



# **Avaya Identity Engines Ignition Server Configuration**

**Avaya Identity Engines Ignition Server**  
Release 7.0

Document Status: **Standard**  
Document Number: **NN47280-500**  
Document Version: **02.02**  
Date: **December 2010**

© 2010 Avaya Inc.  
All Rights Reserved.

#### **Notices**

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**

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

#### **Link disclaimer**

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) 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 this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>

**Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.**

#### **Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://SUPPORT.AVAYA.COM/LICENSEINFO/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER, AND 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").

#### **Copyright**

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) 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. 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.

#### **Third Party Components**

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

#### **Trademarks**

*The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.*

#### **Downloading documents**

For the most current versions of documentation, see the Avaya Support. Web site: <http://www.avaya.com/support>

#### **Contact Avaya Support**

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

---

# Customer service

---

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to [www.avaya.com](http://www.avaya.com) or go to one of the pages listed in the following sections.

## Navigation

- [Getting technical documentation](#)
- [Getting Product training](#)
- [Getting help from a distributor or reseller](#)
- [Getting technical support from the Avaya Web site](#)

### Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to [www.avaya.com/support](http://www.avaya.com/support).

### Getting Product training

Ongoing product training is available. For more information or to register, you can access the Web site at [www.avaya.com/support](http://www.avaya.com/support). From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

### Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

### Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at [www.avaya.com/support](http://www.avaya.com/support).



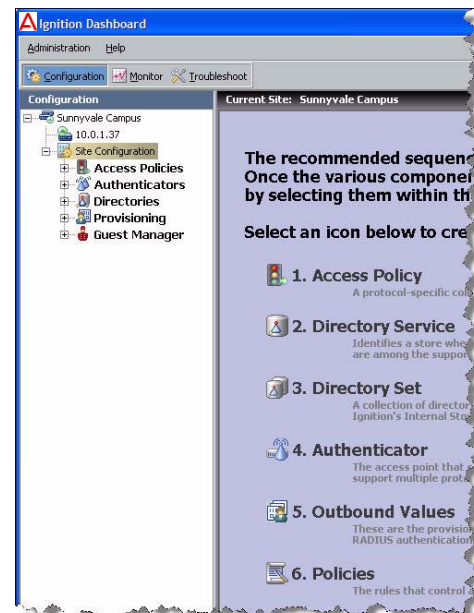
---

# Configuring Avaya Identity Engines Ignition Server

---

The Avaya Identity Engines Ignition Server authenticates users onto your wired and wireless networks and VPNs. This guide shows you how to set up Ignition Server to act as the RADIUS server for your switches and access points, and it shows you how to connect Ignition Server to your Active Directory (AD) or LDAP user database to authenticate users. An optional section shows you how to set rules that place each user on the right VLAN.

The guide 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 *Avaya Identity Engines Ignition Server Getting Started*.



The steps you will follow are:

- [Make Settings on the Ignition Server Appliance](#) (page 7)
- [Create a RADIUS Access Policy](#) (page 10)
- [Create a User in the Internal User Store](#) (page 11)
- [Set up Your Connection to a User Store](#) (page 13)
  - × [Connecting to Active Directory](#) (page 13)
  - × [Connecting to LDAP](#) (page 27)
- [Create a Directory Set](#) (page 35)
- [Create Virtual Groups](#) (page 37)
- [Create Authenticators](#) (page 40)
- [Set Your Authentication Policy](#) (page 42)

- 
- [Set Your Identity Routing Policy](#) (page 44)
  - [Set Your Authorization Policy](#) (page 45)
  - [Test Your Configuration](#) (page 50)



**Note:** Make sure you have a copy of the *Avaya Identity Engines Ignition Server Administrator's Guide* available. The *Configuration Guide* explains a simple configuration, and the *Administrator's Guide* provides a complete reference showing other configuration options.

## 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 *Avaya Identity Engines Ignition Server Getting Started*:
  - × 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 9](#).) 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.

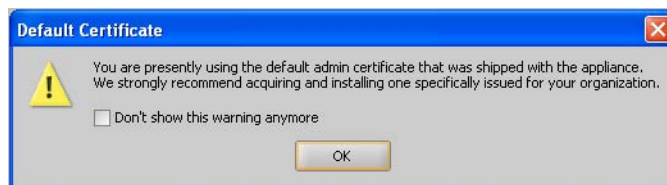
- 
5. **VPN client settings:** If you will use IPSec for VPN access, make sure that client machines (those that will VPN into the network) have an installed VPN client that speaks PAP or MSCHAPv2.

**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.

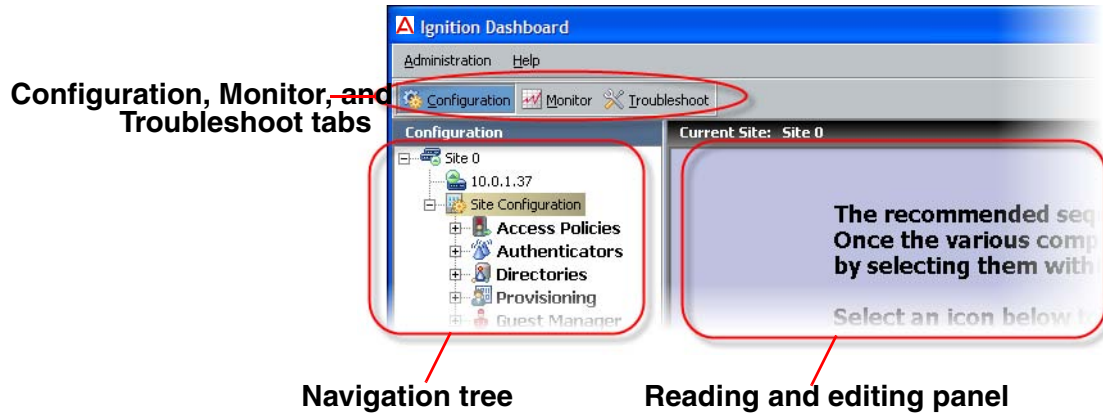
1. **Start Ignition Dashboard:** Double-click Ignition Dashboard icon on your desktop, or select **Start → Programs → Ignition Dashboard → Ignition Dashboard**. The application displays its login window.
2. Type the Ignition Server administrator **User Name** and **Password**. The default login credentials are *admin/admin*. In the **Connect To** field, enter the IP address of your Ignition Server appliance, and click **OK**.



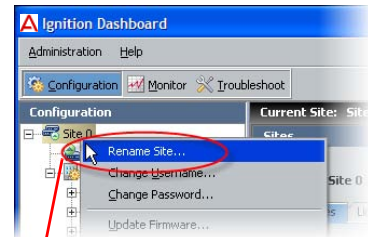
Initially, the **Default Certificate** window appears alerting you that you are using the default *Ignition Dashboard-to-Ignition Server certificate* ("admin certificate") that was shipped with Ignition Dashboard. Click **OK** to dismiss the window. (Avaya recommends that you later consult the

“Certificates” chapter of the *Avaya Identity Engines Ignition Server Administrator’s 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.



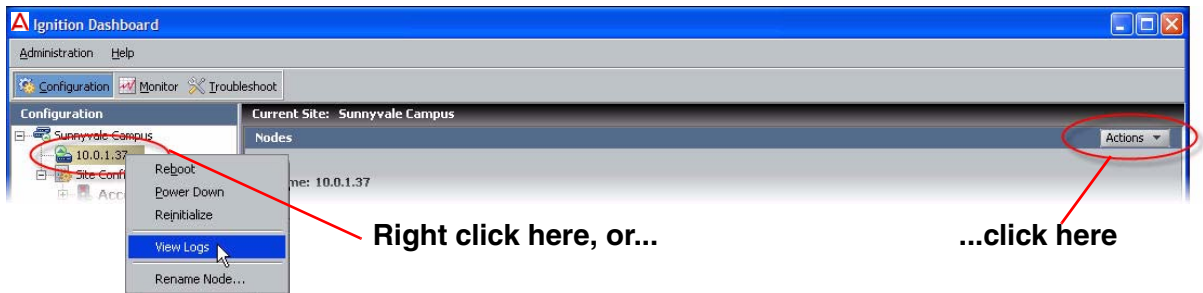
4. In the navigation tree, click on the machine name or IP address of the Ignition Server appliance you wish to configure. The application displays the **Nodes** panel, which allows you to manage network settings on the appliance, and check its current status.

Right-click

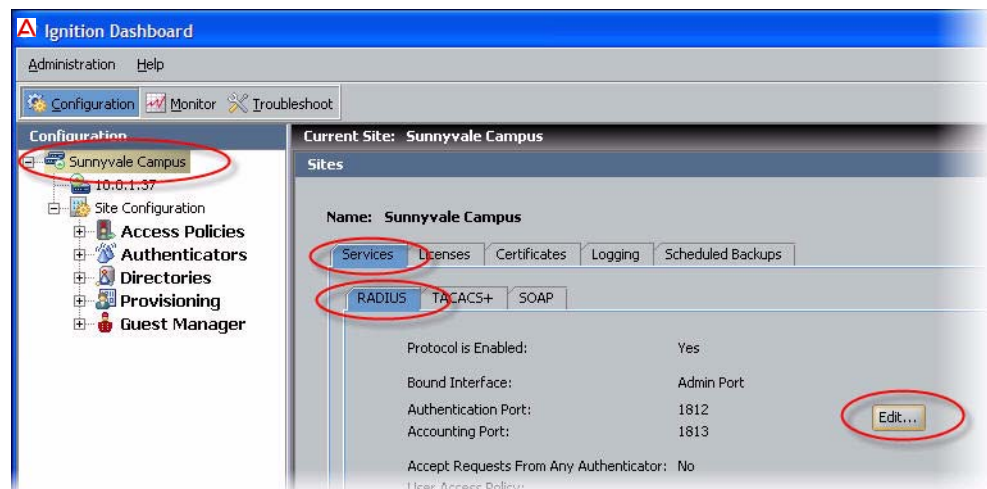
**Hint:** The **Actions** menu allows you to manage the appliance hardware (actions such as rebooting and shutting down). To use the **Actions** menu, right-click the IP address of your Ignition Server in the navigation



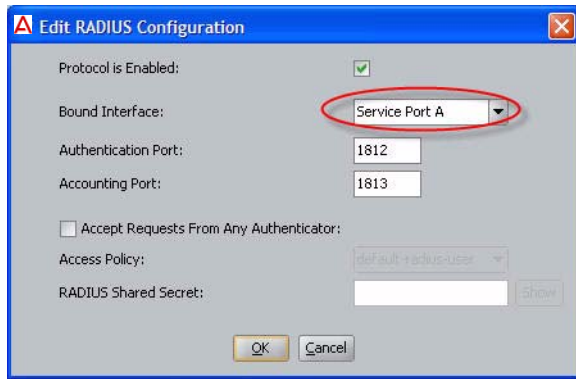
tree, or, with the IP address selected, click the **Actions** menu at the upper right.



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 you 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 you 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**.



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**.



- c. *Do this only if your 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.

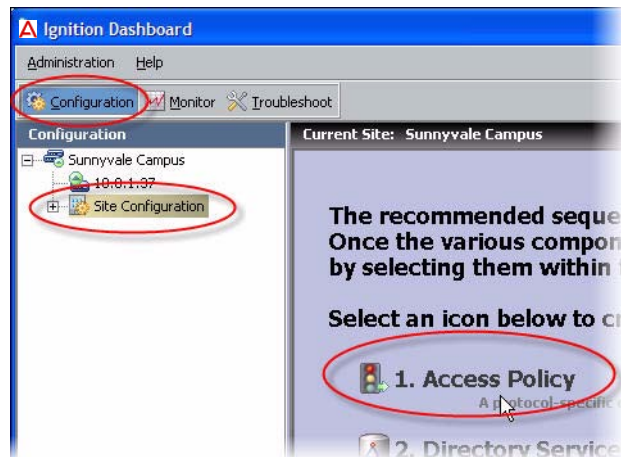
## Create a RADIUS Access Policy

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.

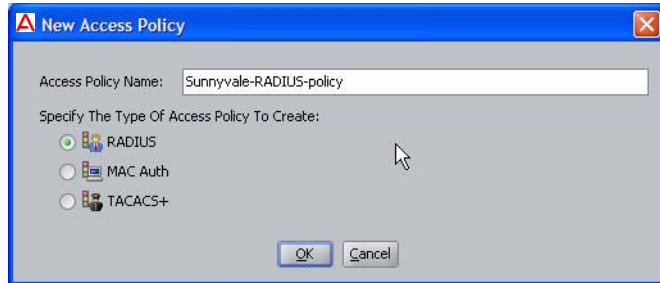
### Procedure:

1. If Dashboard is not connected to your Ignition Server, connect it now by selecting **Administration: Login**.



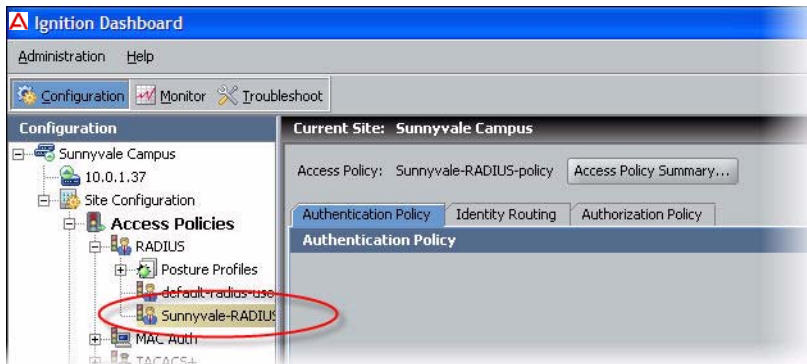
2. In the main window of Dashboard, click **Configuration**, click **Site Configuration** in the navigation tree, and click **Access Policy** in the main window.

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.



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.



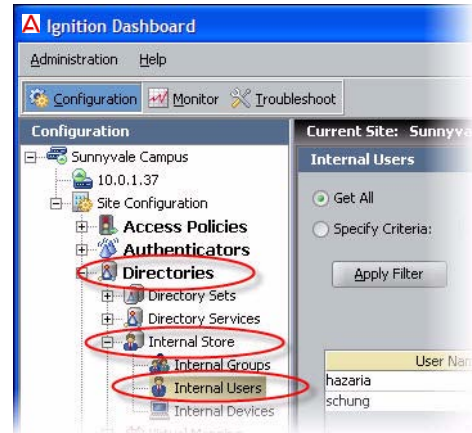
You will add rules to your access policy later, as shown in the section, [“Set Your Authentication Policy” on page 42.](#)

**Next steps:** Create a user account as shown in [“Create a User in the Internal User Store” on page 11.](#)

## Create a User in the Internal User Store

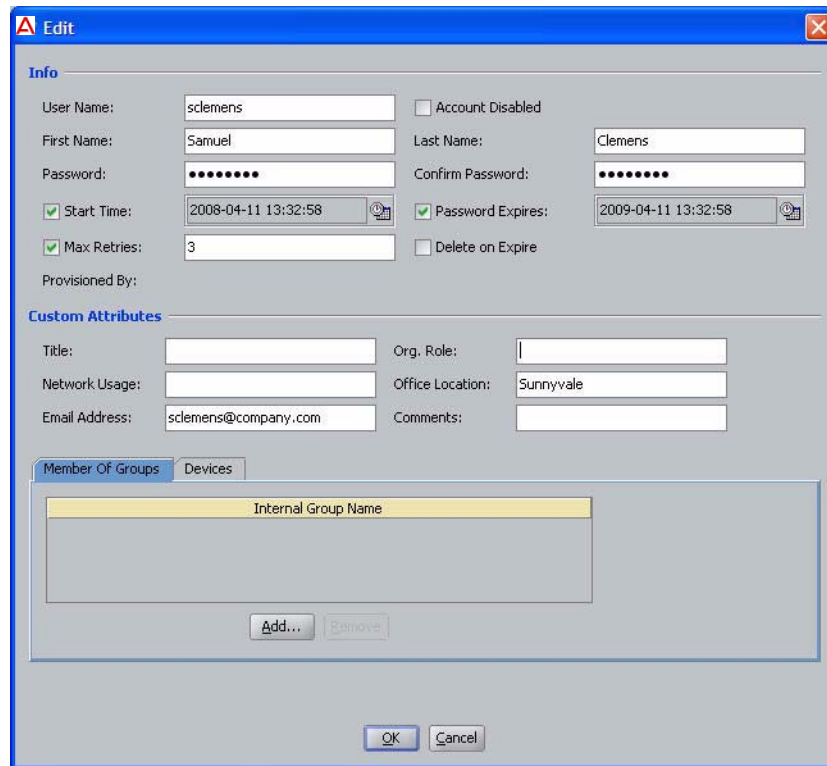
*This section is optional.* If you do not plan to use the Ignition Server internal user store, then you should skip this section and turn to [“Set up Your Connection to a User Store” on page 13.](#)

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 may 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.

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 the **New** button.



- 
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 step:** Connect to your enterprise user store as shown in [“Set up Your Connection to a User Store”](#) on page 13.

## 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* (see page 35) 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 need not create a directory service. Instead, proceed to [“Create a Directory Set”](#) on page 35.

**To connect to your used data store:** Use one of the following procedures:

- [“Connecting to Active Directory”](#), below; or
- [“Connecting to LDAP”](#) on page 27

### 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.

This section consists of:

- [“Gather Active Directory Connection Settings”](#) on page 14
- [“Prepare to Connect to Active Directory”](#) on page 16
- [“Create the Service Account in AD”](#) on page 18
- [“Set the AD Permissions of the Service Account”](#) on page 20
- [“Connect Ignition Server to AD”](#) on page 24
- [“Troubleshoot AD and LDAP Connections”](#) on page 31

---

## Gather Active Directory Connection Settings

Gather your AD connection settings. Use the AD connection settings that you used and created starting on page 18, 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
<b>AD Domain Name</b>	_____
	The <b>AD Domain Name</b> specifies the Active Directory domain that holds your user accounts. Domain names typically carry a domain suffix like “.COM” as in, for example, “COMPANY.COM”.
<b>Service Account Name</b>	_____
	The <b>Service Account Name</b> 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 <i>Ignition Server service account</i> . If you wish to perform MSCHAPv2 authentication, the service account must have permission to <u>create</u> and <u>delete</u> computer accounts (the <i>Create Computer Object</i> and <i>Delete Computer Object</i> permissions) in the <i>Netlogon account root</i> 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 <i>Computers container</i> 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 <i>Netlogon account root</i> 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.  <b>Note:</b> 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 <i>COMPANY.COM/Administrator</i> will usually be <i>Administrator</i> .  For help creating the service account, see <a href="#">“Create the Service Account in AD” on page 18</a> . For help setting its permissions, see <a href="#">“Set the AD Permissions of the Service Account” on page 20</a> .
<b>Service Account Password</b>	_____
	The <b>Service Account Password</b> is the password for the AD service account. <i>Do not record the password here.</i>
<b>Security Protocol</b>	<b>Simple or SSL</b>
	The <b>Security Protocol</b> setting specifies whether Ignition Server should SSL-encrypt traffic to the directory service. Avaya Identity Engines recommends that you use an SSL connection.
<b>IP Address (Primary)</b>	_____
	The <b>IP Address</b> of the primary AD data store.

---

**Table 1 Settings for connecting to an AD store**

Setting Name	Setting Value
--------------	---------------

**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!*

**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 34.

**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 33 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 33 for information on finding this DN.

**Netlogon Account Root DN**

\_\_\_\_\_

**Table 1 Settings for connecting to an AD store**

Setting Name	Setting Value
	<p>The <b>Netlogon Account Root DN</b> 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 <i>well known computer root</i> from the DC and uses that as the Netlogon account root DN.</p> <p>The Netlogon account root DN is typically the Active Directory Computers container (by default, this has a DN similar to <i>cn=computers,dc=company,dc=com</i>). The machine 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 <a href="#">“Set the AD Permissions of the Service Account” on page 20</a>.</p>

**Next steps:** Prepare your environment as explained in [“Prepare to Connect to Active Directory” on page 16](#).

### 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.

1. **Make sure you have gathered your AD connection settings** as explained in [“Gather Active Directory Connection Settings” on page 14](#).
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 NTLMv1 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.

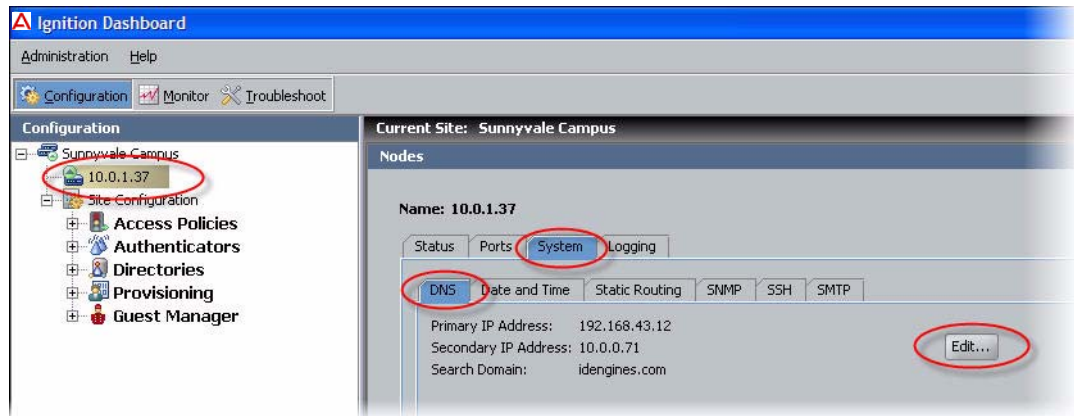
- \* Make sure that the following key is *not* set on the DC:  
`HKLM\System\CurrentControlSet\LSA\DisallowMsvChapv2`



- 
- \* 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 18](#).
  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 20](#).
  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.



**Next steps:** Connect to AD as explained in [“Connect Ignition Server to AD”](#) on page 24.

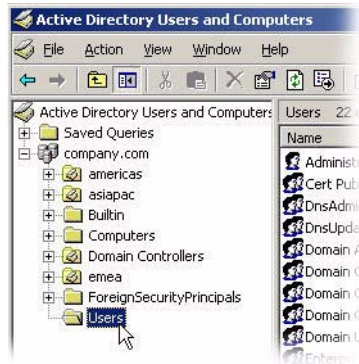
### Create the Service Account in AD

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.

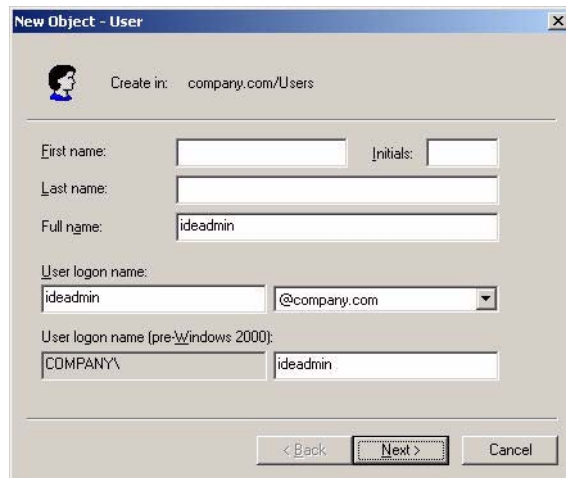
If you have a suitable account already, you may skip this section and turn to [“Set the AD Permissions of the Service Account”](#) on page 20. If you wish to create an account, follow the steps below.

1. Log into your AD server machine as the Domain Administrator or as a user with sufficient privileges to create users.
2. Open the Active Directory Users and Computers snap-in from the Administrative Tools or the Windows Control Panel.

3. In the object tree on the left side, click on the container in which you will create the new user. For this example we'll use the **Users** container.



4. Select the **Action: New: User** command.
5. In the **New Object - User** window, create the Ignition Server service account. Avaya recommends creating an account that will be used exclusively by the Ignition Server appliance. For this example, we use the account name, "ideadmin". Click **Next** after specifying the name.



- Assign a secure password to the account. Follow your organization's password policies. If you wish to ensure the reliability of the service account, check the **User cannot change password** and **Password never expires** checkboxes.



New Object - User

Create in: company.com/americas/serviceaccounts

Password: [dots]

Confirm password: [dots]

User must change password at next logon

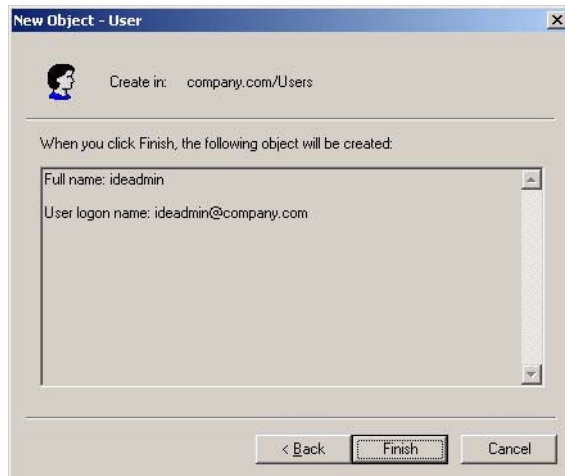
User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

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



New Object - User

Create in: company.com/Users

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

Full name: ideadmin

User logon name: ideadmin@company.com

< Back Finish Cancel

### Set the AD Permissions of the Service Account

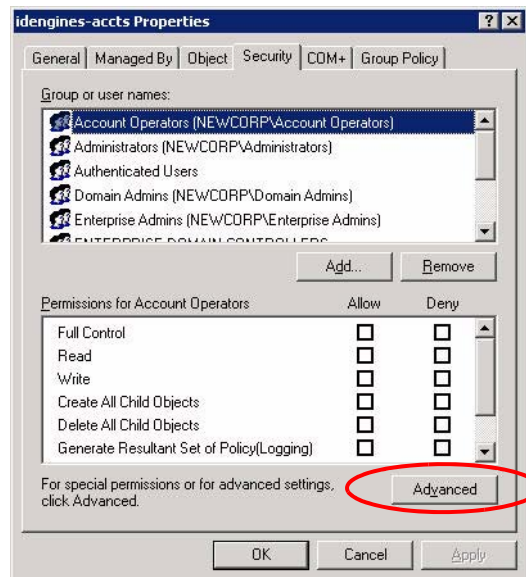
If you plan to support MSCHAPv2 authentication, the Ignition Server service account must have permission to create and delete computer accounts (the *Create Computer Object* and *Delete Computer Object* permissions) in the *Netlogon account root* of your Active Directory service. (For a description of this container, see Netlogon Account Root DN on page 15.)

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 14, instead.

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 on page 15 for information on setting or finding this DN.

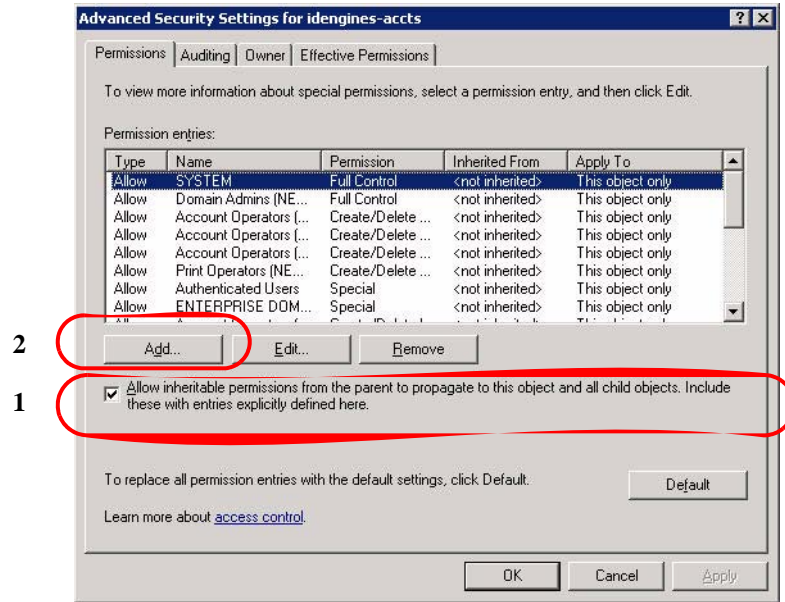
**Note:** If you wish to create a new container that will serve as the Netlogon account root, click on the root domain in the tree and create the new *OU* there.

4. Right click your *Netlogon account root container*, select the **Security** tab, and, under the **Permissions for Account Operators** list, click the **Advanced** button.

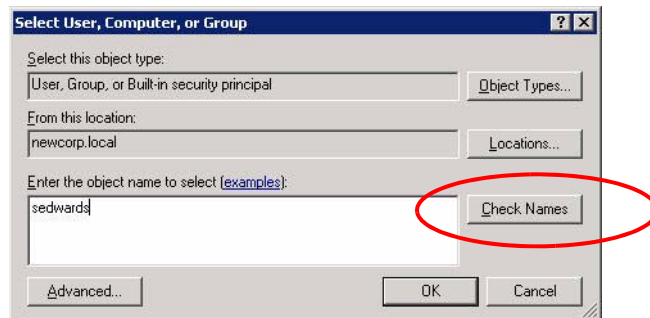


5. In the Advanced Security Settings window, click the permissions tab and:
  - × Make sure the **Allow inheritable permissions from the parent to propagate...** checkbox is checked.

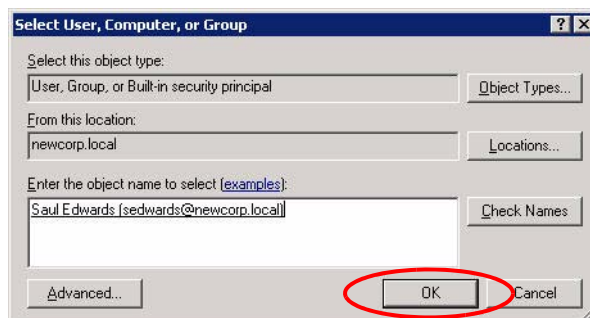
- × Click the **Add...** button.



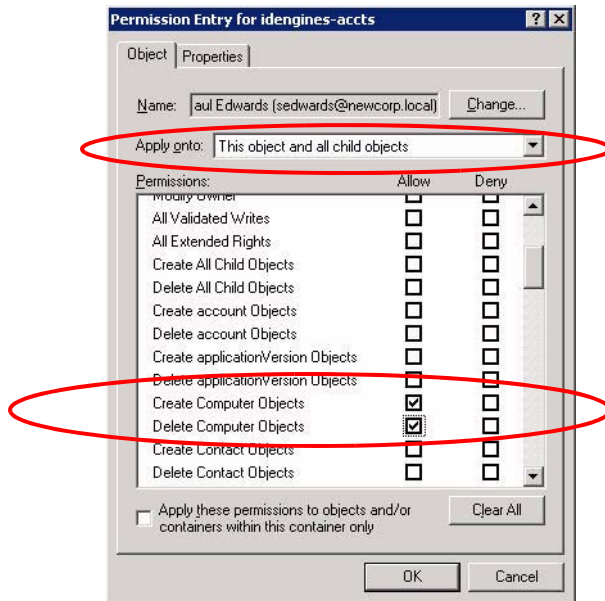
6. In the **Enter the object name** field, type the name or partial name of your Ignition Server service account and click **Check Names**.



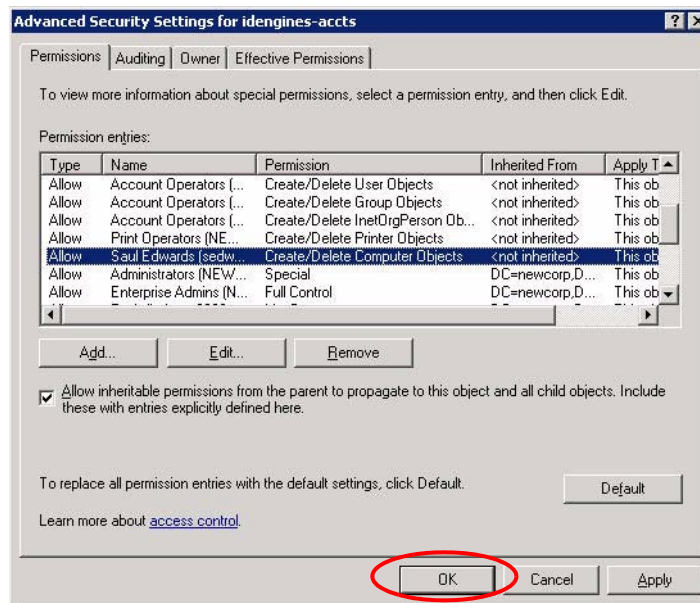
7. The window displays a list of names that match the name you typed. Click the desired account name and click **OK**.



8. In the **Permission Entry** window, click the Object tab and:
  - × In the **Apply onto** field, choose *This object and all child objects*.



- × In the permissions table, scroll to find the rows, **Create Computer Objects** and **Delete Computer Objects**, and click the **Allow** checkbox for each.
  - × Click **OK**.
9. Click **OK** again to dismiss the Advanced Security Settings window and again to close the snap-in.



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 14

### 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 page 35.

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 18.

Connect using Ignition Server’s AD connection wizard in *automatic connection* mode:

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**.



**Note:** If your AD connection attempt fails while you are carrying out the steps below, see [“Troubleshoot AD and LDAP Connections”](#) on page 31.

5. The Connect to Active Directory window appears. Enter the connection settings you gathered on Page 14, or use the login you created starting on page 18.



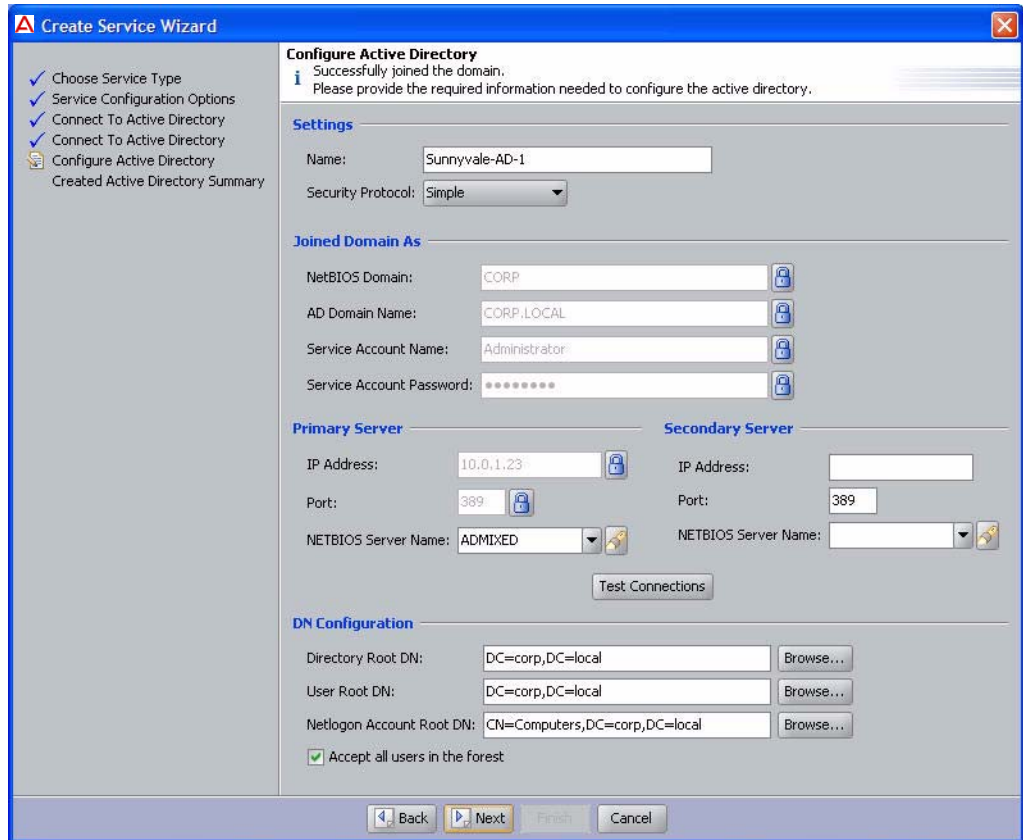


6. In the next screen:

- × 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.



7. The Configure Active Directory window appears.



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 on page 14.

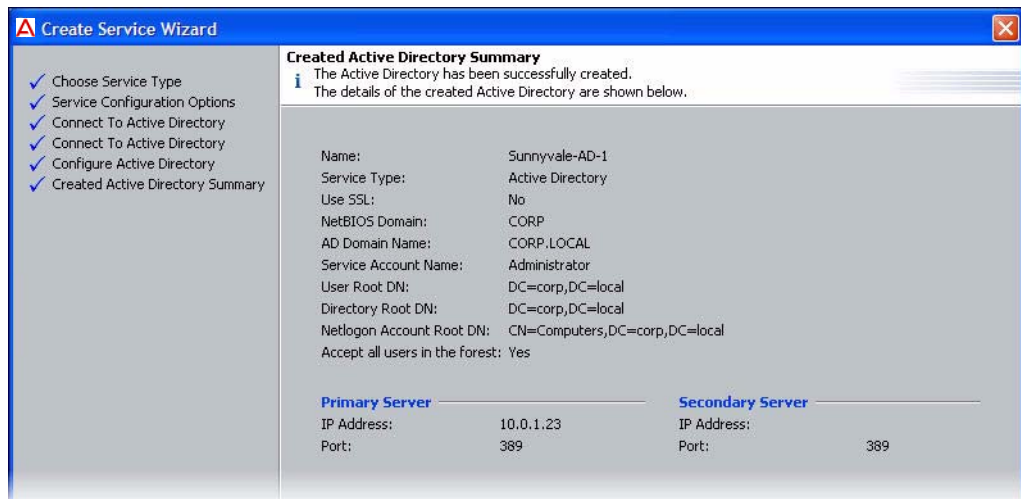
The **Primary Server IP Address** and **Port** fields are populated by the wizard; if necessary, click to unlock and edit them.

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 the table, table on page 14. You may type the DN directly or click the **Browse** button to browse your directory to find it. Note that the schema browser will not display auxiliary classes; those you must type directly.

Click **Next**.

8. 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.



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

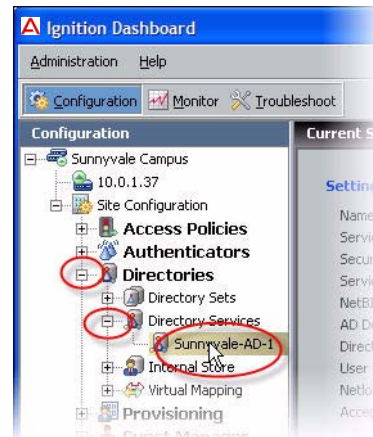
**Next steps:** Do one of the following:

- If the connection attempt succeeded, continue with “[Create a Directory Set](#)” on page 35.
- If your connection attempt failed, see “[Troubleshoot AD and LDAP Connections](#)” on page 31.

**Hint: Editing a Directory Service**

To edit your directory service, follow these steps:

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 on page 35.

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:

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**.



- In the Configuration Options window, click **Automatically configure** and click **Next**.

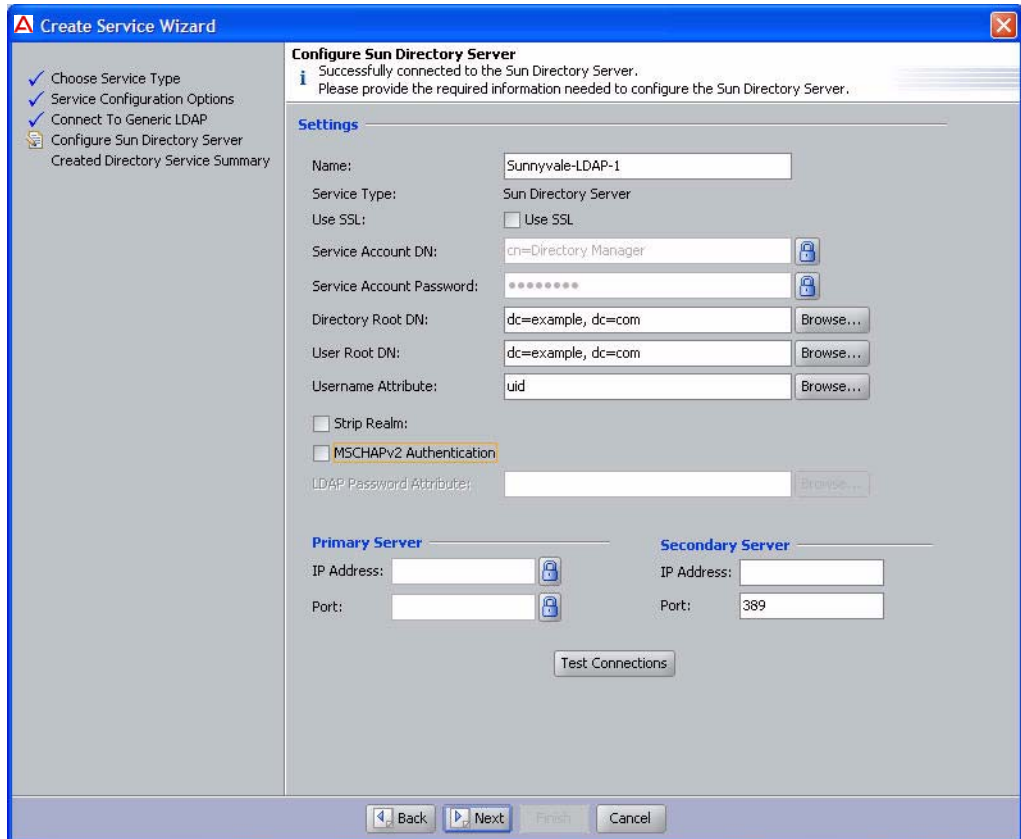
**Note:** If your LDAP connection attempt fails while you are carrying out the steps below, see “[Troubleshoot AD and LDAP Connections](#)” on page 31.

- The Connect to Directory Server window appears. Use the guidelines below for filling out the fields.



- × **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.
- Click **Next**.

The Configure Directory Server window appears.



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.

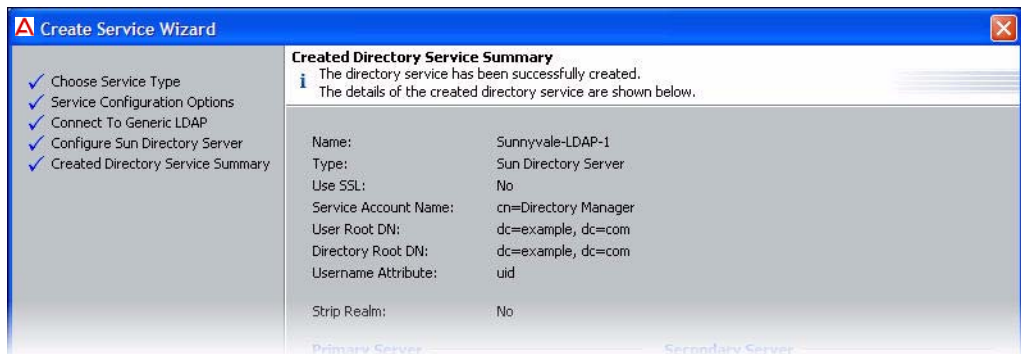
*Optional:* If this LDAP store will support MSCHAPv2 authentication, check the **MSCHAPv2 authentication** check box and, in the **LDAP Password Attribute** field, set the name of LDAP attribute that stores the hash of the user's MSCHAPv2 password. See "Setting up MSCHAPv2 Authentication on LDAP" in the *Ignition Server Administrator's Guide* 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.



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 35.
- If your connection attempt failed, see [“Troubleshoot AD and LDAP Connections”](#) on page 31.

**Hint: Editing a Directory Service**

To edit your directory service, follow these steps:



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**.

**Troubleshoot AD and LDAP Connections**

This section contains tips for:

- [“Checking a Directory Connection”](#) on page 31
- [“Checking Directory Connections and Cache Status”](#) on page 32
- [“Testing a Directory In-Depth”](#) on page 32
- [“Looking Up AD Settings: Finding Your Root DNs”](#) on page 33
- [“Looking Up AD Settings: Finding Domain and NetBIOS Names”](#) on page 34
- [“Looking Up AD Settings: IP Address”](#) on page 34

**Checking a Directory Connection**

To check that Ignition Server is connected to your directory service, do this:

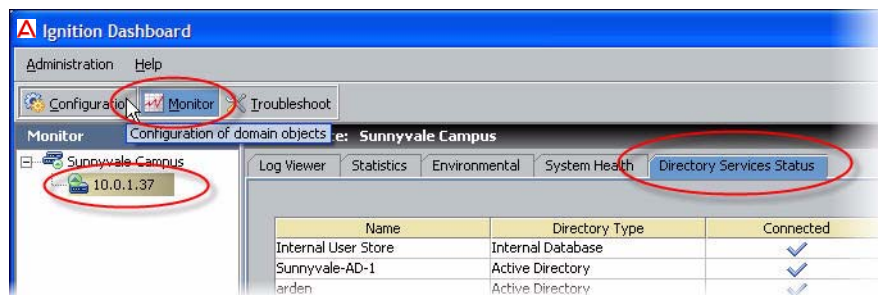
1. In Dashboard’s **Configuration** tab, in the navigation tree, click the plus sign next to **Directories**.
2. Click the plus sign next to **Directory Services**.
3. Click the name of your directory service.
4. Click the **Test Connections** button.

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

To check the connection status and cache status (Ignition Server caches user group memberships) of all of your directory services, do this:



1. Click on Dashboard's **Monitor** tab,
2. In the navigation tree, click the IP address of your node (you Ignition Server).
3. Click the **Directory Services Status** tab.
4. Click the name of your directory service.
5. Click the **Test Connections** button.

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

## Testing a Directory In-Depth

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**, or **Auth User** tab to run your tests. For instructions, see "Advanced Troubleshooting for Directory Services and Sets" in the *Avaya Identity Engines Ignition Server Administrator's Guide*.

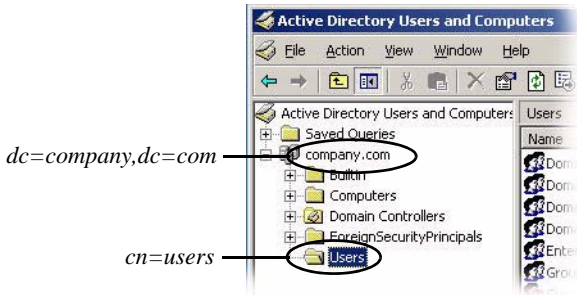


## Looking Up AD Settings: Finding Your Root DNs

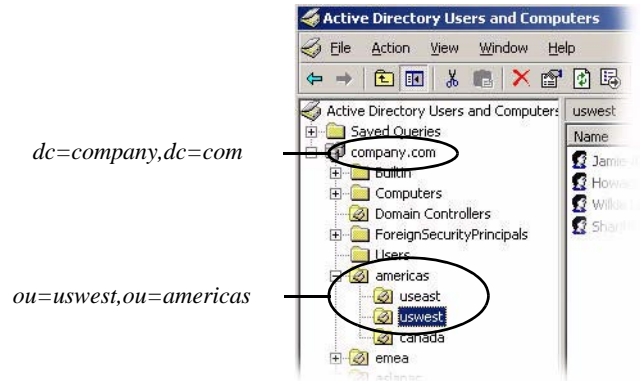
**User Root DN** and **Directory Root DN**: Enter the names of containers in your AD data store using X.500 naming. **User Root DN** points to the AD container that stores your user records. **Directory Root DN** points to the root of your AD tree and will be used to obtain schema and group information.

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.

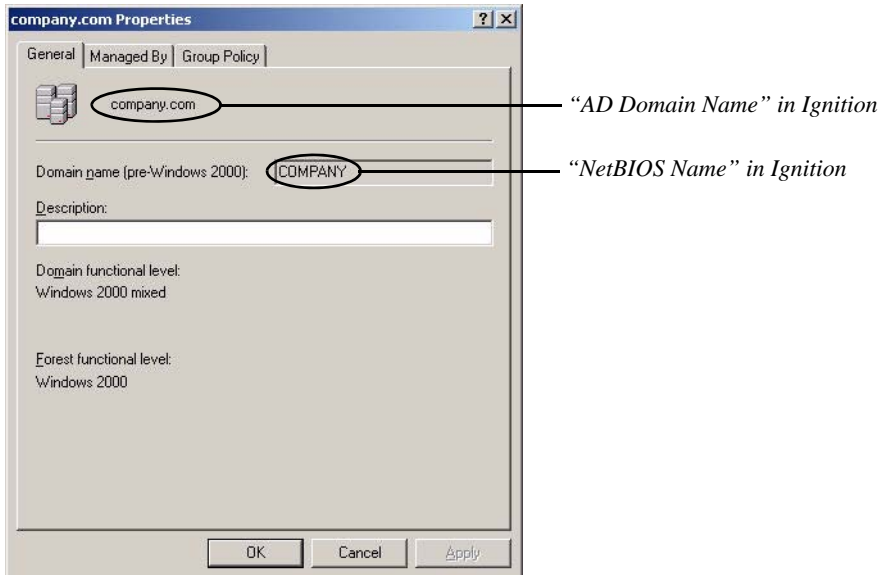
---

## Looking Up AD Settings: Finding Domain and NetBIOS Names

To find the **AD Domain Name** and **NetBIOS Name**, 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”. Right-click the root domain name and select **Properties** to open the Properties window.



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.



## Looking Up AD Settings: IP Address

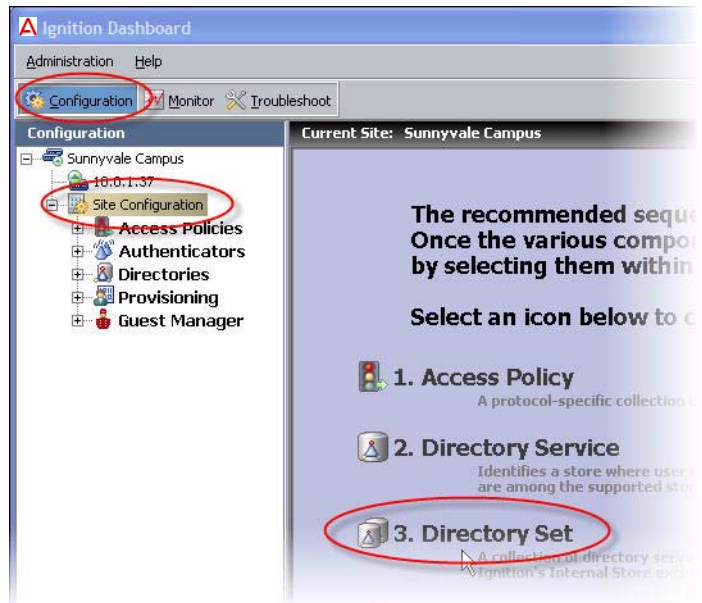
To find the IP address of your AD server, log into the machine that hosts your AD server and use the “ipconfig” tool from the command line, or open the Windows Control Panel and select **Network Connections: Local Area Connection**. In the Local Area Connection Status window, click **Properties**. In the Local Area Connection Properties window, click **TCP/IP** and then click **Properties**. Read the **IP address** from the TCP/IP Properties window.

## Create a Directory Set

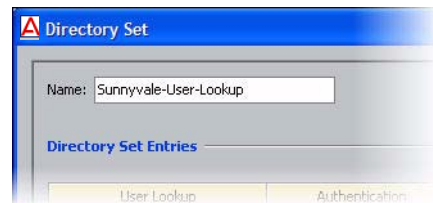
A directory set is the mechanism Ignition Server uses to scan multiple directories for a user account. You will define each user data store (that is, each AD data store, LDAP data store, and the embedded store) as a directory service in Ignition Server, and you will group those directory services into 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:

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 “**3. 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.
5. In the Directory Set Entry window, specify the directory that will provide user account data and group memberships (**User Lookup Service**) and the directory that will authenticate users (**Authentication Service**).



**Note:** Usually 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.

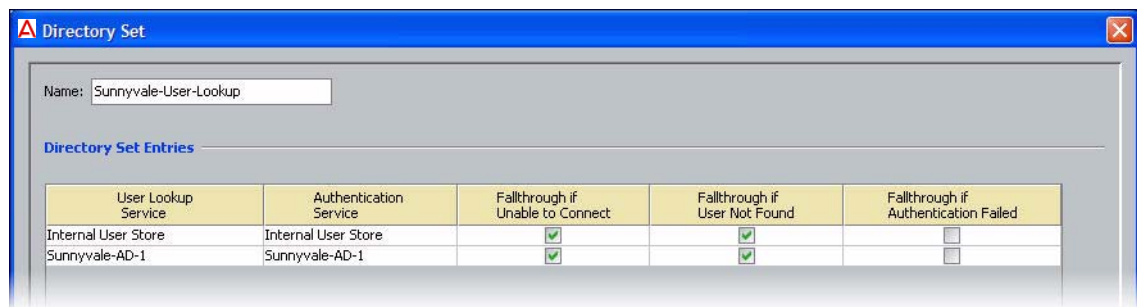
For the example in this document, we'll use the internal user store so that we can later demonstrate an authentication of the user account we created earlier. If you have an LDAP or AD user you can test with, then feel free to use your AD or LDAP store, instead:

- × 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**.



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.



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

**Next step:** Map user groups as shown in “[Create Virtual Groups](#)” on page 37.

## Create Virtual Groups

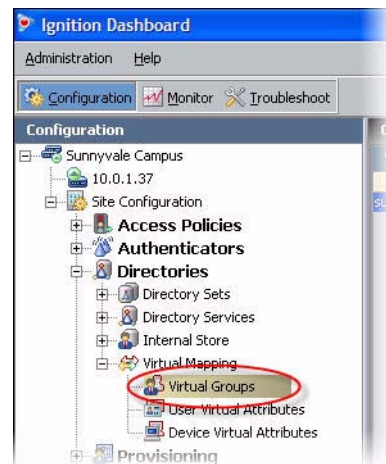
Virtual groups are Ignition Server’s mechanism for abstracting, or standardizing, group names across multiple user databases. You can map an Ignition Server virtual group to many groups in many databases, allowing you to treat these groups as a single group in your policies.

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*”.

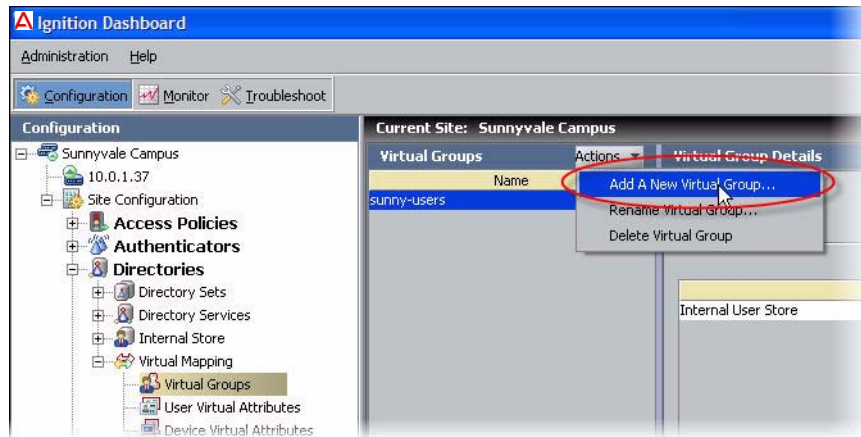
Virtual groups are required if you wish to evaluate group membership in your policies. Ignition Server looks up group membership only by means of a virtual group, so even if you have only one data store, you must create a virtual group.

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:

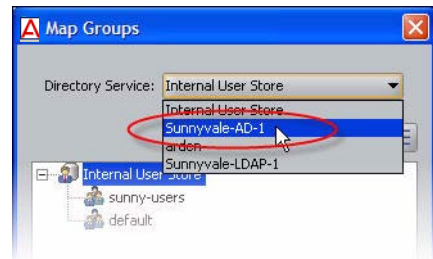
1. In Ignition Dashboard, click **Configuration**, then, in the navigation tree, click the plus sign to expand **Site Configuration**, expand **Directories**, expand **Virtual Mapping**, and click **Virtual Groups**.



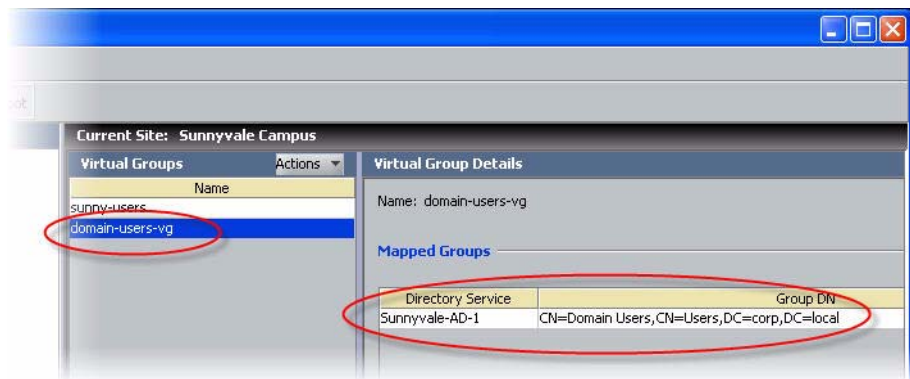
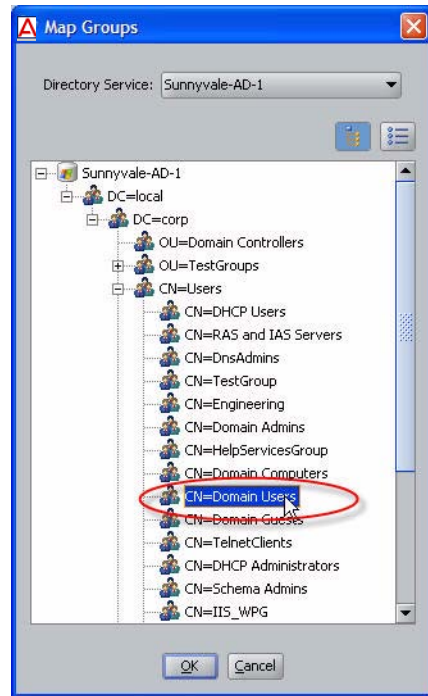
2. In the Virtual Groups panel, click **Actions** and select the command, **Add New Virtual Group...**



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 `domain-users-vg`. This group will contain the members of the “Domain Users” group of the AD server.
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.



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*. (**Note:** If you are using the Embedded Store instead, you may create an embedded group and map your virtual group to that instead.)
7. Click **OK** to close the Map Groups window. The new mapping appears in the Mapped Groups list.



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 may use membership in the group as a criterion for authorization and provisioning.

**Next step:** Create a record in Ignition Server for your switch or access point, as shown in [“Create Authenticators”](#) on page 40.

---

## 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.

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 Connection Settings

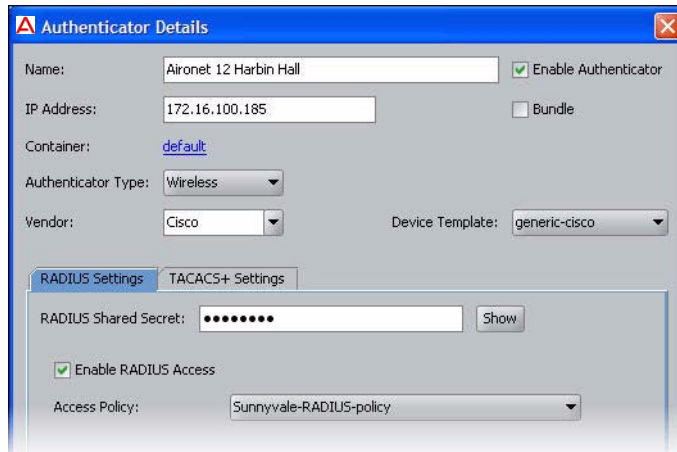
	Authenticator 1	Authenticator 2	Comment
<b>Authenticator Name</b>	_____	_____	Choose a name to identify the authenticator. This name will be used to refer to the authenticator within Ignition Server.
<b>IP Address</b>	_____	_____	IP address of authenticator.
<b>Subnet Mask</b>	_____	_____	<i>Optional:</i> 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.
<b>Container</b>	_____	_____	<i>Optional:</i> If you are grouping your authenticators using Ignition Server’s “Container” mechanism, select this authenticator’s container.
<b>Authenticator Type</b>	_____	_____	One of the following: wired switch, wireless access point, or VPN concentrator.
<b>Vendor</b>	_____	_____	Manufacturer of the switch or access point.
<b>Device Template</b>	_____	_____	Ignition Server template to be used to specify formats (attribute names and types) for communicating with this authenticator.



**Authenticator Connection Settings (continued)**

	<b>Authenticator 1</b>	<b>Authenticator 2</b>	<b>Comment</b>
<b>RADIUS Shared Secret</b>	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.”		
<b>Access Policy</b>	_____	_____	Name of the Ignition Server RADIUS policy that contains your access rules for users connecting through this authenticator. For example, the name of the policy you created in <a href="#">Step 3 on page 11</a> .

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.



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 11](#).



**Note:** For an explanation of the rest of the fields, refer to the “Authenticators” chapter of the *Ignition Server Administrator’s Guide*.

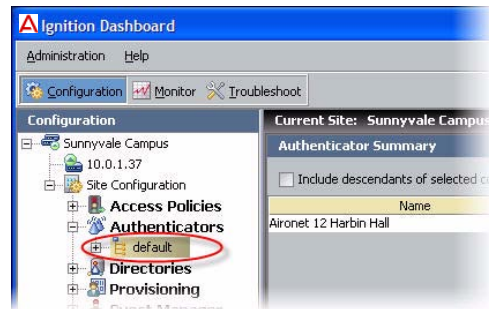
5. Click **Save** to save the settings in the **Authenticator Details** window.

**Next step:** Set your credential verification rules as shown in [“Set Your Authentication Policy” on page 42](#).

### Hint: Editing Authenticators

To edit authenticators, follow these steps:

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 10. 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 Access Policies

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.

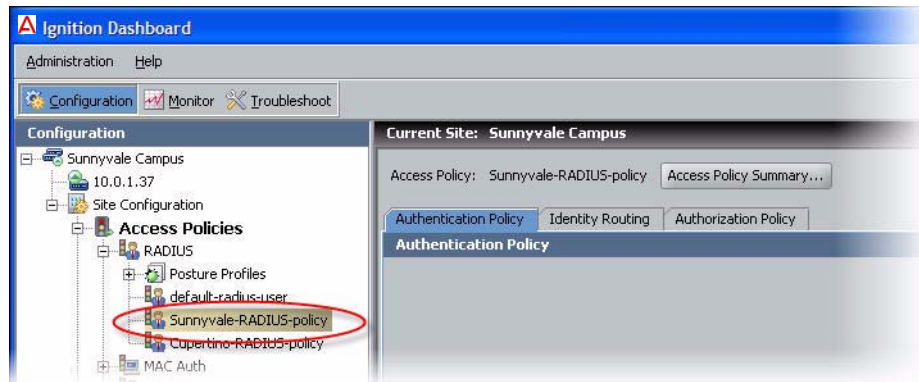
In your Ignition Server system you may define many access policies for the many different segments of your organization, but you will assign one and only one RADIUS access policy to each authenticator. This means that all users connecting through that authenticator are governed by that RADIUS access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

### Procedure

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.

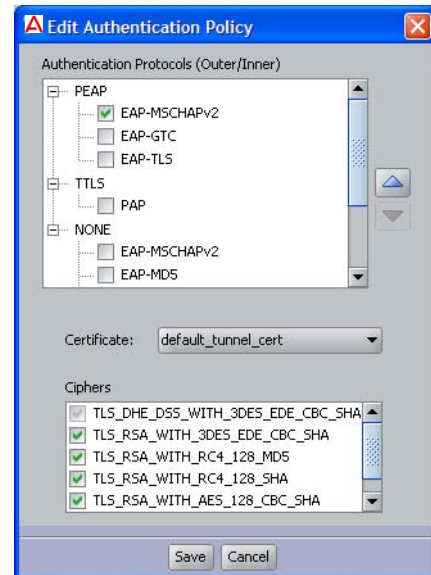
1. From the Dashboard main window, click on the **Configuration** tab, expand the **Site Configuration** item in the tree (click the plus sign to expand an item), and expand the **RADIUS** item in the tree. Click your policy's name to load it into the **Access Policy** panel.



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.



If you wish to verify that an authentication protocol is compatible with your data store, consult the section, “Supported Authentication Types” in the *Avaya Identity Engines Ignition Server Administrator's Guide*.

You may 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.

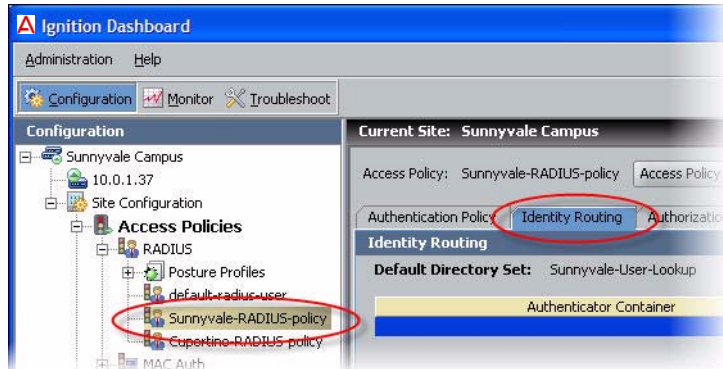


**Note:** If your users are stored in Active Directory and the embedded store, then your policy will typically include at least the PEAP/EAP-MSCHAPv2 and NONE/PAP authentication types.

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.



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 35](#). If you are using the example names, this will be the set called *Sunnyvale-User-Lookup*.
- b. Tick the **Match All Realms** check box.
- c. Tick the **Disable Authenticator Container Matching** check box.
- d. Click **OK**.



Note that in a production system, you could 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:



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. (Note: The authorization policy can also prescribe provisioning for users as explained in the Provisioning chapter of the *Avaya Identity Engines Ignition Server Administrator's Guide*.)

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”](#), below.
- If your user accounts reside in an *AD user store*, see [“Authorization Policy—Example for AD Users”](#), on page 48.

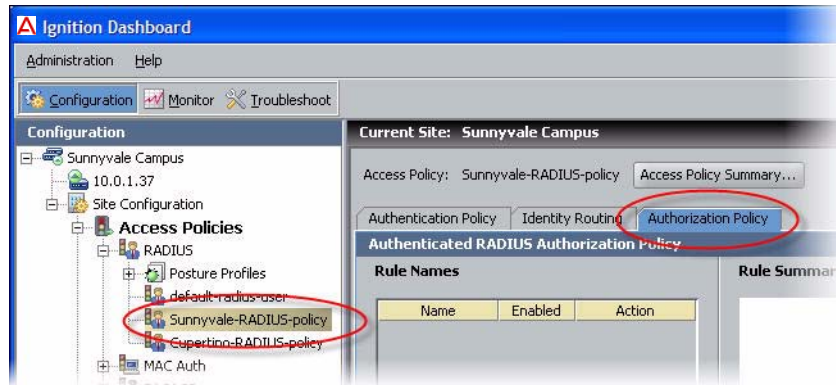
Note that you may store users in the embedded store, AD store, and additional stores at the same time, and handle them all in the same access policy (See [“Set Your Identity Routing Policy”](#) on page 44.)

### Authorization Policy—Example for Embedded Store Users

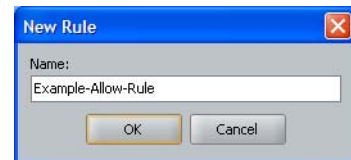
If your user accounts are stored in the Ignition Server internal user store, set up your authorization policy as shown below.

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:

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.



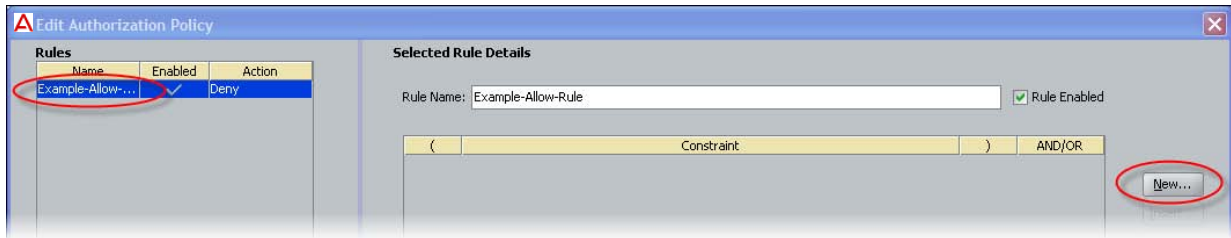
2. The top half of the **Authorization Policy** tab contains your RADIUS authorization policy. Click the top **Edit** button to edit it. The Edit Authorization Policy window appears.
3. In the **Rules** section, in the lower left part of the window, click **Add**. The application displays the New Rule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

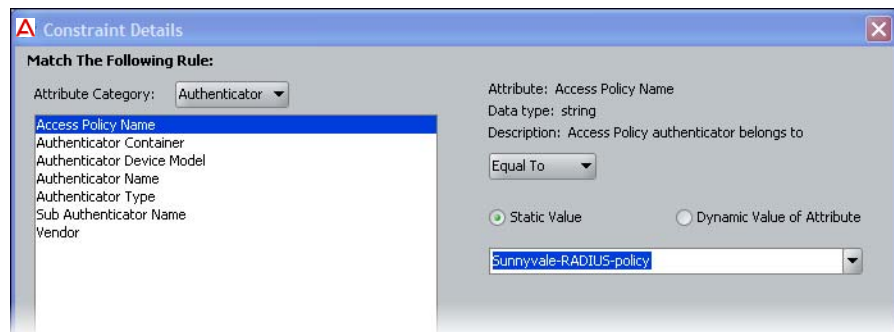
6. With your rule selected, go to the buttons to the right of the **Constraint** list and click **New**, as shown below.



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.

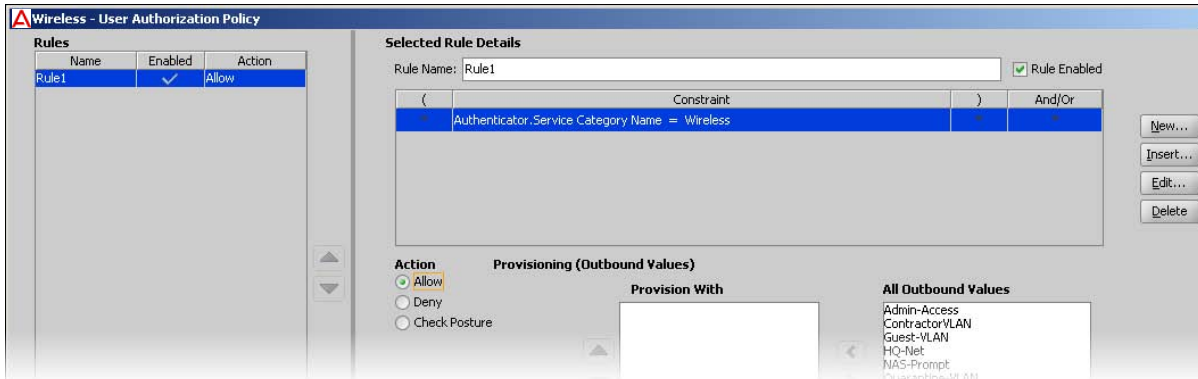
Below, we create a rule that compares the access policy name of the request with the access policy name of this policy; this rule evaluates to true by definition.

- × In the **Attribute Category** drop-down list, select the attribute type, *Authenticator*. In response, the list shows all the attributes of type *Authenticator*. In the list, select the attribute name, *Access Policy Name*.



- × In the top drop down menu on the right, select **Equal to** and tick the **Static Value** checkbox.
  - × In the drop down list directly just below the checkbox, select the access policy you defined earlier in [Step 3 on page 11](#). If you are following this example, the name is *Sunnyvale-RADIUS-policy*.
  - × Click **OK** to close the Constraint Details window and return to the Edit Authorization Policy window.
8. In the **Action** section, click the **Allow** button.

9. In the **Provisioning** section, make no changes.



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

11. You have finished setting policies in your access policy. Click **Close** to exit the Policy Management window.

**Next Steps:** Congratulations! Your example configuration is complete. For information on troubleshooting, see [“Test Your Configuration” on page 50](#).

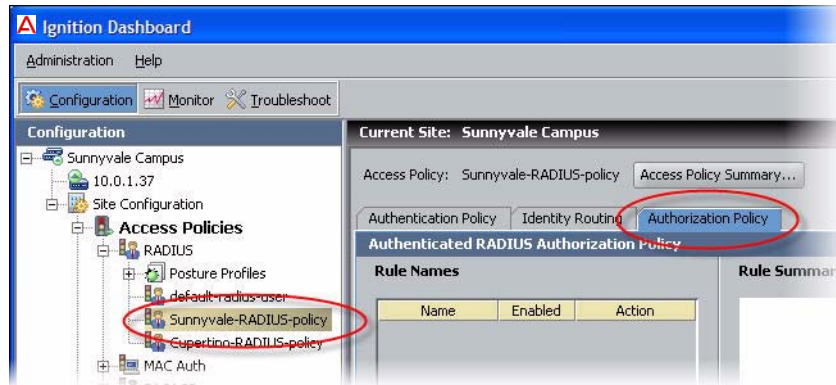
### Authorization Policy—Example for AD Users

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.

To create a rule that checks AD domain membership, follow these steps:

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**.

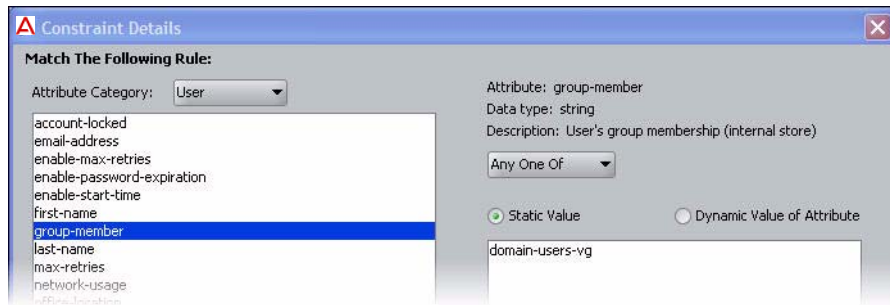


**Note:** To learn how Ignition Server evaluates sets of rules and constraints, consult the *Avaya Identity Engines Ignition Server Administrator's Guide*.

- 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 **Any One Of** 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 *domain-users-vg*. Click **OK** to close the window.

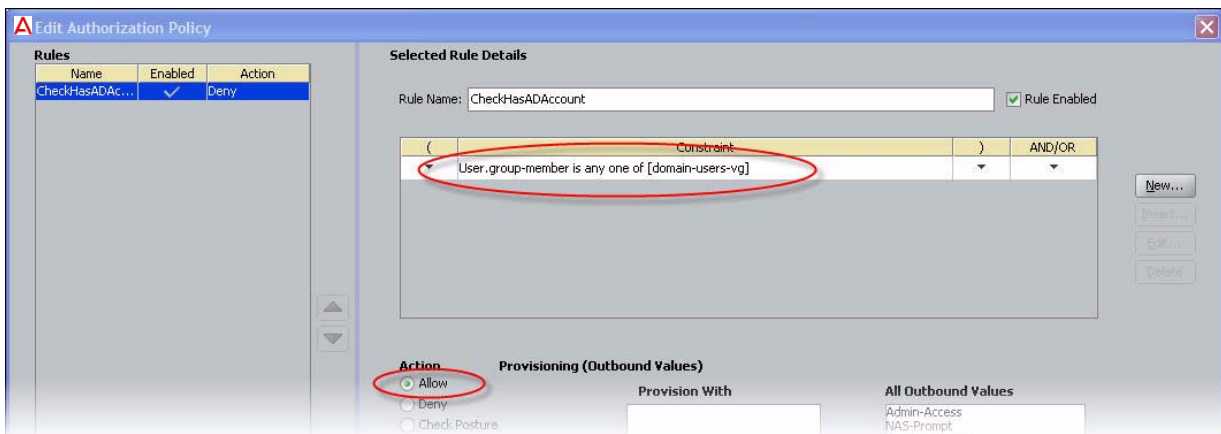


- f. Click **OK** to close the Constraint Details window and return to the Edit Authorization Policy window.



- 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.



- 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 50.](#)

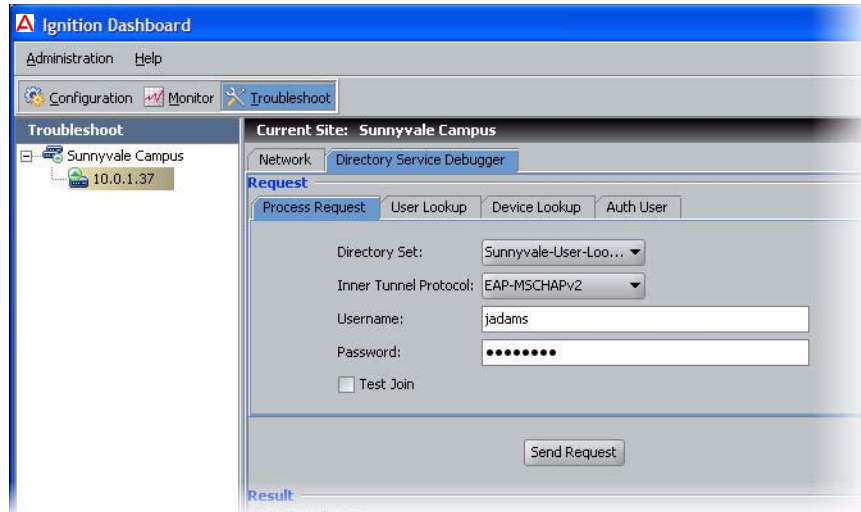
## Test Your Configuration

### Checking User Lookup and Authentication

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

- 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.



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.

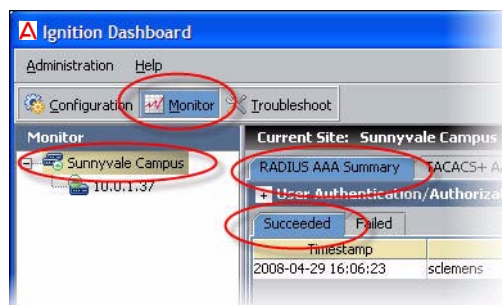
### Use NTRadPing as a Test Authenticator

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. To do this:

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** or **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.



