Avaya Identity Engines Ignition Server Getting Started Configuration

Release 9.0
NN47280-300
Issue 04.01
March 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. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

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 Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, 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

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.

Trademarks

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.

Contents

Chapter 1: Introduction 7
- Purpose 7
- Related resources 7
  - Documentation 7
  - Training 8
  - Avaya Mentor videos 8
- Support 8

Chapter 2: New in this release 11
- Features 11
  - Aura® Single-Sign-On license 11
  - Avaya Product Licensing and Delivery System (PLDS) support 12
  - Enterprise Level Administration 12
- Other changes 12

Chapter 3: Getting started 15
- VMware ESXi server 15
- Installing the Ignition Server virtualization appliance 16
- Preventing automatic VMware tools updates 21
- Checking the VMware Tools status (ESXi 5.x) 22
- Configuring the Ignition Server virtualization appliance 23
- Installing the Ignition Dashboard desktop application 24
- Running the Dashboard 31
- Obtaining the Ignition Server Serial Number 32
- Obtaining PLDS licenses 34
- Obtaining KRS Licenses 34
- Installing the license 35
- Setting up the Service Port (Optional) 39
- Setting the admin password and set user, site, and node names 40
- Further configuration 41

Chapter 4: Configuration 43
- Before you begin 43
- Make settings on the Ignition Server appliance 44
- Create a RADIUS access policy 48
- Create a user in the internal user store 50
- Set up your connection to a user store 51
  - Connecting to Active Directory 52
  - Connecting to LDAP 68
  - Troubleshooting AD and LDAP connections 72
- Setting up a RADIUS proxy server 78
  - Creating a RADIUS proxy authentication service 78
  - Add the RADIUS proxy server to a directory set 79
  - Create an Access Policy that includes the RADIUS proxy server 80
  - Proxying of MAC authentication requests 80
  - Configuration on the remote proxy server 80
- Create a directory set 80

Create virtual groups.... 83
Create authenticators.... 86
    Editing authenticators.... 89
Set your authentication policy.... 90
Set your identity routing policy.... 92
Set your authorization policy.... 94
    Authorization policy—Example for embedded store users.... 94
    Authorization policy—Example for AD users.... 97
Test your configuration.... 100
    Checking user lookup and authentication.... 100
    Use NTRadPing as a test authenticator.... 101

Chapter 1: Introduction

Purpose

The *Avaya Identity Engines Ignition Server Getting Started* guide explains how to install and configure the Avaya Identity Engines Ignition Server. This guide is written for network administrators who want to quickly install and configure the Ignition Server.

The *Avaya Identity Engines Ignition Server Getting Started* guide explains a simple configuration, and the *Avaya Identity Engines Ignition Server Administration* guide provides a complete reference showing other configuration options.

Related resources

Documentation

See the following related documents.

Title	Purpose	Link
Avaya Identity Engines Ignition Server Administration	All configuration options	http://support.avaya.com/
Configuring and Managing Avaya Identity Engines Single-Sign-On	Configuration, management, and deployment	http://support.avaya.com/
Avaya Identity Engines Ignition Guest Manager Configuration	Installation, configuration, and management	http://support.avaya.com/
Avaya Identity Engines Ignition CASE Administration	Installation, configuration, and deployment	http://support.avaya.com/
Avaya Identity Engines Ignition Access Portal Administration	Installation, configuration, and deployment	http://support.avaya.com/

Title	Purpose	Link
Avaya Identity Engines Ignition Analytics	Installation, configuration, and maintenance	http://support.avaya.com/
Avaya Identity Engines Ignition Server Release Notes	Reference	http://support.avaya.com/

Training

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

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.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

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

Chapter 2: New in this release

The following sections detail what is new in *Avaya Identity Engines Ignition Server Getting Started* for Release 9.0.

Features

See the following sections for information about feature changes.

Related topics:

Aura® Single-Sign-On license on page 11
Avaya Product Licensing and Delivery System (PLDS) support on page 12
Enterprise Level Administration on page 12

Aura® Single-Sign-On license

Identity Engines Aura® Single-Sign-On (IDE SSO) is a new licensed feature in Identity Engines Release 9.0. Single-Sign-On (SSO) provides full-fledged Identity Management that allows Identity Engines to not only control network access for a user and devices, but also provides granular policy-based access control to the resources (applications) contained within an enterprise network. SSO supports standards-based Single-Sign-On capabilities and allows various Web applications to make informed authorization decisions for individual access to protected online resources in a privacy-preserving manner.

You must apply the idEngines® Aura® Single-Sign-On license to enable this feature. This license requires at a minimum an Identity Engines Ignition Sever Base license of any size (for example, Ignition Server Base LITE, SMALL, or LARGE license). A single Identity Engines Aura® Single-Sign-On license is required for either a standalone deployment of the Ignition Server or a High Availability (HA) deployment of a pair of Ignition Servers.

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.

For more information, see *Configuring and Managing Avaya Identity Engines Single-Sign-On*, NN47280–502.

Avaya Product Licensing and Delivery System (PLDS) support

Avaya Identity Engines support the KeyCode Retrieval System (KRS) based licensing model. Starting with Identity Engines Release 9.0, Identity Engines support the Avaya PLDS licensing model in addition to KRS.

The Avaya Product Licensing and Delivery System (Avaya PLDS) provides customers, Business Partners, distributors, and Avaya Associates with easy-to-use self-service 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:**
>
> There are important differences between KRS licenses and PLDS license. For more information, see Installing the license on page 35.

For more information on this feature, see Obtaining the Ignition Server Serial Number on page 32 and Obtaining PLDS licenses on page 34.

Enterprise Level Administration

The Enterprise Level Administration feature of Identity Engines (IDE) Ignition Server offers more granularity in terms of administration. Enterprise Level Administration introduces a Role-based Access Control (RBAC) approach to the IDE. By associating a role to a user, IDE can qualify different types of administrators and map them to the functionality that is pertinent to their administration interest or controlled access for a given IDE instance.

Currently, there is only one login account to the IDE. The user of this account is the equivalent of a super-user on Dashboard. This account has no restrictions on configuration or monitoring of the IDE.

As network administration grows in complexity, there is an increasing need to limit or define the capabilities of specific types of administrators for an IDE Server. One administrator can focus on system monitoring while another focuses on system management such as upgrading images and saving configurations. This approach creates boundaries for administrators to work autonomously from one another, and limits administrators to only specifically-defined parts of the system.

Other changes

See the following sections for information about changes that are not feature-related.

New introduction chapter

Release 9.0 replaces the Customer service chapter with a new Introduction chapter with information on Documentation, Training, Avaya Mentor Videos, and Support.

New screen shots

Release 9.0 updates screenshots and information in the following procedures:

- Preventing automatic VMware tools updates on page 21.
- Checking the VMware Tools status (ESXi 5.x) on page 22.
- Installing the Ignition Dashboard desktop application on page 24.

Chapter 3: Getting started

Use this chapter to perform these Avaya Identity Engines Ignition Server (AIEIS) appliance installation and configuration tasks. Perform your set-up in the following phases:

1. Installing the Ignition Server virtualization appliance on page 16
2. Preventing automatic VMware tools updates on page 21
3. Checking the VMware Tools status (ESXi 5.x) on page 22
4. Configuring the Ignition Server virtualization appliance on page 23
5. Installing the Ignition Dashboard desktop application on page 24
6. Running the Dashboard on page 31
7. Obtaining the Ignition Server Serial Number on page 32
8. Obtaining PLDS licenses on page 34 or Obtaining KRS Licenses on page 34
9. Installing the license on page 35
10. Setting up the Service Port (Optional) on page 39 and Setting the admin password and set user, site, and node names on page 40
11. Further configuration on page 41

VMware ESXi server

Hardware platforms supported by VMware's ESXi Servers versions 5.0 and 5.1 are supported. The VM requires an x86_64 capable environment, a minimum of 4 GB of memory, a minimum of 250 GB of available disk storage (thin provisioning is allowed), a minimum of four CPUs, at least one physical NIC card (preferably three NICs), and three Logical NIC cards. VMware lists on its site supported hardware platforms for ESXi.(http://www.vmware.com)

Installation on a VMware ESXi server is done using an OVA file, which already incorporates the OS Red Hat Enterprise Linux.

Reminder: Avaya provides the Identity Engines Ignition Server and Ignition Access Portal as Virtual Appliances. Do not install or uninstall any software components unless Avaya specifically provides the software and/or instructs you to do so. Also, do not modify the configuration or the properties of any software components of the VMs (including VMware Tools) unless Avaya documentation and/or personnel specifically instructs you to do so. Avaya does not support any deviation from these guidelines.

⚠ **Warning:**

Do not install or configure VMware Tools or any other software on the VM shipped by Avaya:

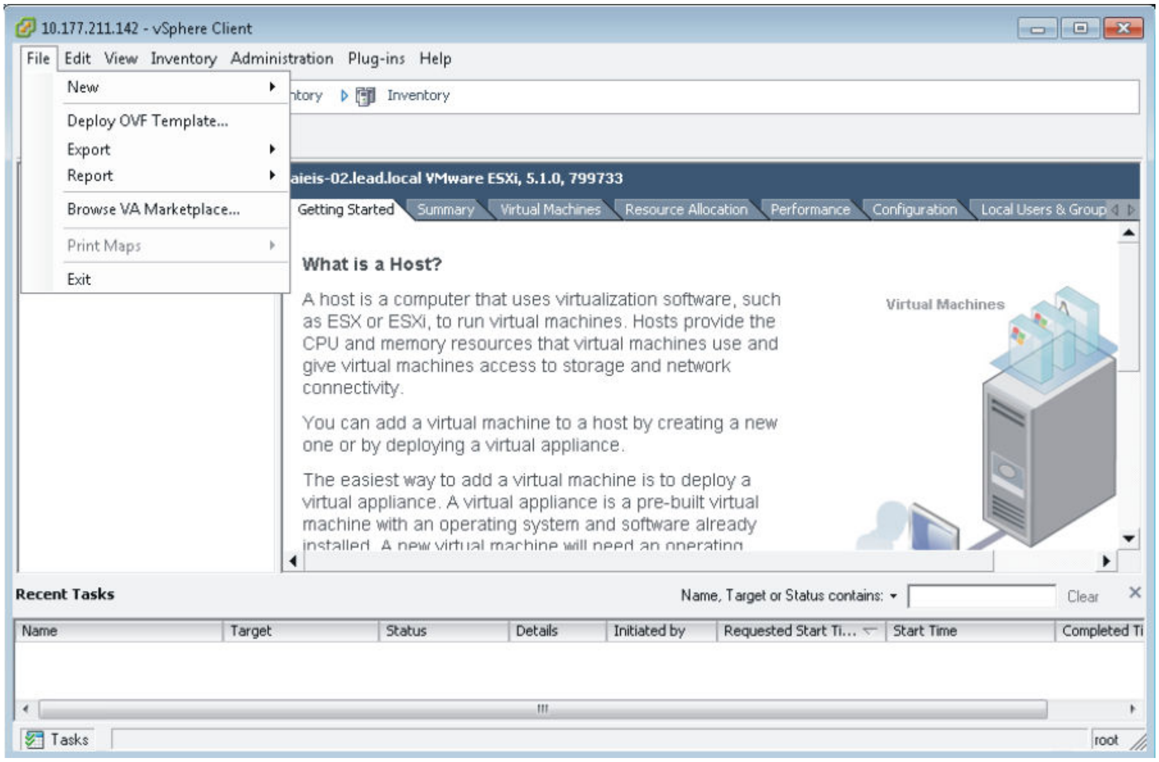
- Avaya does not support manual or automated VMware Tools installation and configuration on Avaya supplied VMs.
- Turn off automatic VMware Tools updates if you have enabled them. Refer to the instructions in Preventing automatic VMware tools updates on page 21 to disable automatic updates and to check if you have accidentally installed VMware tools.
- Avaya determines which VMware Tools to install and configure. When required, Avaya provides these tools as part of the installation or package upgrade procedures. Avaya provides these tools because VMware Tools configures the kernel and network settings and unless Avaya tests and approves these tools, Avaya cannot guarantee the VM will work after the tool is installed and configured.
- Avaya does not support the installation of any VMware specific, RHEL specific, or any third party vendor package or RPM on its VM other than what Avaya ships as a package, image, or OVF.

Installing the Ignition Server virtualization appliance

Use the VMware vSphere Client to import the VM into your system. Start the VMware vSphere Client and log in to the ESXi Server on which you want to install the Avaya Ignition Server. You need to use the Virtual Appliance Deploy OVF Template option.

Procedure

1. From the VSphere Client, select **File > Deploy OVF Template**.



What is a Host?

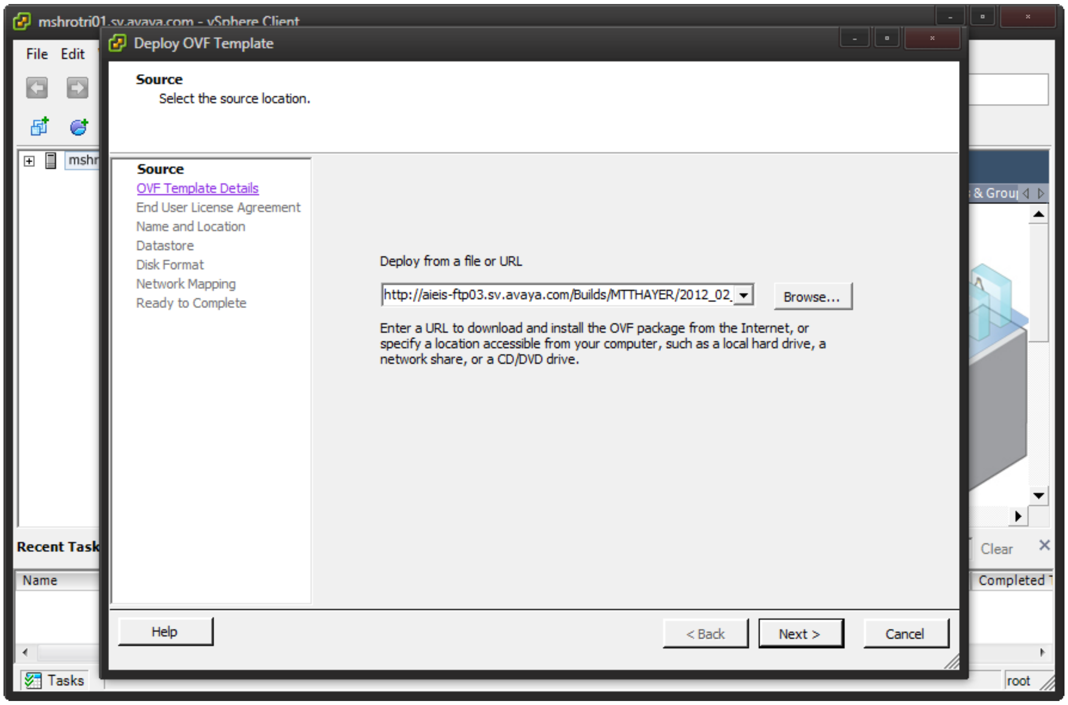
A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating

Figure 1: Deploy OVF Template

2. The **Source** screen displays. Select the location from which you want to import the Ignition Server virtual appliance.



Source

Select the source location.

Deploy from a file or URL

http://aieis-ftp03.sv.avaya.com/Builds/MTTHAYER/2012_02_

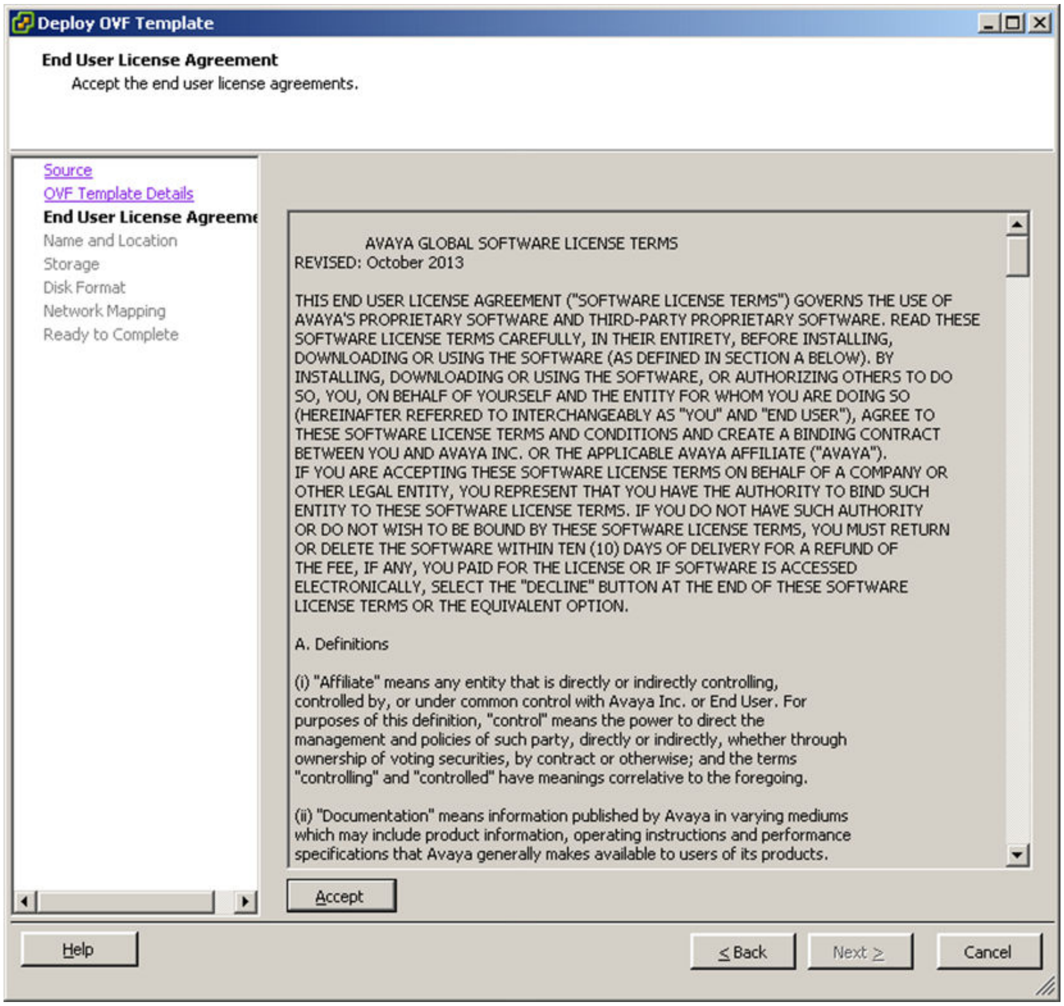
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Figure 2: Source

3. Click **Next**.

   In the OVF Template Details screen, review your settings. You can click **Back** to make changes, or click **Next** to continue.

4. The **End User License Agreement** screen displays. Click **Accept** to accept the license and click **Next**.



End User License Agreement

Accept the end user license agreements.

AVAYA GLOBAL SOFTWARE LICENSE TERMS
REVISED: October 2013

THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE TERMS") GOVERNS THE USE OF AVAYA'S PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (AS DEFINED IN SECTION A BELOW). 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 DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE SOFTWARE LICENSE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). IF YOU ARE ACCEPTING THESE SOFTWARE LICENSE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE SOFTWARE LICENSE TERMS. IF YOU DO NOT HAVE SUCH AUTHORITY OR DO NOT WISH TO BE BOUND BY THESE SOFTWARE LICENSE TERMS, YOU MUST RETURN OR DELETE THE SOFTWARE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OF THE FEE, IF ANY, YOU PAID FOR THE LICENSE OR IF SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" BUTTON AT THE END OF THESE SOFTWARE LICENSE TERMS OR THE EQUIVALENT OPTION.

A. Definitions

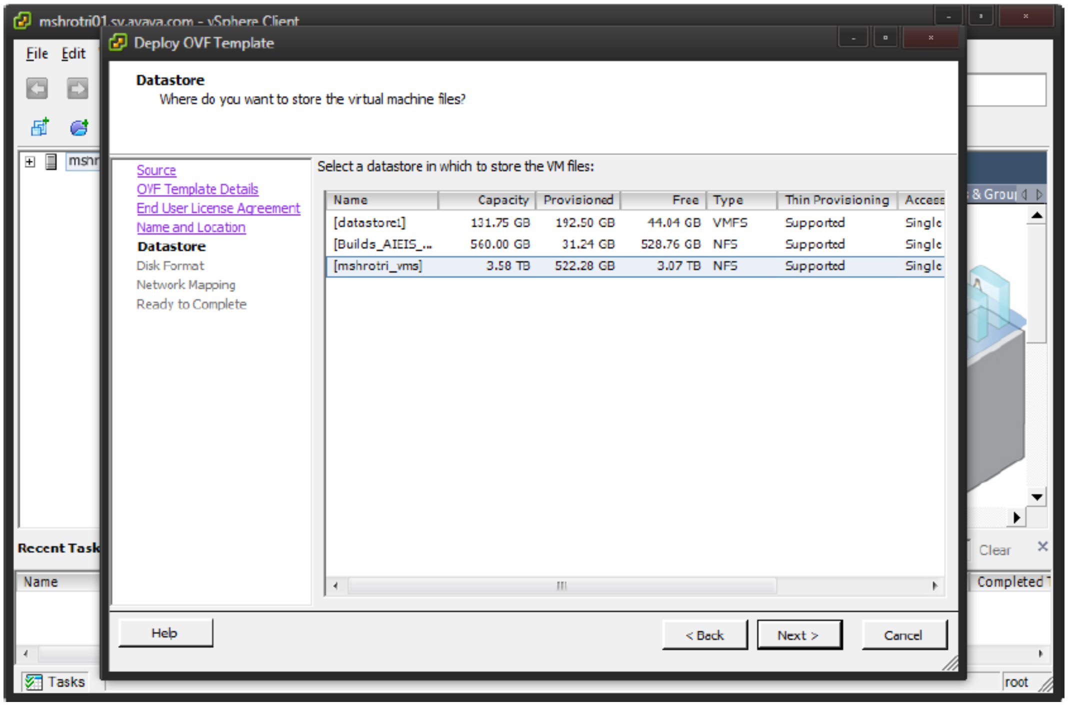
(i) "Affiliate" means any entity that is directly or indirectly controlling, controlled by, or under common control with Avaya Inc. or End User. For purposes of this definition, "control" means the power to direct the management and policies of such party, directly or indirectly, whether through ownership of voting securities, by contract or otherwise; and the terms "controlling" and "controlled" have meanings correlative to the foregoing.

(ii) "Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products.

Figure 3: End User License Agreement

5. The **Name and Location** screen displays. You can either accept the default name or choose to rename the virtual machine. Click **Next**.

6. The **Datastore** screen displays. Select the location where you want to store the files for the virtual appliance and click **Next**.



Datastore

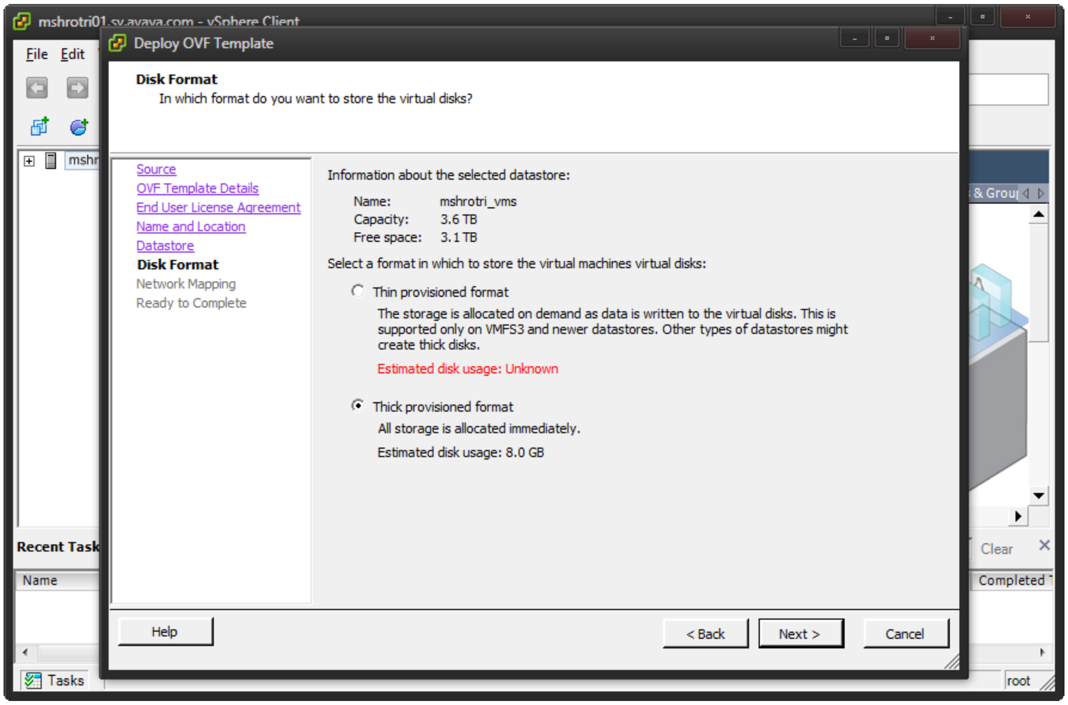
Where do you want to store the virtual machine files?

Select a datastore in which to store the VM files:

Name	Capacity	Provisioned	Free	Type	Thin Provisioning	Access
[datastore1]	131.75 GB	192.50 GB	44.04 GB	VMFS	Supported	Single
[Builds_AIEIS_...	560.00 GB	31.24 GB	528.76 GB	NFS	Supported	Single
[mshrotri_vms]	3.58 TB	522.28 GB	3.07 TB	NFS	Supported	Single

Figure 4: Datastore

7. The **Disk Format** screen displays. Select a format in which to store the virtual machine’s virtual disks and click **Next**.



Disk Format

In which format do you want to store the virtual disks?

Information about the selected datastore:

Name: mshrotri_vms
Capacity: 3.6 TB
Free space: 3.1 TB

Select a format in which to store the virtual machines virtual disks:

○ Thin provisioned format

The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks.

Estimated disk usage: Unknown

● Thick provisioned format

All storage is allocated immediately.

Estimated disk usage: 8.0 GB

Figure 5: Disk Format

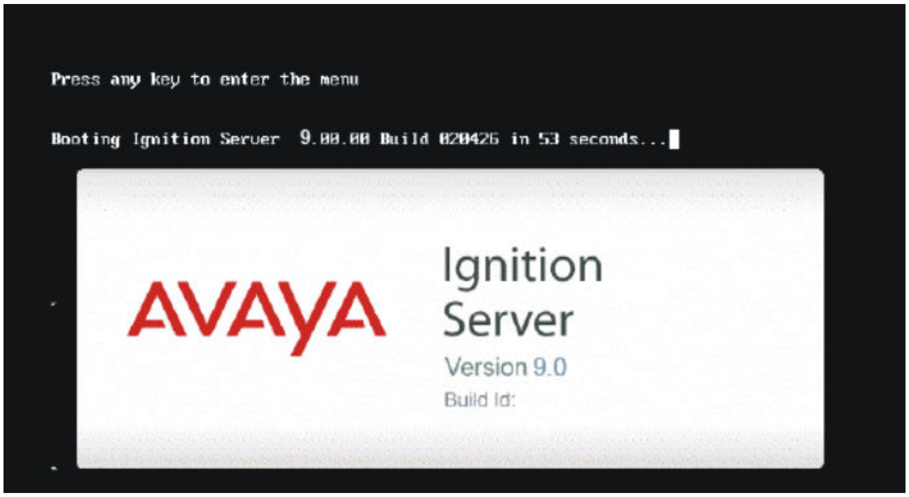
8. The **Network Mapping** screen displays. Associate the Avaya Ignition Server NICs to the correct VM Network based on your site configuration. Then click on **Next**.
9. The **Ready to Complete** screen displays. Review your settings. Use the **Back** button to make any changes or click **Finish** to start the import.

   The Import now starts. Once the import completes you should see a **Summary** window display.
10. After the import completes, you must verify and adjust some of the VM settings. Open the VM setting dialog and select the **Options** tab. Do the following:

    a. Click the **Synchronize guest time with host** option.

    b. Change the **System Default Power Off** from **Power off** to **Shutdown Guest**. Click **OK**.

    c. Open the VM setting dialog and select the **Hardware** tab. Adjust the **Network Adapter (1/2/3)** settings and configure the right NIC for each interface. You are now ready to boot the Avaya Ignition Server for the first time. A splash screen displays as the boot up starts.



```
Press any key to enter the menu

Booting Ignition Server  9.00.00 Build 020426 in 53 seconds...
```

Figure 6: Boot up

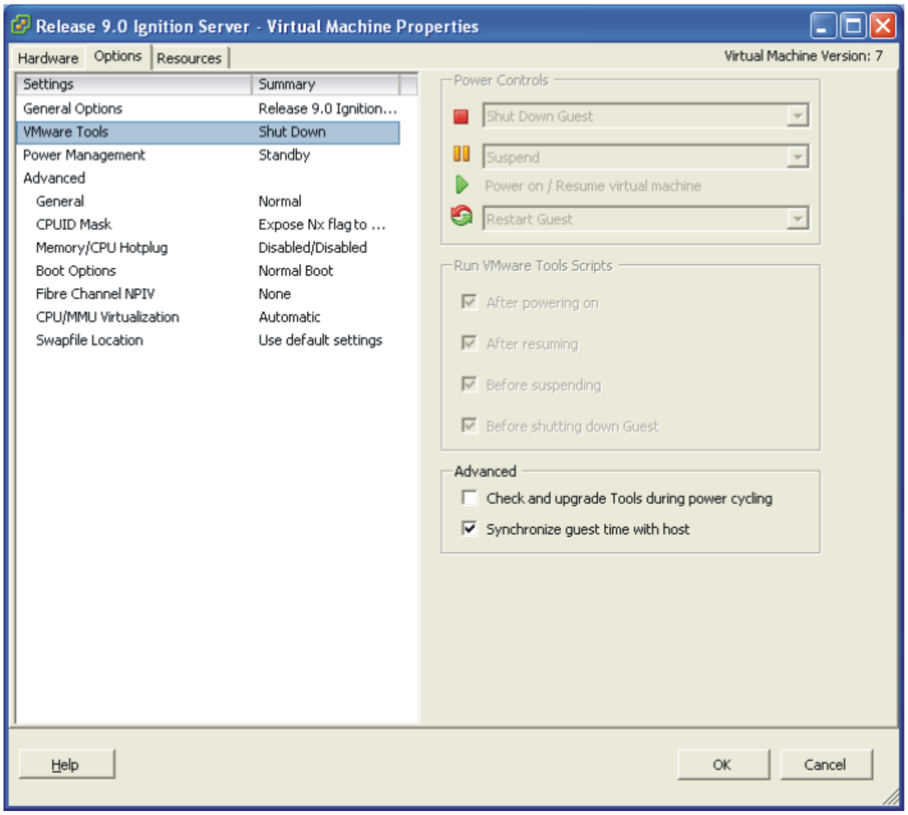
    d. Avaya does not support manual or automated VMware Tools installation and configuration on Avaya supplied VMs. Refer to Preventing automatic VMware tools updates on page 21 for information on how to prevent automatic updates for VMWare Tools.
11. Once the Ignition Server Console login prompt displays, you are ready to enter the administration IP address. Login using *admin* for the user name and *admin* for the password. You should change the password after you login.

Preventing automatic VMware tools updates

Use this procedure to prevent automatic VMware Tools updates.

Procedure

1. Use the Vmware vSphere Client to log in to the ESXi Server hosting the Ignition VM.
2. Select the VM corresponding to the Ignition Server.
3. Go to **Getting Started** > **Edit Virtual Machine Settings** > **Options** > **VMware Tools** > **Advanced**, and ensure the **Check and upgrade Tools during power cycling** check box is not selected. This is the supported setting.
4. Click **OK**.


Release 9.0 Ignition Server - Virtual Machine Properties
Hardware
Options
Resources
Virtual Machine Version: 7
Help
OK
Cancel

Settings	Summary
General Options	Release 9.0 Ignition...
VMware Tools	Shut Down
Power Management	Standby
Advanced	
General	Normal
CPUID Mask	Expose Nx flag to ...
Memory/CPU Hotplug	Disabled/Disabled
Boot Options	Normal Boot
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

Power Controls

Shut Down Guest

Suspend

Power on / Resume virtual machine

Restart Guest

Run VMware Tools Scripts

☑ After powering on

☑ After resuming

☑ Before suspending

☑ Before shutting down Guest

Advanced

□ Check and upgrade Tools during power cycling

☑ Synchronize guest time with host

Figure 7: Preventing automatic VMware tools updates

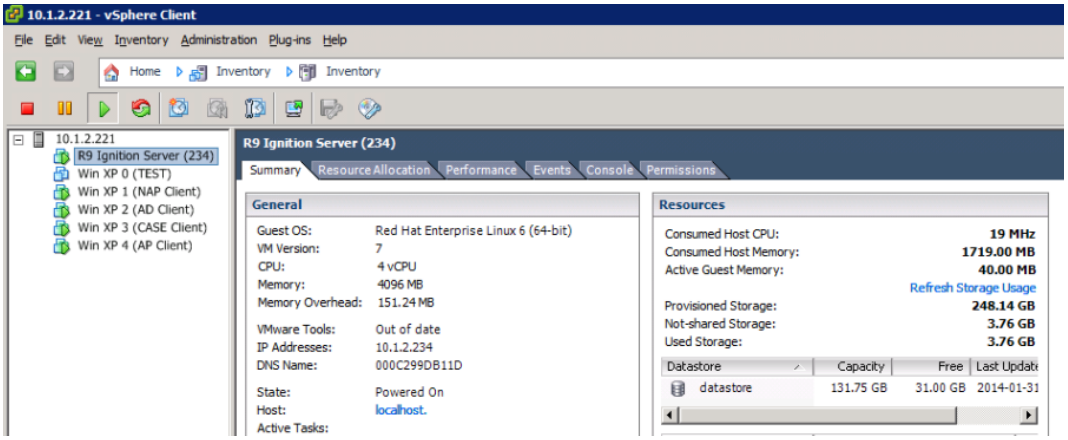
Checking the VMware Tools status (ESXi 5.x)

Use this procedure to check the VMware Tools status on an ESXi 5.x server.

Procedure

1. Use the VI Client to log in to the ESXi Server hosting the Ignition VM.
2. Go to the **Summary** tab.

   If you are using the vmware-tools supplied by Avaya and did not upgrade, the status displays as “VMware Tools: Out-of-date”.



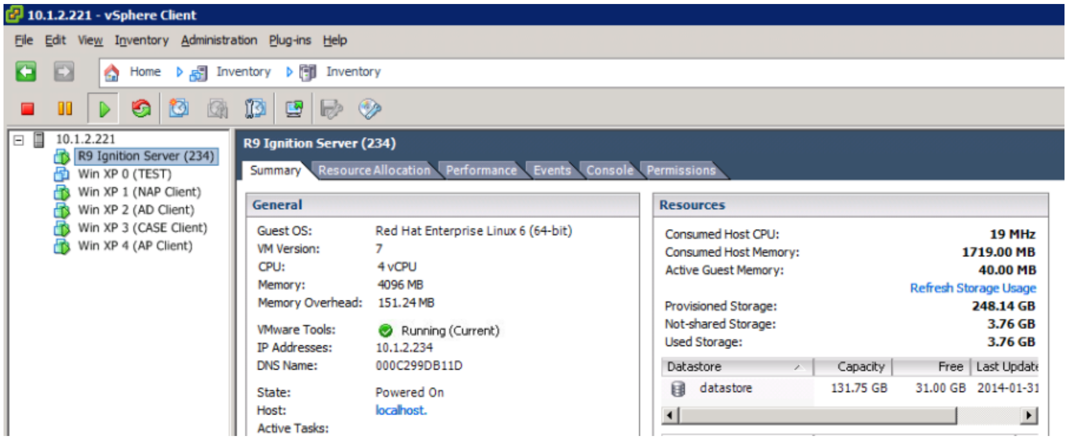
Guest OS: Red Hat Enterprise Linux 6 (64-bit)
VM Version: 7
CPU: 4 vCPU
Memory: 4096 MB
Memory Overhead: 151.24 MB
VMware Tools: Out of date
IP Addresses: 10.1.2.234
DNS Name: 000C299DB11D
State: Powered On
Host: localhost.
Active Tasks:

Consumed Host CPU: 19 MHz
Consumed Host Memory: 1719.00 MB
Active Guest Memory: 40.00 MB
Provisioned Storage: 248.14 GB
Not-shared Storage: 3.76 GB
Used Storage: 3.76 GB

Datastore	Capacity	Free	Last Updat
datastore	131.75 GB	31.00 GB	2014-01-31

Figure 8: VMware Tools: Out-of-date

If you upgraded the VMware Tools, the status displays as “VMware Tools: Running (Current)”.



Guest OS: Red Hat Enterprise Linux 6 (64-bit)
VM Version: 7
CPU: 4 vCPU
Memory: 4096 MB
Memory Overhead: 151.24 MB
VMware Tools: ✓ Running (Current)
IP Addresses: 10.1.2.234
DNS Name: 000C299DB11D
State: Powered On
Host: localhost.
Active Tasks:

Consumed Host CPU: 19 MHz
Consumed Host Memory: 1719.00 MB
Active Guest Memory: 40.00 MB
Provisioned Storage: 248.14 GB
Not-shared Storage: 3.76 GB
Used Storage: 3.76 GB

Datastore	Capacity	Free	Last Updat
datastore	131.75 GB	31.00 GB	2014-01-31

Figure 9: VMware Tools: Running (Current)

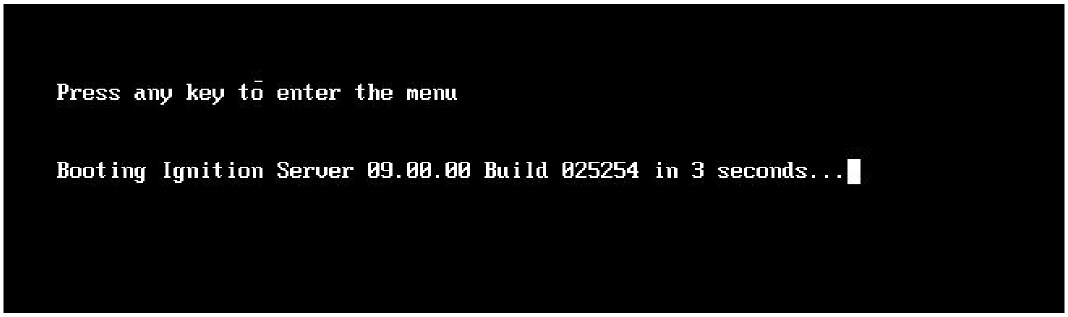
Configuring the Ignition Server virtualization appliance

About this task

Use this procedure to configure the Ignition Server virtualization appliance.

Procedure

1. Boot the Avaya Ignition Server for the first time. A splash screen displays as the boot up starts.

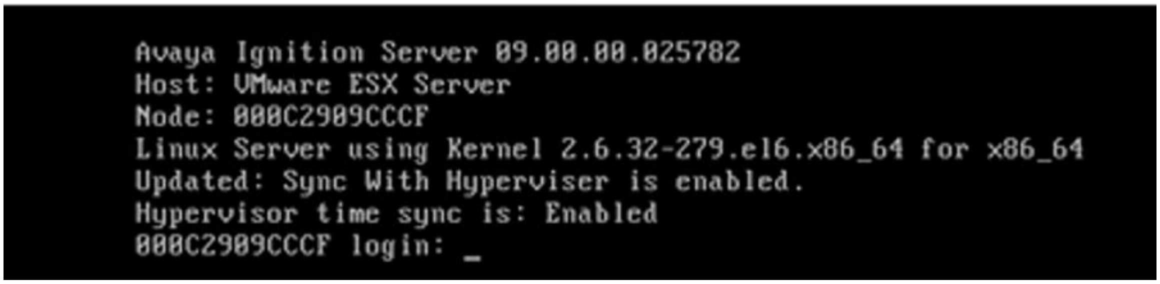
   

   ```
   Press any key to enter the menu

   Booting Ignition Server 09.00.00 Build 025254 in 3 seconds...
   ```

   Figure 10: Boot up

2. Once the Ignition Server Console login prompt displays, you are ready to enter the administration IP address. Login using *admin* for the user name and *admin* for the password. You should change the password after you login.

   ```
   Avaya Ignition Server 09.00.00.025782
   Host: VMware ESX Server
   Node: 000C2909CCCF
   Linux Server using Kernel 2.6.32-279.el6.x86_64 for x86_64
   Updated: Sync With Hyperviser is enabled.
   Hypervisor time sync is: Enabled
   000C2909CCCF login: _
   ```

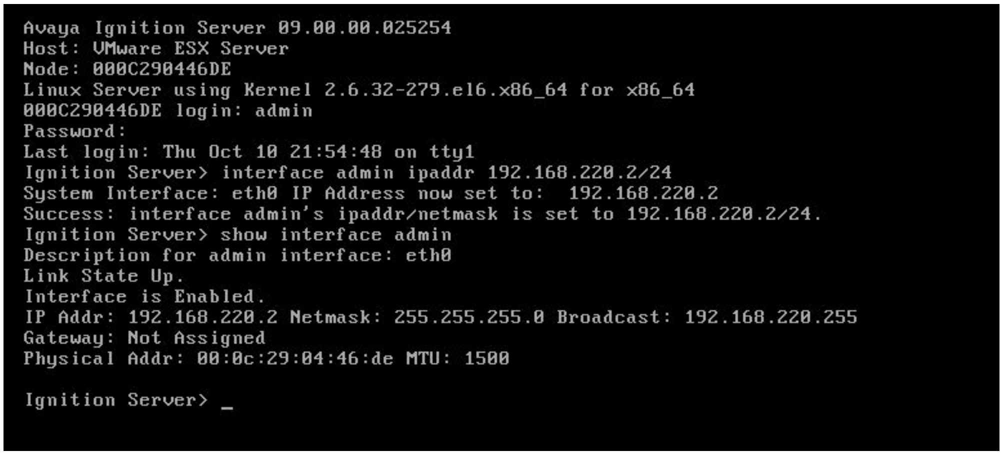
   Figure 11: Console

3. Use the interface commands as shown in the next screen to configure the admin interface.

   - Only Static IP configuration is supported.
   - Configure your admin interface with an IP address.

     CLI command example: “interface admin ipaddr x.y.z.x/netmask”
   - If needed, configure your default route.

     CLI command example: “route add 0.0.0.0/0 <gw-ip> “



```
Avaya Ignition Server 09.00.00.025254
Host: VMware ESX Server
Node: 000C290446DE
Linux Server using Kernel 2.6.32-279.el6.x86_64 for x86_64
000C290446DE login: admin
Password:
Last login: Thu Oct 10 21:54:48 on tty1
Ignition Server> interface admin ipaddr 192.168.220.2/24
System Interface: eth0 IP Address now set to:  192.168.220.2
Success: interface admin's ipaddr/netmask is set to 192.168.220.2/24.
Ignition Server> show interface admin
Description for admin interface: eth0
Link State Up.
Interface is Enabled.
IP Addr: 192.168.220.2 Netmask: 255.255.255.0 Broadcast: 192.168.220.255
Gateway: Not Assigned
Physical Addr: 00:0c:29:04:46:de MTU: 1500

Ignition Server> _
```

Figure 12: Admin interface commands

Installing the Ignition Dashboard desktop application

The Avaya Ignition Dashboard is a desktop application that enables you to manage the Ignition Server appliance. The Avaya Ignition Dashboard enables you to create, view, or alter configuration information for authenticators, service categories, and the policies that apply to authentication and authorization.

Before you begin

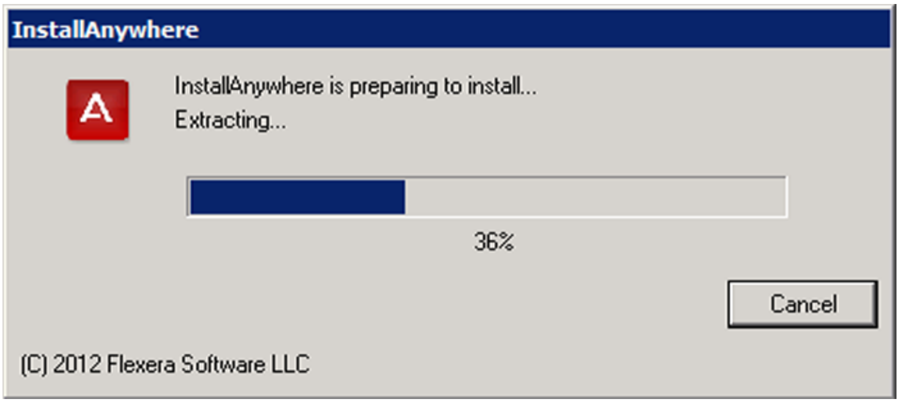
To proceed with the Ignition Dashboard installation, have the following tools and information ready:

- The Identity Engines product software shipped with your Ignition Server appliance.
- A computer running Windows XP Service Pack 3 (32 bit), Windows 7 (32 bit or 64 bit), Windows 8 (32 bit or 64 bit), Windows Server 2003 (32 bit or 64 bit), or Windows Server 2008 (32 bit or 64 bit).
- A minimum of 2 GB of RAM memory.
- The default System administrator name (`admin`) and password (`admin`).

Procedure

1. If any version of the Avaya Ignition Dashboard exists on the computer, ensure the Ignition Dashboard application is not currently running. If the Ignition Dashboard is running, shut it down now.
2. Place the Ignition Server CD into the CD drive of your computer. On Windows, the Windows AutoRun feature runs the Installer immediately.

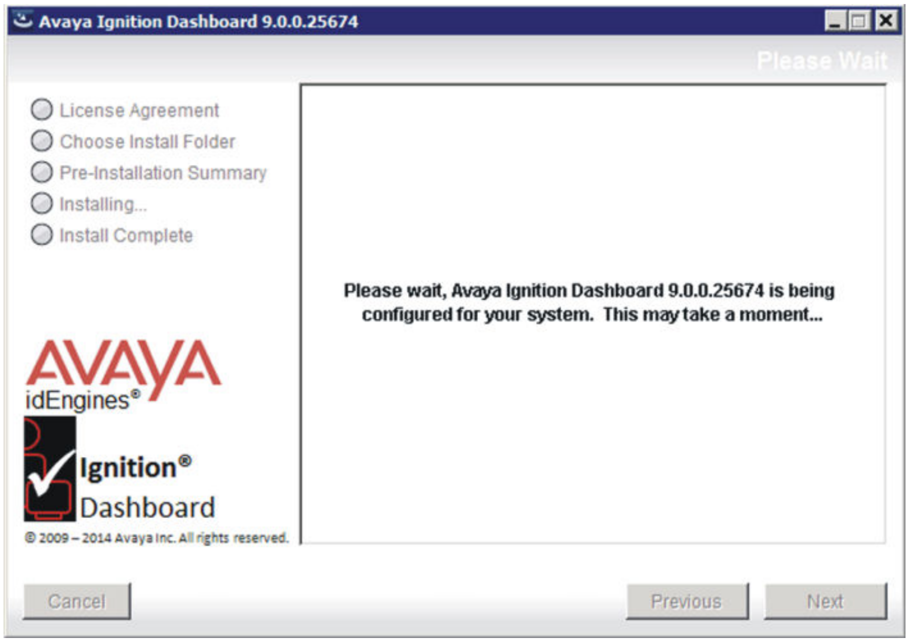
Note: If the AutoRun feature is disabled on your computer, navigate to your CD drive and double-click the installer file. It has a name like DashboardInstaller-9.0.0<Build Number>.exe.



InstallAnywhere is preparing to install...
Extracting...

(C) 2012 Flexera Software LLC

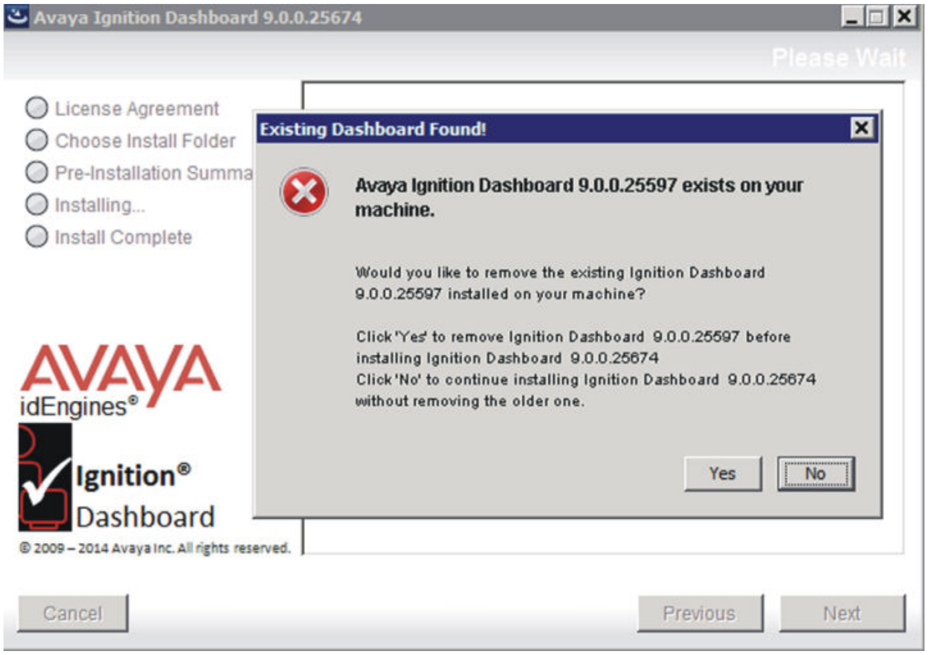
Figure 13: AutoRun feature runs



Please wait, Avaya Ignition Dashboard 9.0.0.25674 is being configured for your system. This may take a moment...

Figure 14: Ignition Dashboard prepares to install

3. If an older version of Ignition Dashboard exists on your device, the **Existing Dashboard Found!** window displays. To remove the old Ignition Dashboard, select **Yes**. To install the new version of Ignition Dashboard without removing the older version, select **No**.



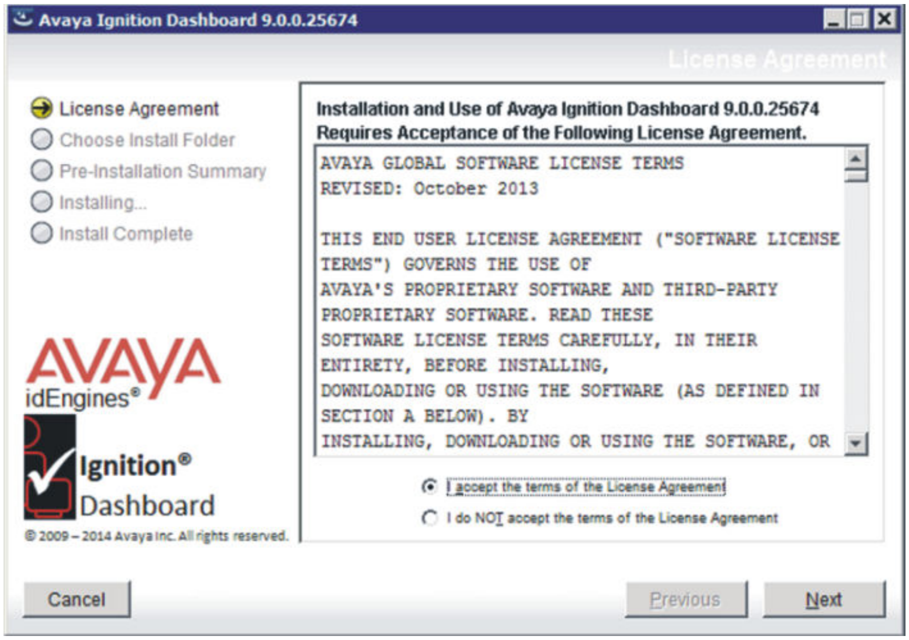
Avaya Ignition Dashboard 9.0.0.25597 exists on your machine.

Would you like to remove the existing Ignition Dashboard 9.0.0.25597 installed on your machine?

Click 'Yes' to remove Ignition Dashboard 9.0.0.25597 before installing Ignition Dashboard 9.0.0.25674
Click 'No' to continue installing Ignition Dashboard 9.0.0.25674 without removing the older one.

Figure 15: Remove existing Ignition Dashboard

4. In the **License Agreement** screen, scroll down to read the entire license. Select the radio button to accept the license and click **Next**.



Installation and Use of Avaya Ignition Dashboard 9.0.0.25674 Requires Acceptance of the Following License Agreement.

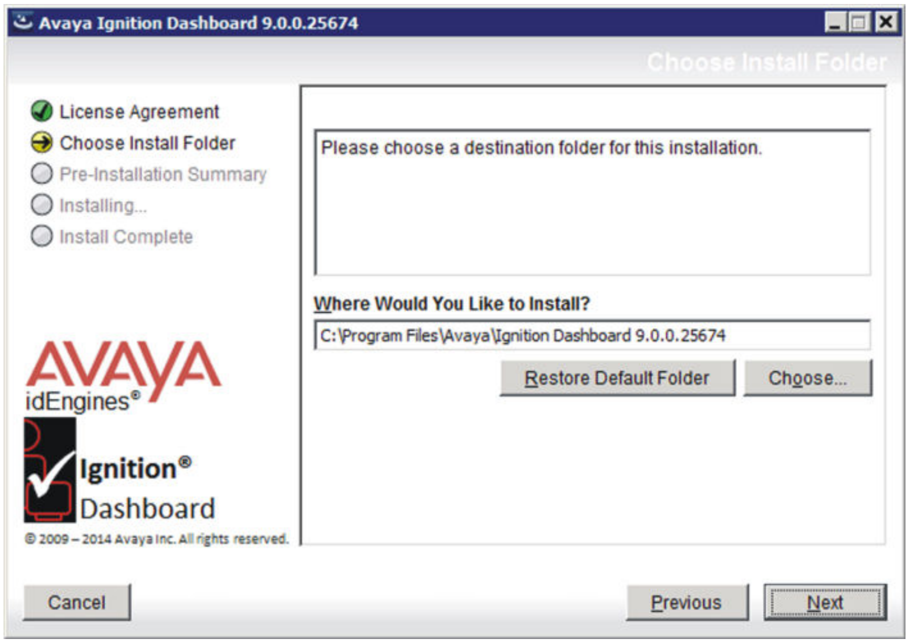
```
AVAYA GLOBAL SOFTWARE LICENSE TERMS
REVISED: October 2013

THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE
TERMS") GOVERNS THE USE OF
AVAYA'S PROPRIETARY SOFTWARE AND THIRD-PARTY
PROPRIETARY SOFTWARE. READ THESE
SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR
ENTIRETY, BEFORE INSTALLING,
DOWNLOADING OR USING THE SOFTWARE (AS DEFINED IN
SECTION A BELOW). BY
INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR
```

● I accept the terms of the License Agreement
○ I do NOT accept the terms of the License Agreement

Figure 16: License Agreement screen

5. In the **Choose Install Folder** screen, choose your destination folder and click **Next**.



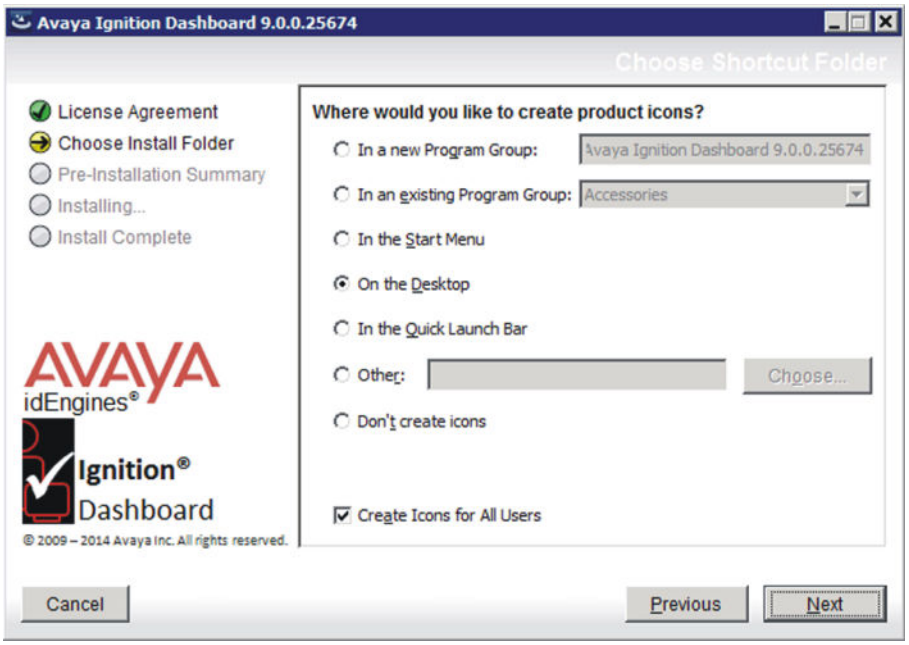
Please choose a destination folder for this installation.

Where Would You Like to Install?

C:\Program Files\Avaya\Ignition Dashboard 9.0.0.25674

Figure 17: Choose Install Folder screen

6. In the **Choose Shortcut Folder** screen, indicate where you want the Dashboard shortcut to appear, and click **Next**.



Where would you like to create product icons?

○ In a new Program Group: Avaya Ignition Dashboard 9.0.0.25674

○ In an existing Program Group: Accessories

○ In the Start Menu

● On the Desktop

○ In the Quick Launch Bar

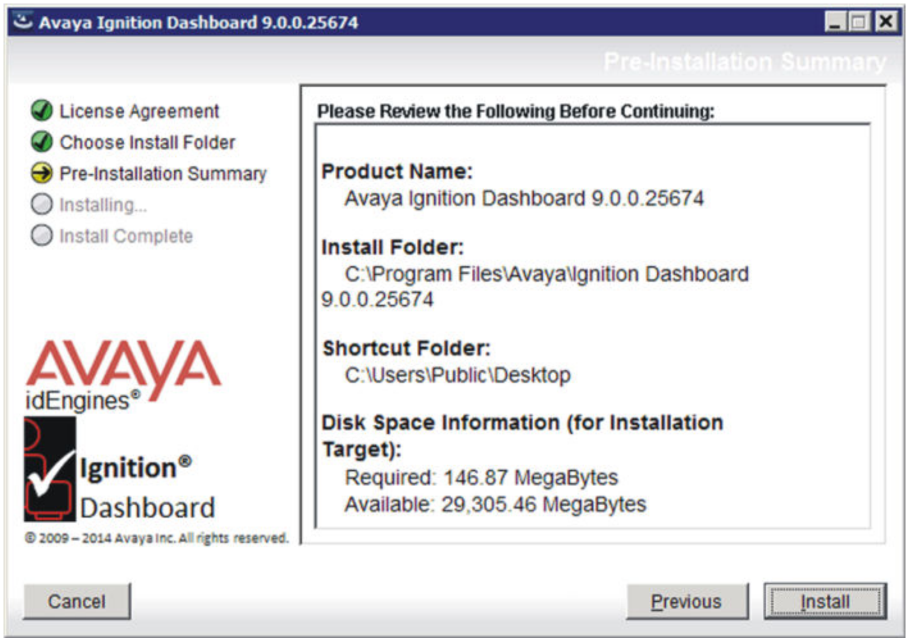
○ Other:

○ Don't create icons

☑ Create Icons for All Users

Figure 18: Dashboard shortcut location

7. In the **Pre-Installation Summary** screen, review your installation settings. If you want to make changes, click **Previous** to edit the details of the locations of the installation. When you finish your configuration, click **Install**. The installer displays a pre-install confirmation window.



Please Review the Following Before Continuing:

Product Name:
Avaya Ignition Dashboard 9.0.0.25674

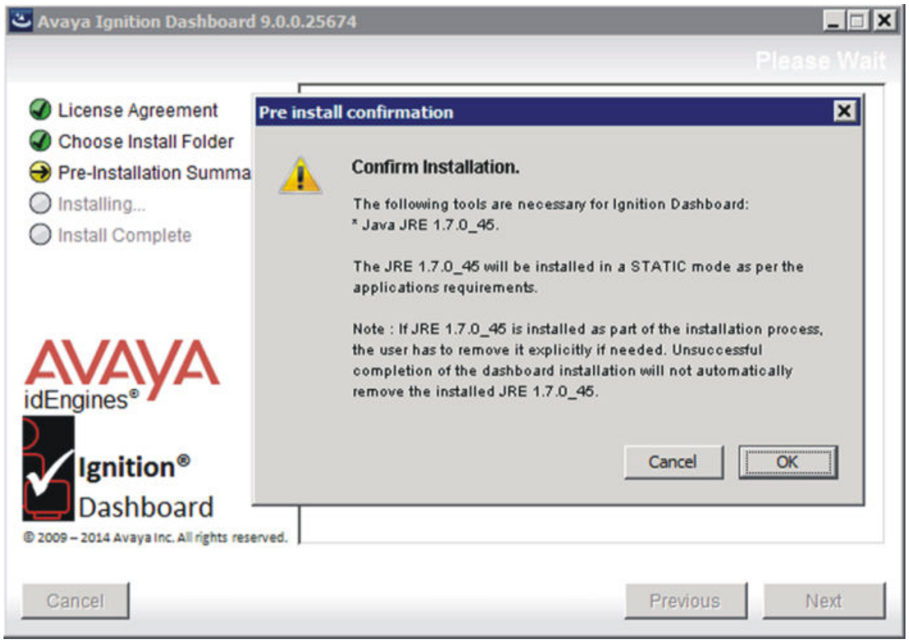
Install Folder:
C:\Program Files\Avaya\Ignition Dashboard 9.0.0.25674

Shortcut Folder:
C:\Users\Public\Desktop

Disk Space Information (for Installation Target):
Required: 146.87 MegaBytes
Available: 29,305.46 MegaBytes

Figure 19: Pre-Installation Summary screen

8. In the **Pre-Installation Summary** confirmation window, click **OK** to confirm the installation.



Confirm Installation.

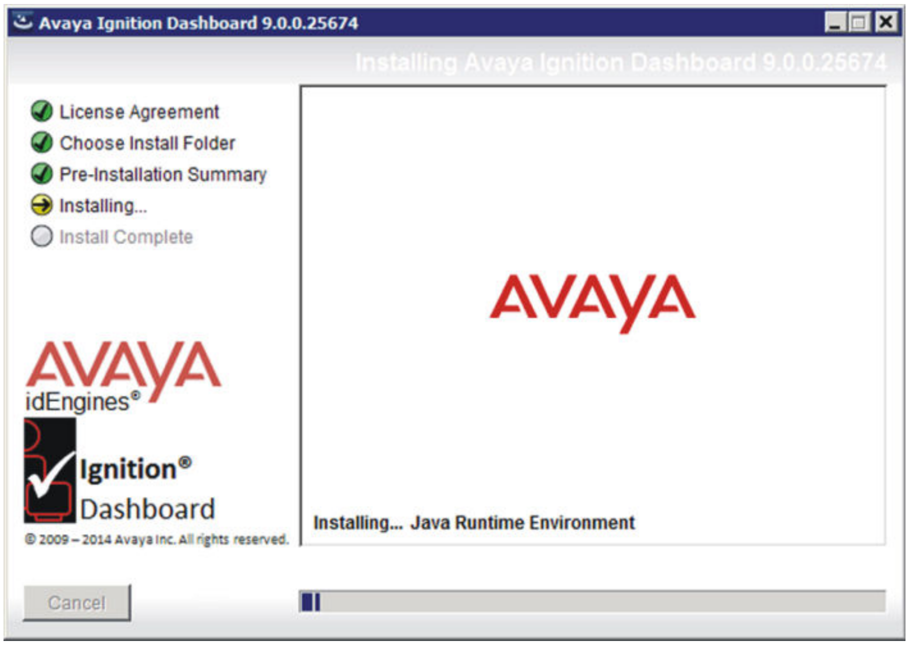
The following tools are necessary for Ignition Dashboard:
* Java JRE 1.7.0_45.

The JRE 1.7.0_45 will be installed in a STATIC mode as per the applications requirements.

Note : If JRE 1.7.0_45 is installed as part of the installation process, the user has to remove it explicitly if needed. Unsuccessful completion of the dashboard installation will not automatically remove the installed JRE 1.7.0_45.

Figure 20: Pre install confirmation window

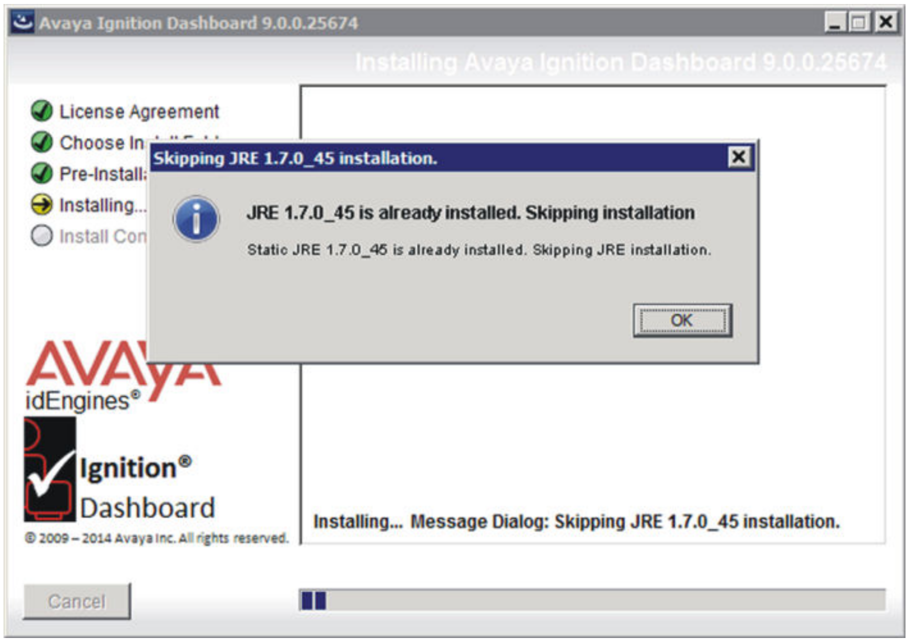
The installation starts. The installer displays a dialog box that displays the progress of the installation.



Installing... Java Runtime Environment

Figure 21: Installation progress

9. If the appropriate Java Runtime Environment (JRE) is already installed, a window appears to allow you to skip re-installing JRE. Click **OK** to skip the re-installation of JRE.


Avaya Ignition Dashboard 9.0.0.25674
Installing Avaya Ignition Dashboard 9.0.0.25674
License Agreement
Choose In
Pre-Install
Installing...
Install Con
Skipping JRE 1.7.0_45 installation.
OK
AVAYA
idEngines®
Ignition®
Dashboard
© 2009 – 2014 Avaya Inc. All rights reserved.
Cancel

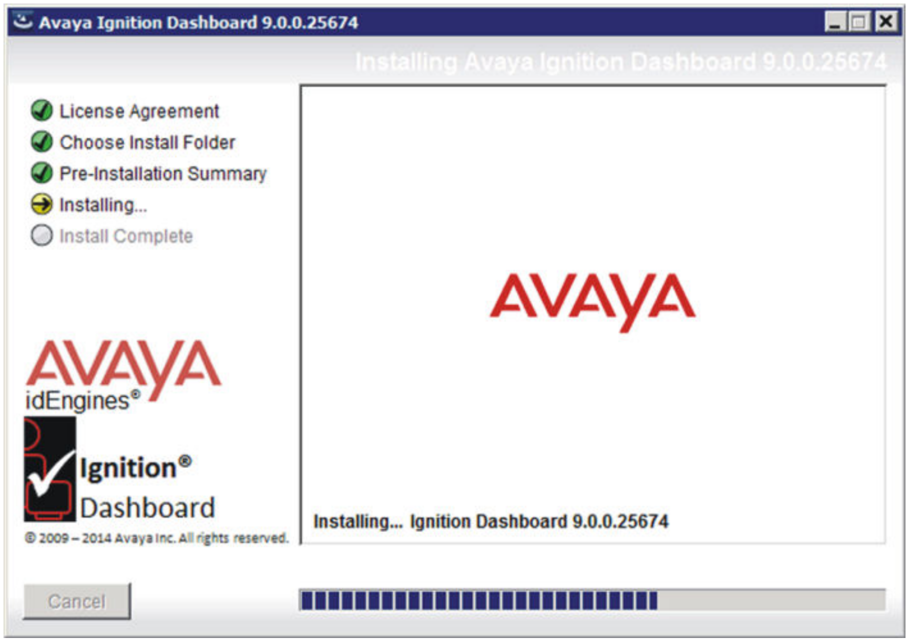
JRE 1.7.0_45 is already installed. Skipping installation

Static JRE 1.7.0_45 is already installed. Skipping JRE installation.

Installing... Message Dialog: Skipping JRE 1.7.0_45 installation.

Figure 22: JRE already installed

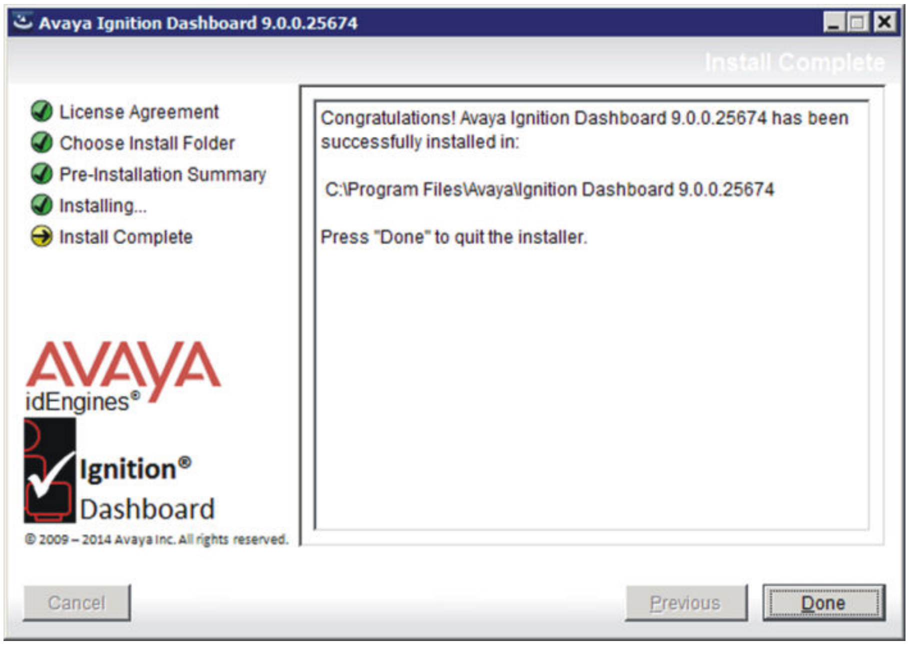
The installation continues. The installer displays a dialog box showing the progress of the installation.



Installing... Ignition Dashboard 9.0.0.25674

Figure 23: Installing Ignition Dashboard

10. When the installation is complete, the installer displays the **Install Complete** screen. In the **Install Complete** screen, click **Done**. An icon for Ignition Dashboard appears in the location you designated.



Congratulations! Avaya Ignition Dashboard 9.0.0.25674 has been successfully installed in:

C:\Program Files\Avaya\Ignition Dashboard 9.0.0.25674

Press "Done" to quit the installer.

Figure 24: Install Complete screen

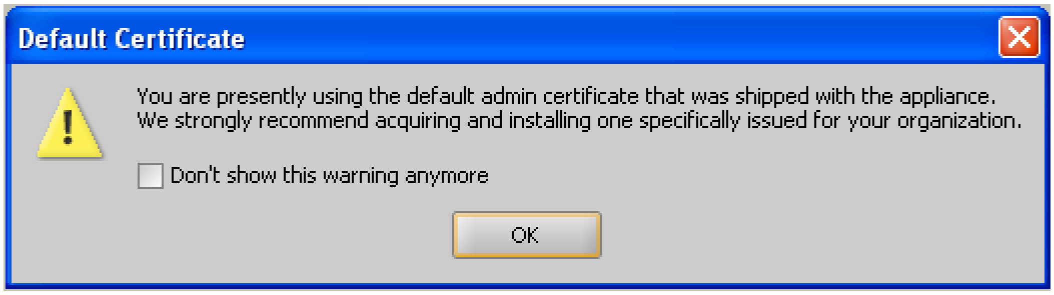
Installing multiple versions of the Ignition Dashboard: You can install multiple versions of Ignition Dashboard on a single workstation. When you run the installer, it installs the new version in its own folder. The new installation does not interfere with existing Ignition Dashboard installations and creates a new icon to launch the new version of Ignition Dashboard. The installer leaves the existing Ignition Dashboard installation and icon intact.

Running the Dashboard

If your Ignition Server appliance is connected only via its Admin Port, skip this section and go to Further configuration on page 41. If your installation will use Service Port A, follow these steps:

Procedure

1. On your administration computer, start Ignition Dashboard by doubleclicking its icon on the desktop.
2. In the login screen, type the default **User Name**: `admin`. Type the default **Password**: `admin`.
3. In the **Connect To**: field, type the fully-qualified domain name or the IP address you assigned to the Ignition Server appliance Admin Port.
4. A dialog box appears saying **Base License Required**. You can install the license later as described in Installing the license on page 35. Be sure to first read Obtaining the Ignition Server Serial Number on page 32. For now, dismiss the popup by clicking **OK**.
5. A warning dialog appears reminding you to replace the default certificate shipped with the Ignition Server appliance. Ignore the warning. (For instructions on replacing the certificate, see the *Avaya Identity Engines Ignition Server Administration Guide*.)



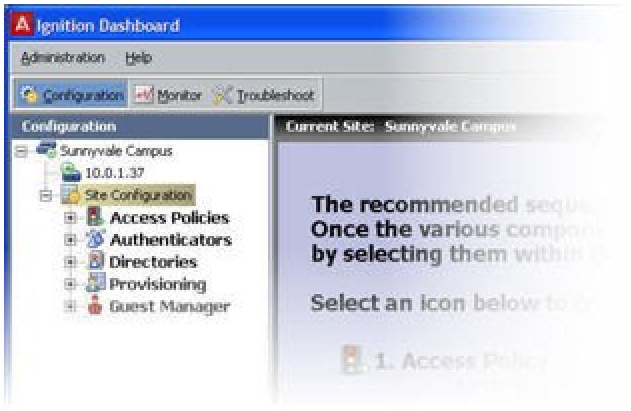
Default Certificate

You are presently using the default admin certificate that was shipped with the appliance. We strongly recommend acquiring and installing one specifically issued for your organization.

□ Don't show this warning anymore

Figure 25: Default Certificate

After you dismiss the warning dialog, Ignition Dashboard appears:



The recommended sequ
Once the various compon
by selecting them within

Select an icon below to

Figure 26: Ignition Dashboard

Next steps

If you already have your Ignition Server license, go to Installing the license on page 35.

Obtaining the Ignition Server Serial Number

The Avaya Identity Engines Ignition Server software ships without any licenses. There are seven different software licenses that can be installed on Ignition Server: Base License, Guest Manager License, NAP Posture License, TACACS+ License, Ignition Reports License, Access Portal License, and Avaya Aura® Single-Sign-On (SSO) License. At a minimum, you must obtain the Base License to be able to configure and run the server.

If you are applying a NAP Posture License or an Access Portal License, select the Access Portal License that matches the Ignition Server Base License (LITE, SMALL, or LARGE).

Note:

As of Identity Engines Release 9.0, Identity Engines start to transition from DVD delivery to electronic software delivery. Depending on how you place your order, you may receive DVDs with paper LACs, or electronic software delivery and electronic LACs. With each method you will receive instructions on how to obtain your licenses.

Procedure

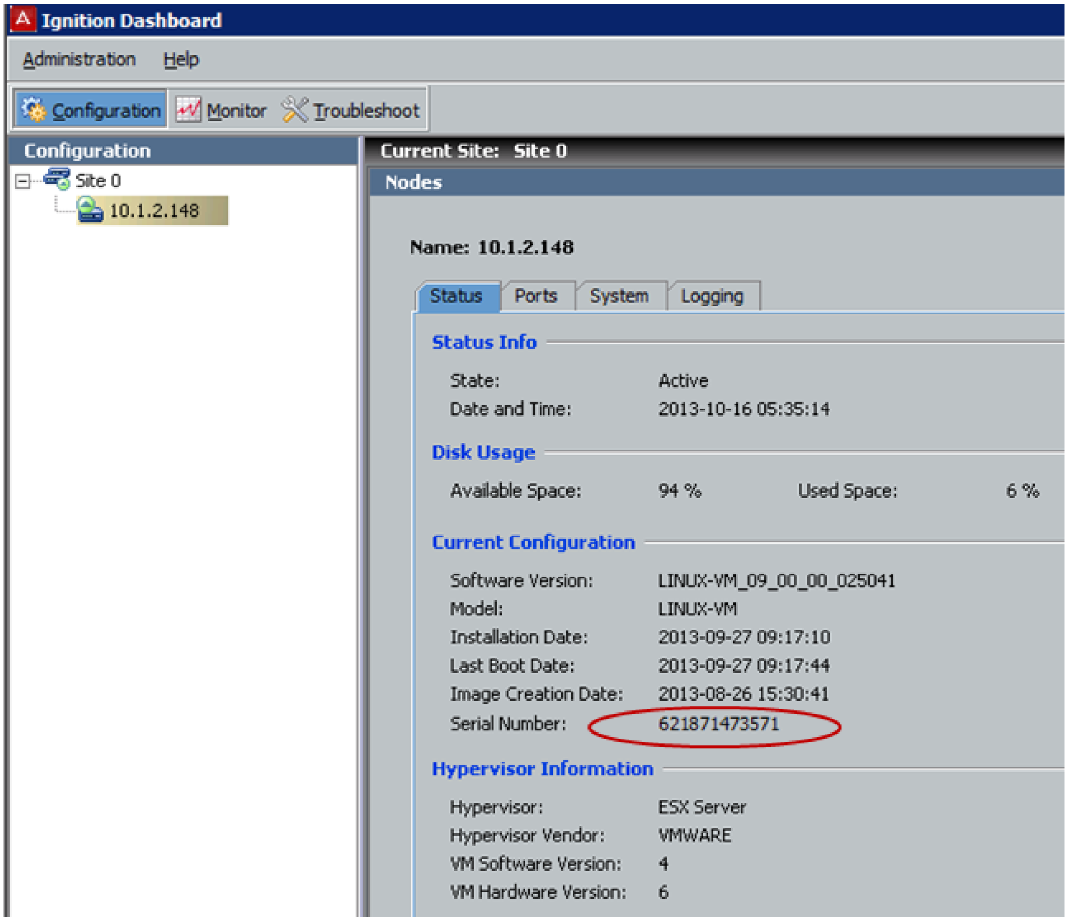
1. Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/.
2. Once you have purchased Identity Engines, then depending on how you placed your order, you receive either a set of DVDs accompanied with paper LACs (License

Authorization Codes), or else you receive electronic delivery of your LAC by email and you then download the software from Avaya support site via PLDS.

Once you have installed both the Ignition Server Virtual Appliance and the Ignition Dashboard, you must obtain the Ignition Server node Serial Number (also known as the Host-ID) from the Dashboard. The Ignition Server Serial Number is required in order to generate licenses regardless of whether they are KRS licenses or PLDS licenses.

If you have a High Availability (HA) deployment, you need to obtain the Serial Numbers of both Ignition Servers that make up the HA-pair.

To obtain the Ignition Server Serial Number, go to **Dashboard** > **Configuration** > **Node** > **Status tab** > **Serial Number** as shown in the following figure.



Name: 10.1.2.148

Status Info

State: Active
Date and Time: 2013-10-16 05:35:14

Disk Usage

Available Space: 94 % Used Space: 6 %

Current Configuration

Software Version: LINUX-VM_09_00_00_025041
Model: LINUX-VM
Installation Date: 2013-09-27 09:17:10
Last Boot Date: 2013-09-27 09:17:44
Image Creation Date: 2013-08-26 15:30:41
Serial Number: 621871473571

Hypervisor Information

Hypervisor: ESX Server
Hypervisor Vendor: VMWARE
VM Software Version: 4
VM Hardware Version: 6

Figure 27: Obtaining the Ignition Server Serial Number

Another method of obtaining the Ignition Server Serial Number is by logging in the Ignition Server CLI (via the VMware VM Console) and typing the command `show version` on the command line.

Note: As of Identity Engines Release 9.0, the Ignition Server Serial Numbers is always a string of 12 digits.

Obtaining PLDS licenses

If you have received your LAC by electronic delivery (email), your licenses are PLDS licenses.

Using the Avaya Product Licensing and Delivery System (PLDS), you can activate the license entitlements and download the products.

Upon your purchase of Identity Engines, you receive an electronic LAC with which you, as a customer or Avaya Business Partner who has permissions in PLDS for your site or sales order, can access PLDS and generate license entitlements for you. You must provide the Serial Number, also known as the host ID, of the Identity Engines Ignition Server and your LAC in order to generate a license. The LAC helps you to identity the product among other Avaya products you hold licenses for and to keep track of the number downloads, while keeping the required groups and coordinators informed through e-mail messages. The LAC e-mail recipients must be identified during the order placement process by providing their e-mail addresses.

With the LACs in hand, you can use the Quick Activation screen to activate the LACs and download the product.

Obtaining KRS Licenses

If you received paper LACs with your purchase, follow the instructions on the paper LACs regarding how to obtain your licenses. These will be KRS licenses.

You need to send an email to datalicensing@avaya.com to request your KRS licenses and you need to include the following information:

1. End user company name and full mailing address (no mailboxes).
2. End user company URL.
3. End user contact name.
4. End user corporate email address.
5. End user phone number.

6. License Authorization Code (LAC) that shows in the box at the bottom right of the LAC certificate.
7. Serial Number or Serial Numbers if you have an HA deployment.

After the information is verified, licenses are sent to you by email.

Installing the license

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

From release 9.0 onwards, 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.

There are a few key differences between the two types of licenses which are important to understand especially if you will be using both types of licenses.

Important:

Note the following:

- 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.
- 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.
- A PLDS license file ALWAYS has at a minimum a Base license.
- KRS licenses can be exported from the Dashboard and saved on your desktop.
- PLDS licenses cannot be exported from the Dashboard. Therefore, it is very important to ALWAYS safeguard the PLDS license file you have received from PLDS. You may be able to log back in to PLDS and regenerate the license file again.
- Installing PLDS licenses deletes any PLDS and KRS licenses that are already installed . Therefore, it is important to export all KRS licenses before installing PLDS licenses in order to safeguard your KRS licenses.

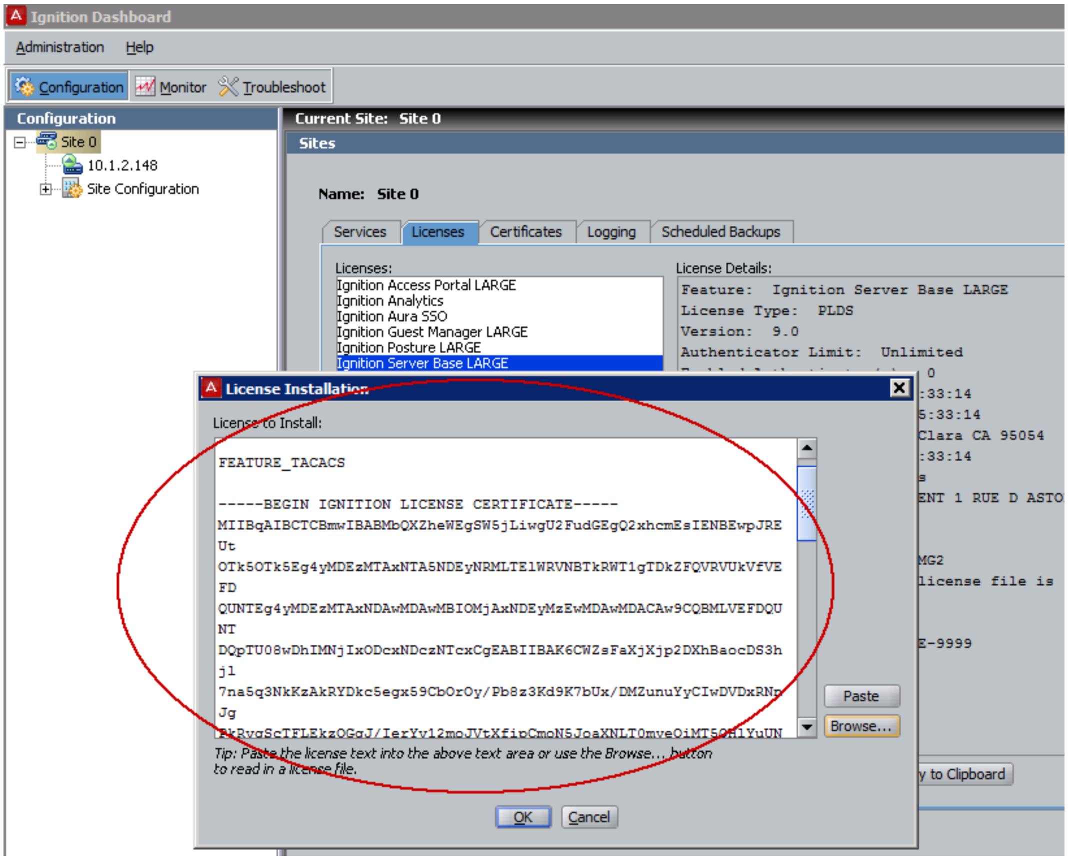
- Since KRS licenses are deleted when installing PLDS license, before installing PLDS license you MUST export and save the KRS licenses if any already exists.
- Installing KRS licenses, overwrites any installed PLDS licenses.

About this task

You can install the license on the Ignition Server using Dashboard. Use this procedure to install the license. The procedure for installing PLDS and KRS license is the same.

Procedure

1. Select the **Configuration** tab.
2. Select the **Site**.
3. Select the **Licenses** tab.
4. Click on **Install**.
5. Browse to the license file location, select, and click **OK**.



Name: Site 0

Licenses:

- Ignition Access Portal LARGE
- Ignition Analytics
- Ignition Aura SSO
- Ignition Guest Manager LARGE
- Ignition Posture LARGE
- Ignition Server Base LARGE

License Details:

```
Feature:  Ignition Server Base LARGE
License Type:  PLDS
Version:  9.0
Authenticator Limit:  Unlimited
```

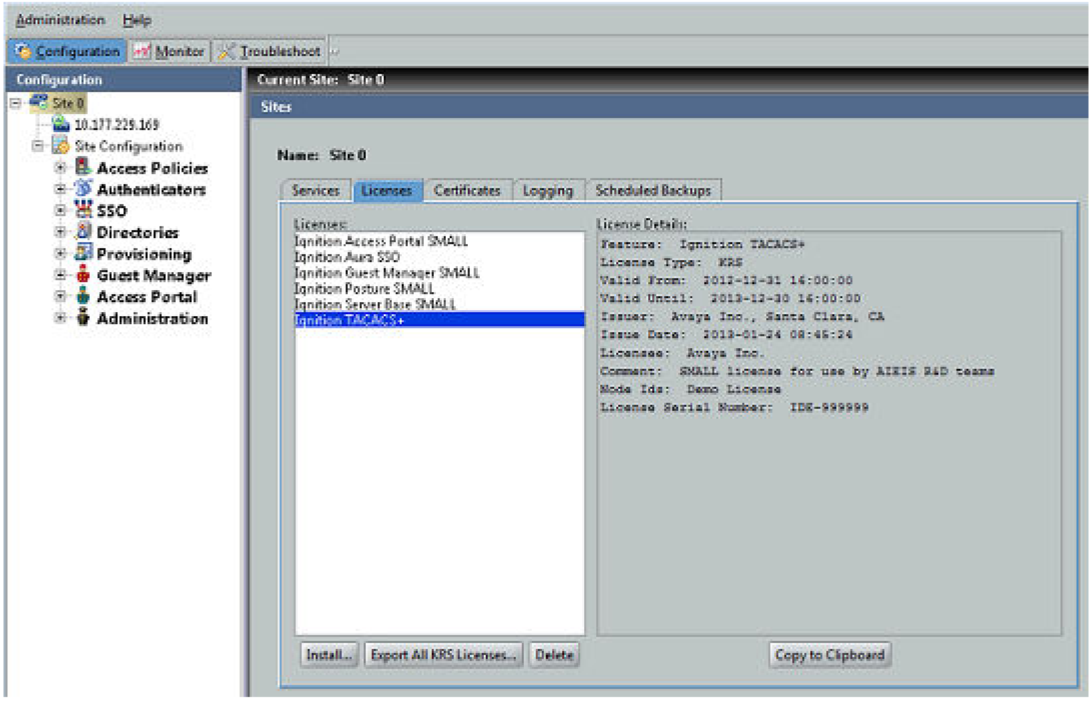
License to Install:

```
FEATURE_TACACS

-----BEGIN IGNITION LICENSE CERTIFICATE-----
MIIBqAIBCTCBmwIBABMbQXZheWEgSW5jLiwgU2FudGEgQ2xhcmEsIENBEwpJRE
Ut
OTk5OTk5Eg4yMDEzMTAxNTA5NDEyNRMLTE1WRVNBTkRWT1gTDkZFQVRVUkVfVE
FD
QUNTEg4yMDEzMTAxNDAwMDAwMBIOMjAxNDEyMzEwMDAwMDACAw9CQBMLVEFDQU
NT
DQpTU08wDhIMNjIxODcxNDczNTcxCgEABIIBAK6CWZsFaXjXjp2DXhBaocDS3h
jl
7na5q3NkKzAkRYDkc5egx59CbOrOy/Pb8z3Kd9K7bUx/DMZunuYyCIwDVDxRNp
Jg
```

Tip: Paste the license text into the above text area or use the Browse... button to read in a license file.

Figure 28: Installing KRS license



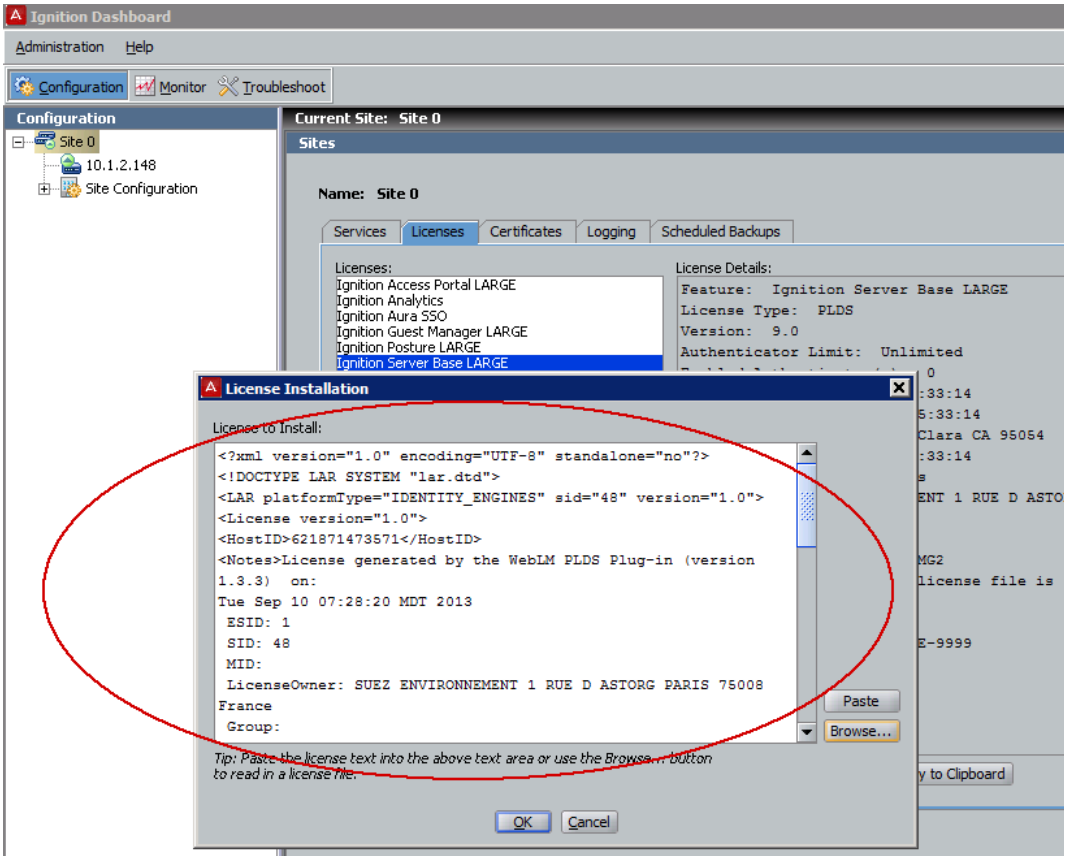
Name: Site 0

Licenses:
- Ignition Access Portal SMALL
- Ignition Aura SSO
- Ignition Guest Manager SMALL
- Ignition Posture SMALL
- Ignition Server Base SMALL
- Ignition TACACS+

License Details:

```
Feature:  Ignition TACACS+
License Type:  KRS
Valid From:  2012-12-31 16:00:00
Valid Until:  2013-12-30 16:00:00
Issuer:  Avaya Inc., Santa Clara, CA
Issue Date:  2013-01-24 08:46:24
Licensee:  Avaya Inc.
Comment:  SMALL license for use by AIEIS R&D teams
Node Ids:  Demo License
License Serial Number:  IDE-999999
```

Figure 29: Installed KRS license



Name: Site 0

Licenses:

- Ignition Access Portal LARGE
- Ignition Analytics
- Ignition Aura SSO
- Ignition Guest Manager LARGE
- Ignition Posture LARGE
- Ignition Server Base LARGE

License Details:

```
Feature:  Ignition Server Base LARGE
License Type:  PLDS
Version:  9.0
Authenticator Limit:  Unlimited
```

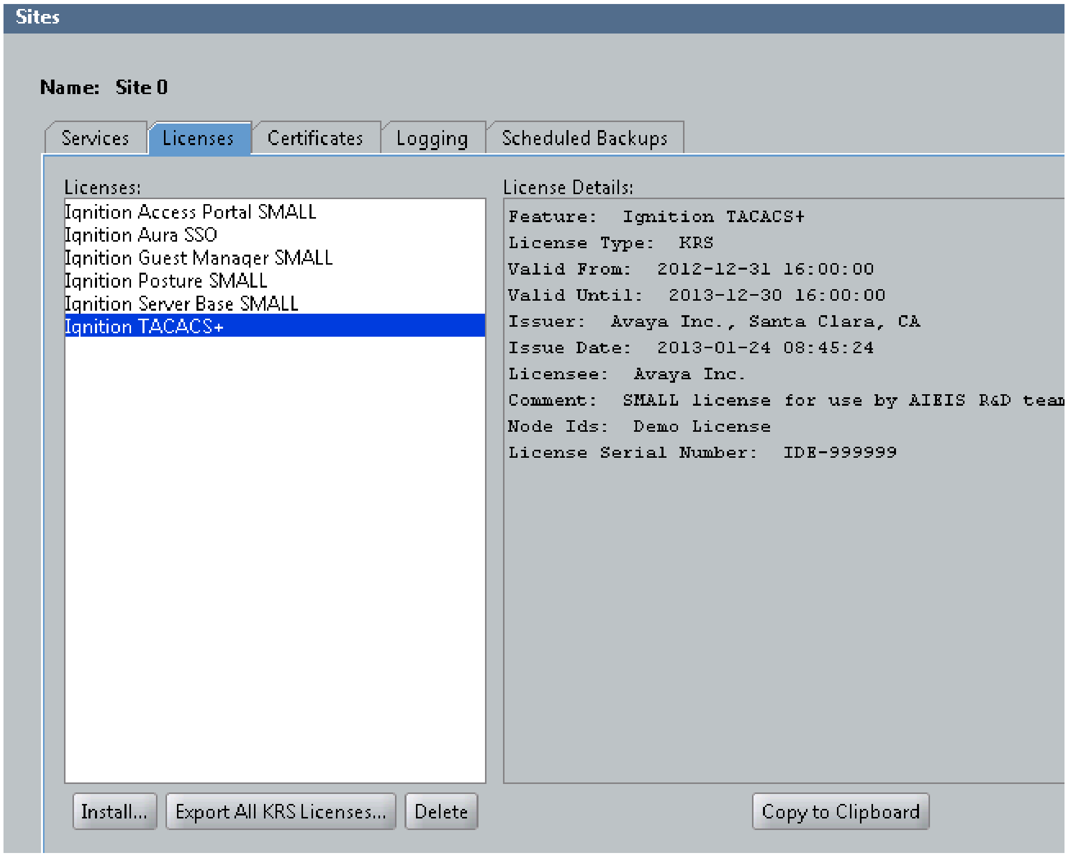
License Installation

License to Install:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE LAR SYSTEM "lar.dtd">
<LAR platformType="IDENTITY_ENGINES" sid="48" version="1.0">
<License version="1.0">
<HostID>621871473571</HostID>
<Notes>License generated by the WebLM PLDS Plug-in (version
1.3.3)  on:
Tue Sep 10 07:28:20 MDT 2013
 ESID: 1
 SID: 48
 MID:
 LicenseOwner: SUEZ ENVIRONNEMENT 1 RUE D ASTORG PARIS 75008
France
 Group:
```

Tip: Paste the license text into the above text area or use the Browse... button to read in a license file.

Figure 30: Installing PLDS license



```
Feature:  Ignition TACACS+
License Type:  KRS
Valid From:  2012-12-31 16:00:00
Valid Until:  2013-12-30 16:00:00
Issuer:  Avaya Inc., Santa Clara, CA
Issue Date:  2013-01-24 08:45:24
Licensee:  Avaya Inc.
Comment:  SMALL license for use by AIEIS R&D tea
Node Ids:  Demo License
License Serial Number:  IDE-999999
```

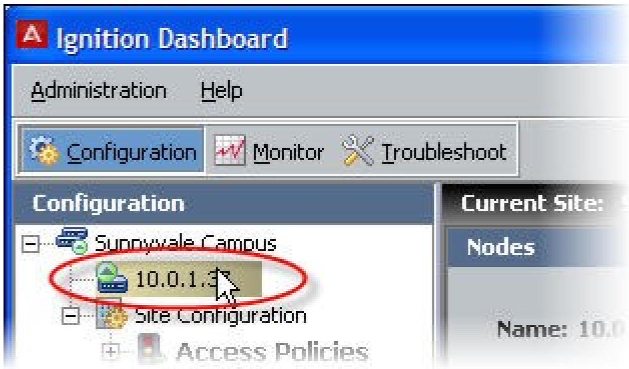
Figure 31: Installed PLDS license

Setting up the Service Port (Optional)

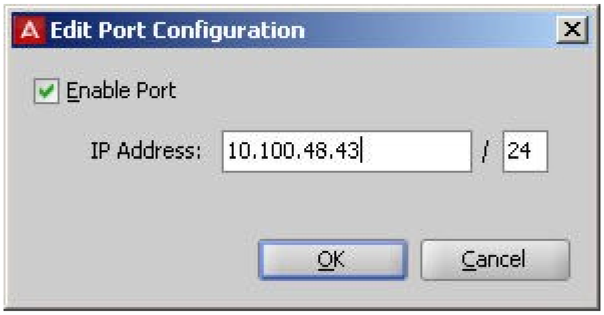
Use this procedure to configure the Service Port.

Procedure

1. In the Dashboard navigation tree, click on the IP address or name of your Ignition Server appliance (node).



2. In the Nodes panel, click the **Ports** tab, and click the **Service Port** row.
3. Click the **Edit** button.
4. In the Edit Port Configuration window, do the following:



☑ Enable Port

IP Address: 10.100.48.43 / 24

- Click **Enable Port**.
- Set the port address in the **IP Address** field, and set the subnet mask in the field to the right. Use the port settings you wrote down in Step 3 on page 23. You must enter the subnet using network prefix notation (an integer between 0 and 32 representing the number of bits in the address that will be used in the comparison).

Setting the admin password and set user, site, and node names

Use this procedure to configure the administration password, user, site, and node names.

Procedure

1. In the main navigation tree of Dashboard, click on the site (called “Site 0” by default, this is typically the top item in the tree).

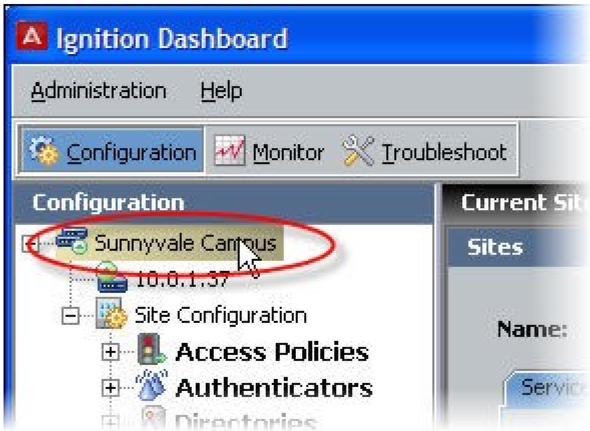


Figure 32:

2. Select the command, **Actions: Change User Name** to change the administrator login name.
3. Select the command, **Actions: Change Password** to change the administrator password.
4. Select the command, **Actions: Rename Site** to rename the site. A site is typically a pair of Ignition Servers, but it may consist of just one server.
5. To rename your node (your Ignition Server appliance) do this: In Dashboard's main navigation tree, right-click on the IP address or name of your Ignition Server appliance and choose the command **Rename Node**.

Next steps

Your basic set-up is complete. See Further configuration on page 41 below for your next steps.

Further configuration

To prepare the Ignition Server appliance for testing or production use, your next step is to connect it to your switches, wireless access points, and user data stores, as explained in the next chapter, Configuration on page 43. For more detailed information on Ignition features, consult the *Avaya Identity Engines Ignition Server Administration Guide*.

Chapter 4: Configuration

The chapter assumes you are familiar with network terminology, have experience setting up and maintaining networks and network security, and have installed your Ignition Server appliance as shown in the previous chapter, Getting started on page 15.

The following steps describe how to configure Ignition Server for providing Network Access Control:

- Create a RADIUS access policy on page 48
- Create a user in the internal user store on page 50
- Set up your connection to a user store on page 51
    - Connecting to Active Directory on page 52
    - Connecting to LDAP on page 68
- Setting up a RADIUS proxy server on page 78
- Create a directory set on page 80
- Create virtual groups on page 83
- Set your authentication policy on page 90
- Set your authorization policy on page 94
- Set your identity routing policy on page 92
- Set your authorization policy on page 94
- Test your configuration on page 100

Make sure you have a copy of *Administering Avaya Identity Engines Ignition Server*, NN47280–600 available. *Avaya Identity Engines Ignition Server Getting Started Configuration* explains a simple configuration, whereas *Administering Avaya Identity Engines Ignition Server* provides a complete reference showing other configuration options.

See *Configuring And Managing Avaya Identity Engines Single-Sign-On* (NN47280–502) for help configuring Ignition Server to provide Single-Sign-On for applications.

Before you begin

Make sure you have completed the following set-up tasks before you start configuring the Ignition Server appliance.

1. **Network settings:** Complete the steps shown in the previous chapter, Getting started on page 15
   - Set up the Ignition Server appliance and set its network settings.
   - Install Ignition Dashboard on your Windows OS.
2. **Switch settings:** Configure each authenticator (network switch or wireless access point) to recognize the Ignition Server appliance as its RADIUS server. To do this, use the management tools of each switch to set the switch's RADIUS server address to the Ignition Server ADMIN or SVC interface IP address. (By default, Ignition Server handles RADIUS requests on its ADMIN interface, but you can change this to the SVC interface as shown in Step 5 on page 46.) Use UDP port 1812 as the RADIUS server port.
3. **802.1X settings:** If you will use 802.1X authentication:
   - Use the management tools of each switch or access point to enable 802.1X authentication on that device.
   - On client machines that will connect to the network, make sure a wireless/wired, 802.1X-capable supplicant is installed and configured for 802.1X authentication.
   - If you wish to follow the example configuration in this document, make sure the supplicant is set up for PEAP/MSCHAPv2 authentication.
4. **RADIUS accounting settings:** If you will use RADIUS accounting, configure your switch or access point to send its accounting packets to the Ignition Server appliance. To do this, use the management tools of your device, setting the appropriate Ignition Server IP address as the RADIUS server address and port 1813 as the RADIUS accounting port.
5. **VPN client settings:** If you will use IPSec for VPN access, make sure that client machines (those that will VPN into the network) have an installed VPN client that speaks PAP or MSCHAPv2.

Next Steps: Proceed to the next section to set up the Ignition Server appliance.

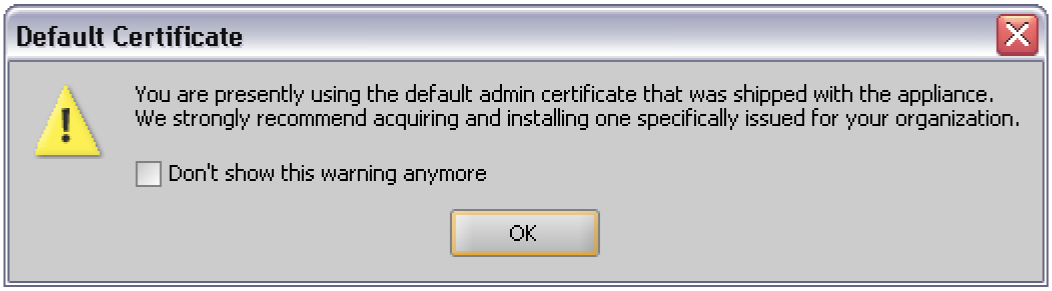
Make settings on the Ignition Server appliance

You use Ignition Dashboard to set the Ignition Server appliance, perform network configurations, and specify the network parameters for the RADIUS Service.

Procedure

1. Start Ignition Dashboard: Double-click Ignition Dashboard icon on your **Start** > **Programs** > **Ignition Dashboard** > **Ignition Dashboard**. The application displays its login window.

2. Type the System administrator **User Name** and **Password**. The default login credentials are `admin/admin`. In the **Connect To** field, enter the IP address of your Ignition Server appliance, and click **OK**.



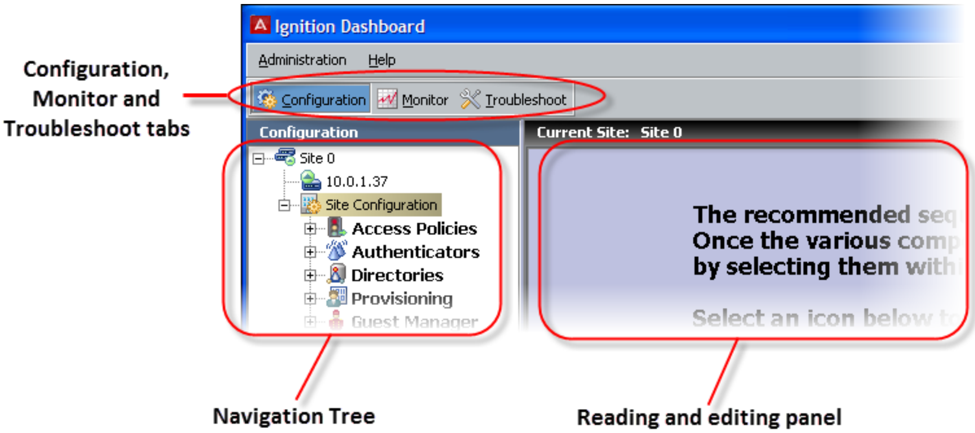
Default Certificate

You are presently using the default admin certificate that was shipped with the appliance.
We strongly recommend acquiring and installing one specifically issued for your organization.

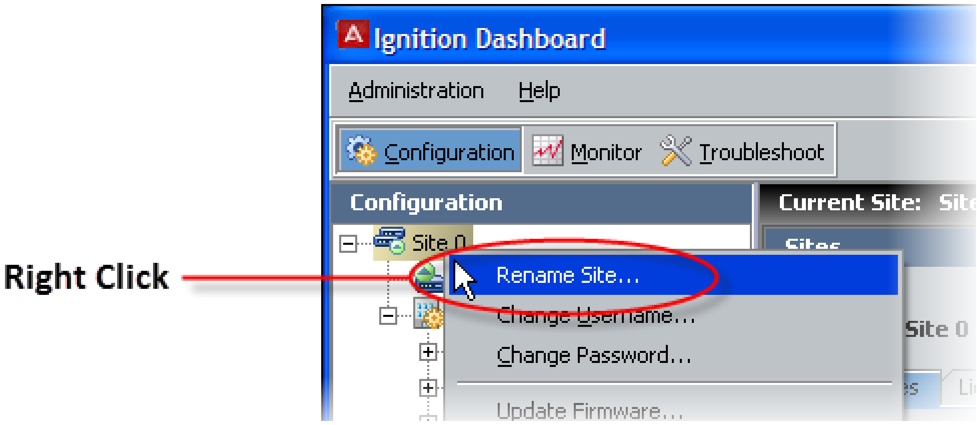
□ Don't show this warning anymore

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.

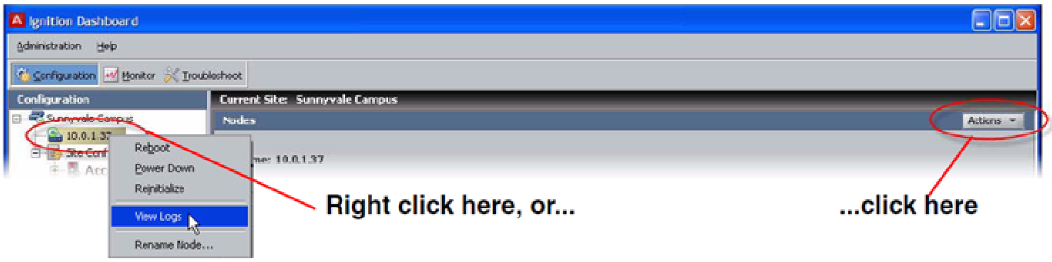


3. In the **Configuration** tree, click on Site 0, then right-click on Site 0 and select the **Rename Site** command. In the **Rename Site** dialog, type a name for your site. Your site is your Ignition Server or your HA pair of Ignition Servers. In this example, we'll use the name Sunnyvale Campus. Click **OK** to accept the new name.



4. In the navigation tree, click on the machine name or IP address of the Ignition Server appliance you wish to configure. The application displays the Nodes panel, which allows you to manage network settings on the appliance, and check its current status.

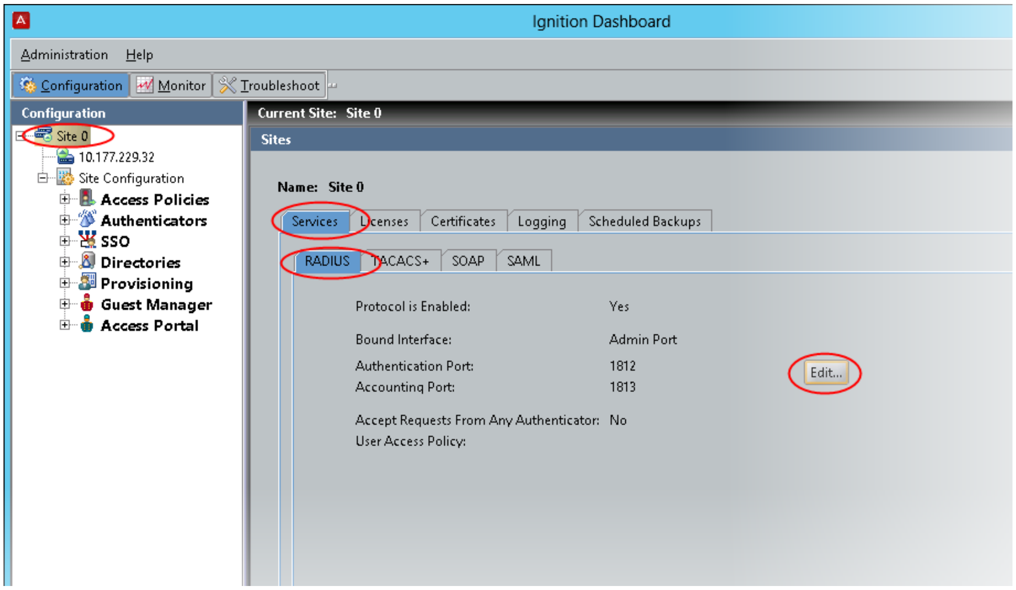
   Hint: The **Actions** menu allows you to manage the appliance hardware (actions such as rebooting and shutting down). To use the Actions menu, right-click the IP address of your Ignition Server in the navigation tree, or, with the IP address selected, click the Actions menu at the upper right.



5. Optional: If you intend to separate your *authentication network* from your *network management* network, do the following. For most installations, this is not necessary.

   a. *Do this only if your authentication network is separate from your management network.* **Activate the Service Port (“SVC”)**: In Dashboard’s navigation tree, click the IP address/name of your node. Click the **Ports** tab, click the **Service Port** row, and click **Edit**. Click the **Enable** check box and, in the **IP Address** field assign an address to the port. In the adjacent field type the net mask. Click **OK**.

   b. *Do this only if your authentication network is separate from your management network.* Bind Ignition Server’s RADIUS service to the service port (“SVC”): In Dashboard’s navigation tree, click the name of your site (for example, Site 0 or Sunnyvale-Campus). Click the **Services** tab, click the **RADIUS** tab, and click **Edit**.



Name: Site 0

Protocol is Enabled: Yes

Bound Interface: Admin Port

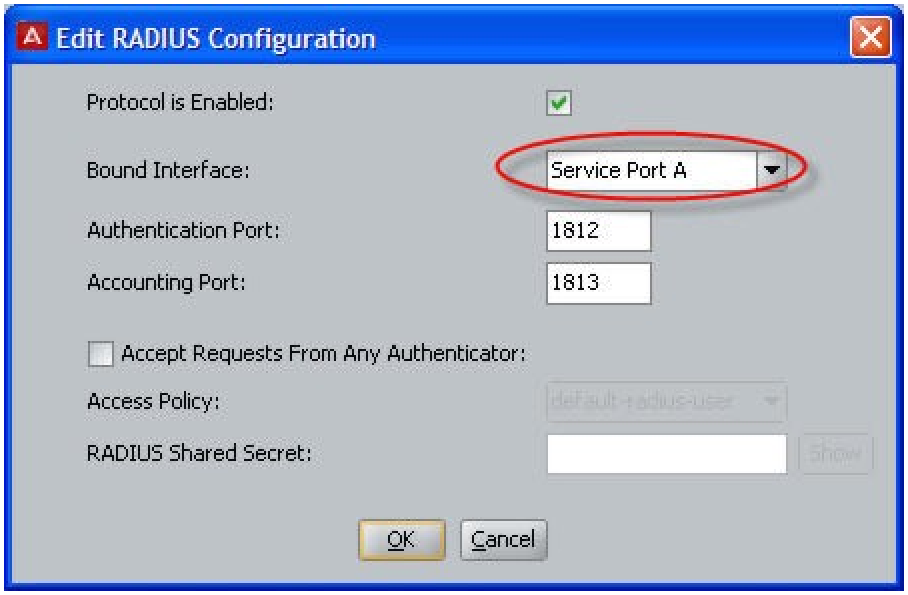
Authentication Port: 1812

Accounting Port: 1813

Accept Requests From Any Authenticator: No

User Access Policy:

In the Edit RADIUS Configuration window, set the Bound Interface to Service Port. In the Authentication Port and Accounting Port fields, use the default values of 1812 and 1813 unless your authenticators require a different RADIUS server port. Click **OK**.



Protocol is Enabled: ☑

Bound Interface: Service Port A

Authentication Port: 1812

Accounting Port: 1813

☐ Accept Requests From Any Authenticator:

Access Policy: default-radius-user

RADIUS Shared Secret:

c. *Do this only if you authentication network is separate from your management network: Make sure you have plugged in the cable connecting the Ignition Server's* **SVC** interface to the network that contains your switches, access points, and other authenticators.

6. Reboot your Ignition Server by right-clicking its IP address in the navigation tree and selecting the **Reboot** command.

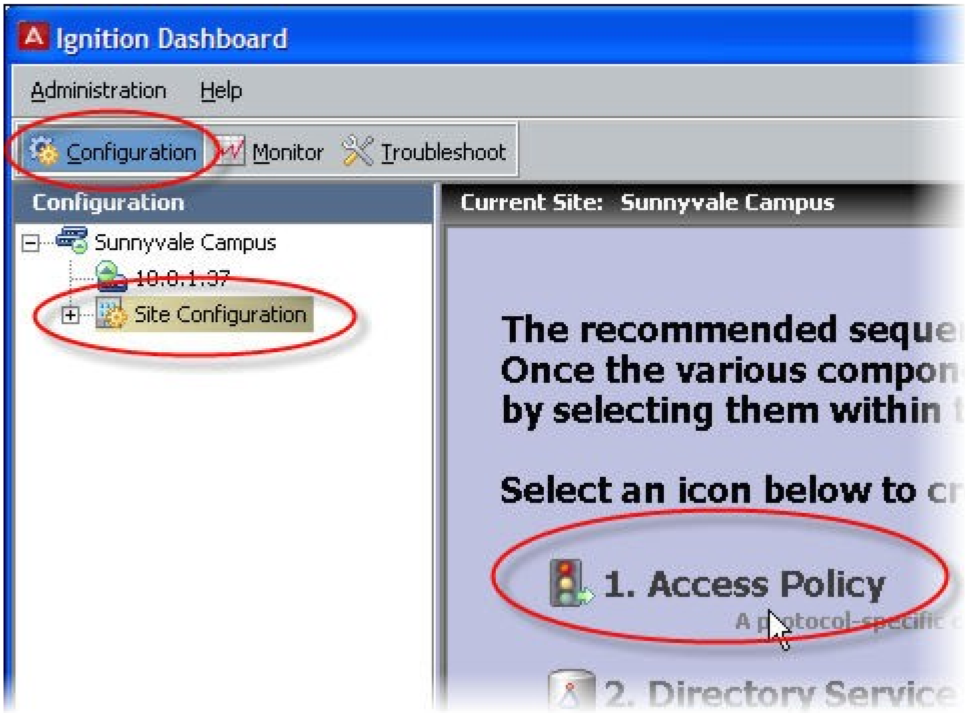
Next steps

Proceed to the next section to create a basic access policy.

Create a RADIUS access policy

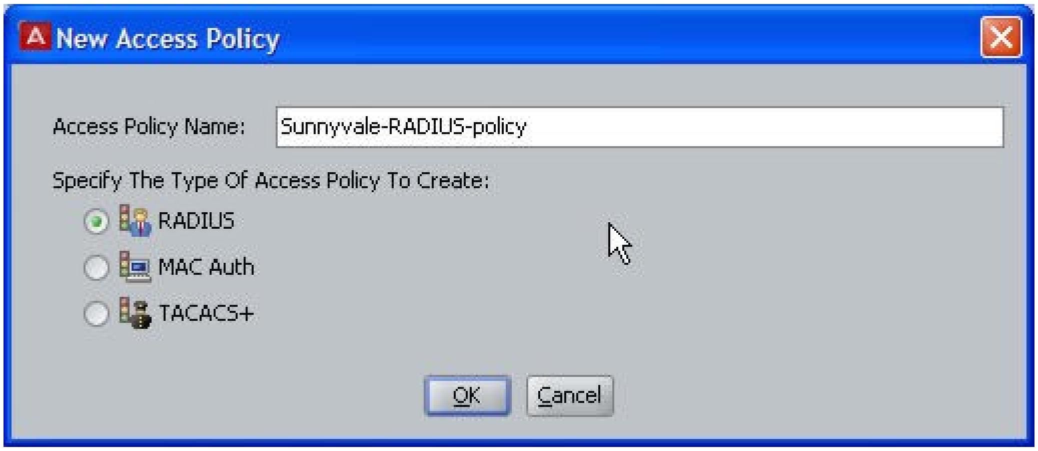
Your RADIUS access policy contains the rules that determine how a user must authenticate and, based on the user's identity, what network the user will be allowed to use.

Each authenticator has one RADIUS access policy applied to it, meaning that all users connecting through that authenticator are governed by that RADIUS access policy.



Procedure

1. If Dashboard is not connected to your Ignition Server, connect it now by selecting **Administration: Login**.
2. In the main window of Dashboard, click **Configuration**, click **Site Configuration** in the navigation tree, and click **Access Policy** in the main window.
3. In the New Access Policy window, type a name for your policy and click the **RADIUS** check box. The name typically offers a clue as to which authenticators will use this policy. For example, the name may indicate the location of the authenticators.



Access Policy Name: Sunnyvale-RADIUS-policy

Specify The Type Of Access Policy To Create:

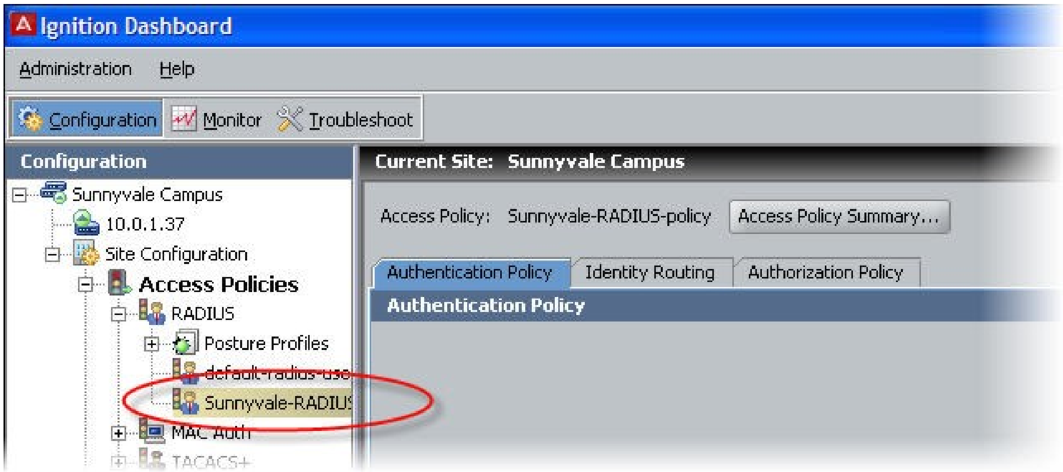
● RADIUS

○ MAC Auth

○ TACACS+

4. Click **OK**.

   Your access policy has been saved. For now, we will leave the policy empty. Later, you can add rules to it by clicking on the **Configuration** tab, expanding the **Site Configuration** item in the tree (click the plus sign to expand an item), and expanding the **RADIUS** item in the tree. Click the name of your policy and use the tabs and **Edit** buttons in the main panel to edit the policy.



Current Site: Sunnyvale Campus

Access Policy: Sunnyvale-RADIUS-policy

   You will add rules to your access policy later, as shown in the section, Set your authentication policy on page 90.

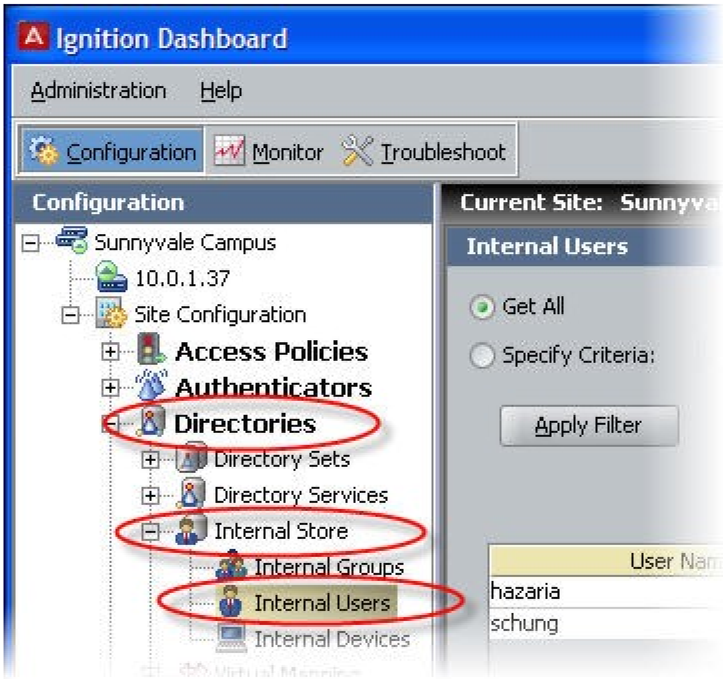
Next steps

Create a user account as shown in Create a user in the internal user store on page 50.

Create a user in the internal user store

This section is optional. If you do not plan to use the Ignition Server internal user store, skip this section and go to Set up your connection to a user store on page 51.

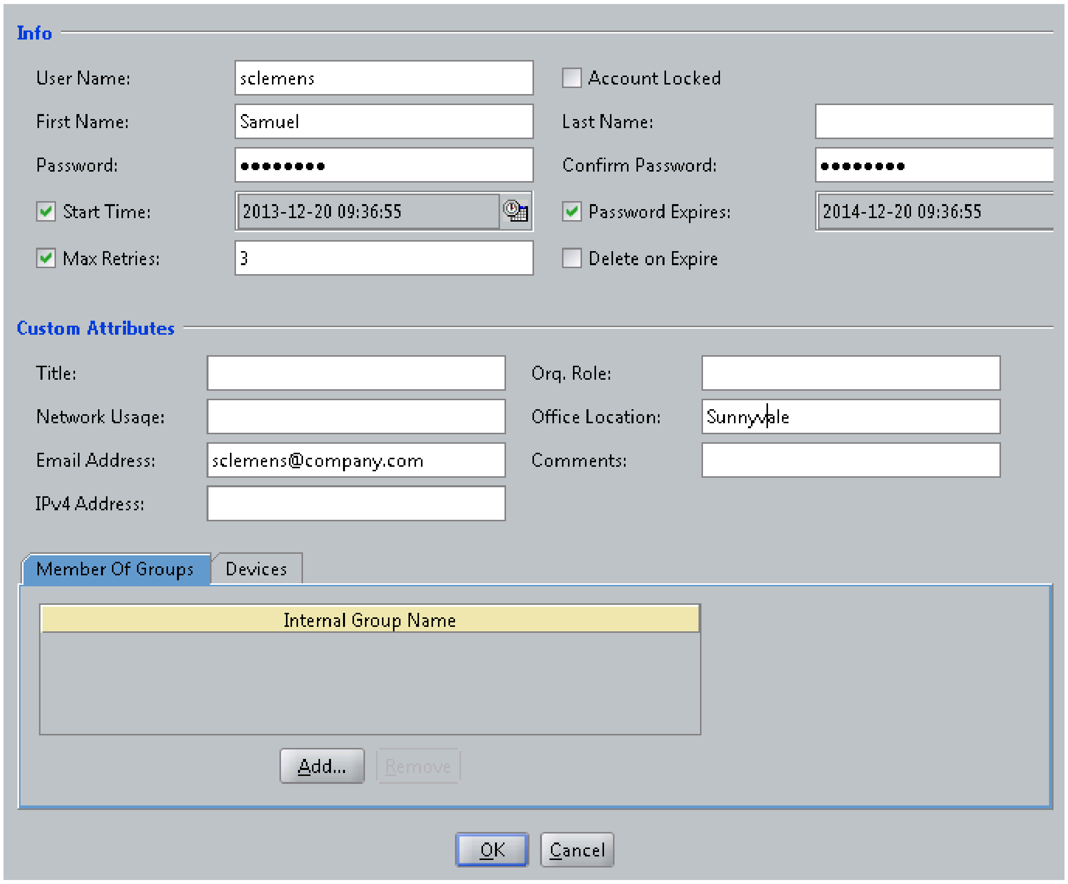
Ignition Server typically authenticates users against your corporate user store (for example an Active Directory or LDAP store), but the Ignition Server appliance also contains a local store, called the internal user store. You can use the embedded store to complement your corporate AD or LDAP store. For example, you may wish to create temporary guest user accounts in the embedded store, rather than placing them in the corporate user store where employee accounts reside.



This section creates a user account in the internal user store. Later, we will build the access policy to determine this user’s access rights.

Procedure

1. In Dashboard’s **Configuration** tab, click the plus sign next to **Directories** and click the plus sign next to **Internal Store**. Click on **Internal Users**. At the bottom of the window, click **New** .



Info

User Name: sclemens

☐ Account Locked

First Name: Samuel

Last Name:

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

☑ Start Time: 2013-12-20 09:36:55

☑ Password Expires: 2014-12-20 09:36:55

☑ Max Retries: 3

☐ Delete on Expire

Custom Attributes

Title:

Org. Role:

Network Usage:

Office Location: Sunnyvale

Email Address: sclemens@company.com

Comments:

IPv4 Address:

2. In the user editing window, in **User Name**, enter `sclemens`, in **First Name** enter `Samuel`, in **Last Name** enter `Clemens`, in **Password** enter `secret12` (or any password you like), in **Confirm Password** enter the password again. Click **OK** to save the user.

Next steps

Connect to your enterprise user store as shown in Set up your connection to a user store on page 51

Set up your connection to a user store

The Avaya Identity Engines' Ignition Server appliance can be configured to retrieve users from any combination of internal and external data stores, including external Active Directory (AD) and LDAP stores, as well as the internal user store of the Ignition Server 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 will define one directory service. After you define your directory services, you will place them in directory sets that tell Ignition Server when to use which service.

Note:

If you are using only the Ignition Server embedded store to store user accounts, you do not need to create a directory service. Instead, proceed to Create a directory set on page 80.

To connect to your used data store, use one of the following procedures:

- Prepare to connect to Active Directory on page 55
- Connecting to LDAP on page 68

Related topics:

Connecting to Active Directory on page 52
Troubleshooting AD and LDAP connections on page 72

Connecting to Active Directory

The rest of this section explains how to connect to an Active Directory data store that contains your site's user accounts and groups. Once the Ignition Server has connected to AD and joined the domain, it can authenticate users against Active Directory.

Related topics:

Gather Active Directory connection settings on page 52
Prepare to connect to Active Directory on page 55
Create the Service Account in AD on page 57
Set the AD permissions of the service account on page 59
Connect Ignition Server to AD on page 63
Editing a directory service on page 68

Gather Active Directory connection settings

Gather your AD connection settings. Use the AD connection settings that you used and created, or talk to your AD administrator to find the connection settings for your AD data store. Record them in the table that follows. Gather this information for each store that will authenticate users.

Table 1: Settings for connecting to an AD store

Setting name	Setting value
AD Domain Name	The AD Domain Name specifies the Active Directory domain that holds your user accounts. Domain names

Setting name	Setting value
	typically carry a domain suffix like ".COM" as in, for example, "COMPANY.COM".
Service Account Name	The **Service Account Name** is the name of the AD administrator account that the Ignition Server will use to connect to the AD server. In the documentation, we refer to this account as the *Ignition Server service account*. If you wish to perform MSCHAPv2 authentication, the service account must have permission to create and delete computer accounts (the Create Computer Object and Delete Computer Object permissions) in the Netlogon account root in Active Directory. See "Netlogon account root DN," below. 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. ✱ **Note:** Make sure that the name you enter here is the sAMAccountName of the administrator. The sAMAccountName is usually the user id of the user without the domain prefix. For example, the sAMAccountName for the user COMPANY.COM/Administrator will usually be Administrator. For help creating the service account, see Create the Service Account in AD on page 57. For help setting its permissions, see Set the AD permissions of the service account on page 59.
Service Account Password	The **Service Account Password** is the password for the AD service account. *Do not record the password here.*
Security Protocol	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). *Please use the LDAP ports (389 and 636) only!*

Setting name	Setting value
Name	The Name is a name you will 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, as in, “COMPANY”. This setting applies only to Active Directory stores. For instructions on using Microsoft tools to find this name, see Looking up AD settings: Finding Domain and NetBIOS names on page 76.
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.
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 will attempt to choose a Directory Root DN for you. See Looking up AD settings: Finding your Root DNs on page 75 for information on finding this DN.
User Root DN	The User Root DN specified the AD container that holds your user records, expressed using X.500 naming. For example, cn=users,dc=company,dc=com or ou=uswest,ou=americas,dc=company,dc=com. When you connect the directory service, the Ignition Server Create Service wizard will attempt to choose a User Root DN for you. See Looking up AD settings: Finding your Root DNs on page 75 for information on finding this DN.
Netlogon Account Root DN	The Netlogon Account Root DN is the container in AD where the Ignition Server will create its own machine account when joining the AD domain. This setting is optional. If specified, Ignition Server will only attempt to create its 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.The Netlogon account root DN is typically the Active Directory Computers container (by default, this has a DN similar to cn=computers,dc=company,dc=com). The machine

Setting name	Setting value
	account is required so that Ignition Server can perform Netlogon authentication requests for MSCHAPv2 traffic to AD. If you wish to perform MSCHAPv2 authentication, then your service account must have appropriate permissions in this DN. For help setting account permissions, see Set the AD permissions of the service account on page 59.

Next steps: Prepare your environment as explained in Prepare to connect to Active Directory on page 55.

Prepare to connect to Active Directory

Check and, if needed, address the following before you try to connect.

⚠ **Warning:**

If you plan to use MSCHAPv2 authentication, you must perform the checks listed here.

Procedure

1. **Make sure you have gathered your AD connection settings** as explained in Gather Active Directory connection settings on page 52
2. **Check your clock settings.** When the Ignition Server connects to an Active Directory server, the Ignition Server clock must be in sync with the clock on the Active Directory Server. If the clocks are out of sync, then the Ignition Server cannot connect to the Active Directory store.
3. **Check your firewall settings.** If a firewall protects your Active Directory server, make sure 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. **Check your Active Directory security settings.** Ignition Server works with all default installations of AD, but if you have adjusted your AD installation to prohibit NTLMv1 authentication, then Ignition Server cannot perform MSCHAPv2 authentication.

   To make sure NTMLv1 authentication is enabled in your AD installation, check the following two settings in the Windows registry of your Windows domain controller (DC). Use the Windows *regedit* tool to do this.

   - Make sure that the following key is not set on the DC:

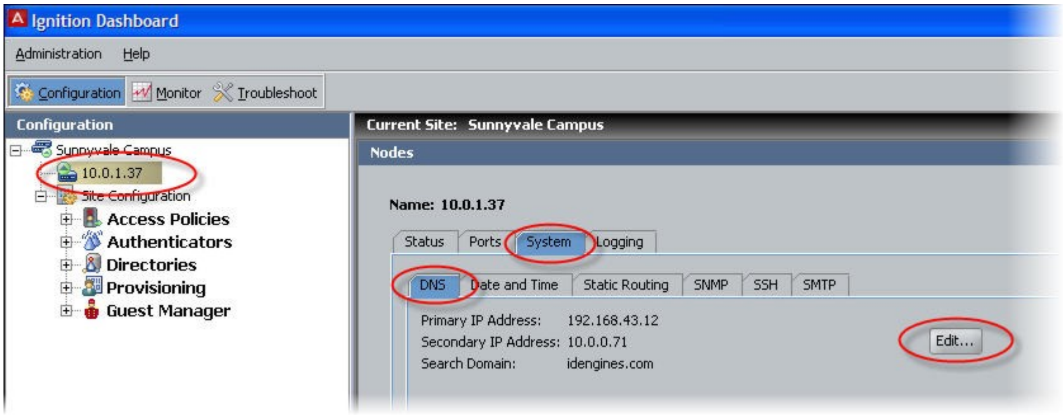
     ```
     HKLM\System\CurrentControlSet\LSA\DisallowMsvChapv
     ```

- Make sure that the following key is set to a value of 1, 2, 3, or 4. A setting of 5 will cause Ignition Server's support for MSCHAPv2 authentication to fail in all cases. The key name is:

```
HKLM\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel
```

5. **Find or create your service account.** Make sure you have a user account in AD that can act as the Ignition Server Service Account. If you need to create a new account, follow the instructions in Create the Service Account in AD on page 57.
6. **Set permissions on your service account.** If you wish to perform MSCHAPv2 authentication, make sure your Ignition Server Service Account has, at a minimum, permission to create and delete computer accounts in the Netlogon account root of AD. If you need set this up, follow the instructions in Set the AD permissions of the service account on page 59.
7. **Optional: Check your machine authentication settings.** If your organization's security policy requires a script to run on each client before that client may connect, then do the following:
   - Make sure all client machine names are saved in the correct location in AD, which is typically under "cn=computers, ...".
   - Make sure this location is set in Ignition Server as the User Root DN or any container above that in the directory tree.
8. **Recommended: Make DNS settings on Ignition Server.** If your site uses MSCHAPv2 authentication, Avaya strongly recommends that you configure your Ignition Server appliance's DNS settings so that Ignition Server can resolve the address of your AD server.

   To check and edit your DNS settings, click **Configuration** in the Dashboard main window, click the name of your node in the navigation tree, then click the **System Tab**, and click the **DNS** tab. Click **Edit**. You can check and edit the addresses of your DNS servers in the **Edit DNS** Configuration window.



Current Site: Sunnyvale Campus

Name: 10.0.1.37

Primary IP Address: 192.168.43.12
Secondary IP Address: 10.0.0.71
Search Domain: idengines.com

Next steps

Connect to AD as explained in Connect Ignition Server to AD on page 63.

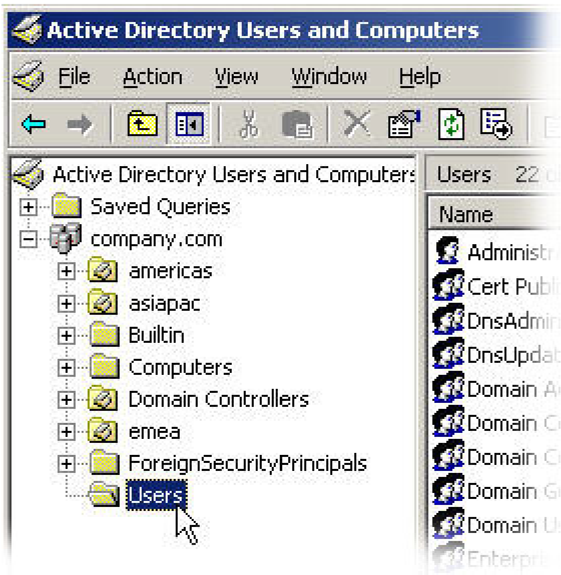
Create the Service Account in AD

To connect to Active Directory, the Ignition Server appliance requires a user account (which we call a service account) in Active Directory. If you wish to perform MSCHAPv2 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.

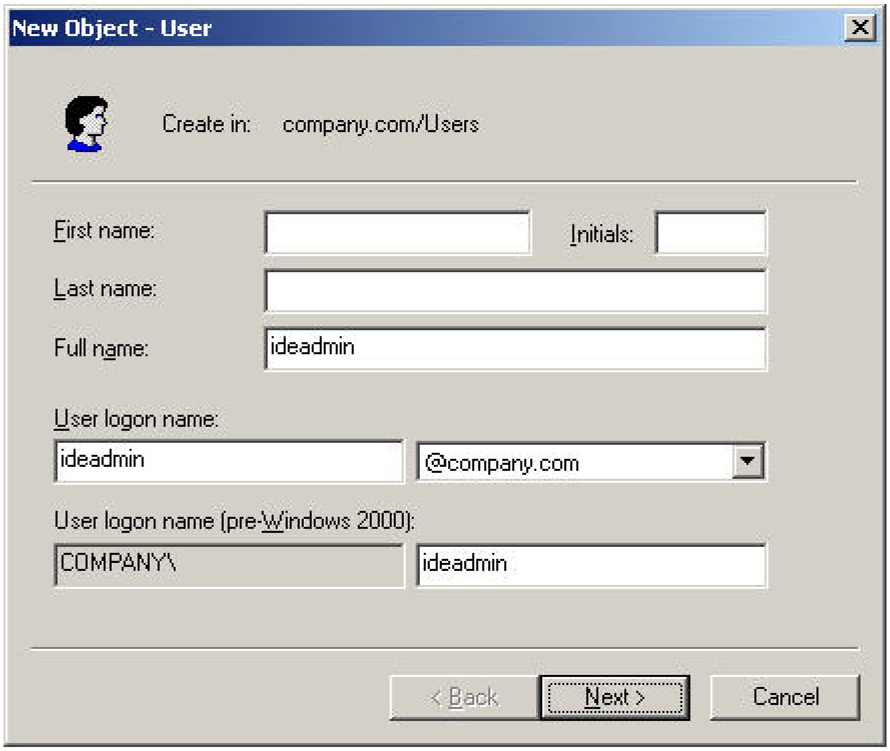
If you have a suitable account already, you may skip this section and go to Set the AD permissions of the service account on page 59. If you wish to create an account, follow the steps below.

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 **Action > New > User**.
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 appliance. For this example, we use the account name, "ideadmin". Click **Next** after specifying the name.



New Object - User

Create in: company.com/Users

First name:

Initials:

Last name:

Full name: ideadmin

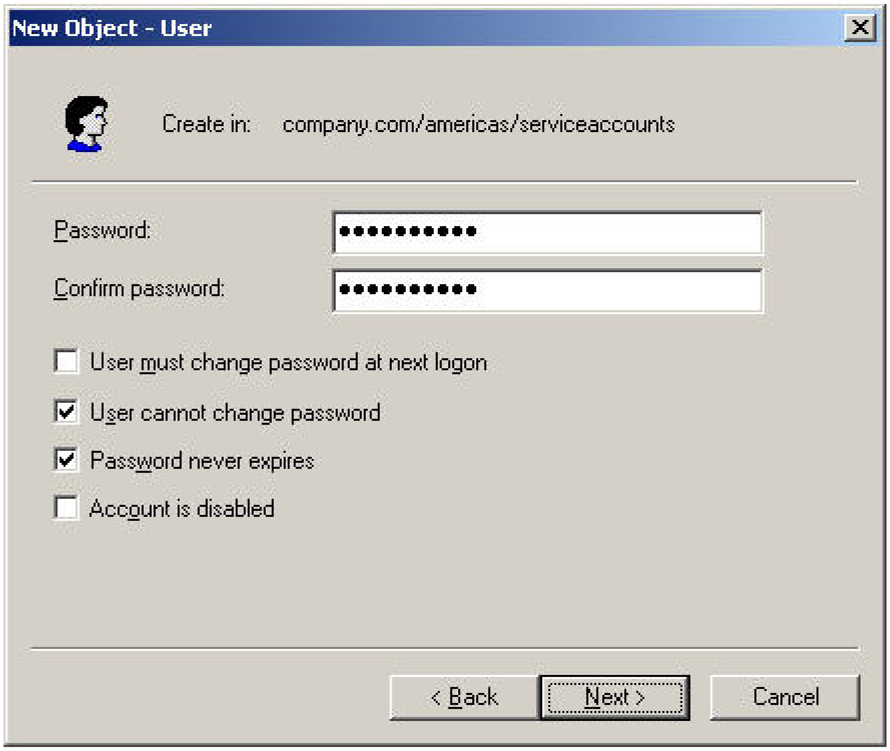
User logon name:

ideadmin @company.com

User logon name (pre-Windows 2000):

COMPANY\ ideadmin

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** check boxes.



New Object - User

Create in: company.com/americas/serviceaccounts

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

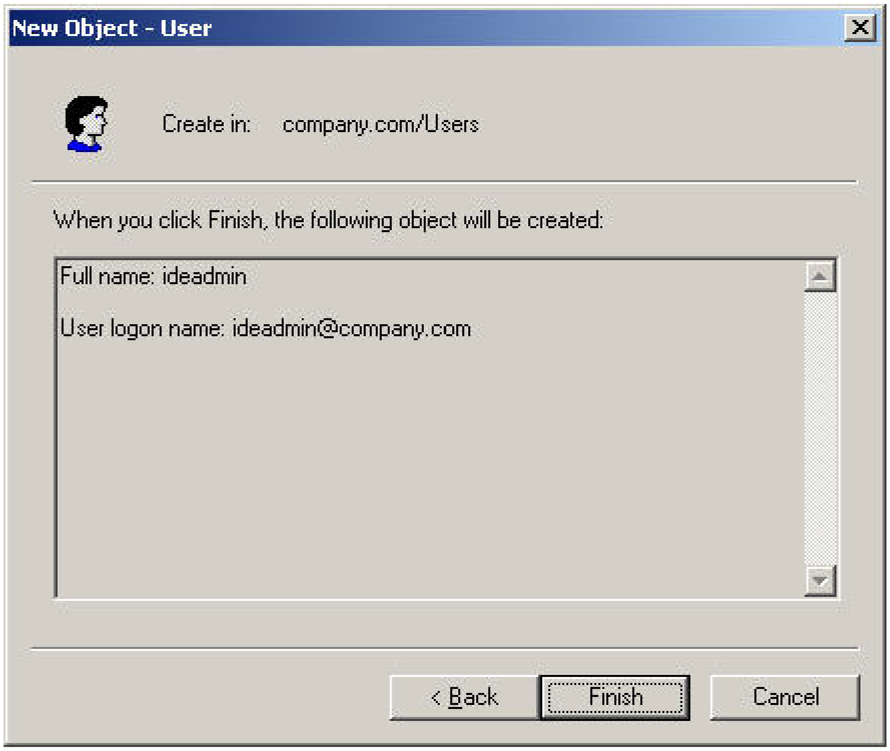
□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

7. Click **Finish** to save the new account.



Create in: company.com/Users

When you click Finish, the following object will be created:

Full name: ideadmin

User logon name: ideadmin@company.com

Set the AD permissions of the service account

If you plan to support MSCHAPv2 authentication, the Ignition Server service account must have permission to create and delete computer accounts (the *Create Computer Object* and *Delete Computer Object* permissions) in the *Netlogon account root* of your Active Directory service. (For a description of this container, see Netlogin Account Root DN in Settings for connecting to an AD Store on page 52 .

This section shows you how to grant the minimal required permissions to your service account. If your service account already has the right permissions, proceed to Gather Active Directory connection settings on page 52 instead.

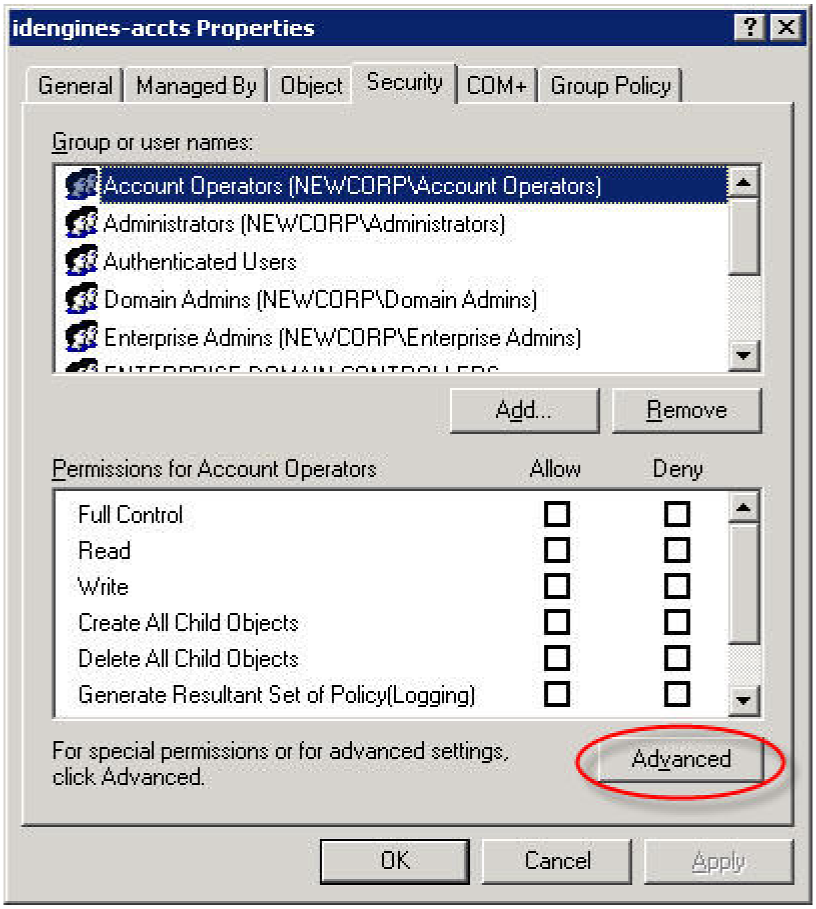
Procedure

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 may configure the location Ignition Server will use as

the Netlogon account root. See Netlogin Account Root DN in Settings for connecting to an AD Store on page 52 for information on setting or finding this DN.

If you want to create a new container that will 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**.



Group or user names:

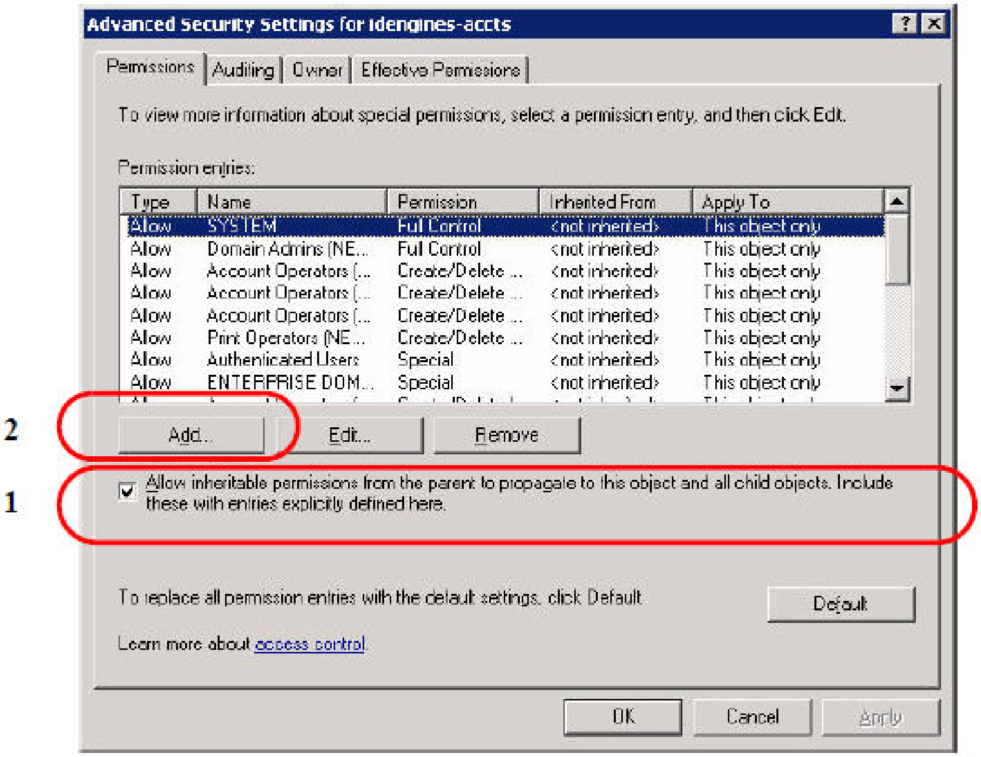
- Account Operators (NEWCORP\Account Operators)
- Administrators (NEWCORP\Administrators)
- Authenticated Users
- Domain Admins (NEWCORP\Domain Admins)
- Enterprise Admins (NEWCORP\Enterprise Admins)

Permissions for Account Operators	Allow	Deny
Full Control	□	□
Read	□	□
Write	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Generate Resultant Set of Policy(Logging)	□	□

For special permissions or for advanced settings, click Advanced.

5. In the **Advanced Security Settings** window, click the **Permissions** tab and:

   - Make sure the **Allow inheritable permissions from the parent to propagate...** check box is selected.
   - Click **Add**.



Advanced Security Settings for idengines-accts

Permissions | Auditing | Owner | Effective Permissions

To view more information about special permissions, select a permission entry, and then click Edit.

Permission entries:

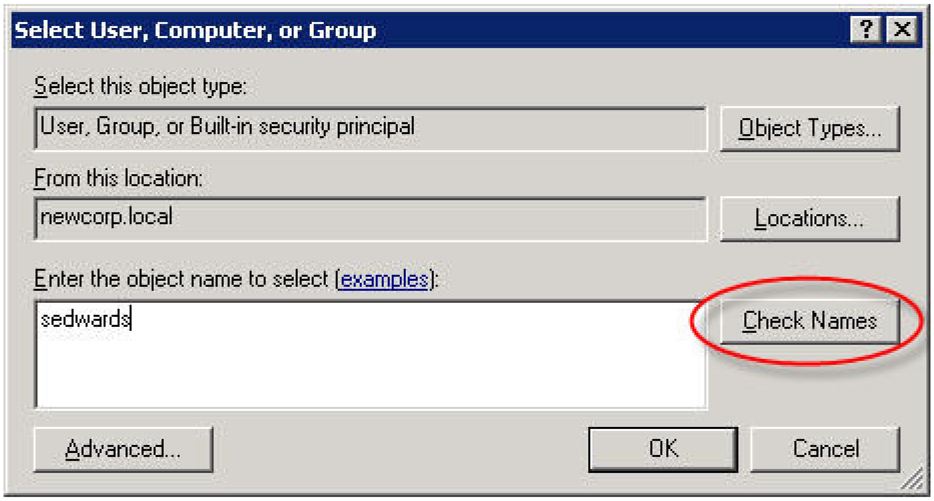
Type	Name	Permission	Inherited From	Apply To
Allow	SYSTEM	Full Control	<not inherited>	This object only
Allow	Domain Admins (NE...	Full Control	<not inherited>	This object only
Allow	Account Operators (...	Create/Delete ...	<not inherited>	This object only
Allow	Account Operators (...	Create/Delete ...	<not inherited>	This object only
Allow	Account Operators (...	Create/Delete ...	<not inherited>	This object only
Allow	Print Operators (NE...	Create/Delete ...	<not inherited>	This object only
Allow	Authenticated Users	Special	<not inherited>	This object only
Allow	ENTERPRISE DOM...	Special	<not inherited>	This object only

☑ Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

To replace all permission entries with the default settings, click Default.

Learn more about access control.

6. In the **Enter the object name** field, type the name or partial name of your Ignition Server service account and click **Check Names**.



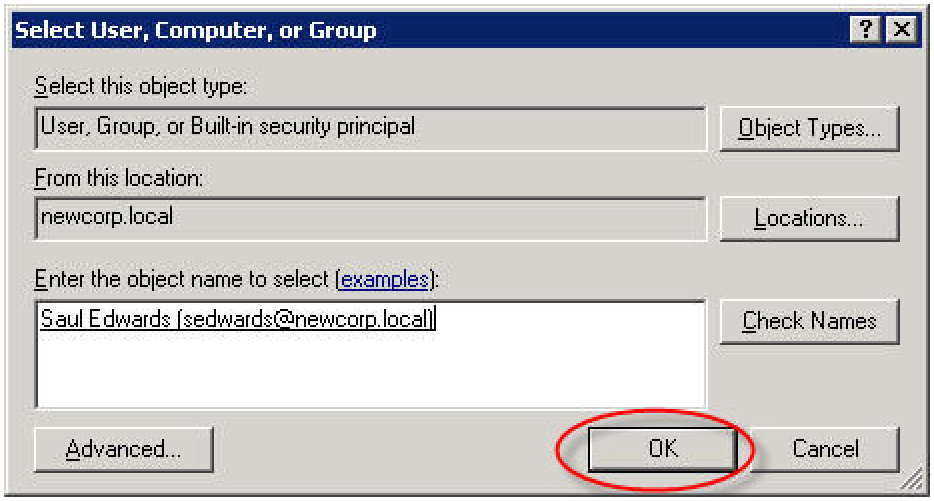
Select User, Computer, or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
newcorp.local

Enter the object name to select (examples):
sedwards

7. The window displays a list of names that match the name you typed. Click the desired account name and click **OK**.



Select User, Computer, or Group

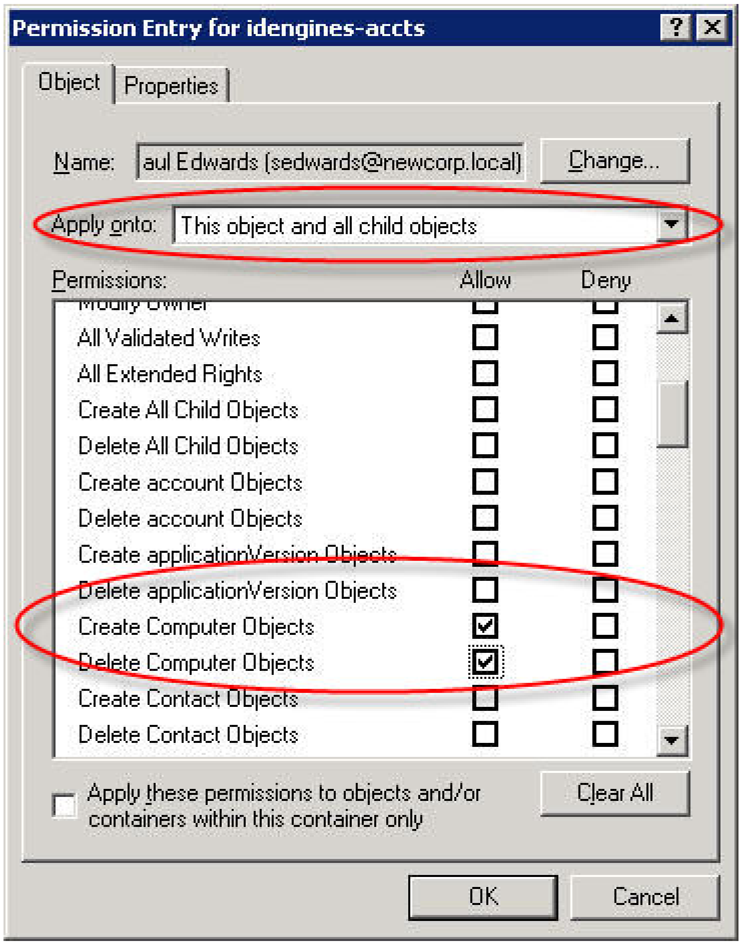
Select this object type:
User, Group, or Built-in security principal

From this location:
newcorp.local

Enter the object name to select (examples):
Saul Edwards (sedwards@newcorp.local)

8. In the **Permission Entry** window, click the **Object** tab and:

    - In the **Apply onto** field, choose **This object and all child objects**.



Permission Entry for idengines-accts

Name: aul Edwards (sedwards@newcorp.local)

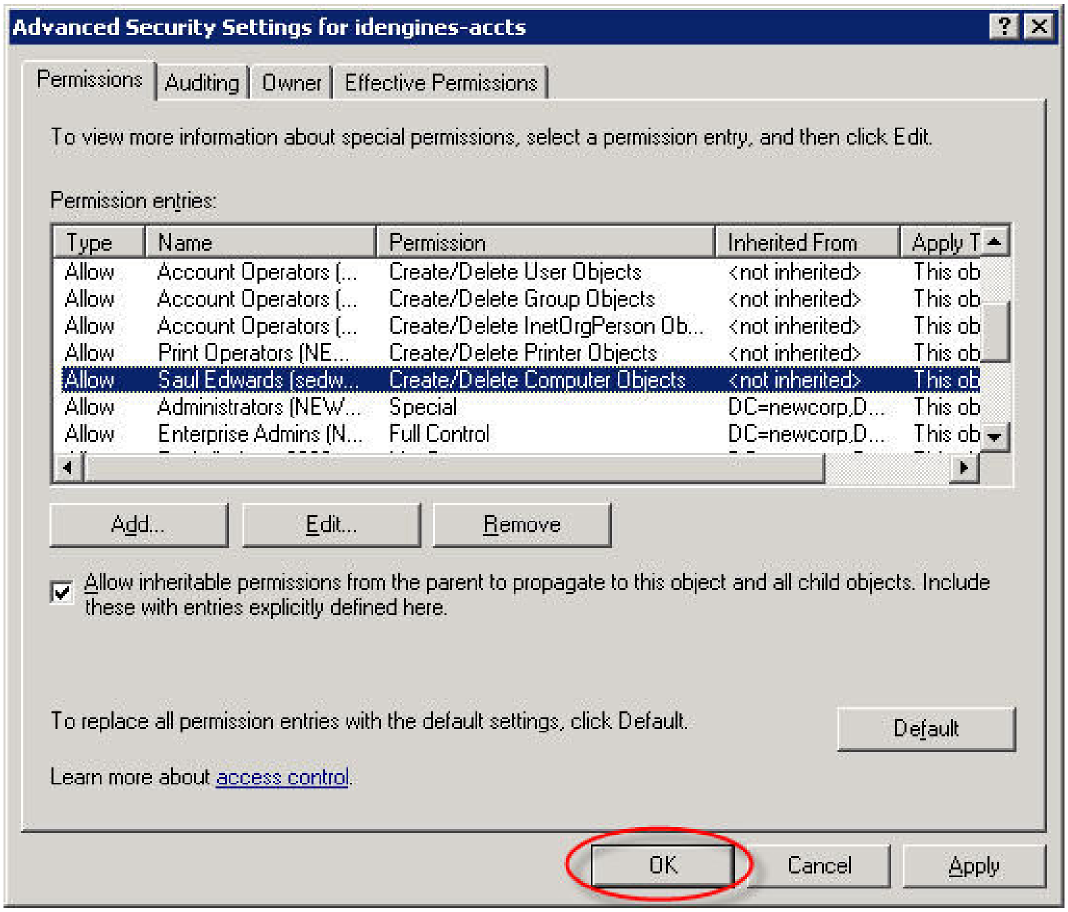
Apply onto: This object and all child objects

Permissions:	Allow	Deny
Modify Owner	□	□
All Validated Writes	□	□
All Extended Rights	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Create account Objects	□	□
Delete account Objects	□	□
Create applicationVersion Objects	□	□
Delete applicationVersion Objects	□	□
Create Computer Objects	☑	□
Delete Computer Objects	☑	□
Create Contact Objects	□	□
Delete Contact Objects	□	□

□ Apply these permissions to objects and/or containers within this container only

- In the permissions table, scroll to find the rows, **Create Computer Objects** and **Delete Computer Objects**, and select the **Allow** check box for each.
- Click **OK**.

9. Click **OK** again to dismiss the Advanced Security Settings window and again to close the snap-in.



To view more information about special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply T
Allow	Account Operators (...	Create/Delete User Objects	<not inherited>	This ob
Allow	Account Operators (...	Create/Delete Group Objects	<not inherited>	This ob
Allow	Account Operators (...	Create/Delete InetOrgPerson Ob...	<not inherited>	This ob
Allow	Print Operators (NE...	Create/Delete Printer Objects	<not inherited>	This ob
Allow	Saul Edwards (sedw...	Create/Delete Computer Objects	<not inherited>	This ob
Allow	Administrators (NEW...	Special	DC=newcorp,D...	This ob
Allow	Enterprise Admins (N...	Full Control	DC=newcorp,D...	This ob

☑ Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

To replace all permission entries with the default settings, click Default.

Learn more about access control.

Now that you have granted the Ignition Server service account the appropriate permissions, the Ignition Server can authenticate users against the AD service.

Next steps

Gather Active Directory connection settings on page 52

Connect Ignition Server to AD

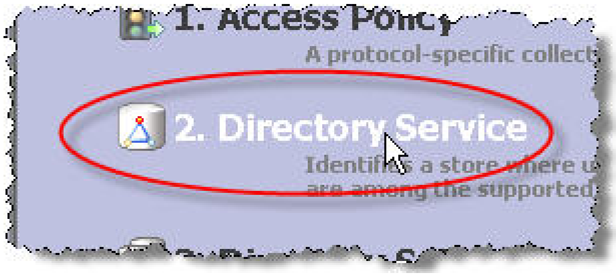
To connect Ignition Server to your Active Directory data store, you will save the AD store as a directory service in Ignition Server. The *directory service* specifies the connection settings that Ignition Server uses to connect to AD. You will create one directory service for each AD domain you wish to connect to, and you can search across multiple directory services by grouping them into a directory set as explained on Create a directory set on page 80.

The sections that follow assume that your user data resides in Active Directory 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, turn to Create the Service Account in AD on page 57.

Connect using Ignition Server's AD connection wizard in *automatic connection* mode.

Procedure

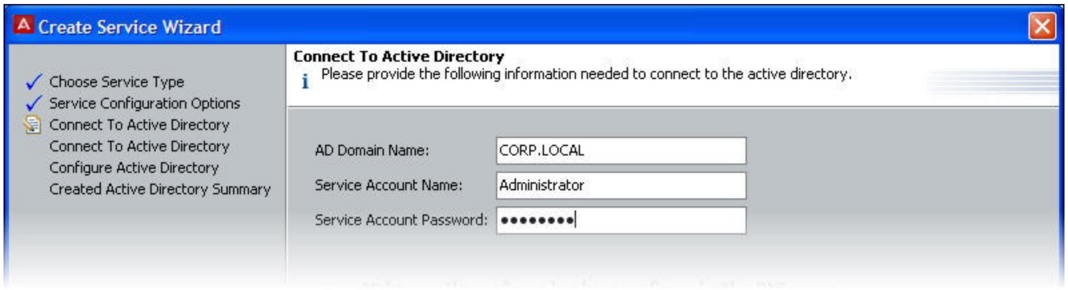
1. In Dashboard's **Configuration** tab, in the navigation tree, click **Site Configuration**.
2. Click the **Directory Service** link in the main panel.



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**.

   If your AD connection attempt fails while you are carrying out the following steps , see Troubleshooting AD and LDAP connections on page 72.
5. The **Connect to Active Directory** window displays.

   Enter the connection settings you gathered in Gather Active Directory connection settings on page 52, or use the login you created in Create the Service Account in AD on page 57.



Create Service Wizard

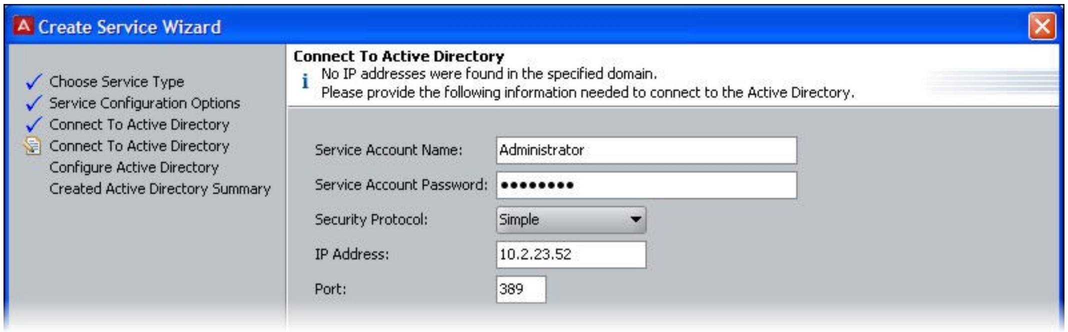
✓ Choose Service Type
✓ Service Configuration Options
Connect To Active Directory
Connect To Active Directory
Configure Active Directory
Created Active Directory Summary

Connect To Active Directory
Please provide the following information needed to connect to the active directory.

AD Domain Name: CORP.LOCAL
Service Account Name: Administrator
Service Account Password: ••••••••

6. In the next screen:
   - Enter the AD service account credentials in the **Service Account Name** and **Password** fields.

  - Pick the **Security Protocol**: choose **Simple** for unencrypted communication with AD, or choose **SSL** for encrypted communication.
  - In the **IP Address** field, type the address of your desired AD server.
- Check the **Port** setting and edit it if needed. Ignition Server defaults to the port number used by most AD servers.


Create Service Wizard
✓ Choose Service Type
✓ Service Configuration Options
✓ Connect To Active Directory
Connect To Active Directory
Configure Active Directory
Created Active Directory Summary

Connect To Active Directory

No IP addresses were found in the specified domain.
Please provide the following information needed to connect to the Active Directory.

Service Account Name: Administrator

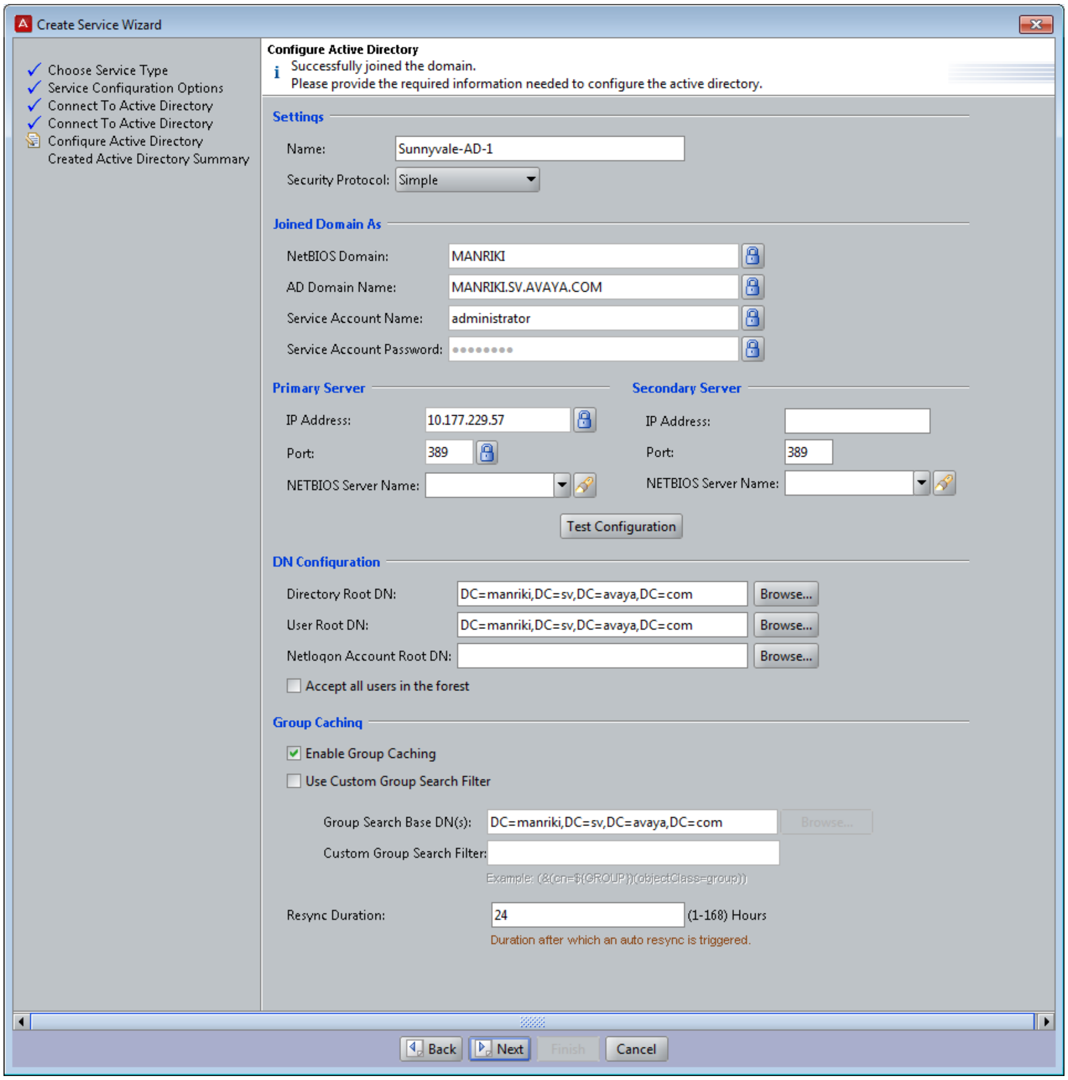
Service Account Password: ••••••••

Security Protocol: Simple

IP Address: 10.2.23.52

Port: 389

7. The **Configure Active Directory** window displays.



Create Service Wizard

✓ Choose Service Type
✓ Service Configuration Options
✓ Connect To Active Directory
✓ Connect To Active Directory
Configure Active Directory
Created Active Directory Summary

Configure Active Directory
Successfully joined the domain.
Please provide the required information needed to configure the active directory.

Settings

Name: Sunnyvale-AD-1
Security Protocol: Simple

Joined Domain As

NetBIOS Domain: MANRIKI
AD Domain Name: MANRIKI.SV.AVAYA.COM
Service Account Name: administrator
Service Account Password: ••••••••

Primary Server

IP Address: 10.177.229.57
Port: 389
NETBIOS Server Name:

Secondary Server

IP Address:
Port: 389
NETBIOS Server Name:

DN Configuration

Directory Root DN: DC=manriki,DC=sv,DC=avaya,DC=com
User Root DN: DC=manriki,DC=sv,DC=avaya,DC=com
Netlogon Account Root DN:
☐ Accept all users in the forest

Group Caching

☑ Enable Group Caching
☐ Use Custom Group Search Filter

Group Search Base DN(s): DC=manriki,DC=sv,DC=avaya,DC=com
Custom Group Search Filter:
Example: (&(cn=${GROUP})(objectClass=group))

Resync Duration: 24 (1-168) Hours
Duration after which an auto resync is triggered.

In the **Settings** section, type a **Name** for this directory service. For this example, call it `Sunnyvale-AD-1`.

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. For an explanation of each field, see the table in Gather Active Directory connection settings on page 52.

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

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

The **DN Configuration** fields are populated by the wizard; if necessary, edit them. The Directory Root, User Root, and Netlogon Account Root are explained in Settings for connecting to an AD Store on page 52. You can type the DN directly or click **Browse** to browse your directory to find it. Note that the schema browser does not display auxiliary classes; those you must type directly.

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

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.

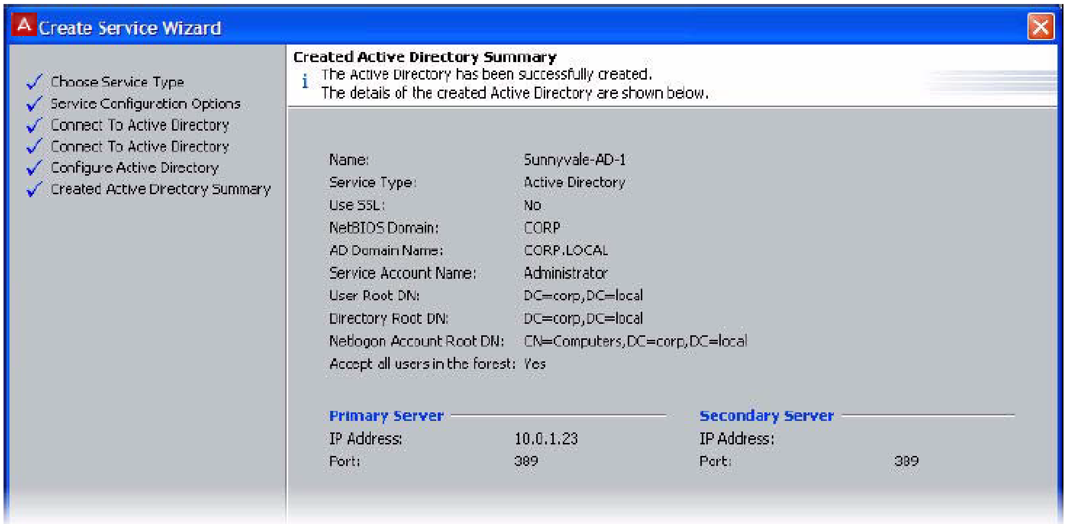
By default, Ignition Server looks for groups starting at the Directory Root DN. You can change this default behavior by specifying **Group Search Base DNs**. This is useful in case of huge AD deployments, where starting at the root DN can take up a substantial amount of time. In addition, you can restrict 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.

Click **Next**.

8. The wizard applies your settings to create the directory service in Ignition Server and displays the confirmation page shown in the following example. If the settings are correct, click **Finish** to create the directory service.


Create Service Wizard
✓ Choose Service Type
✓ Service Configuration Options
✓ Connect To Active Directory
✓ Connect To Active Directory
✓ Configure Active Directory
✓ Created Active Directory Summary

Created Active Directory Summary

The Active Directory has been successfully created.
The details of the created Active Directory are shown below.

Name:	Sunnyvale-AD-1
Service Type:	Active Directory
Use SSL:	No
NetBIOS Domain:	CORP
AD Domain Name:	CORP.LOCAL
Service Account Name:	Administrator
User Root DN:	DC=corp,DC=local
Directory Root DN:	DC=corp,DC=local
Netlogon Account Root DN:	CN=Computers,DC=corp,DC=local
Accept all users in the forest:	Yes

Primary Server		Secondary Server	
IP Address:	10.0.1.23	IP Address:	
Port:	389	Port:	389

Your directory service has been saved in Ignition Server.

Next steps

Do one of the following:

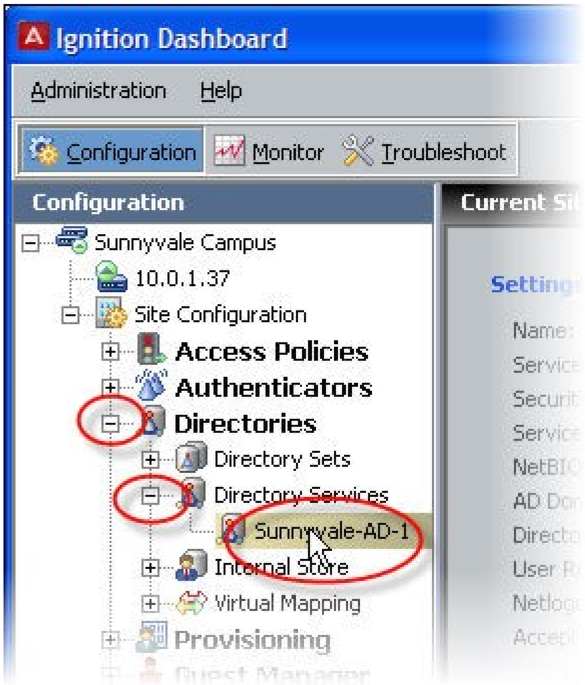
- If the connection attempt succeeded, continue with Create a directory set on page 80.
- If your connection attempt failed, see Troubleshooting AD and LDAP connections on page 72.

Editing a directory service

Use this procedure to edit 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. The main panel displays the connection details of the service. To test the connection, click the **Test Connections** button. To edit the connection, click **Edit**.

Connecting to LDAP

To connect Ignition Server to your LDAP store, you will save the store as a directory service in Ignition Server. The *directory service* specifies the connection settings that Ignition Server uses to connect to LDAP. You will create one directory service for each LDAP server you wish to connect to, and you can search across multiple directory services by grouping them into a *directory* set as explained in Create a directory set on page 80.

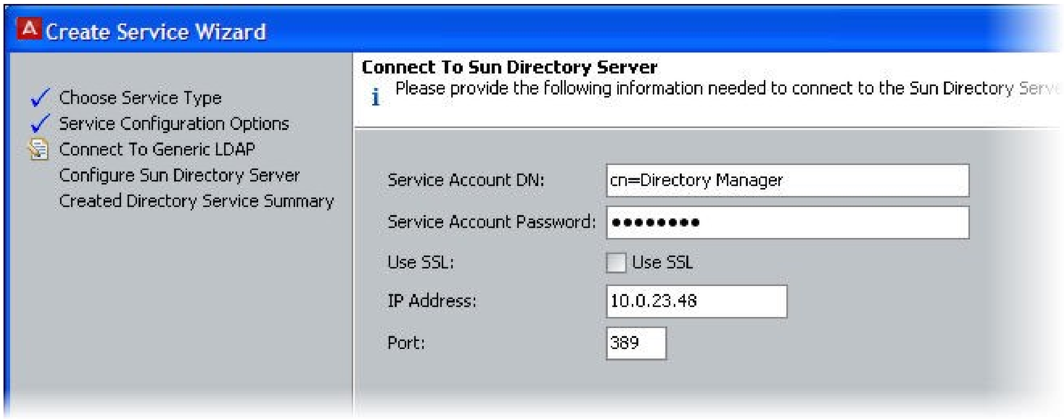
The sections that follow assume that your user data resides in LDAP and that you have an LDAP administrator account that you can use as the Ignition Server service account.

You will connect using Ignition Server's LDAP connection wizard in *automatic connection* mode.

Procedure

1. In Dashboard's **Configuration** tab, in the navigation tree, click **Site Configuration**.
2. Click the **Directory Service** link in the main panel.
3. In the Choose Service Type window, click your type of LDAP store (for example, *Sun Directory Server*) and click **Next**.
4. In the Configuration Options window, click **Automatically configure** and click **Next**.

   If your LDAP connection attempt fails while you are carrying out the steps below, see Troubleshooting AD and LDAP connections on page 72.
5. The Connect to Directory Server window appears. Use the guidelines below for filling out the fields.



Create Service Wizard
✓ Choose Service Type
✓ Service Configuration Options
Connect To Generic LDAP
Configure Sun Directory Server
Created Directory Service Summary
Connect To Sun Directory Server
Please provide the following information needed to connect to the Sun Directory Serv

Service Account DN: cn=Directory Manager

Service Account Password: ●●●●●●●●

Use SSL: □ Use SSL

IP Address: 10.0.23.48

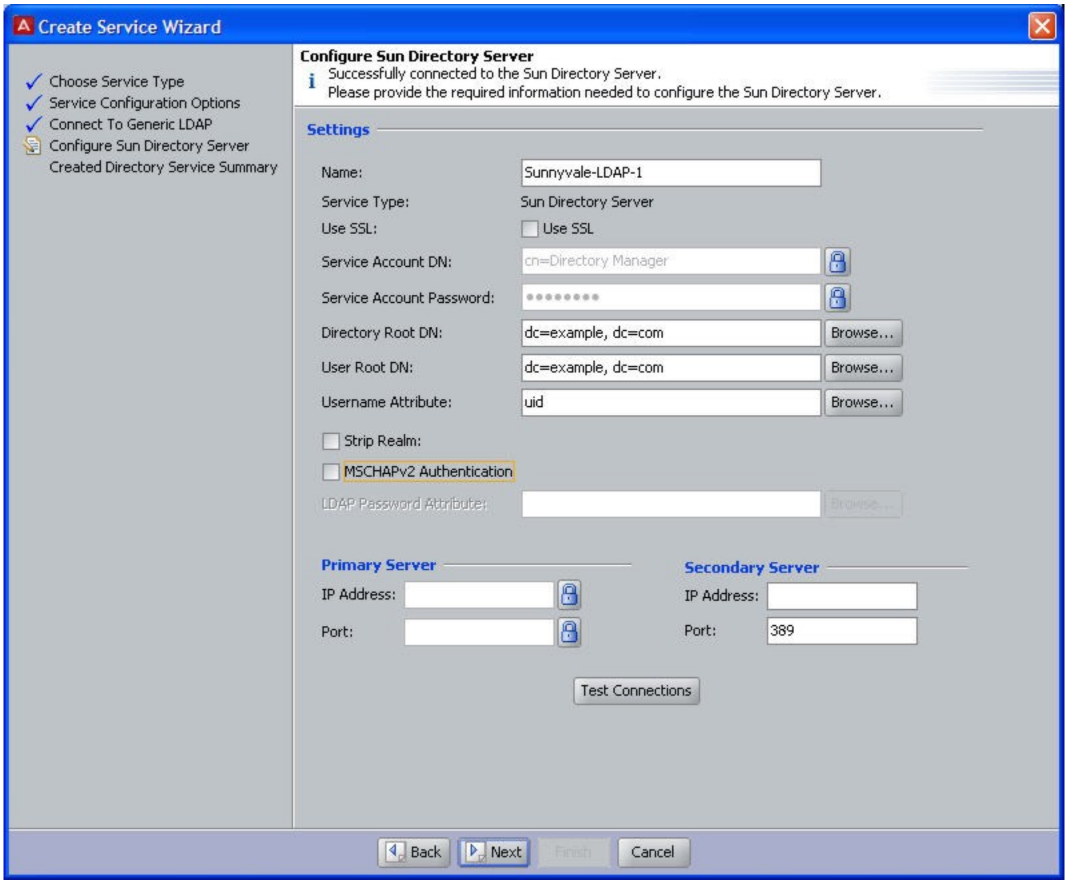
Port: 389

- **Service Account DN**: DN of the LDAP administrator account. Ignition Server will connect as this administrator. For example, cn=Directory Manager.
- **Service Account Password**: Password of the LDAP administrator.
- **Use SSL**: If Use SSL is turned on, Ignition Server uses SSL to encrypt traffic to the directory service. Warning: If you choose to connect to LDAP using a non-SSL connection, your service account credentials will travel over the network in unencrypted form. Avaya strongly recommends using an SSL connection to connect to your directory server.
- **IP Address**: IP address of the primary LDAP server.

- **Port**: Port number at which the LDAP service can be reached. When Use SSL is selected, the Port Entry is typically 636. When Use SSL is not selected, the Port Entry is typically 389.

6. Click **Next**.

   The Configure Directory Server window appears.



Create Service Wizard

✓ Choose Service Type
✓ Service Configuration Options
✓ Connect To Generic LDAP
Configure Sun Directory Server
Created Directory Service Summary

Configure Sun Directory Server
Successfully connected to the Sun Directory Server.
Please provide the required information needed to configure the Sun Directory Server.

Settings

Name: Sunnyvale-LDAP-1
Service Type: Sun Directory Server
Use SSL: □ Use SSL
Service Account DN: cn=Directory Manager
Service Account Password: ••••••••
Directory Root DN: dc=example, dc=com
User Root DN: dc=example, dc=com
Username Attribute: uid
□ Strip Realm:
□ MSCHAPv2 Authentication
LDAP Password Attribute:

Primary Server
IP Address:
Port:

Secondary Server
IP Address:
Port: 389

7. In the **Settings** section, type a **Name** for this directory service. For this example, call it `Sunnyvale-LDAP-1`.

   The **DN** and **Username** fields are populated by the wizard; if necessary, edit them or click the Browse button to set them. Note that the schema browser will not display auxiliary classes; those you must type directly. The fields are:

   - **Directory Root DN**: DN where the LDAP schema containing your users and groups may be found. For example, dc=company,dc=com. When you connect the directory service, the Ignition Server Create Service wizard will attempt to choose a Directory Root DN for you.
   - **User Root DN**: DN of the LDAP container Ignition Server from where will load user records. For example, cn=users,dc=starironinc,dc=com. When you connect the directory service, the Ignition Server Create Service wizard will attempt to choose a User Root DN for you.

- **Username Attribute**: An LDAP attribute that stores the user name. Typically, this is uid.

  Optional: If you wish to have Ignition Server strip the realm name from the username before submitting it for authentication, click the **Strip Realm** check box. If this box is checked, then, for example, the user name jsmith@company.com would be submitted to LDAP as jsmith.

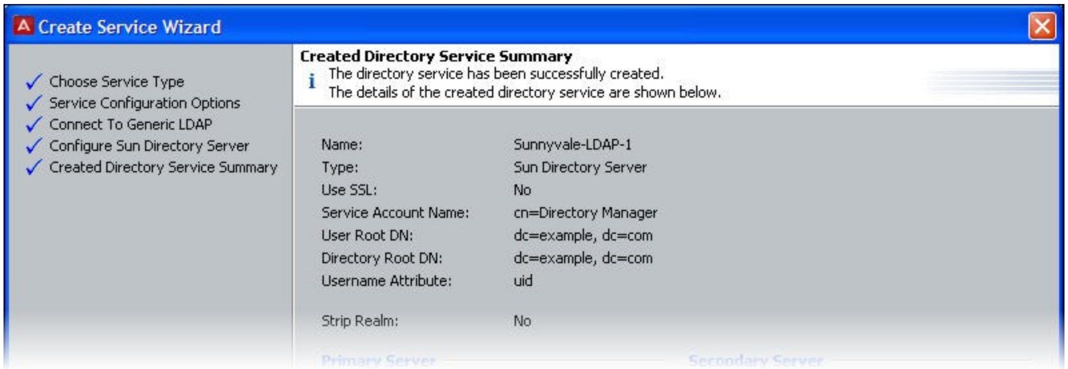
  Optional: If this LDAP store will support MSCHAPv2 authentication, check the **MSCHAPv2 authentication** check box and, in the **LDAP Password Attribute** field, set the name of LDAP attribute that stores the hash of the user's MSCHAPv2 password. See "Setting up MSCHAPv2 Authentication on LDAP" in *Avaya Identity Engines Ignition Server Administration*, NN47280-600 for details.

  The **Primary Server 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.

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

8. Click **Next**.

   The wizard applies your settings to create the directory service in Ignition Server and displays the confirmation page shown below. If the settings are correct, click **Finish** to create the directory service.



Create Service Wizard

✓ Choose Service Type
✓ Service Configuration Options
✓ Connect To Generic LDAP
✓ Configure Sun Directory Server
✓ Created Directory Service Summary

Created Directory Service Summary

The directory service has been successfully created.
The details of the created directory service are shown below.

Name: Sunnyvale-LDAP-1
Type: Sun Directory Server
Use SSL: No
Service Account Name: cn=Directory Manager
User Root DN: dc=example, dc=com
Directory Root DN: dc=example, dc=com
Username Attribute: uid

Strip Realm: No

Primary Server
Secondary Server

   Your directory service has been saved in Ignition Server. To check your connection, see the hint below.

Next steps

Do one of the following:

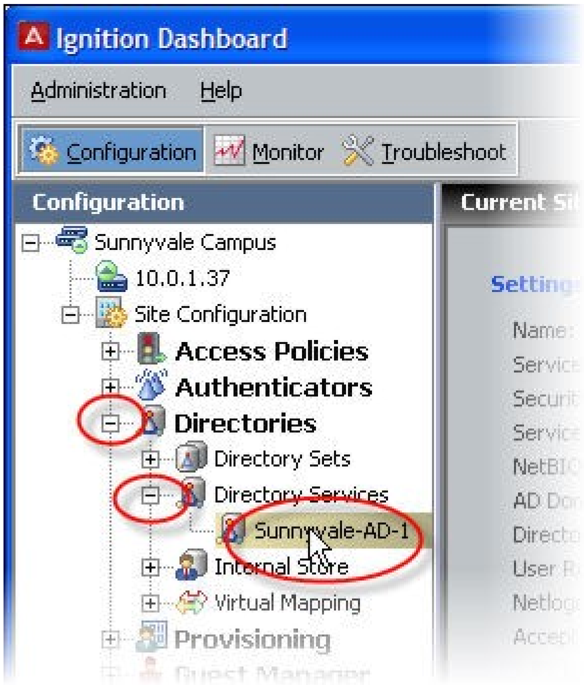
- If the connection attempt succeeded, continue with Create a directory set on page 80.
- If your connection attempt failed, see Troubleshooting AD and LDAP connections on page 72.

Editing a directory service

Use this procedure to edit 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. The main panel displays the connection details of the service. To test the connection, click the **Test Connections** button. To edit the connection, click **Edit**.

Troubleshooting AD and LDAP connections

This section contains tips to troubleshoot AD and LDAP connections.

Related topics:

Checking a directory connection on page 73
Checking directory connections and cache status on page 73

Testing a directory in-depth on page 74
Looking up AD settings: Finding your Root DNs on page 75
Looking up AD settings: Finding Domain and NetBIOS names on page 76
Looking up AD settings: IP Address on page 77

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.

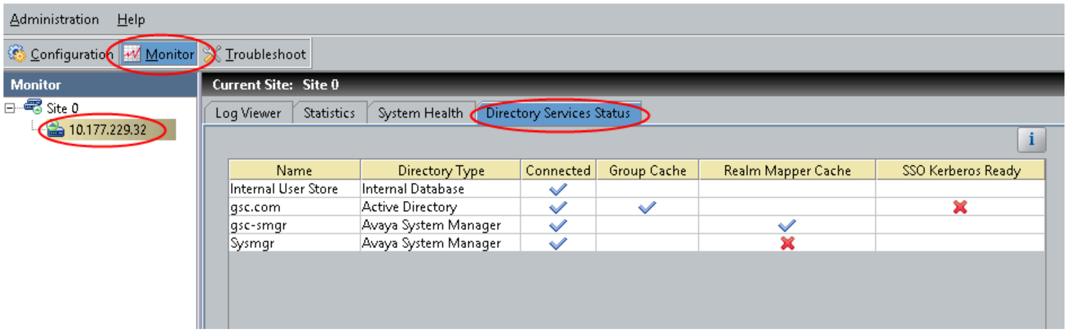
Checking directory connections and cache status

About this task

Use the following procedure to check 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.



Name	Directory Type	Connected	Group Cache	Realm Mapper Cache	SSO Kerberos Ready
Internal User Store	Internal Database	✓			
gsc.com	Active Directory	✓	✓		✗
gsc-smgr	Avaya System Manager	✓		✓	
Sysmgr	Avaya System Manager	✓		✗	

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.

   The **Group Cache** column is applicable only to a Directory Service of type Active Directory.

   The **Realm Mapper Cache** column is applicable only to a Directory Service of type System manager.

   The **SSO Kerberos Ready** column is relevant only for troubleshooting SSO configuration. It is not applicable to NAC (Network Access Control) configuration.

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 the *Avaya Identity Engines Ignition Server Administration* guide.

Looking up AD settings: Finding your Root DNs

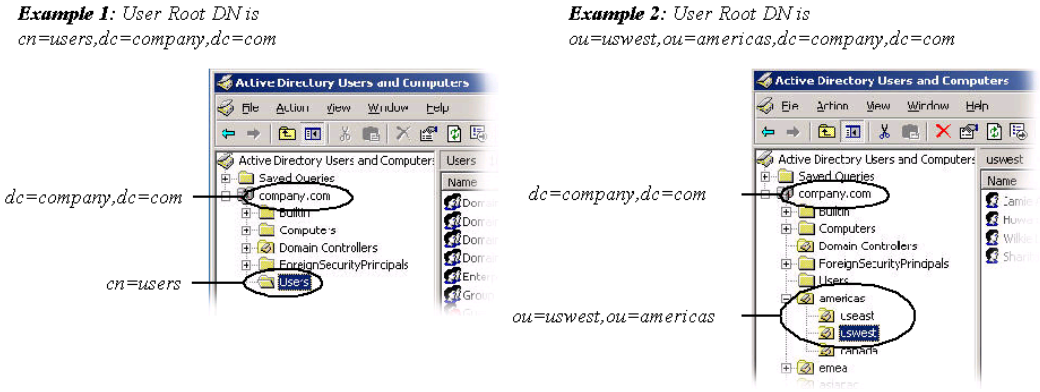
About this task

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 will be used to obtain schema and group information.
2. To find out 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 example below. 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 may 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 two examples above. In the text that follows, we will stick with "cn=users,dc=company,dc=com" as our example DN.

Looking up AD settings: Finding Domain and NetBIOS names

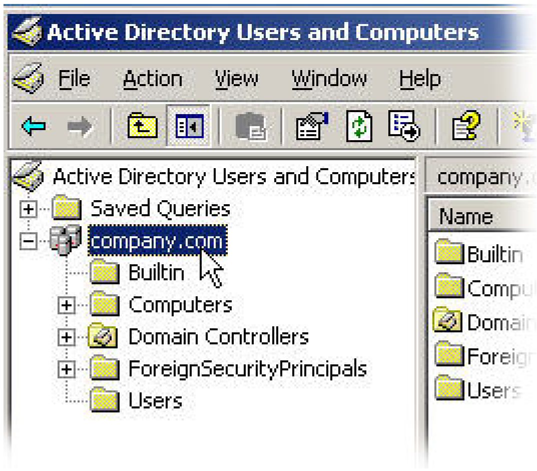
About this task

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

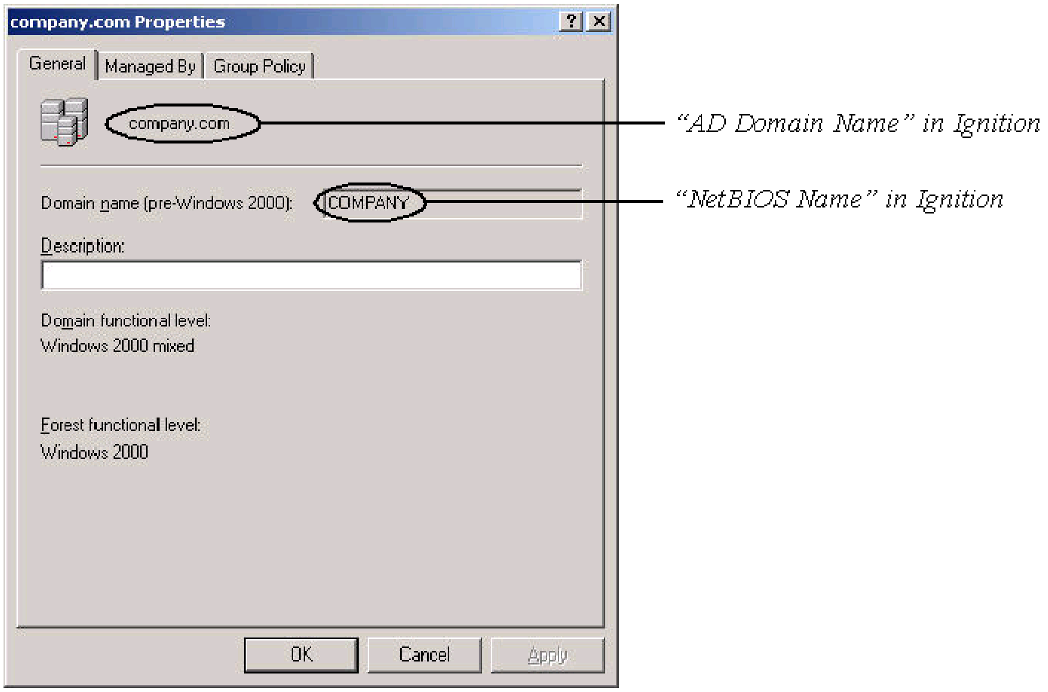
Procedure

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 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.



company.com

Domain name (pre-Windows 2000): COMPANY

Description:

Domain functional level:
Windows 2000 mixed

Forest functional level:
Windows 2000

“AD Domain Name” in Ignition

“NetBIOS Name” in Ignition

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.

Setting up a RADIUS proxy server

A RADIUS proxy server forwards RADIUS requests to a remote server for authentication. The Ignition Server can act as the RADIUS proxy server that forwards the authentication requests, or as the remote server that receives the authentication requests.

If you are using a RADIUS proxy server, you must configure an authentication service in Ignition. In Ignition, you manage authentication services in the Directory Services panel, in the same way you manage directory services.

Related topics:

Creating a RADIUS proxy authentication service on page 78

Add the RADIUS proxy server to a directory set on page 79

Create an Access Policy that includes the RADIUS proxy server on page 80

Proxying of MAC authentication requests on page 80

Configuration on the remote proxy server on page 80

Creating a RADIUS proxy authentication service

Use the procedure to create a RADIUS proxy Authentication Service. The Create Service Wizard guides you through the steps needed to create a RADIUS proxy Authentication Service.

Procedure

1. In the Dashboard Configuration hierarchy tree, click your site, expand Site Configuration, expand Directories, and click Directory Services. Click New.
2. Select the radio button for RADIUS Proxy Service and click Next.
3. In the Configure RADIUS Proxy Service window:
   - Assign the authentication service a name in the Name field. This is the name you will use in your Ignition Server policy to specify that this RADIUS proxy server should be used.
   - Enter the Shared Secret for the RADIUS proxy server.
   - If you want to send a regular “keepalive” ping, check the Enable **Keepalive** checkbox. Optionally, you can specify a **Keepalive User Name** and a **Keepalive Password**. These are the user name and password of a test account in your authentication server.

     With Keepalive turned on, Ignition Server periodically looks up the supplied username/password on the remote server to determine the reachability, and if successful, marks the service as *Connected* in the **Directory Services**

Status tab. By default, Ignition Server uses a predefined username & password (idengines/idengines) to run the keepalive. If you entered a Keepalive User Name and a Keepalive Password, Ignition Server uses these credentials to run the keepalive.

The user credentials you enter to test keepalive do not have to be valid credentials. A reject message from the remote server for looking up invalid credentials is sufficient to determine the reachability.

With Keepalive turned off, the Ignition Server assumes that the remote server is always reachable and marks it as Connected. You can test the connection at any time using the **Test Keepalive** button in this window, or using the Directory Service Debugger tab of Dashboard's Troubleshoot view.

Note:

Avaya recommends that you enable keepalive if you have multiple remote servers that receive requests. If one server is reported down, the requests can be proxied to the next available proxy server as defined in the directory set. If you do not enable keepalive, the Ignition Server assumes the remote server is always connected and the requests may get dropped if the remote server health status is not determined.

- For the primary RADIUS proxy server, and optionally for the secondary RADIUS proxy server, specify the IP Address and Port. If both the primary and secondary servers are configured and the Keepalive is not enabled, RADIUS proxy authentication attempts will occur with the primary server only. To ensure that authentication with the secondary server occurs following a failed authentication attempt with the primary server you must enable the Keepalive mechanism.
- Click the **Test Keepalive** button. Testing the connection might take a few minutes. If a configuration setting is incorrect, Ignition Server warns you.

- Click **Next**.

4. The next window summarizes the connection settings of the service. Click **Finish**.

Result

Your new service appears in the Directory Services list. A blue check mark in the Connected column indicates a successful connection.

Add the RADIUS proxy server to a directory set

After you create a RADIUS proxy authentication service, create a directory set. See Create a directory set on page 80. You add the RADIUS proxy server to a directory set to specify that the RADIUS proxy server is the authentication service that verifies user credentials. You can add multiple remote servers to a directory set. Each remote server can handle different realms, or multiple remote servers can support the same realm to handle a fail-over scenario. When you add a RADIUS proxy server to a directory set, ensure that the **User Lookup Service** field is set to **none**. Note that you cannot add another type of directory service to a Directory set that contains a proxy service.

Create an Access Policy that includes the RADIUS proxy server

The next step is to create an Access Policy that includes the RADIUS proxy server. When you create your Identity routing policy, use the directory set that includes the RADIUS proxy server. In the Realm-Directory Set Map window, configure the realm for which the user wants to proxy the request. See Set your identity routing policy on page 92.

Proxying of MAC authentication requests

MAC authentication is typically used for devices that are incapable of performing 802.1X authentication. MAC authentication requests are also RADIUS requests. MAC authentication verifies that the MAC address submitted by a connecting client device matches an entry on your list of known MAC addresses. Using RADIUS proxy service, Ignition Server can also proxy the MAC authentication requests to a remote server. To proxy MAC authentication requests, enable RADIUS authentication for the authenticator and assign the access policy that is configured to use a proxy directory set. Do not enable MAC authentication for the authenticator which would otherwise do a local MAC authentication. On the remote server, enable MAC auth for this authenticator (proxy server) and configure the necessary MAC authentication policy.

Configuration on the remote proxy server

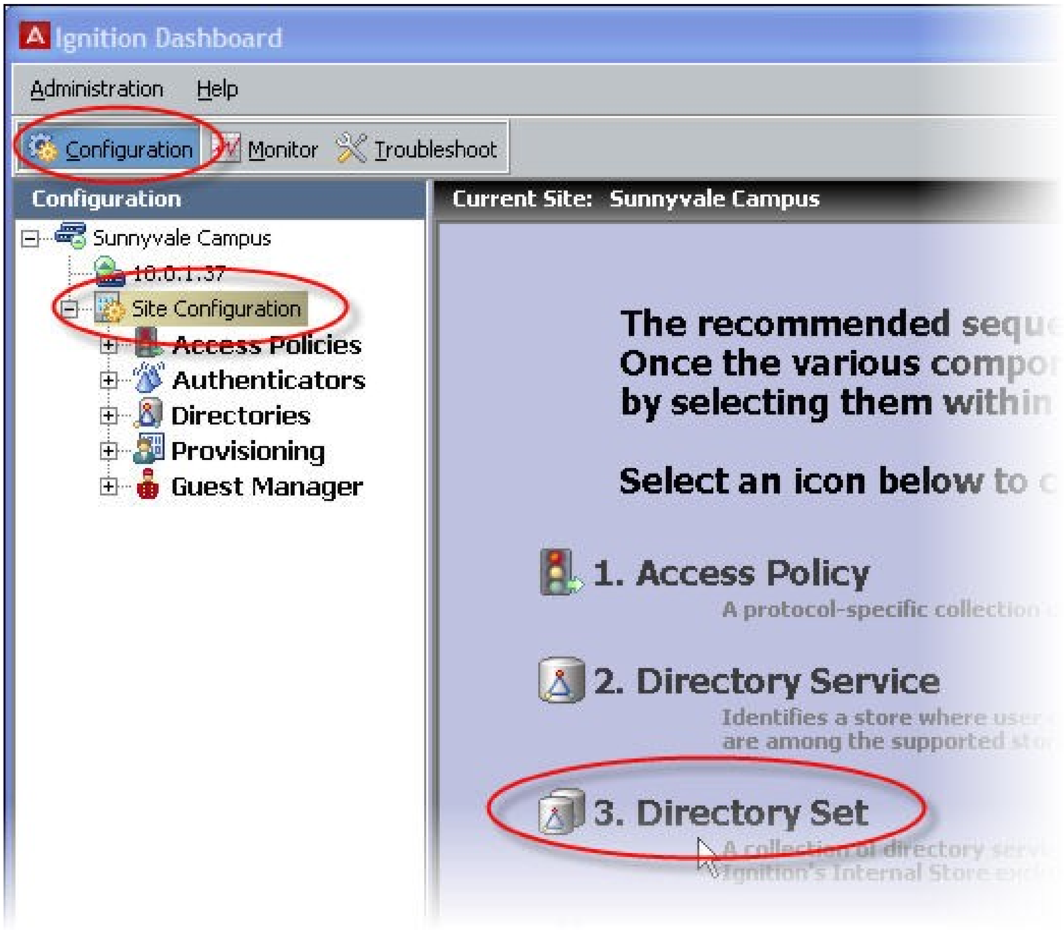
On the remote server that handles the requests coming from the proxy servers, add the proxy server as a regular authenticator and assign the necessary access policy.

Create a directory set

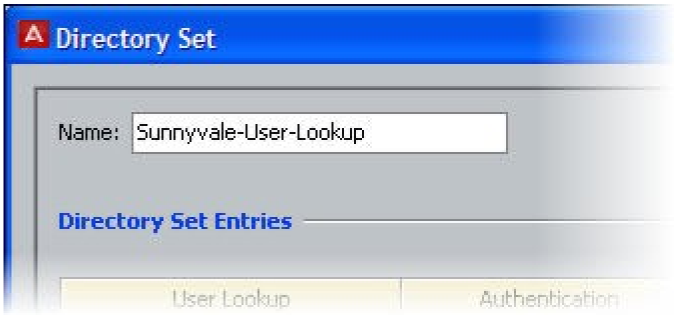
A directory set is the mechanism Ignition Server uses to scan multiple directories for a user account. You will define each user data store (that is, each AD data store, LDAP data store, and the embedded store) as a directory service in Ignition Server, and you will group those directory services into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

Procedure

1. If Dashboard is not connected to your Ignition Server, connect it now by selecting **Administation: Login.**
2. In the main window of Dashboard, click **Configuration**, click **Site Configuration** in the navigation tree, and click **Directory Set** in the main panel.



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.
4. Click the **Add** button to start adding directory services to the set.



Directory Set

Name: Sunnyvale-User-Lookup

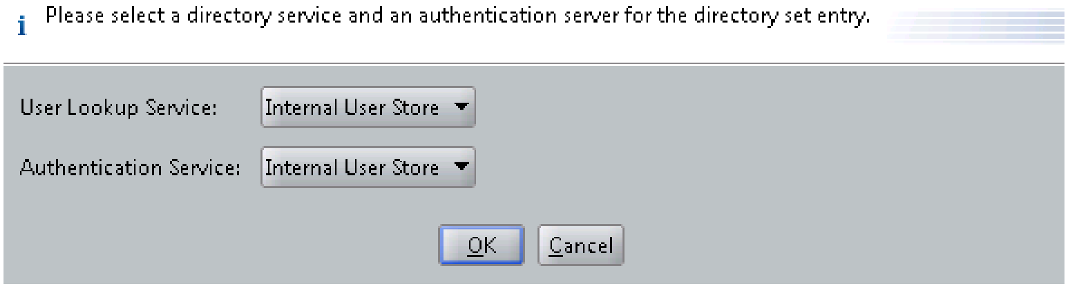
Directory Set Entries

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**).

   Usually these are one and the same directory. You may choose different directories in cases where you wish to split your authentication from your user lookup, as you might when you couple RSA SecurID authentication with authorization based on AD group membership.

   For the example in this document, we will use the internal user store so that we can later demonstrate an authentication of the user account we created earlier. If you have an LDAP or AD user you can test with, then feel free to use your AD or LDAP store, instead:

   - In the **User Lookup Service** drop-down list, select **Internal User Store**.
   - In the **Authentication Service** drop-down list, select **Internal User Store**.
   - Click **OK**.



Please select a directory service and an authentication server for the directory set entry.

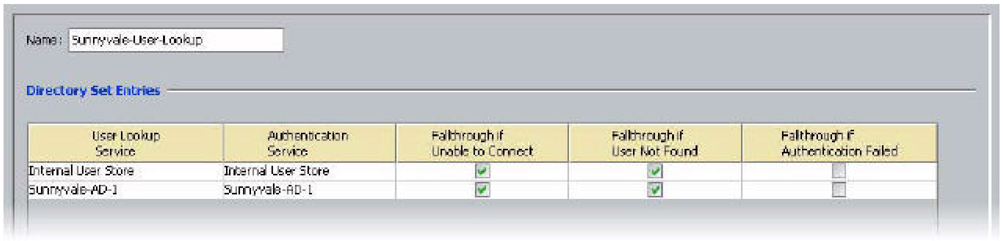
User Lookup Service: Internal User Store

Authentication Service: Internal User Store

6. If you are using an AD or LDAP user store, do the following:

   - In the Directory Set window, click **Add...** again.
   - In the **User Lookup Service** drop-down list, select the directory service you created earlier. In the example, we use the name `Sunnyvale-AD-1`.
   - In the Authentication Service drop-down list, select your directory service again.
   - Click **OK**.
   - In the directory Set window, click the **Fallthrough** checkboxes 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 *ActiveDirectory1* if the user's lookup in the *Internal User Store* fails.



Name: Sunnyvale-User-Lookup

Directory Set Entries

User Lookup Service	Authentication Service	Fallthrough if Unable to Connect	Fallthrough if User Not Found	Fallthrough if Authentication Failed
Internal User Store	Internal User Store	☑	☑	□
Sunnyvale-AD-1	Sunnyvale-AD-1	☑	☑	□

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

Next steps

Map user groups as shown in Create virtual groups on page 83.

Create 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.

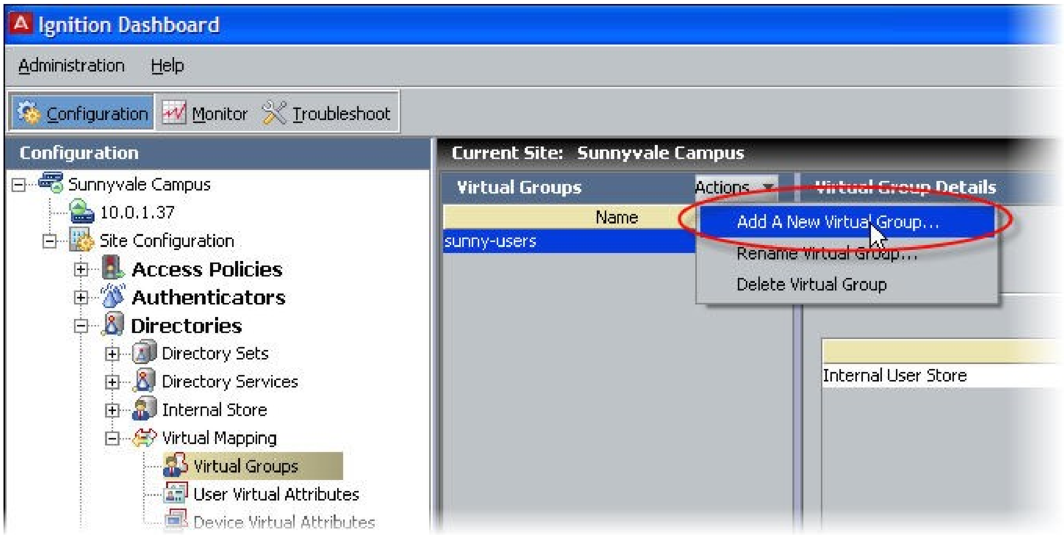
For example, you might create an Ignition Server virtual group called, *"Administrators"* and map it to the DN, *"ou=admin,ou=Users,dc=company,dc=com"* in the user database of your Fresno office, and also map it to the nsRole value *"AdminGroup"* in the user database in your Irvine office. Your access 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.

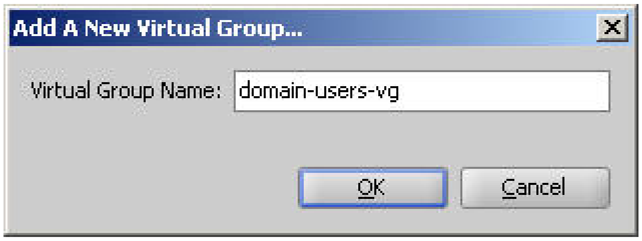
In this example, we will create a virtual group that maps to the Domain Users group in the AD store. Create the virtual group as follows.

Procedure

1. In Ignition Dashboard, click **Configuration**, then, in the navigation tree, click the plus sign to expand **Site Configuration**, expand **Directories**, expand **Virtual Mapping**, and click **Virtual Groups**.
2. In the Virtual Groups panel, click **Actions** and select the command, **Add New Virtual Group…**



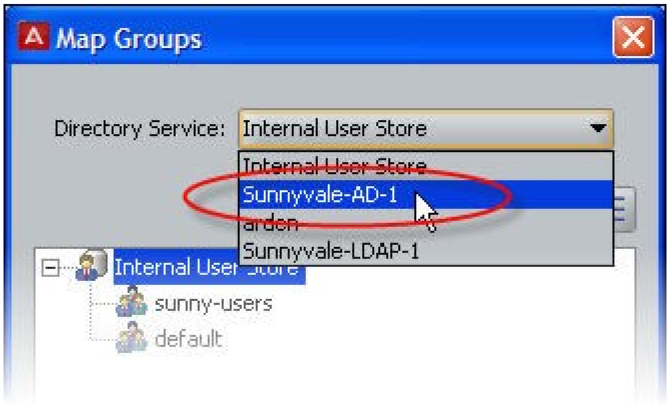
3. In the Add a New Virtual Group window, type the virtual group name and click **OK**. In this example, we give the virtual group the name `domainusers-vg`. This group will contain the members of the “Domain Users” group of the AD server.



Virtual Group Name: domain-users-vg

4. In the Virtual Groups list, select the group name you just created. At the bottom of the Virtual Group Details panel, click **Add…**

5. In the Map Groups window, click in the Directory Service drop down list and select the name of your Directory Service.

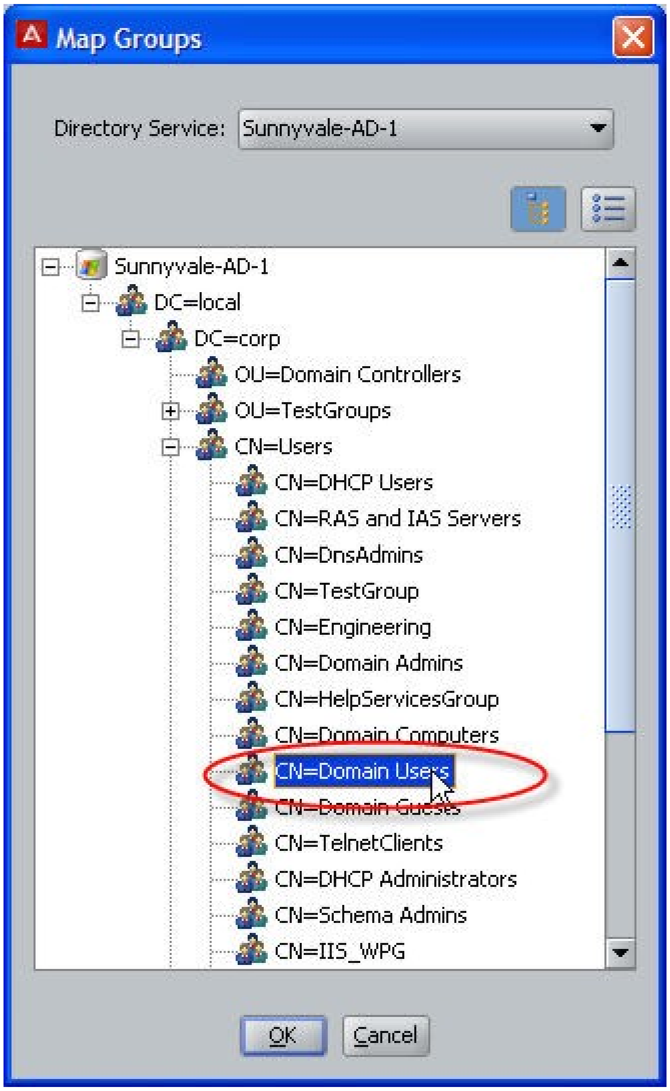


Directory Service: Internal User Store

6. Use the tree list to find the group (AD container) you wish to map. In this example, we’ll use the Active Directory group, “CN=Domain Users”. This will enable us to

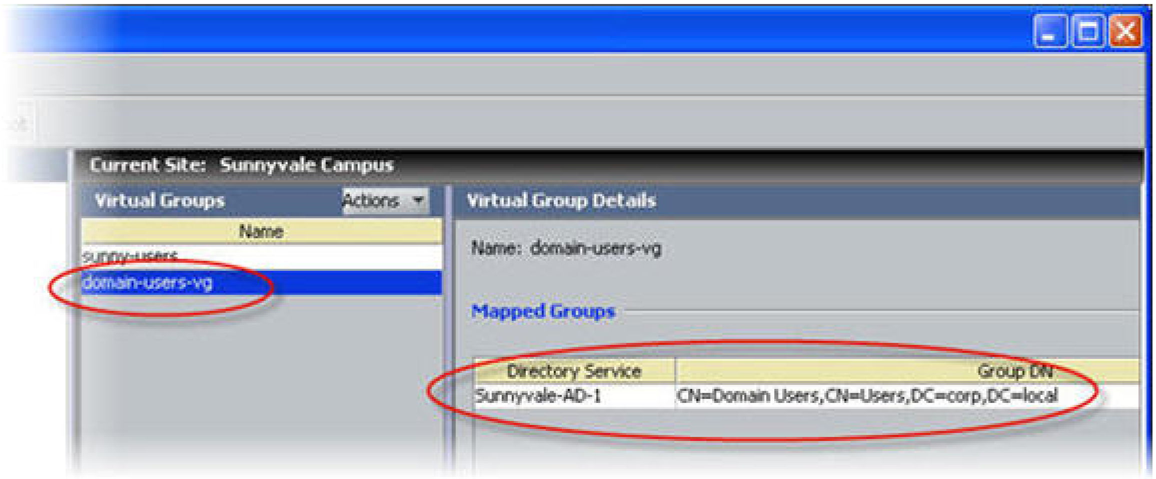
create an Ignition Server authorization rule that grants access to any user who is a member of *Domain Users*.

If you are using the Embedded Store, you can create an embedded group and map your virtual group to that instead.



Directory Service: Sunnyvale-AD-1

7. Click **OK** to close the Map Groups window. The new mapping appears in the Mapped Groups list.



Name
sunny-users
domain-users-vg

Name: domain-users-vg

Directory Service	Group DN
Sunnyvale-AD-1	CN=Domain Users,CN=Users,DC=corp,DC=local

The Ignition Server virtual group, domain-users-vg, maps to the AD group, CN=Domain Users, CN=Users, DC=corp, DC=local, in the ActiveDirectory1 user

Now that you have finished creating a virtual group, you can use membership in the group as a criterion for authorization and provisioning.

Next steps

Create a record in Ignition Server for your switch or access point, as shown in Create authenticators on page 86.

Create authenticators

The network devices (switches, wireless access points, and VPN concentrators) that you secure with Ignition Server are called authenticators. Once you have created an authenticator, you will apply your authentication, authorization, and provisioning policies to it.

In the procedure that follows, you will create an authenticator for each switch and/or access point that will authenticate against Ignition Server.

Procedure

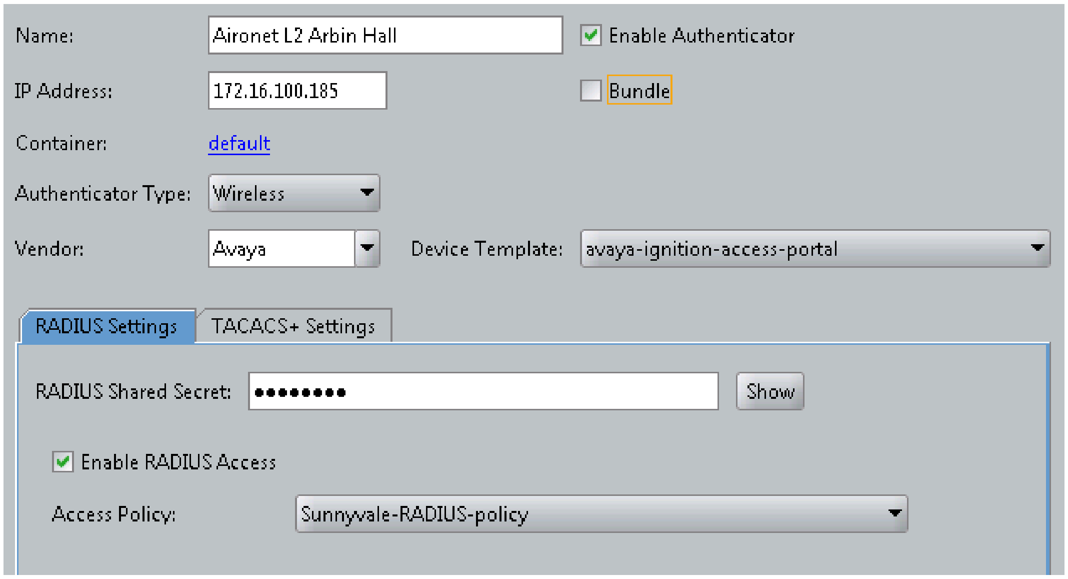
1. Gather the IP addresses and other settings of each authenticator you will connect. Ignition Server can handle a large number of authenticators; we provide space to capture the settings of two authenticators here. You will use these connection details in Step 4 below.

	Authenticator 1	Authenticator 2	Authenticator 3
Authenticator Name	________	________	Choose a name to identify the

	Authenticator 1	Authenticator 2	Authenticator 3
			authenticator. This name will be used to refer to the authenticator within Ignition Server.
IP Address	_______________	_______________	IP address of authenticator.
Subnet Mask	_______________	_______________	*Optional*: If you wish to create one record (a “bundle”) to represent a number of authenticators, this field holds the mask describing the subnet in which all authenticators will be treated as one authenticator.
Container	_______________	_______________	Optional: If you are grouping your authenticators using Ignition Server’s “Container” mechanism, select this authenticator’s container.
Authenticator Type	_______________	_______________	One of the following: wired switch, wireless access point, or VPN concentrator.
Vendor	_______________	_______________	Manufacturer of the switch or access point.
Device Template	_______________	_______________	Ignition Server template to be used to specify formats (attribute names and types) for communicating

	Authenticator 1	Authenticator 2	Authenticator 3
			with this authenticator.
RADIUS Shared Secret	To connect, you must have the shared secret of each device. Do not record the shared secret here. In your switch documentation, the shared secret may also be referred to as a “specific key string” or an “encryption string.”		
Access Policy	________________	________________	Name of the Ignition Server RADIUS policy that contains your access rules for users connecting through this authenticator.

2. In Dashboard’s **Configuration** tab, in the navigation tree, click **Site Configuration**.
3. Click the **Authenticator** link in the main panel.
4. The application displays the **Authenticator Details** window.



Name: Aironet L2 Arbin Hall ☑ Enable Authenticator

IP Address: 172.16.100.185 □ Bundle

Container: default

Authenticator Type: Wireless

Vendor: Avaya Device Template: avaya-ignition-access-portal

RADIUS Shared Secret: ••••••••

☑ Enable RADIUS Access

Access Policy: Sunnyvale-RADIUS-policy

Do the following:

- Fill in the fields using the information you collected in Step 1 above.
- Make sure the **Enable RADIUS Access** checkbox is checked.
- For **Access Policy**, choose the name of the policy you created in Step 3 on page 48.

For an explanation of the rest of the fields, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

5. Click **Save** to save the settings in the **Authenticator Details** window.

Next steps

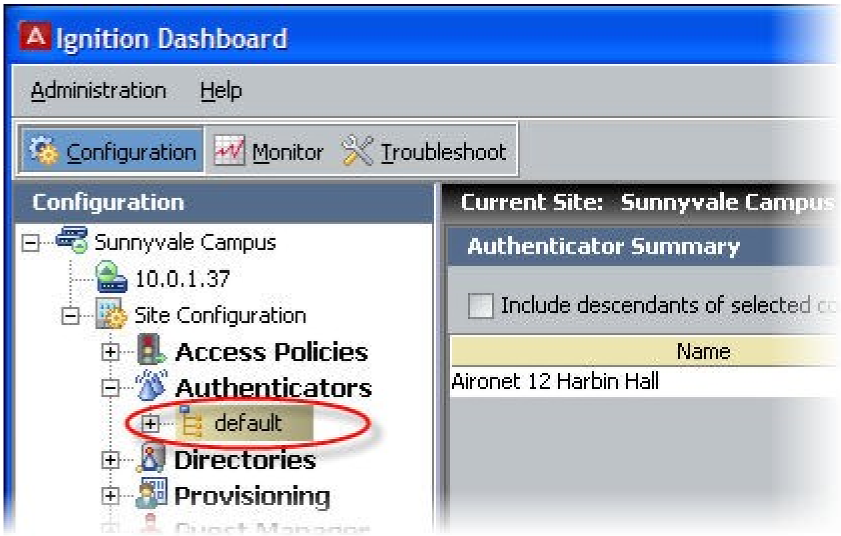
Set your credential verification rules as shown in Set your authentication policy on page 90.

Editing authenticators

To edit authenticators, follow these steps:

Procedure

1. In Dashboard's **Configuration** tab, click the plus sign next to **Authenticators**. One or more items will appear in the list below **Authenticators**.



Each name listed under the **Authenticators** node in the tree (for example, *default*) is an *authenticator container*. Authenticator containers are used to group authenticators so that you can apply a common treatment to them in your access rules. Many sites do not use this feature, and leaving all your authenticators in the *default* container is a common practice.

2. Click on the node that contains your authenticator. For example, click on the *default* node to open the authenticator you created earlier.

Set your authentication policy

You created an empty access policy in the section Create a RADIUS access policy on page 48. In this section and the ones that follow, you will use the Access Policy panel to add an authentication policy and add the various rules that make up your access policy.

About this task

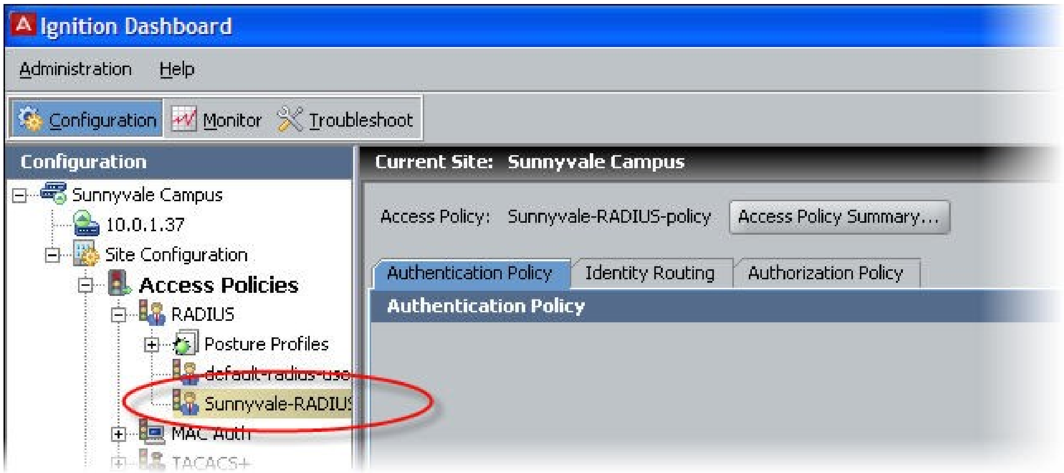
As mentioned earlier, your access policy is a set of rules that govern user authentication, secure communications for authentication, search order for user lookups (called “identity routing” in Ignition Server), authorization, and provisioning. In other words, the access policy controls whether and how that user will be permitted to use the network, as well as how the authentication transaction is to be done.

In your Ignition Server system you may define many access policies for the many different segments of your organization, but you will assign one and only one RADIUS access policy to each authenticator. This means that all users connecting through that authenticator are governed by that RADIUS access policy. You may use a single RADIUS access policy for any number of authenticators.

First you must set up your tunnel protocol policy. This policy specifies how to encrypt communications among the supplicant, authentication server (the Ignition Server appliance) and the user store during an authentication attempt. The outer tunnel secures the connection between the supplicant and the Ignition Server appliance, and the inner tunnel secures the connection from the supplicant to the user store if an external user store (like AD) is used.

Procedure

1. From the Dashboard main window, click on the **Configuration** tab, expand the **Site Configuration** item in the tree (click the plus sign to expand an item), and expand the **RADIUS** item in the tree. Click your policy’s name to load it into the Access Policy panel.

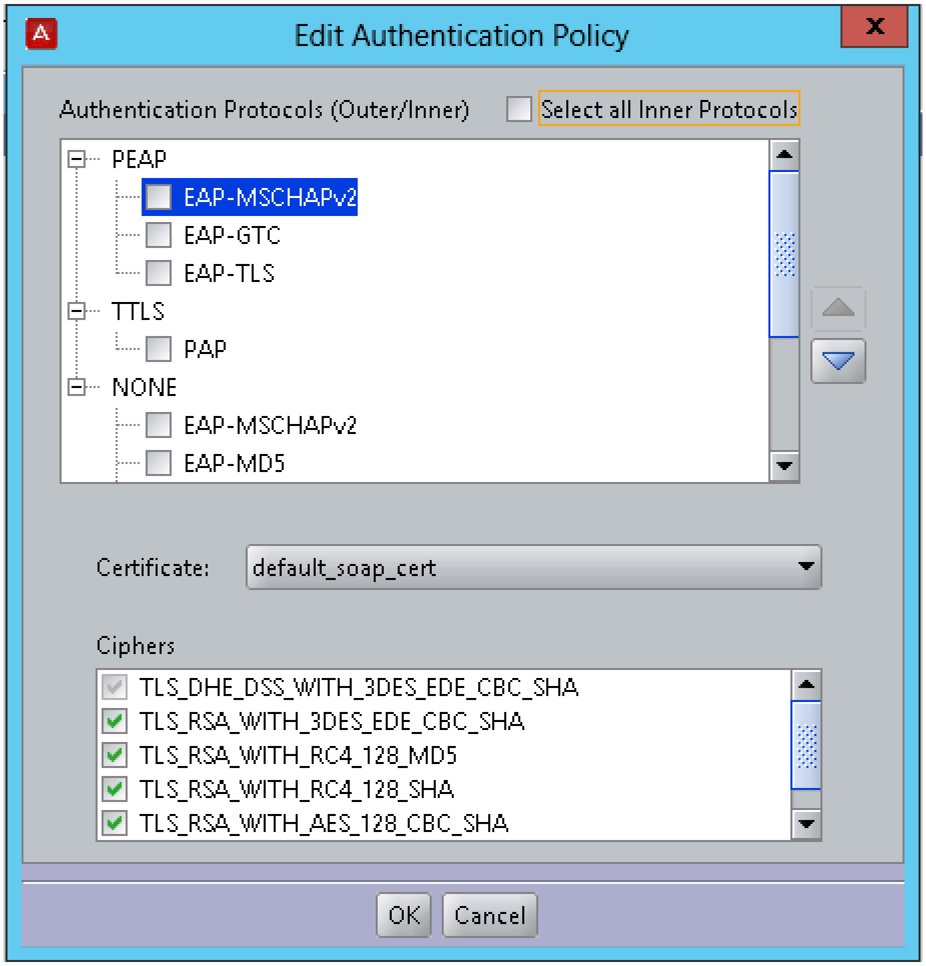


Access Policy: Sunnyvale-RADIUS-policy

2. Click the **Authentication Policy** tab and click the **Edit** button.

3. In the **Edit Authentication Policy** window, the **Authentication Protocols** section lets you establish the set of outer tunnel types and inner authentication protocols that your access policy supports. In the **Authentication Protocols** section, choose each authentication type as follows. The top-level headings (PEAP, TTLS, and NONE) represent the outer tunnel types. Click the +/- toggles to view the authentication types available for each tunnel type. Then:

   - In the **PEAP** section, click the **EAP-MSCHAPv2** check box.
   - In the **NONE** section, click the **PAP** check box.



Edit Authentication Policy

Authentication Protocols (Outer/Inner) □ Select all Inner Protocols

- PEAP
  - □ EAP-MSCHAPv2
  - □ EAP-GTC
  - □ EAP-TLS
- TTLS
  - □ PAP
- NONE
  - □ EAP-MSCHAPv2
  - □ EAP-MD5

Certificate: default_soap_cert

Ciphers

- ☑ TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- ☑ TLS_RSA_WITH_3DES_EDE_CBC_SHA
- ☑ TLS_RSA_WITH_RC4_128_MD5
- ☑ TLS_RSA_WITH_RC4_128_SHA
- ☑ TLS_RSA_WITH_AES_128_CBC_SHA

If you want to verify that an authentication protocol is compatible with your data store, consult the section, “Supported Authentication Types” in *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

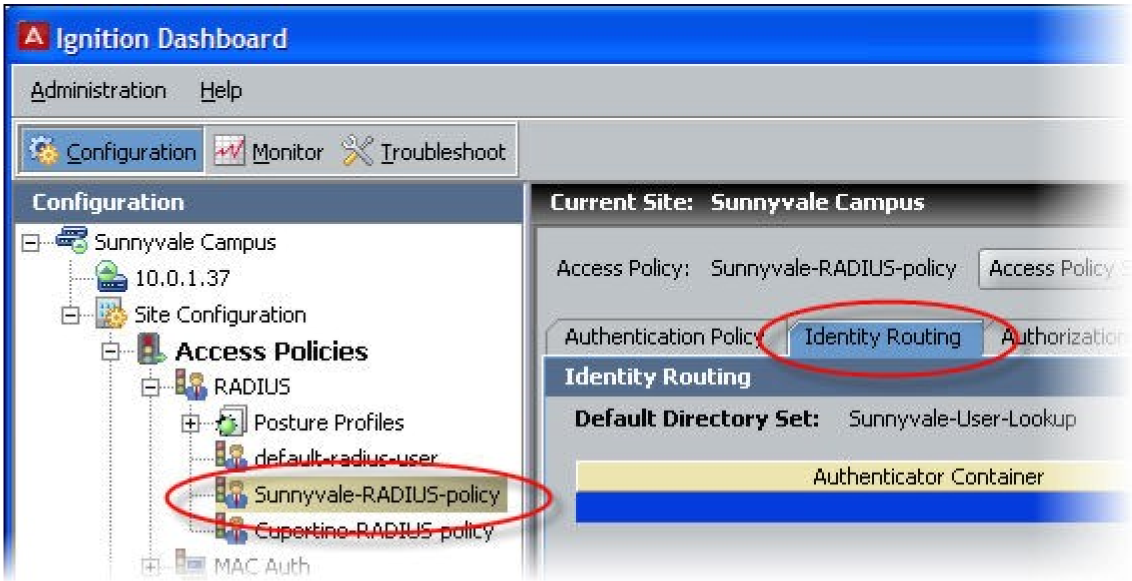
You can sort the order in which Ignition Server will attempt to apply the authentication types to an authentication request by clicking the name of the authentication type or tunnel type and clicking the up/down arrows to sort the list.

If your users are stored in Active Directory and the embedded store, then your policy will typically include at least the PEAP/EAPMSCHAPv2 and NONE/PAP authentication types.

4. Click **Save**.

Set your identity routing policy

The next policy to be set 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 sets a catch-all policy that will use a single directory set for all users.

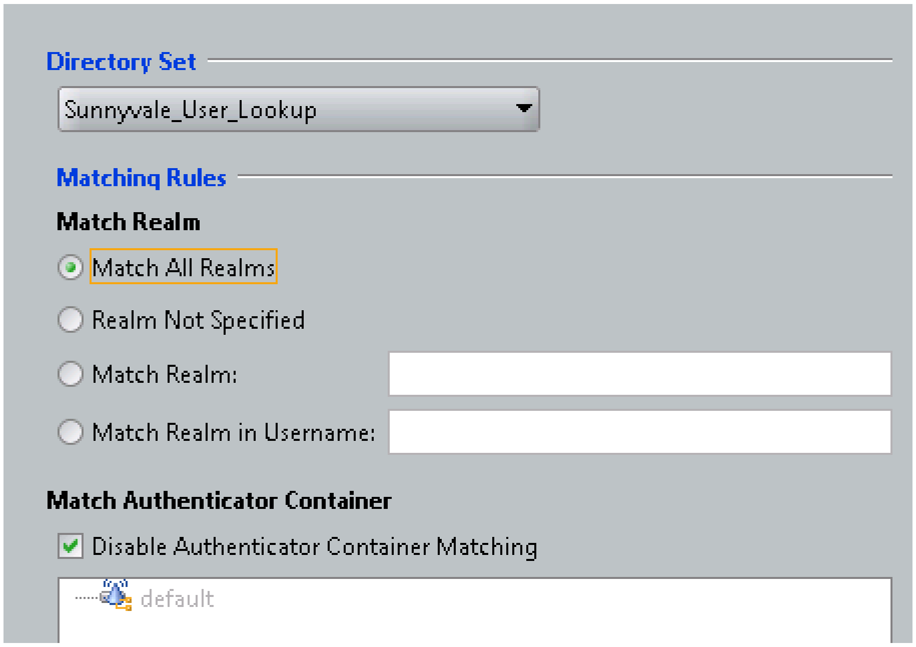


Access Policy: Sunnyvale-RADIUS-policy

Default Directory Set: Sunnyvale-User-Lookup

Procedure

1. In the **Access Policy** panel, click the **Identity Routing** tab and click **Edit…**
2. In the Edit Identity Routing Policy window, click **New...**
3. In the Realm-Directory Set Map window:
    a. In the **Directory Set** drop down menu, select the directory set you created in Step 3 on page 81. If you are using the example names, this will be the set called *Sunnyvale-User-Lookup*.



Directory Set

Sunnyvale_User_Lookup

Matching Rules

Match Realm

● Match All Realms

○ Realm Not Specified

○ Match Realm:

○ Match Realm in Username:

Match Authenticator Container

☑ Disable Authenticator Container Matching

default

b. Tick the **Match All Realms** check box.

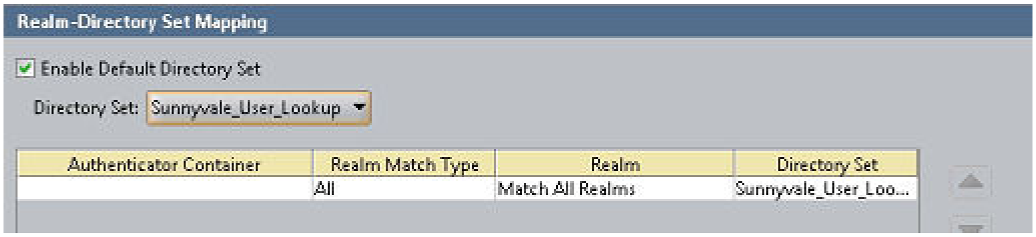
c. Tick the **Disable Authenticator Container Matching** check box.

d. Click **OK**.

In a production system, you can add more realm-directory set mappings in order to look up various groups of users in various directory sets. When you do this, if you have an entry that is set to **Match All Realms**, then you must use the **down arrow** button to move that entry to the bottom of the list.

4. In the Edit Identity Routing Policy window, click **Enable Default Directory Set** and, in the **Directory Set** drop down list, pick *Sunnyvale-User-Lookup*.

   The Edit Identity Routing Policy window now looks like the one shown below. Your directory set name may differ from the one in this screenshot:



Realm-Directory Set Mapping

☑ Enable Default Directory Set

Directory Set: Sunnyvale_User_Lookup

Authenticator Container	Realm Match Type	Realm	Directory Set
	All	Match All Realms	Sunnyvale_User_Loo...

5. Click **Save** to save your routing and close the window.

Set your authorization policy

The next policy to be set in your access policy is the authorization policy. This policy is a set of rules that govern which users are granted access to which networks. Ignition Server can be set to evaluate user attributes, device attributes, and the context of the access request in order to decide whether to authorize the user.

The authorization policy can also prescribe provisioning for users as explained in the Provisioning chapter of the *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

This guide provides separate examples, depending on where you store your user accounts:

- If your user accounts reside in the *Ignition Server internal user store*, see Authorization policy—Example for embedded store users on page 94.
- If your user accounts reside in an *AD user store*, see Authorization policy—Example for AD users on page 97.

Note that you may store users in the embedded store, AD store, and additional stores at the same time, and handle them all in the same access policy (See Set your identity routing policy on page 92).

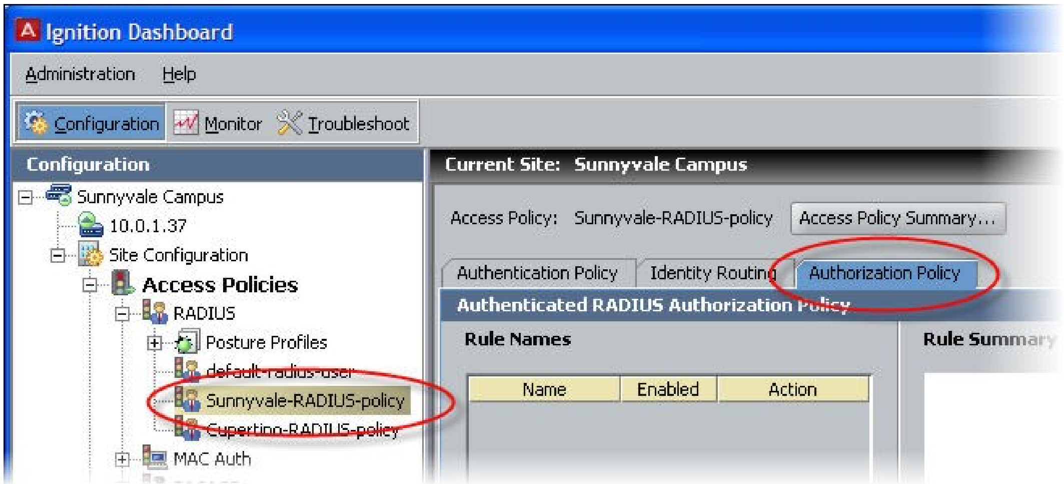
Authorization policy—Example for embedded store users

If your user accounts are stored in the Ignition Server internal user store, set up your authorization policy as shown below.

This section shows you how to create an authentication-only policy. Ignition Server always performs both authentication and authorization before it grants a user access, but in some installations, you may decide that authentication alone—checking the user's credentials—is sufficient to grant the user access. This example creates such a rule. To create your authentication-only rule, follow these steps.

Procedure

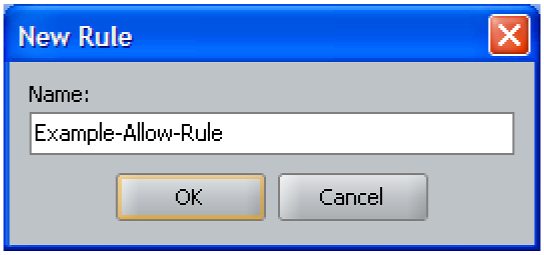
1. Click the **Configuration** tab. In the navigation tree, expand **Site Configuration**, expand **Access Policies**, and expand **RADIUS**. Click the name of your policy and click the **Authorization** policy tab.



Current Site: Sunnyvale Campus

Access Policy: Sunnyvale-RADIUS-policy

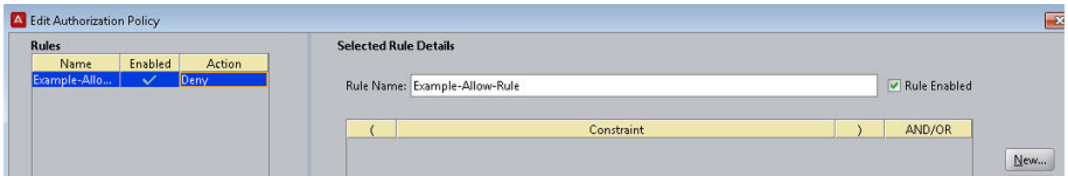
2. The top half of the **Authorization Policy** tab contains your RADIUS authorization policy. Click the top **Edit** button to edit it. The Edit Authorization Policy window appears.
3. In the **Rules** section, in the lower left part of the window, click **Add**. The application displays the New Rule dialog, where you name the new rule.



Name: Example-Allow-Rule

4. Type *Example-Allow-Rule* 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 allows you to edit the rule you have selected in the list.
5. In the **Rules** list, click the rule you just created. The **Selected Rule Details** section displays the **Constraints** that form the rule. Right now there are none.
6. With your rule selected, go to the buttons to the right of the **Constraint** list and click **New**, as shown below.



Name	Enabled	Action
Example-Allo...	✓	Deny

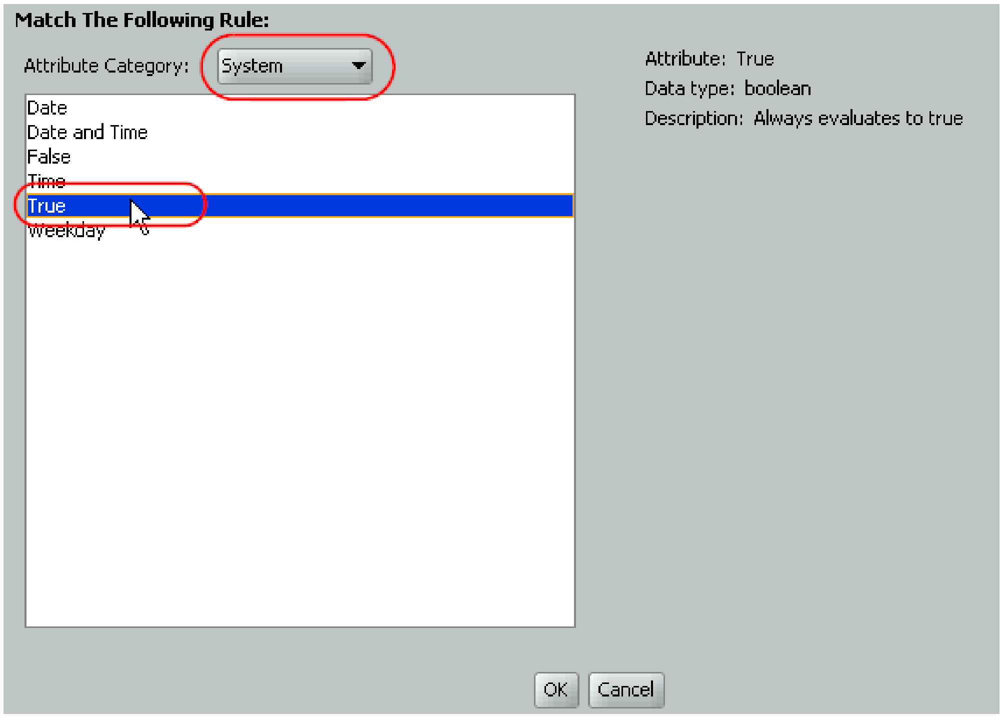
Rule Name: Example-Allow-Rule ☑ Rule Enabled

(	Constraint	)	AND/OR

7. In the Constraint Details window, do the following. The steps below create a rule that always evaluates to true. Creating such a rule is pointless in a production system, but it allows us to demonstrate rule setting in this exercise. Bear in mind

that, even if you have an *always-allow* rule like this, the authenticating user must still *authenticate successfully* and *pass all* DENY *rules* before she can trigger an *ALLOW* rule.

- In the **Attribute Category** drop-down list, select the attribute category, **System**. In response, the list shows all the attributes for **System**.
- In the list, select the attribute **True**.



Match The Following Rule:

Attribute Category: System

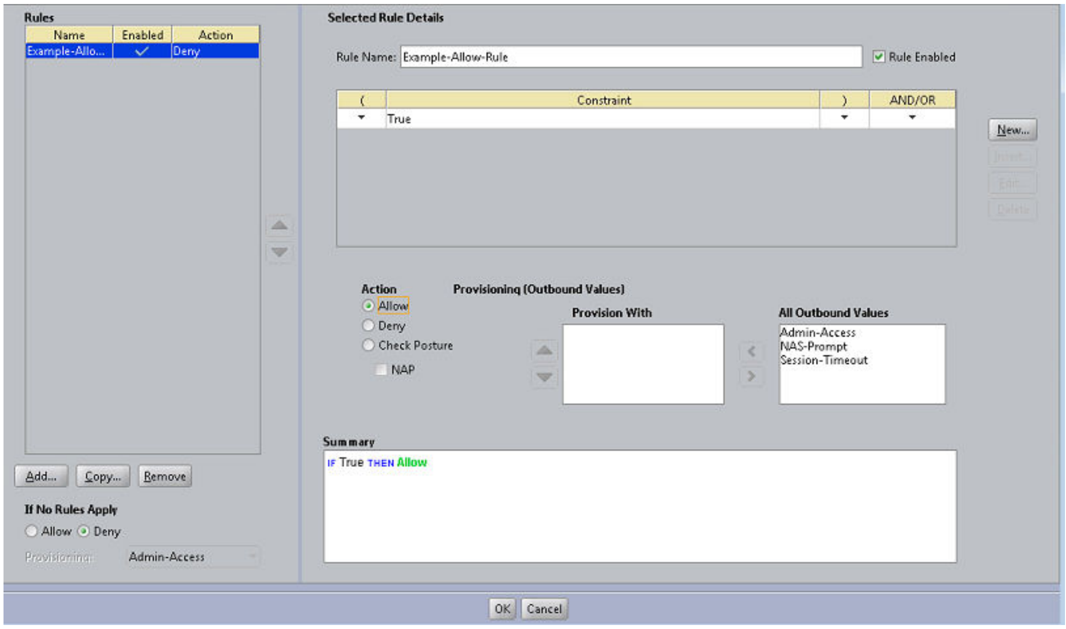
Attribute: True

Data type: boolean

Description: Always evaluates to true

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

8. In the **Action** section, select the **Allow** radio button.



Rules

Name	Enabled	Action
Example-Allo...	✓	Deny

Selected Rule Details

Rule Name: Example-Allow-Rule ☑ Rule Enabled

(	Constraint	)	AND/OR
	True		

Action

● Allow
○ Deny
○ Check Posture
□ NAP

Provisioning (Outbound Values)

Provision With

All Outbound Values: Admin-Access, NAS-Prompt, Session-Timeout

Summary

IF True THEN Allow

If No Rules Apply

○ Allow ● Deny

Provisioning: Admin-Access

9. In the Provisioning section, make no changes.
10. Click **OK** to close the Edit Authorization Policy window and return to the Access Policy window. You have finished setting policies in your access policy.

Next steps

Congratulations! Your example configuration is complete. For information on troubleshooting, see Test your configuration on page 100.

Authorization policy—Example for AD users

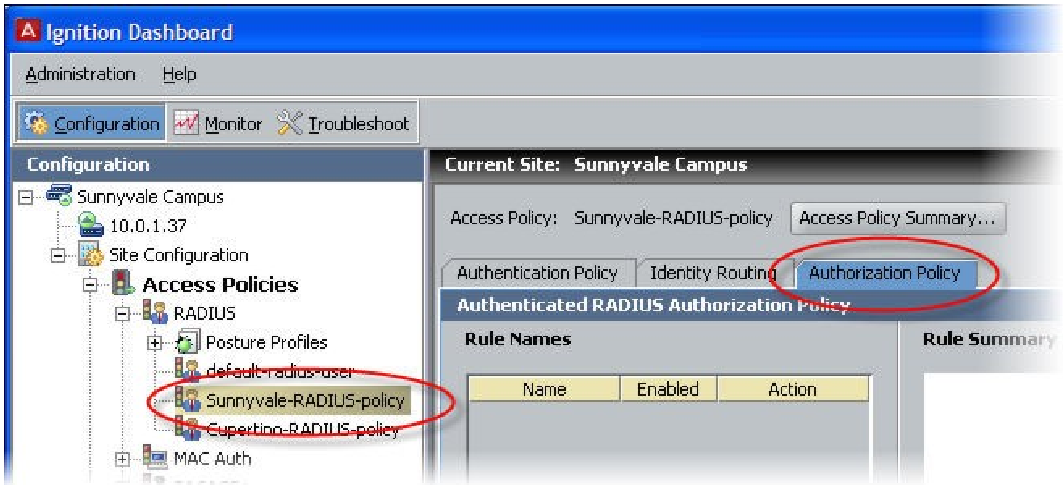
The steps below show you how to create a policy that authorizes access for any user who has a user account on the AD domain (that is, if he or she has an account in the Domain Users group). Upon authentication, the user is provisioned based on his or her virtual group name. Note that the virtual group may map to a single AD workgroup or multiple workgroups on one or more domain controllers.

About this task

Use the following procedure to create a rule that checks AD domain membership.

Procedure

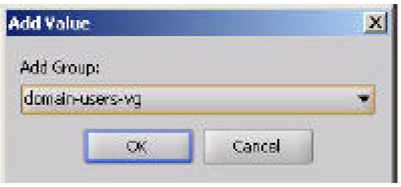
1. Click the **Configuration** tab. In the navigation tree, expand the **Site** Configuration item and expand the **RADIUS** item. Click the name of your policy and click the Authorization policy tab. Click the **Edit** button to edit the policy.



2. The top half of the **Authorization Policy** tab contains your RADIUS authorization policy. Click the top **Edit** button to edit it. The Edit Authorization Policy window appears.
3. 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.
4. 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 have selected in the list.
5. With **CheckHasADAccount** selected in the **Rules** list, go to the buttons to the right of the **Constraint** list and click **New**.

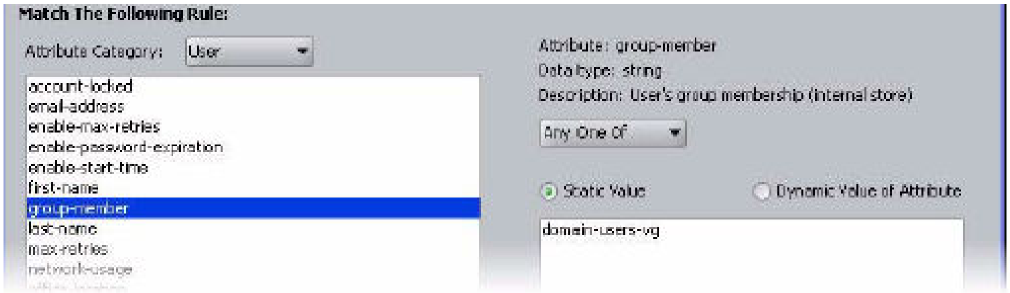
   To learn how Ignition Server evaluates sets of rules and constraints, consult the *Avaya Identity Engines Ignition Server Administration*, NN47280-600.
6. In the Constraint Details window, create your constraint as follows:
   a. In the drop down menu at the top of Constraint Details window, select the 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. In the drop down menu of the Phrase section, select **Contains Any** and click the **Static Value** radio button.
   d. Click the **Add...** button.
   e. In the Add Value window, select the virtual group you created Step 3. If you are following the example, it is *domainusers-vg*. Click **OK** to close the window.



Add Value

Add Group: domain-users-vg

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



Match The Following Rule:

Attribute Category: User

Attribute: group-member

Data type: string

Description: User's group membership (internal store)

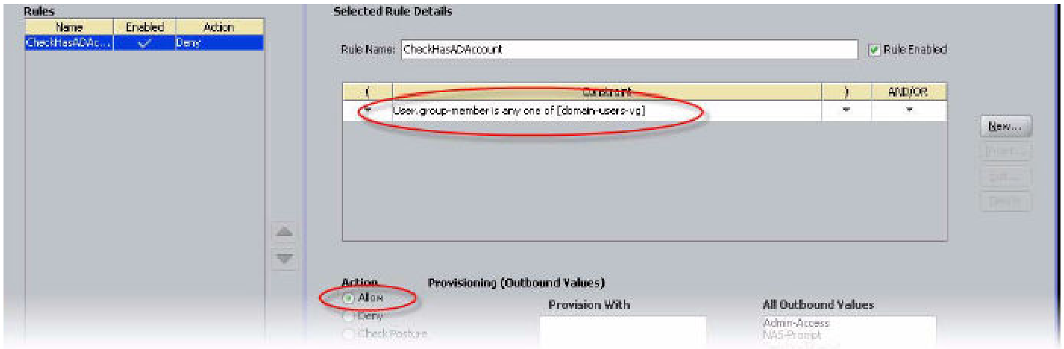
Any One Of

● Static Value ○ Dynamic Value of Attribute

domain-users-vg

7. In the **Action** section of the Edit Authorization Policy window, click the **Allow** button. 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.



Rules

Name	Enabled	Action
CheckHasADAc...	✓	Deny

Selected Rule Details

Rule Name: CheckHasADAccount ☑ Rule Enabled

(	Constraint	)	AND/OR
	User.group-member is any one of [domain-users-vg]		

Action

● Allow
○ Deny
○ Check Posture

Provisioning (Outbound Values)

8. Click **Save** to close the Edit Authorization Policy window and return to the Policy Management window.

Next steps

Congratulations! Your example configuration is complete. For information on troubleshooting, see Test your configuration on page 100.

Test your configuration

Related topics:

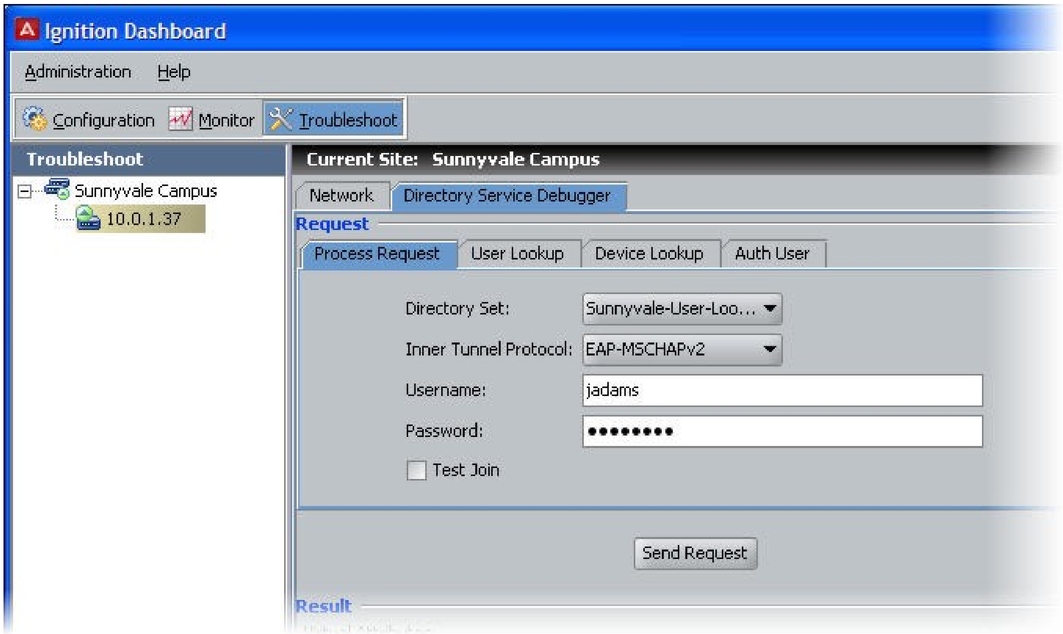
[Checking user lookup and authentication](#) on page 100
[Use NTRadPing as a test authenticator](#) on page 101

Checking user lookup and authentication

Use Dashboard's Directory Service Debugger to perform a test login with a user account from your directory service.

Procedure

1. Click Dashboard's **Troubleshoot** tab.
2. In the navigation tree, click the IP address of your Ignition Server.
3. Click the **Directory Service Debugger** tab.



Directory Set: Sunnyvale-User-Loo...
Inner Tunnel Protocol: EAP-MSCHAPv2
Username: jadams
Password: ••••••••
□ Test Join

4. Click the **Process Request** tab.
5. Choose the **Directory Set**, *Sunnyvale-User-Lookup*.
6. Set the **Inner Tunnel Protocol** (authentication type) to one of:
    - EAP-MSCHAPv2 for AD-stored users, or

- PAP for users stores in the internal user store.

7. Type a test **Username** and **Password**.
8. Click **Send Request**. The test results and retrieved user attributes appear in the **Results** panel.

Use NTRadPing as a test authenticator

For testing, you can use a test tool such as Novell's NTRadPing to send authentication requests directly from your computer to the Ignition Server.

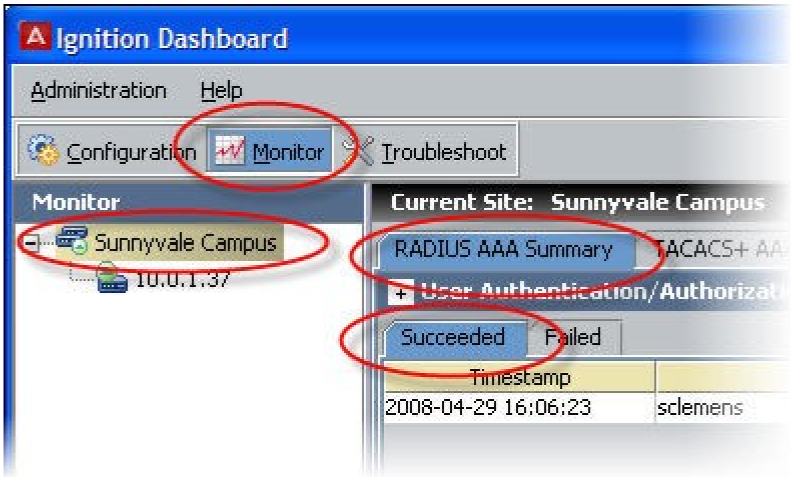
Procedure

1. Download the free NTRadPing tool from Novell and install it on your computer.
2. Define your NTRadPing installation in Dashboard as an Authenticator:
   - In Dashboard, click the **Configuration** tab. In the navigation tree, click **Site Configuration**. Click the **Authenticator** link in the main panel.
   - In the Authenticator Details window, type a **Name** for your test authenticator. Enter the **IP Address** of the computer on which you installed NTRadPing. In **RADIUS Shared Secret** enter any string of characters to use as the shared secret. Make sure the **Enable RADIUS Access** checkbox is ticked and choose your **Access Policy** in the drop down list. In this example, we used the name *Sunnyvale-RADIUS-policy*. Click **OK** to save.
3. Run NTRadPing and perform these steps in the NTRadPing window:
   - In the **RADIUS Server** field, type the Ignition Server IP address that hosts the Ignition Server RADIUS service is running. You can find this IP address in Dashboard. Click your server's IP address in the navigation tree. If you are using only one Ethernet interface on your Ignition Server, then this is your RADIUS server IP address. Otherwise, click the **Ports** tab to see the other IP addresses of your Ignition Server. If you use multiple interfaces and need to determine which of them hosts the RADIUS service, click the top node in Dashboard's navigation tree, click the **Services** tab, click the **RADIUS** tab. The **Bound Interface** field shows which interface hosts the service.
   - In the **RADIUS port** field, type the port number of the Ignition Server RADIUS service, which defaults to 1812. To find out the port number, click the **Services** tab and click the **RADIUS** tab, as shown above. The Authentication Port field shows the port.
   - In the **RADIUS Secret Key** field, type the shared secret you specified earlier in Dashboard.
   - Type your test credentials in the **User-Name** and **Password** fields.

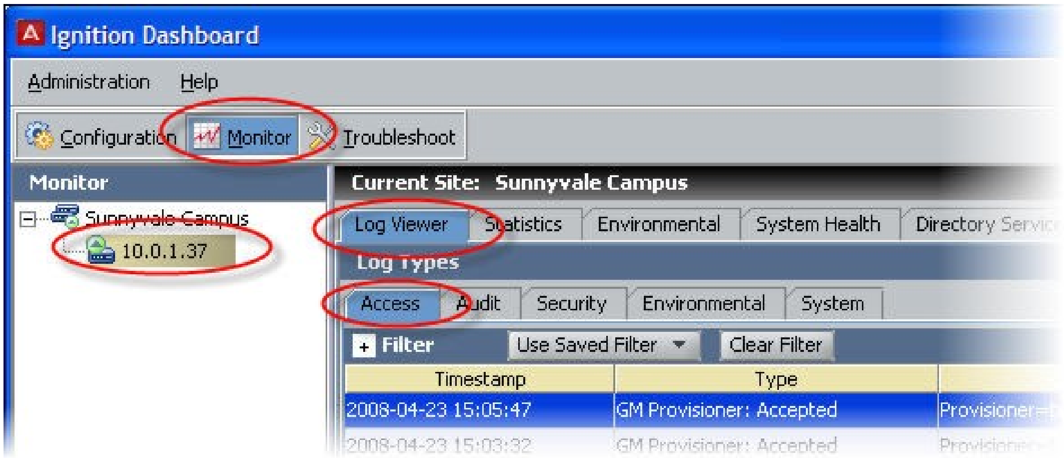
- Click **Send**. The field in the lower part of the NTRadPing window indicates success or failure and shows the details of the transaction.

4. Check Dashboard's Log Viewer for details on your test authentication attempt.

- For a quick list of successful and failed authentication attempts, use the RADIUS AAA Summary. To do this: In Dashboard, click **Monitor**, click the *name of your Ignition Server site* ("Sunnyvale-Campus" in this example), click **RADIUS AAA** Summary, and click either **Succeeded** of **Failed**.



- For a detailed look at an authentication attempt, use the Log Viewer. To do this: In Dashboard, click **Monitor**, click the **IP address** of your Ignition Server, click the **Log Viewer** tab, and click the **Access** tab. Search through the list of log entries to find the message that describes your authentication request. For more details, click the record and click the **Access Record Details** link near the bottom of the page.


Ignition Dashboard
Administration
Help
Configuration
Monitor
Troubleshoot
Monitor
Sunnyvale Campus
10.0.1.37
Current Site: Sunnyvale Campus
Log Viewer
Statistics
Environmental
System Health
Directory Servic
Log Types
Access
Audit
Security
Environmental
System
Filter
Use Saved Filter
Clear Filter
Timestamp
Type
2008-04-23 15:05:47
GM Provisioner: Accepted
Provisioner=
2008-04-23 15:03:32
GM Provisioner: Accepted
Provisione