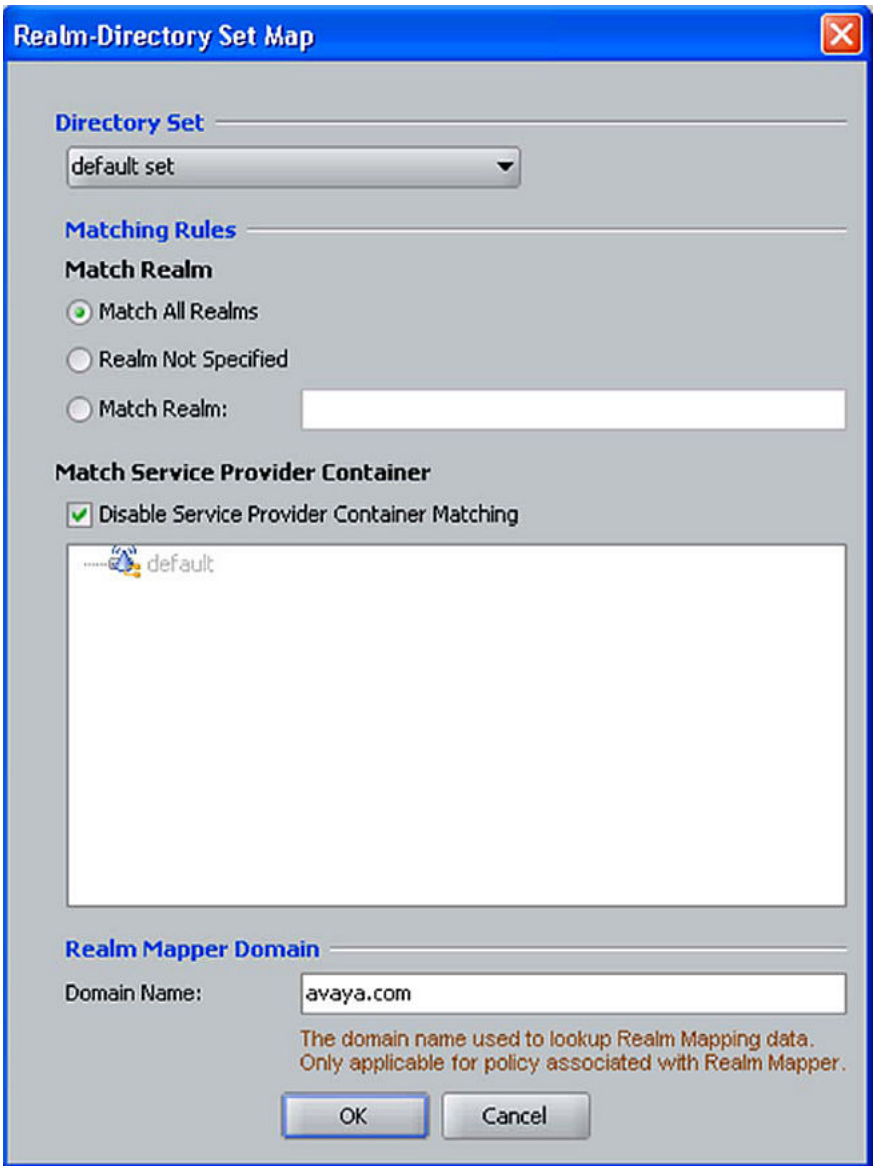
- If the user has logged in as user@domain.com, Ignition Server finds a matching record in Realm Mapper cache, as the domain in System Manager is domain.com.
- If however, the user logs in with userid <user>, Identity Engines behaves as follows:
  - The system first searches for a match in the Realm Mapper cache for "<user>@<AD domain>" (in this example, "<user>@global.domain.com"). In this example, the AD domain and SMGR domains are not the same, so no match is found.

- The system then searches for "<user>@<user domain>". In this example, since there is no domain in the request, it cannot find a matching entry.
- If both conditions 1 and 2 are not met, then the system uses the domain name as defined in the identity routing. You must therefore configure the correct domain in the identity routing.

1. In the Dashboard **Configuration** tree, expand the **Site Configuration** > **Access Policies** > **SAML** folders, and select the Access Policy.
2. Click the **Identity Routing** tab.
3. Click **Edit**.

   The **Edit Identity Routing Policy** window displays.
4. Select an existing entry and click **Edit** to edit it, or click **New** to create a new entry.
5. Select the **Realm-Directory Set Mapping**, and click **Edit** to edit an existing entry, or click **New** to enter a new entry.

6. In the **Realm Mapper Domain** section, enter the domain as defined on SMGR in the **Domain Name** field. In the following example, the domain is “avaya.com”.



Verify Realm Mapping data

After defining the correct Realm Mapping data, if the login through Flare still does not work, check if the correct Realm Mapping data is being returned for the user who is logging in. Use a browser to perform a WebSSO to the Realm Mapper URL. If the configuration is correct, either the browser will directly show the data (Firefox, Chrome) or prompt to download a file containing Realm Mapping data. This Realm Mapping data is in the JSON format.

1. In the Dashboard, select the site, click the **Services** tab, and then click the **SAML** tab. Make note of the Access Policy in place under the **Realm Mapping** section.

2. In the **Configuration** tree, expand the **Access Policies** > **SAML** folders, and select the Access Policy.
3. Click the **Authentication Policy** tab, click **Edit**, and check if Web SSO is enabled. The default is enabled. If necessary, select either **SPNEGO/HTTP Basic Authentication** or **Form Based Login** to enable Web SSO.
4. Type the following URL into a browser: https://<IDE hostname>:<port number (if not default port)>/RealmMapper/getCredentials

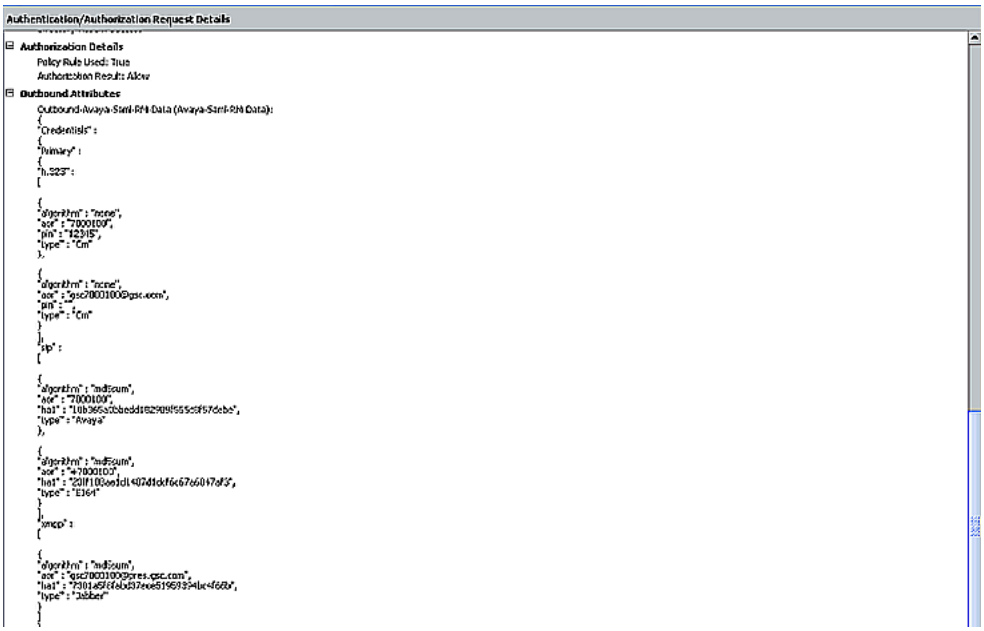
   For example:

   - running default port: https://ide.domain.com/RealmMapper/getCredentials
   - running port 4444: https://ide.domain.com:4444/RealmMapper/getCredentials

   If the configuration is correct, you will see a JSON type string returned as the response, similar to the following example:


```
{
   "Credentials" :
   {
         "Primary" :
         {
               "h.323" :
               [

                     {
                           "algorithm" : "none",
                           "aor" : "20010",
                           "pin" : "",
                           "type" : "Cm"
                     }
               ],
               "sip" :
               [

                     {
                           "algorithm" : "md5sum",
                           "aor" : "20010",
                           "ha1" : "18374db283b991317da5116fcf317fda",
                           "type" : "Avaya"
                     },

                     {
                           "algorithm" : "md5sum",
                           "aor" : "+20010",
                           "ha1" : "d0b87e9b844f35080162b365acb3e723",
                           "type" : "E164"
                     }
               ],
               "xmpp" :
               [

                     {
                           "algorithm" : "md5sum",
                           "aor" : "20010@ps.sip.avaya.local",
                           "ha1" : "40498b6e1ddf6a47a9bd24f3197bb60e",
                           "type" : "Jabber"
                     }
               ]
         }
   }
}
```

Alternatively, you can see the response on the Ignition Server in the Access logs for SAML Authorization, under Outbound Values:



Further troubleshoot Active Directory and System Manager mismatch

If the expected JSON response was not returned, there is still a mismatch between Active Directory and System Manager attributes. Confirm all of the following information.

1. Confirm that outbound value `Avaya-RM-Data` is present and is being returned in the allow response in the policy.
2. Confirm the presence and mapping of two outbound attributes for outbound value `Avaya-RM-Data`. In the Dashboard **Configuration** tree, expand the **Provisioning** > **SAML** > **Outbound Values** folders. Select **Avaya-RM-Data** and click **Edit**. Confirm that the following two attributes are present:
   - `Outbound-Avaya-Saml-RM-Data` mapped to `User Attributes.avaya-rm-data`
   - `Outbound-Avaya-Saml-Principal-Name` mapped to `User Attributes.avaya-rm-principal-name`
3. Confirm the mapping of two outbound attributes. In the Dashboard **Configuration** tree, expand the **Provisioning** > **SAML** > **Outbound Attributes** folders. Confirm that the following two attributes are present:
   - `Outbound-Avaya-Saml-Principal-Name` mapped to `Avaya-Saml-Principal-Name`
   - `Outbound-Avaya-Saml-RM-Data` mapped to `Avaya-Saml-RM-Data`

   Note that these two attribute names are populated in the logs for successful logins.
4. Confirm that the following user virtual attribute is *not* mapped to anything. In the Dashboard **Configuration** tree, expand the **Directories** > **Virtual Mapping** > **User Virtual Attributes** folders. Click the `ayaya-rm-data` attribute and confirm that it is not mapped to anything.

Ignition Server automatically populates this attribute with the value of `SAML Attribute Avaya-Saml-RM-Data`

Click the `avaya-rm-principle-name` attribute and check the mapping. For internal store it should be mapped to the attribute `username` and for an AD it should be mapped to the AD attribute `userPrincipalName`. Note that there are cases when this attribute in AD could be different. For example, in some AD deployments the `userPrincipalName` attribute is not populated. In those cases, the `mail` attribute can be used..

If after confirming all settings, the problem persists, locate the debug logs, which may provide further useful information.

Debug if Realm Mapping data verification fails

1. Enable debug logging. In the Dashboard, click the **Troubleshoot** tab. On the right side of the tab, click **Actions** and select **Enable Debug Logs** and **Enable Advanced Log Levels**.
2. Select the node and click the **Logging** tab, and then click the **Advanced Levels** tab.
3. Click **Edit**, then click **Add Logger** and select **Debug.Protocol**, click **OK**, and then on right column select **Trace** from the drop-down menu.
4. Check the Dashboard debug logs. Click the **Monitor** tab and select the site name. Click the **Debug** tab under **Log Types**. Look for a log called `Skipping Outbound Attribute Outbound-Avaya-Saml-RM-Data because….`
5. Look for the logs in that region to see the value of the attribute `Outbound-Avata-Saml-Principal-Name` that is being looked up in the Realm Mapper cache. This would be the `<username>@<domainname>` that was entered in Flare or the browser and was authenticated against the AD.

   Note that you can enter a username either with or without the domain (<username> or <username>@<domain>.com) to log in through Flare. Ignition Server accepts the login in both forms.
6. Check if there is a username attribute mismatch.

   Search for a record for the expected username in `Saml-Principal-Name`. If a record for that username is not present, check the Realm Mapper cache for a record of the user. Look at the record to see what username is specified.

Related Links

Troubleshooting Flare for IPad specific issues on page 109

IM not working with Single-Sign-On

For IM on Flare to work in Single-Sign-On mode, ensure that the Digest-MD5 mechanism for SASL authentication is enabled on the Presence Server.

Related Links

Troubleshooting Flare for IPad specific issues on page 109