Extreme™
Customer-Driven Networking

Identity Engines Ignition Server Getting Started

Release 9.5.0
9035375 Rev 01
October 2018

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: http://www.extremenetworks.com/support/contact/

For product documentation online, visit: https://www.extremenetworks.com/documentation/

Contents

Chapter 1: About this Document

Purpose

The *Identity Engines Ignition Server Getting Started document* explains how to install and configure the Identity Engines Ignition Serverand is authored for network administrators who want to quickly install and configure the Ignition Server. For advanced configuration information, see *Identity Engines Ignition Server Configuration document*.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons

Icon	Alerts you to...
Important:	Key information that does not carry with it the risk of personal injury, death, system failure, service interruption, loss of data, damage to equipment, or electrostatic discharge.
Note:	Important features or instructions.
Tip:	Helpful tips and notices for using the product.
Warning:	A potential hazard exists that, if not avoided, can result in harm to hardware or equipment.
Caution:	Practices that are not safe or are potential hazards not covered by danger or warning messages.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2018-09-12 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/open-source-declaration/.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- **GTAC (Global Technical Assistance Center) for Immediate Support**
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **Extreme Portal** — Search the GTAC knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- **The Hub** — A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.

2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

   Note:
   You can modify your product selections or unsubscribe at any time.
4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this Document

This sections describes what is new in *Identity Engines Ignition Server Getting Started document* for Release 9.5.0.

Guest and IoT Manager Enhancements

The current release of Identity Engines Guest and IoT Manager adds the following new enhancements:

Platform Updates

- Underlying Operating System has been updated to RHEL 6.7 version.
- Open SSL libraries have been updated to address vulnerabilities.
- Default Root CA and Server Certificates have been replaced with Extreme trusted Root and Server Certificates.

IoT Device Registration (IDR) Android App

The IDR Android App is available with enhanced User Interface and supports connection over HTTPS services.

Ignition Server Enhancements

The current release of Ignition Server adds the following new enhancements:

Ignition Server Integration with Extreme Management Center

Ignition Server now support Extreme Management Center, which is a single pane of Glass Management system that provides control of wired / wireless visibility from the data center to the mobile edge. It can also send Access Logs to be displayed on Extreme Control Dashboard. This is useful for the customers who have purchased Extreme Control and are interested to co-deploy Ignition Server.

Platform Updates

- Underlying Operating System has been updated to RHEL 6.7 version.
- Open SSL libraries have been updated to address vulnerabilities.
- Default Root CA and Server Certificates have been replaced with Extreme trusted Root and Server Certificates.

RADIUS Vendor-Specific Attributes Support for ExtremeXOS based Network Switches and Enterasys switches.

In this release, the full set of RADIUS Vendor-Specific Attributes have been added to the default database on the Ignition Server to provide seamless integration with the ExtremeXOS based Switches and Enterasys family of Switches. Administrators can create inbound / outbound attributes for these VSAs and utilize them in the Authorization Policies as needed.

Hardware Specifications

IDE 9.5.0 release supports installation of the Ignition Dashboard desktop application only on computer running on any one of the following:

- Windows 7 (64 bit)
- Windows 8 or Windows Server 2008 (64 bit)
- Windows Server 2012 (64 bit)
- Windows 10 (64 bit)

For more information on the Ignition Dashboard installation, see Installing the Ignition Dashboard Desktop Application on page 21.

Note:

You can now perform Identity Engines Dashboard installation on non-English Windows platform.

Chapter 3: Getting Started

This chapter describes to perform Identity Engines Ignition Server installation and configuration tasks. Perform your set-up in the following phases:

1. Installing the Ignition Server Virtualization Appliance on page 12
2. Preventing Automatic VMware Tools Updates on page 17
3. Configuring the Ignition Server Virtualization Appliance on page 19
4. Installing the Ignition Dashboard Desktop Application on page 21
5. Running the Dashboard on page 27
6. Obtaining the Ignition Server Serial Number on page 28
7. Obtaining Perpetual Production Licenses on page 31
8. Installing the License on page 31
9. Setting up the Service Port (Optional) on page 32 and Setting the Admin Password and User, Site, and Node Names on page 33
10. Further Configuration on page 35

VMware ESXi Server

Hardware platforms supported by VMware ESXi versions are 5.5, 6.0 and 6.5. 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: Extreme Networks provides the Identity Engines Ignition Server, Ignition Guest and IoT Manager, and Ignition Access Portal as Virtual Appliances. Do not install or uninstall any software components unless Extreme Networks 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 Extreme Networks documentation and/or personnel specifically instructs you to do so. Extreme Networks 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 Extreme Networks:

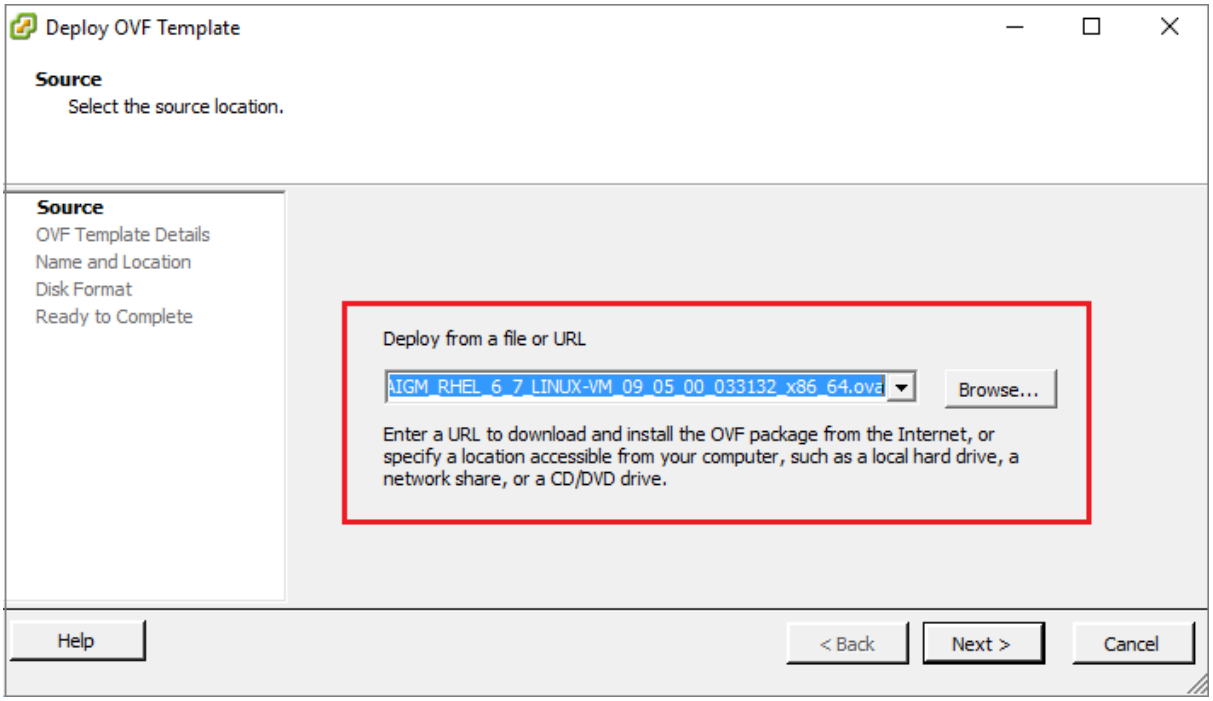
- Extreme Networks does not support manual or automated VMware Tools installation and configuration on Extreme supplied VMs.
- Turn off automatic VMware Tools updates if you have enabled them. Refer to the instructions in Preventing Automatic VMware Tools Updates on page 17 to disable automatic updates and to check if you have accidentally installed VMware tools.
- Extreme Networks determines which VMware Tools to install and configure. When required, Extreme Networks provides these tools as part of the installation or package upgrade procedures. Extreme Networks provides these tools because VMware Tools configures the kernel and network settings and unless Extreme Networks tests and approves these tools, Extreme Networks cannot guarantee the VM can work after the tool is installed and configured.
- Extreme Networks 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 Extreme Networks ships as a package, image, or OVF.

Installing the Ignition Server Virtualization Appliance

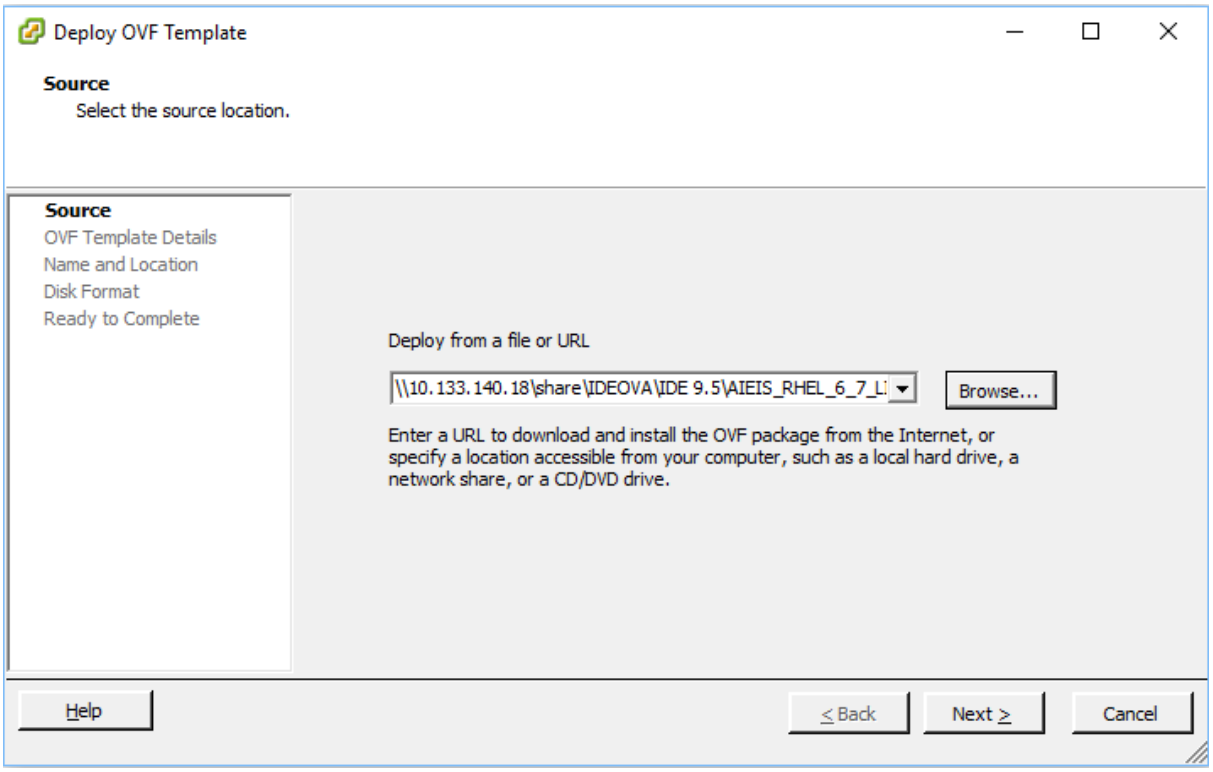
Use the VMware vSphere Client to import the VM into your system. Start the VMware vSphere Client and log in to the ESXi Server on which you want to install the Ignition Server. You need to use the Virtual Appliance Deploy OVF Template option.

Procedure

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



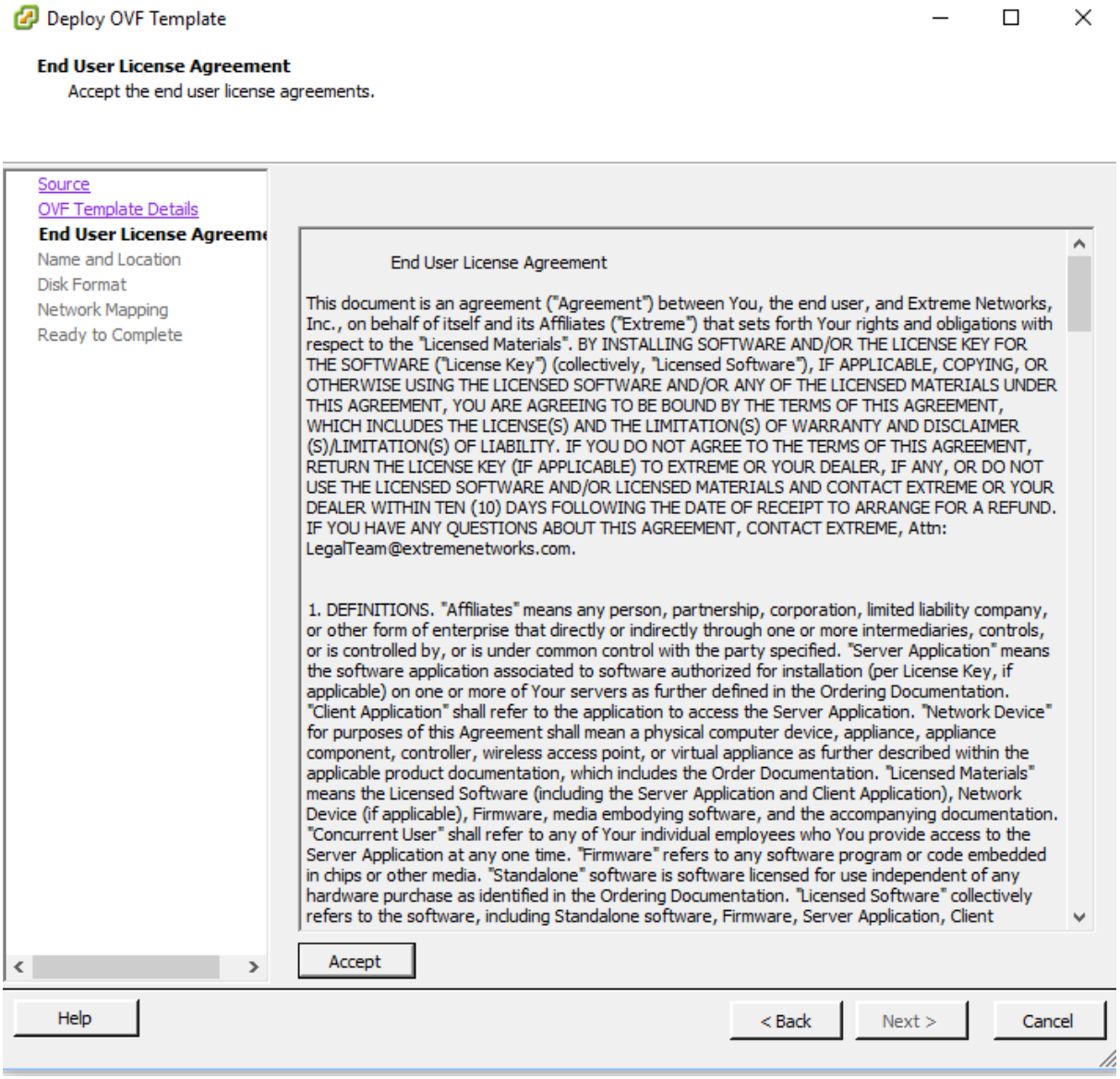
2. The Source window is displayed. Select the location from which you want to import the Ignition Server virtual appliance.



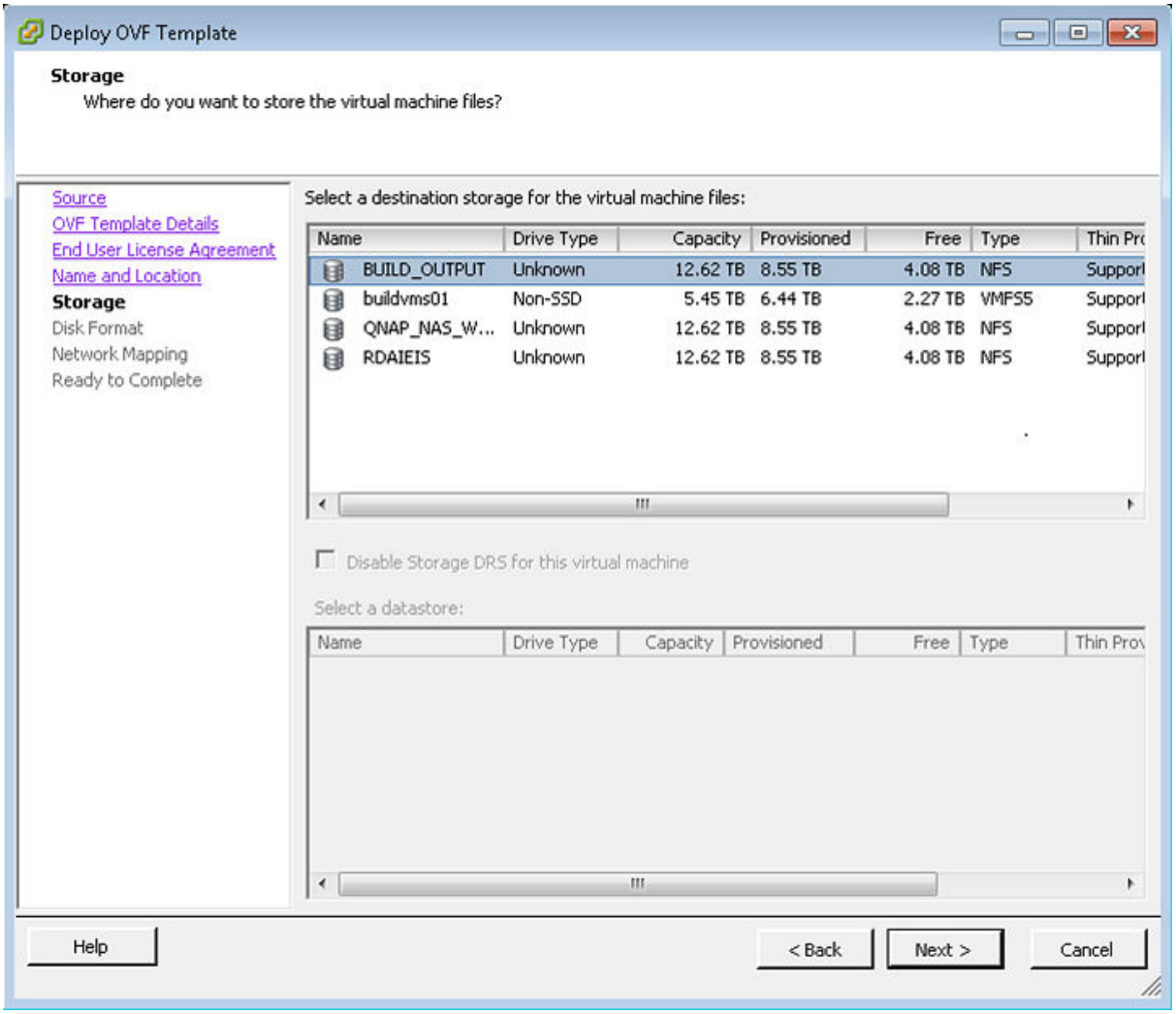
3. Click **Next**.

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

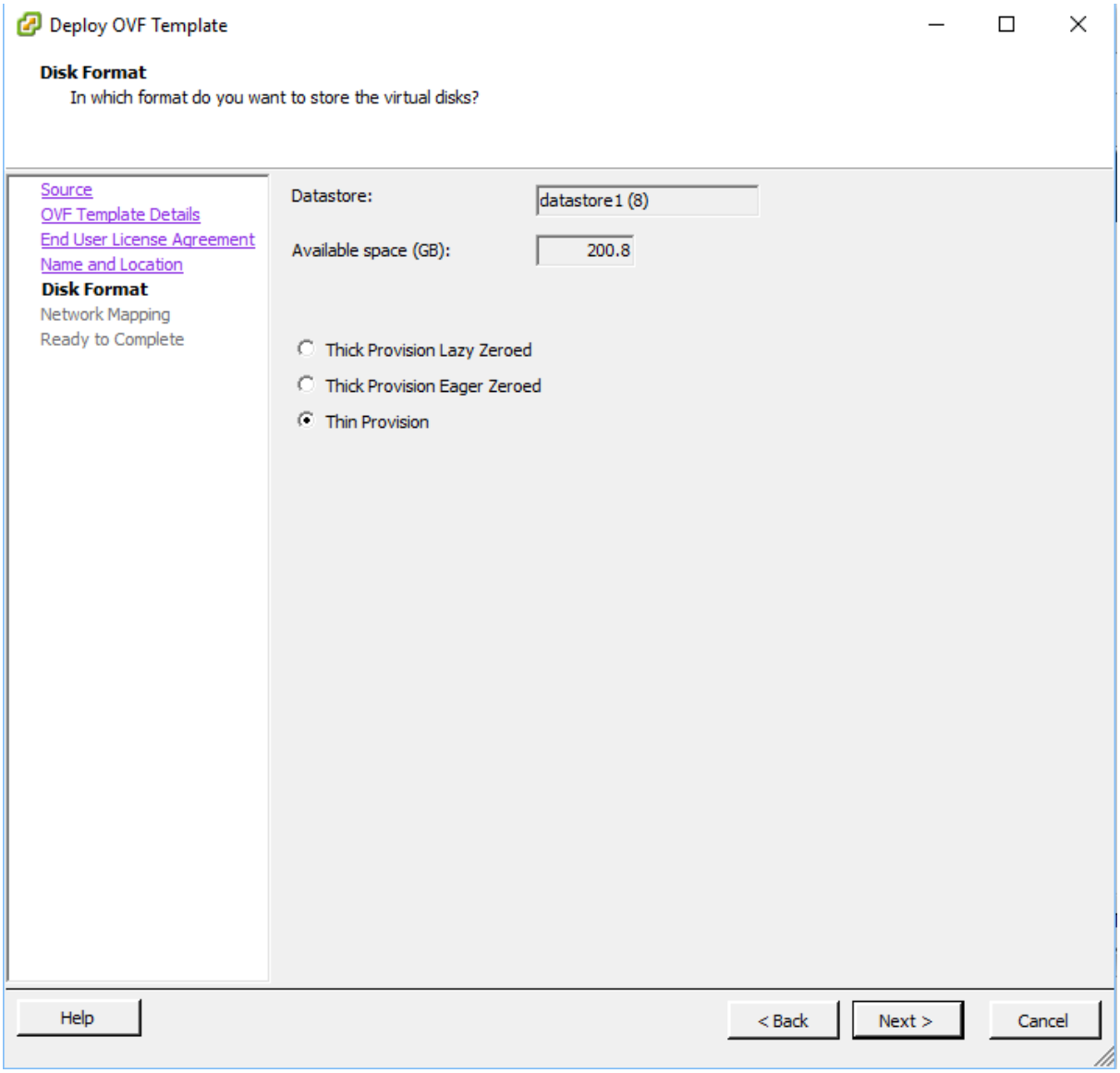
4. The End User License Agreement window is displayed. Click **Accept** to accept the license and click **Next**.



5. The Name and Location window is displayed. You can either accept the default name or choose to rename the virtual machine. Click **Next**.
6. The Datastore window is displayed. Select the location where you want to store the files for the virtual appliance and click **Next**.



7. The Disk Format window is displayed. Select a format in which to store the virtual machine's virtual disks and click **Next**.



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

   The Import now starts. When the import completes you should see a Summary window is displayed.
10. After the import completes, you must verify and adjust some of the VM settings. Open the VM setting window 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 window 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 Ignition Server for the first time. A splash window displays as the boot up starts.

d. Extreme Networks does not support manual or automated VMware Tools installation and configuration on Extreme Networks supplied VMs. For more information, see Preventing Automatic VMware Tools Updates on page 17.

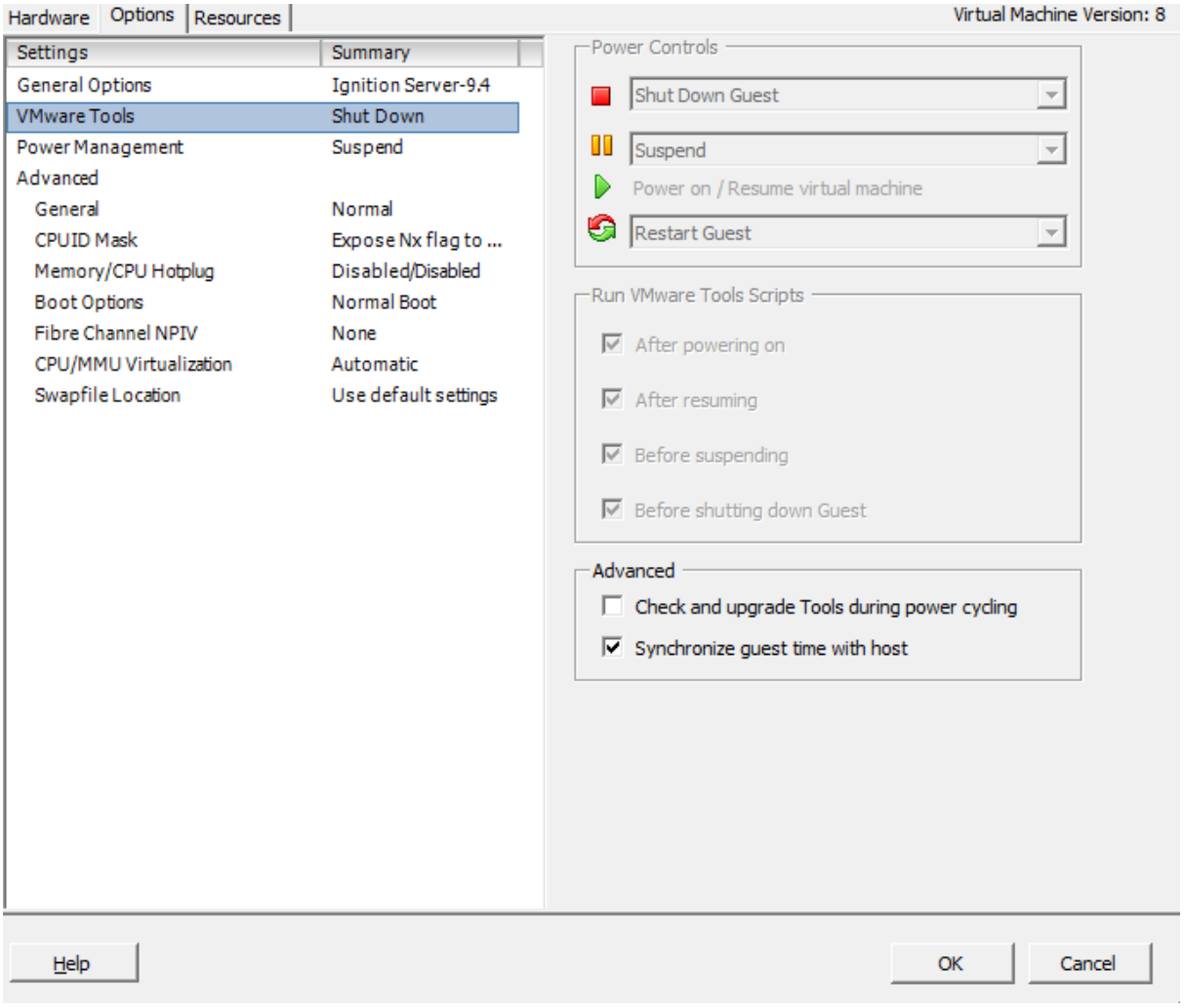
11. When the Ignition Server Console login window is displayed, you are ready to enter the administration IP address. Login using *admin* for the user name and *admin* for the password. You should change the password after you login.

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** checkbox is not selected. This is the supported setting.
4. Click **OK**.



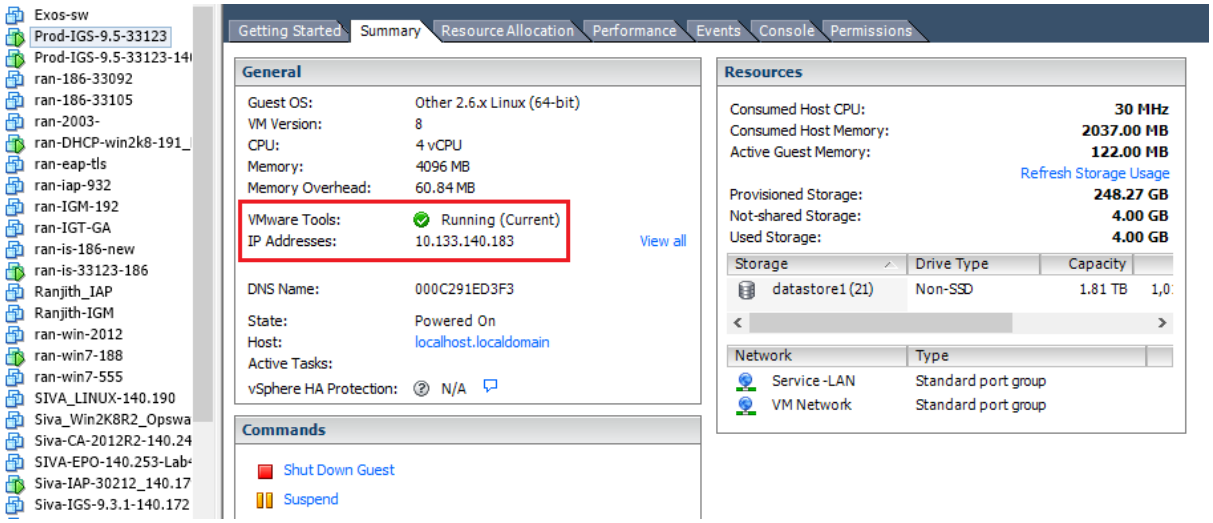
Checking the VMware Tools Status on an ESXi Server

The **Summary** tab of the VM describes the VMware Tools status. Use this procedure to check the VMware Tools status on an ESXi server versions 5.5, 6.0 or 6.5.

Procedure

1. Use the vSphere client to log in to the ESXi Server.
2. Go to the **Summary** tab.

   After a fresh install, the VMware Tools status displays as “VMware Tools: Running (Current)”.



Note:

VMware Tools may show as not installed. This is a known VMware issue where VMware Tools may not be detected correctly on certain hardware. However, this does not interfere with the functioning of the tools. It is a display issue only.

Configuring the Ignition Server Virtualization Appliance

Use this procedure to configure the Ignition Server virtualization appliance.

Procedure

1. Boot the Ignition Server for the first time.
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. It is recommended to change the password.

```
Ignition Server 09.04.00.032826
Host: VMware ESX Server
Node: 0050568B89D1
Linux Server using Kernel 2.6.32-642.11.1.el6.x86_64 for x86_64
Build From: VASONA sustainingcurrent_09_03_00
Updated: Sync With Hyperviser is enabled.
Hypervisor time sync is: Enabled
0050568B89D1 login:
```

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> “

```
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> _
```

Setting the Administrator Password Using CLI

The administrative password must meet the following complexity checks:

- Use minimum of eight characters in the password.
- Password must be a combination of the following character types:
  - Include at least one lowercase letter
  - Include at least one uppercase letter
  - Include at least one number
  - Include at least one special character from `!, @, #, $, %, ^, &, *, (, ), –, +`
- New password cannot match the three recently used passwords.

Note:

It is recommended to change the Ignition Server password from the CLI. This is true for both fresh installation and Software Upgrade using Package (PKG) file.

If the password you enter does not meet the above mentioned password complexity rules, then the system displays the following error messages, in such a case enter a new password that meets all the password complexity rules.

```
Ignition Server> set password
Enter Current Admin Password:
Enter New Admin Password:
Failed to set the admin account's password. Password Complexity has not been
 met.
Use the following guidelines for passwords:
  -Use a minimum of 8 characters.
  -Include at least one capital letter.
  -Include at least one lowercase letter.
  -Include at least one number.
  -Include at least one special char from !, @, #, $, %, ^, &, *, (, ), -, +
Ignition Server> _
```

Installing the Ignition Dashboard Desktop Application

The Ignition Dashboard is a desktop application that enables you to manage the Ignition Server appliance. The 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

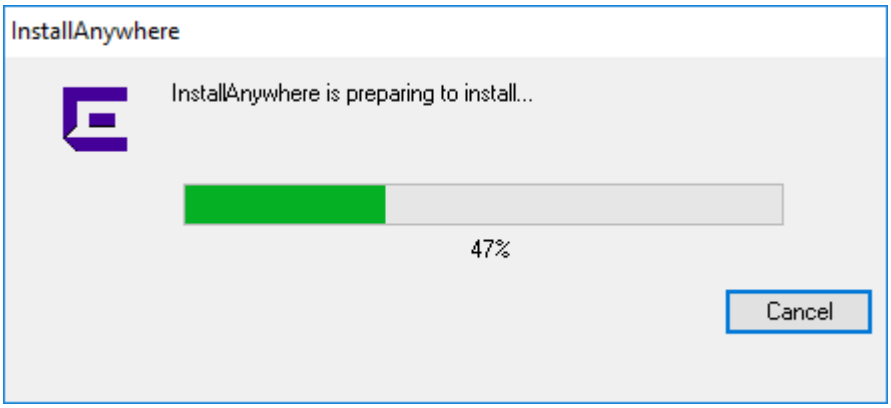
To proceed with the Ignition Dashboard installation, have the following tools and information ready:

- The Identity Engines product software shipped with your Ignition Server appliance.
- A computer running Windows 7 (64 bit), Windows 8 (64 bit), Windows Server 2008 (64 bit) or Windows Server 2012 (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 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.

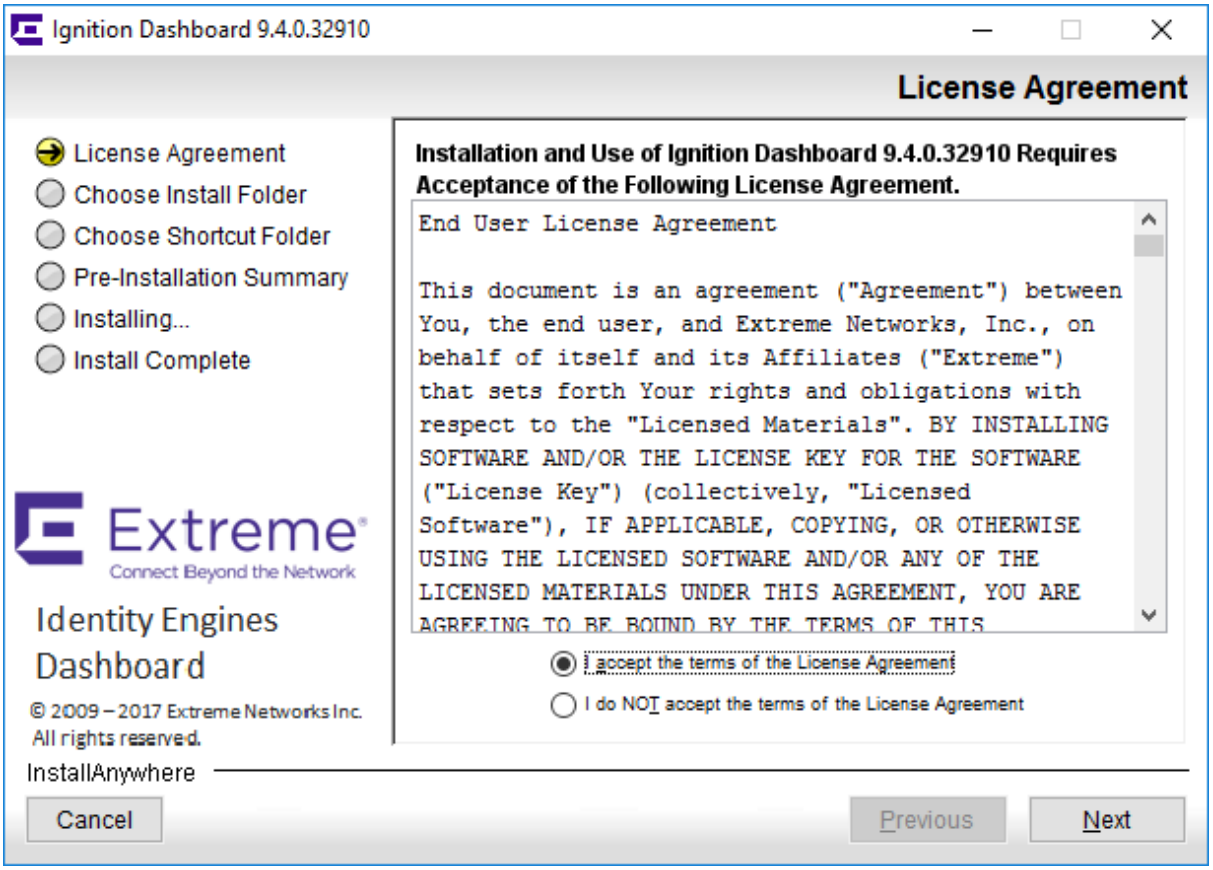
   Note: If the AutoRun feature is disabled on your computer, navigate to your CD drive and double-click the installer file. It has a name like DashboardInstaller-*<Release_Number><Build Number>*.exe.



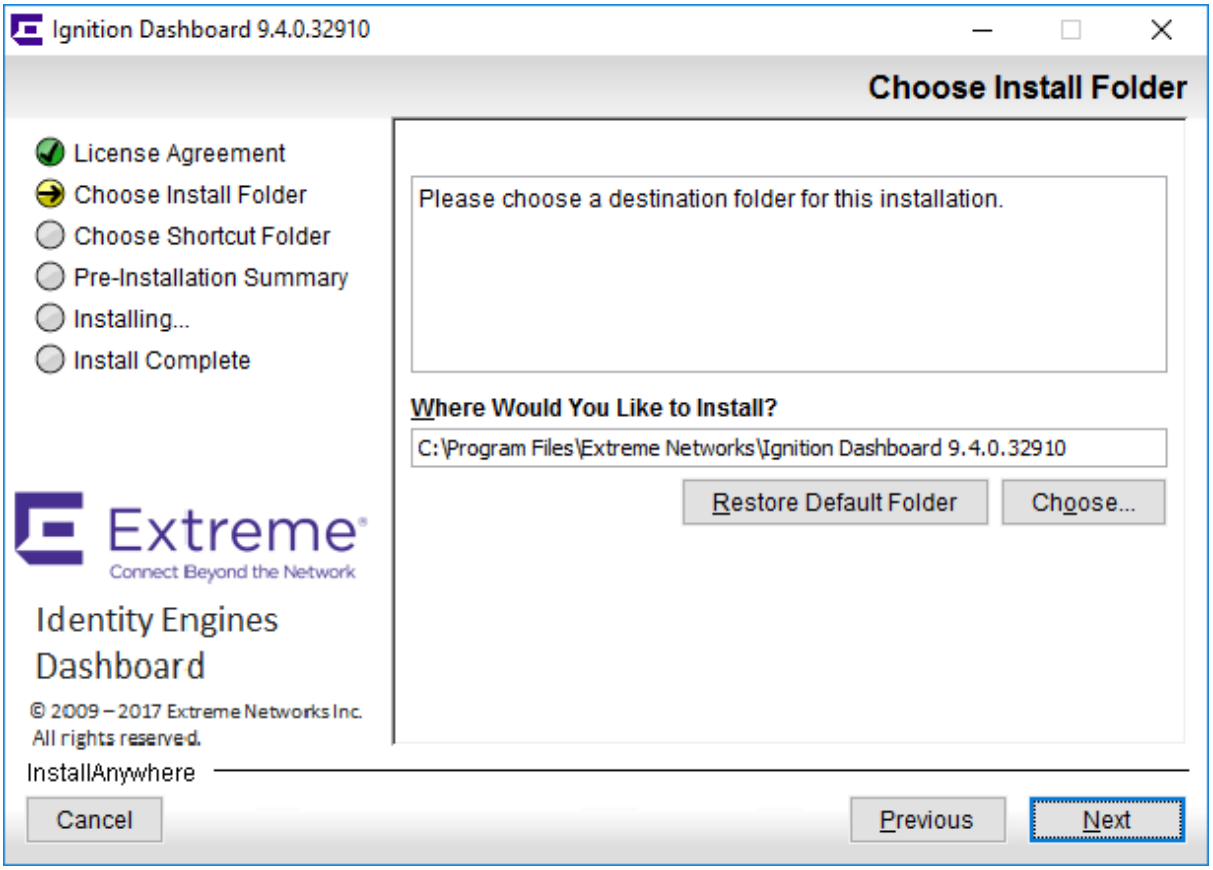
Note:

Older version of Ignition Dashboard is not deleted after installing the new version.

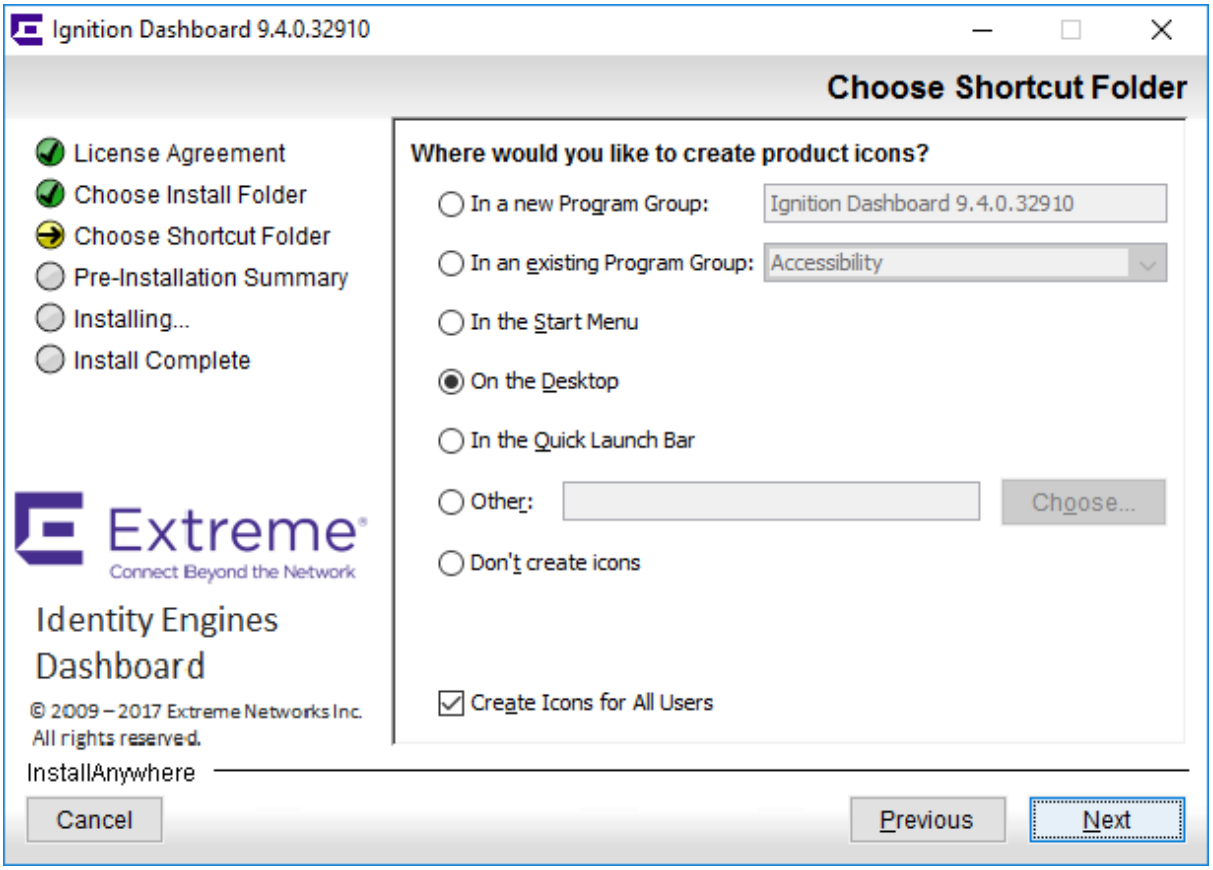
3. In the License Agreement window, scroll down to read the entire license. Select the radio button to accept the license and click **Next**.



4. In the Choose Install Folder window, choose your destination folder and click **Next**.



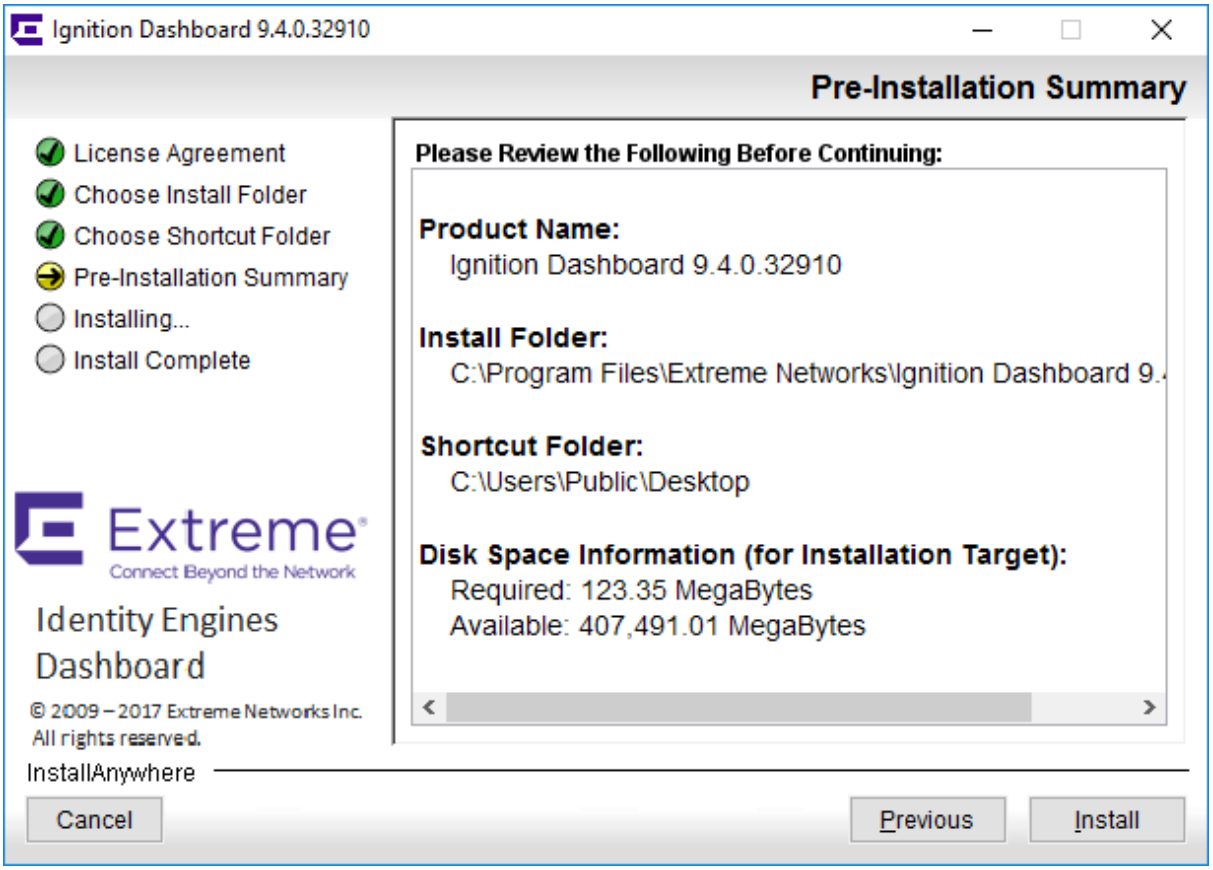
5. In the Choose Shortcut Folder window, indicate where you want the Dashboard shortcut to appear, and click **Next**.



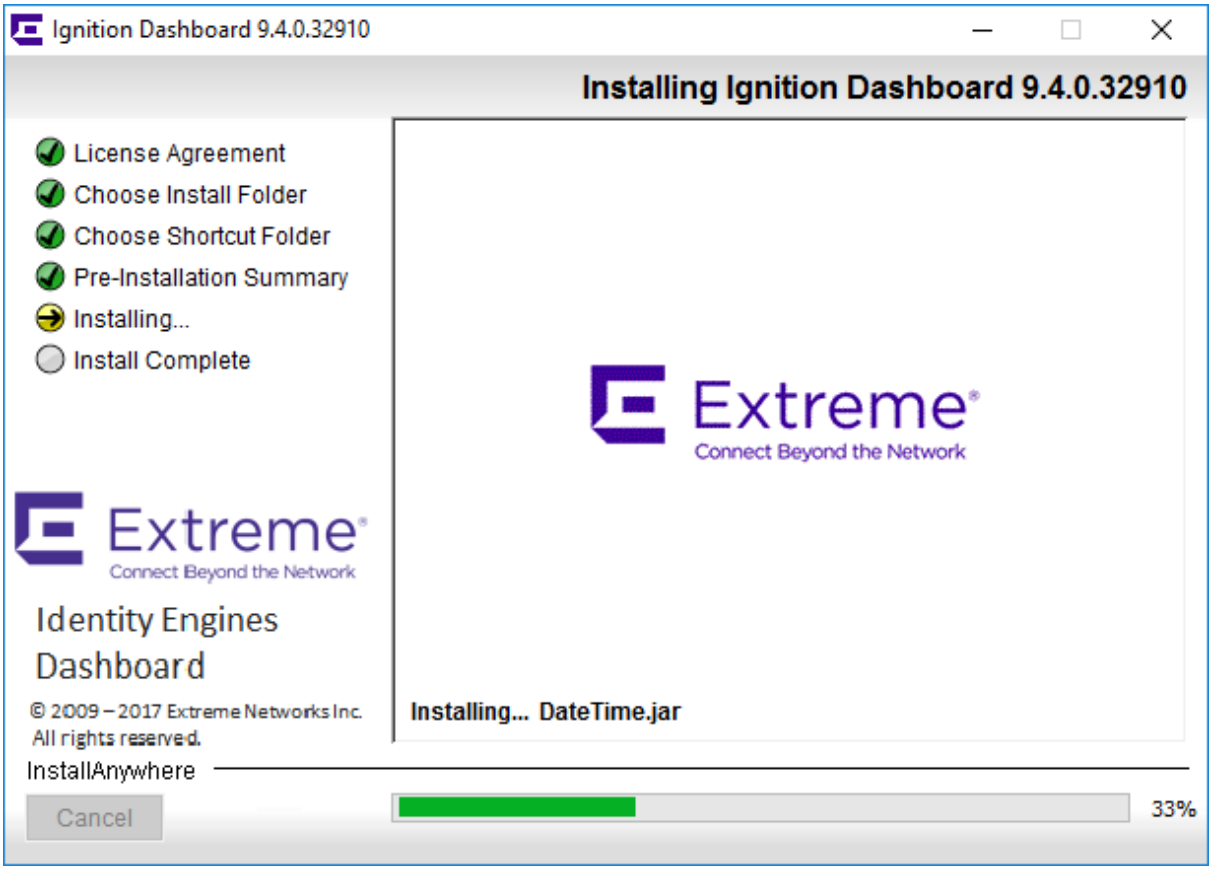
6. In the Pre-Installation Summary window, review your installation settings. If you want to make changes, click **Previous** to edit the details of the locations of the installation. When you finish your configuration, click **Install**.

Important:

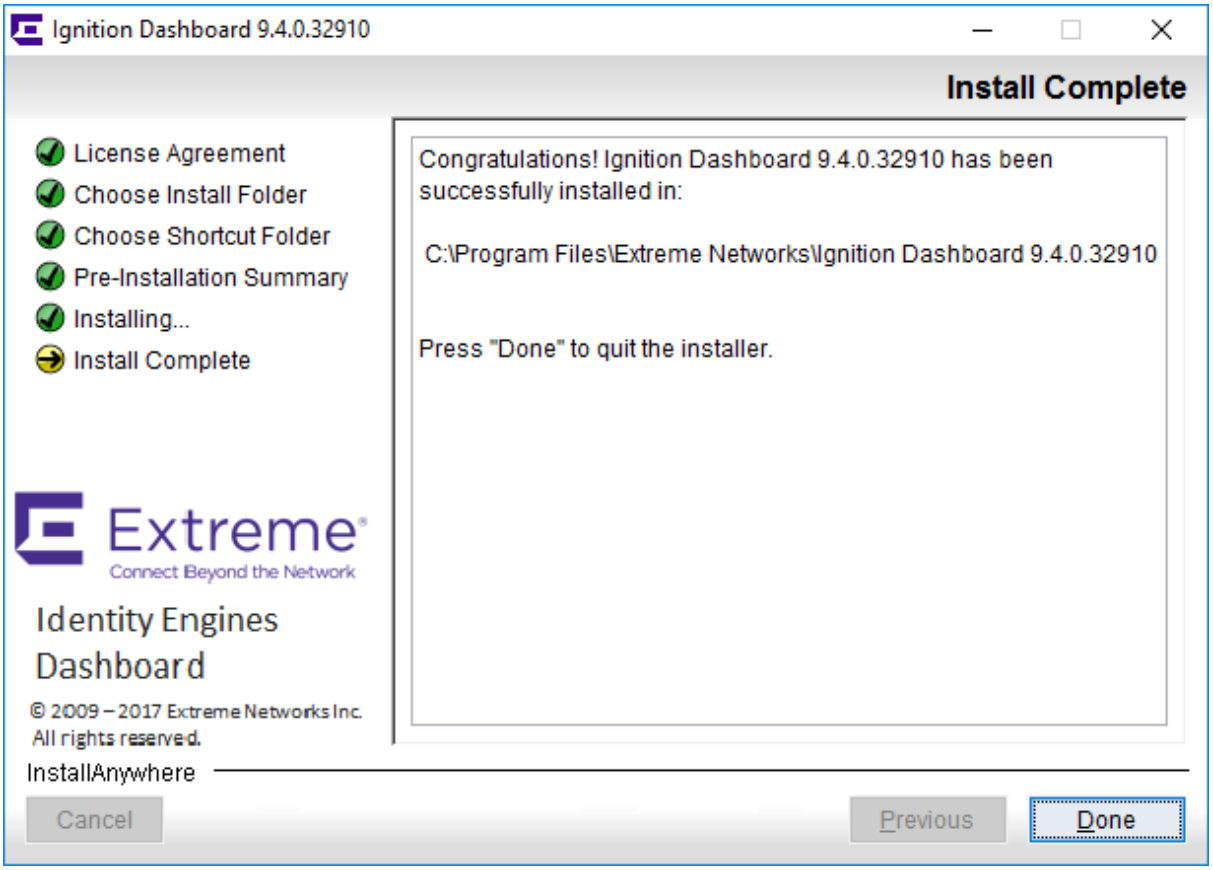
Ignition Dashboard installation no longer installs any JRE on the target machine.Ignition Dashboard now uses the JRE, which comes pre-installed with the Dashboard Installer software and does not attempt to install or check for any JRE nor update any registry entries. In essence, Ignition Dashboard uses the concept of private JRE for its installation, launch and subsequent functioning.



7. The installation starts. The installer displays the progress of the installation.



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



Note:

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.

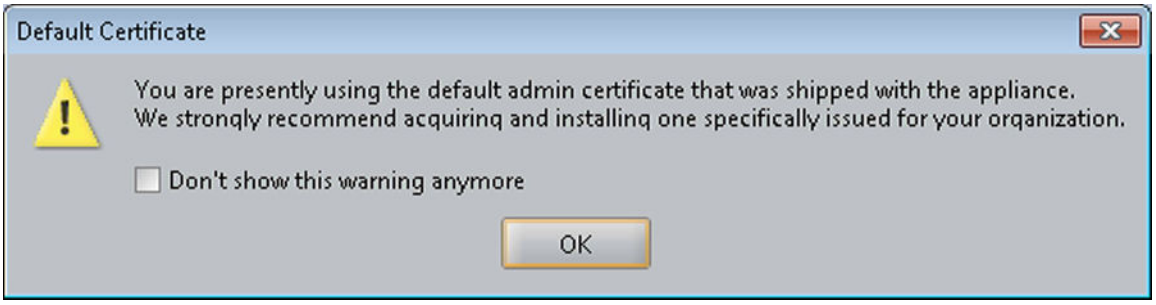
Running the Dashboard

If your Ignition Server appliance is connected only via its Admin Port, skip this section and go to Further Configuration on page 35. Use this procedure, If your installation uses Service Port A.

Procedure

1. On your administration computer, start Ignition Dashboard by doubleclicking its icon on the desktop.

2. In the login window, 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 window is displayed with **Base License Required**. You can install the license later as described in Installing the License on page 31. Be sure to first read Obtaining the Ignition Server Serial Number on page 28. For now, dismiss the popup by clicking **OK**.
5. A warning window is displayed reminding you to replace the default certificate shipped with the Ignition Server appliance. Ignore the warning. (For more information on replacing the certificate, see *Identity Engines Ignition Server Configuration document*.)



After you dismiss the warning window, the Ignition Dashboard is displayed.

Next steps

If you already have your Ignition Server license, go to Installing the License on page 31.

Obtaining the Ignition Server Serial Number

The Identity Engines Ignition Server software ships without any licenses. The following software licenses can be installed on Ignition Server:

- Base License (LITE, SMALL, LARGE)
- Guest and IoT Manager License
- TACACS+ License
- NAP Posture License (End of Sale is announced for Posture licenses. You cannot order these licenses anymore but can continue to use existing licenses).
- Access Portal License (End of Sale is announced for Access Portal licenses. You cannot order these licenses anymore but can continue to use existing licenses).

At a minimum, you must obtain the Base License to be able to configure and run the server.

Note:

Once you have purchased Identity Engines, depending on how you place your order you receive either a set of paper LACs (License Authorization Codes) or electronic delivery of your LAC by email and you then download the software from the support site.

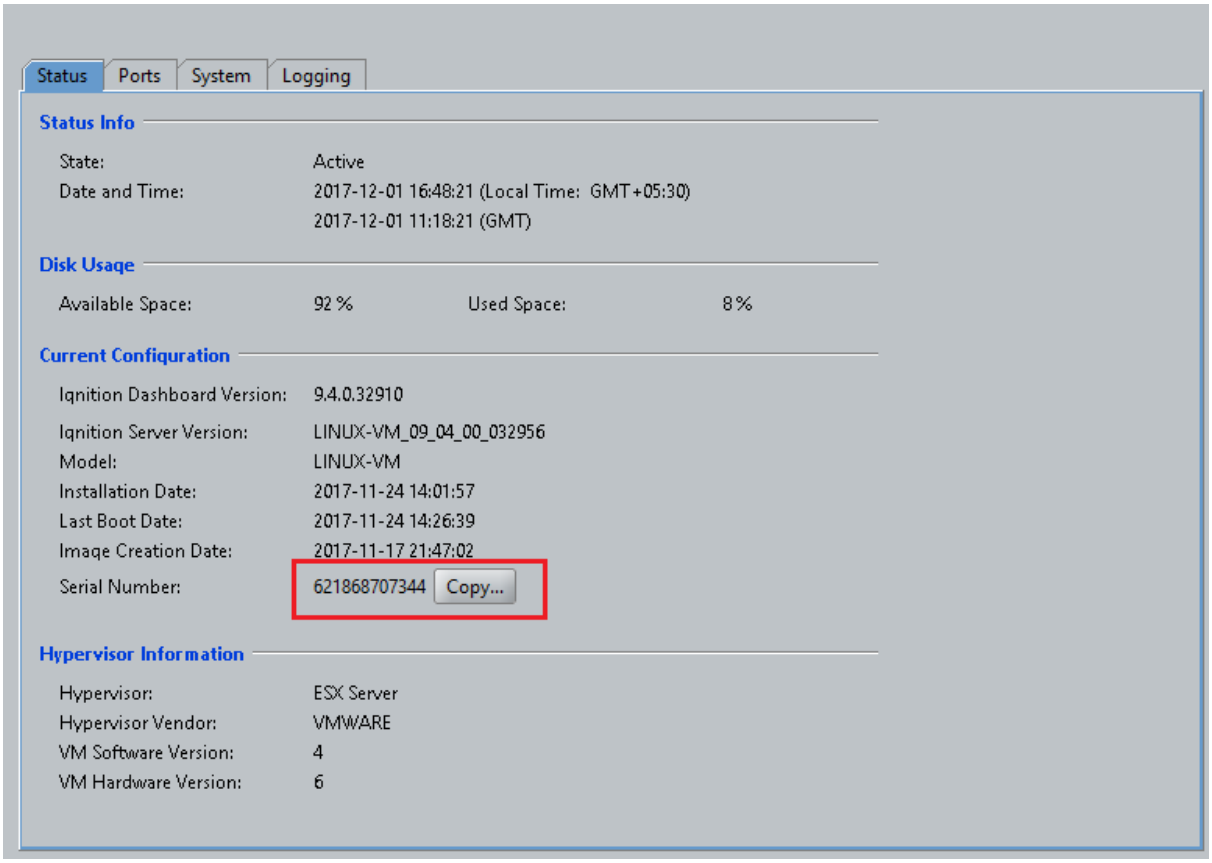
Extreme Networks provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-998-2408 in the United States. For additional support telephone numbers, see the Extreme Networks Web site: http://www.extremenetworks.com/support/contact/.

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. Beginning with Release 9.0, the Ignition Server Serial Number is always a string of 12 digits.

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

Procedure

1. In the VMWare vSphere Client, launch the Ignition Server CLI and enter the command `show version`.
2. **(Optional)** From the Dashboard Configuration tree, click the name or IP address of your node, click the **Status** tab.
3. Click **Copy** to save the Serial Number to the clipboard.



About KeyCode Retrieval System (KRS) Licenses

KRS Licenses are:

- Bound to the Serial Number (or two Serial Numbers in case of HA) of the Ignition Server.
- Individual license files
- Typically available for each feature in a separate licenses file. However, separate KRS License files may be combined into one license file.
- Installed separately. If only KRS licenses is installed, you must have at least a KRS Base license file.

Note:

You can delete or install individual KRS licenses and can export all of the KRS licenses. If you open a KRS license file in a text editor, you cannot figure out what the license is for until you install the license on the Ignition Server.

Obtaining Perpetual Production Licenses

If you received paper LACs with your purchase, follow the instructions on the paper LACs regarding how to obtain your KeyCode Retrieval System (KRS) and if you received electronic LAC via an email from Extreme Networks, follow the instruction on the email.

Send an email to datalicensing@extremenetworks.com with any questions to request your licenses or contact Extreme Support.

Installing the License

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

Procedure

1. In the Dashboard Configuration tree, click the name of your site and click the **Licenses** tab.

   The **Licenses** tab is displayed.

   Note:

   To install a temporary 30-day license, click the link given on the **Licenses** tab in the **License Details** section.

2. Click **Install**.

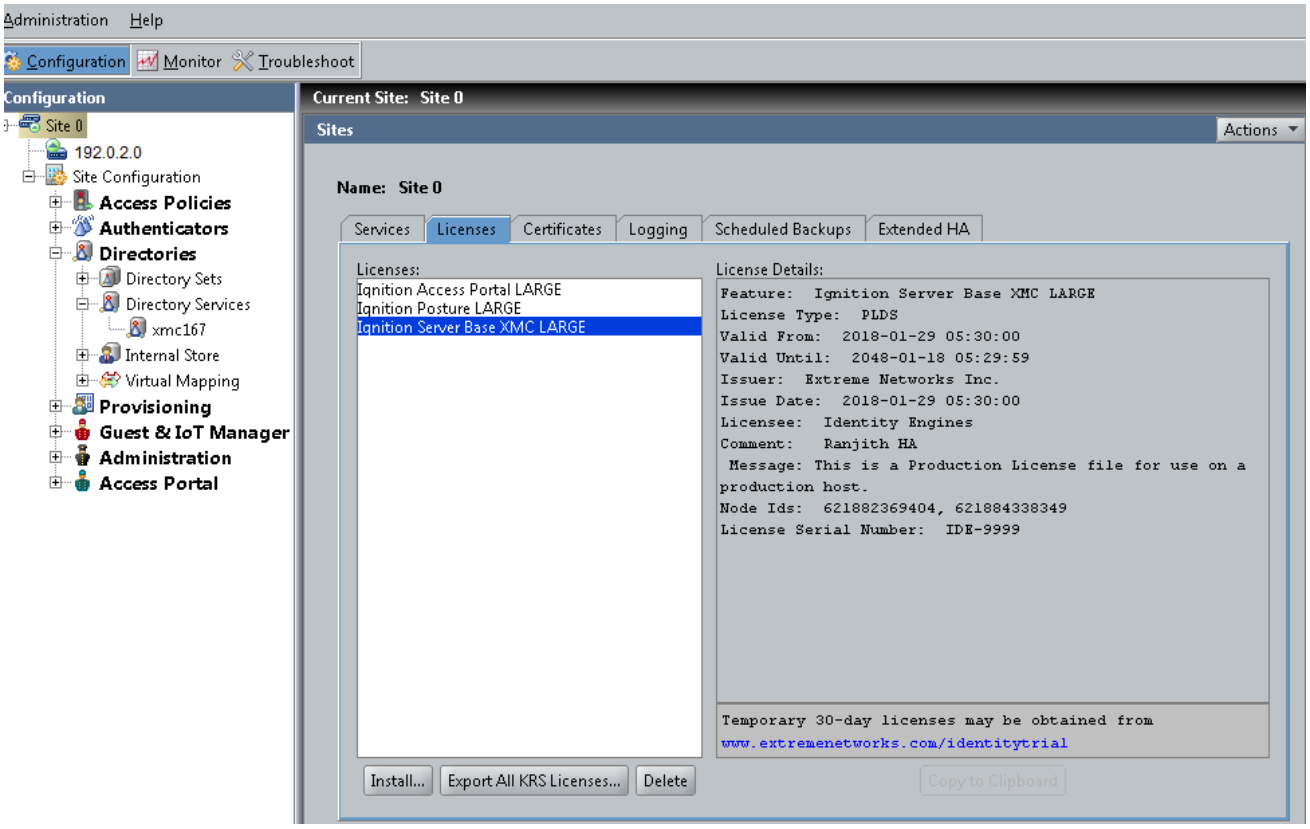
   The License Installation window is displayed.

3. Browse to the license file location, select, and click **OK**.

   You can paste the license text into the text area and click **OK**.

Example

The following example shows **Licenses** tab with installed licenses details:

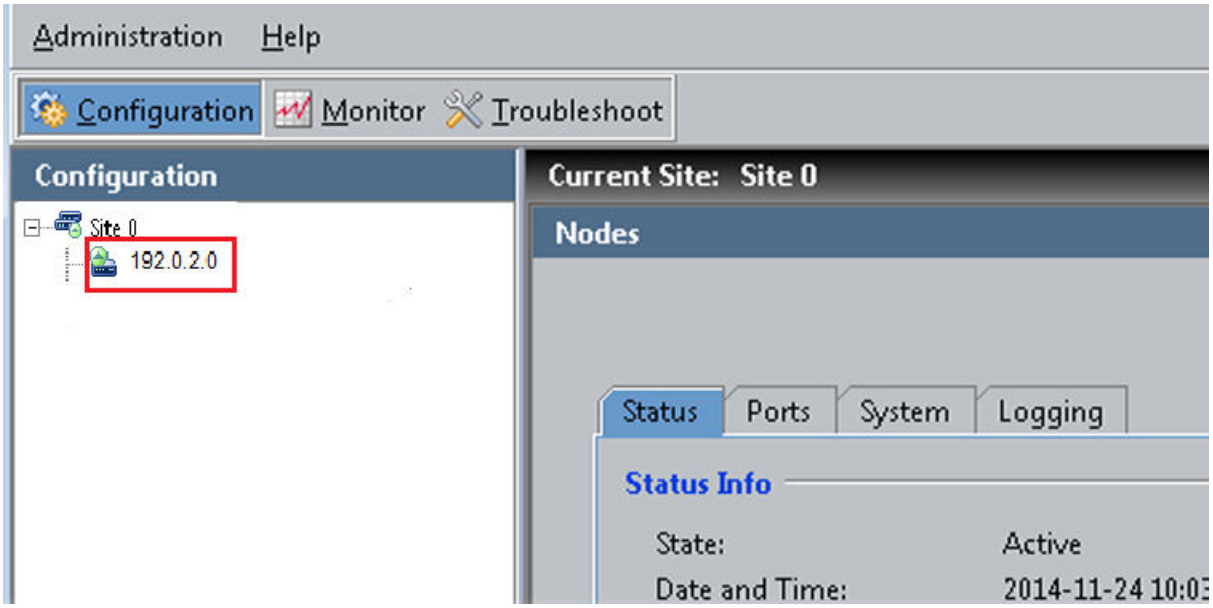


Setting up the Service Port (Optional)

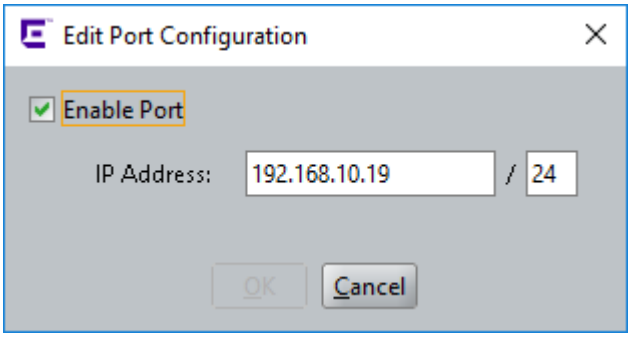
Use this procedure to configure the Service Port.

Procedure

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



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



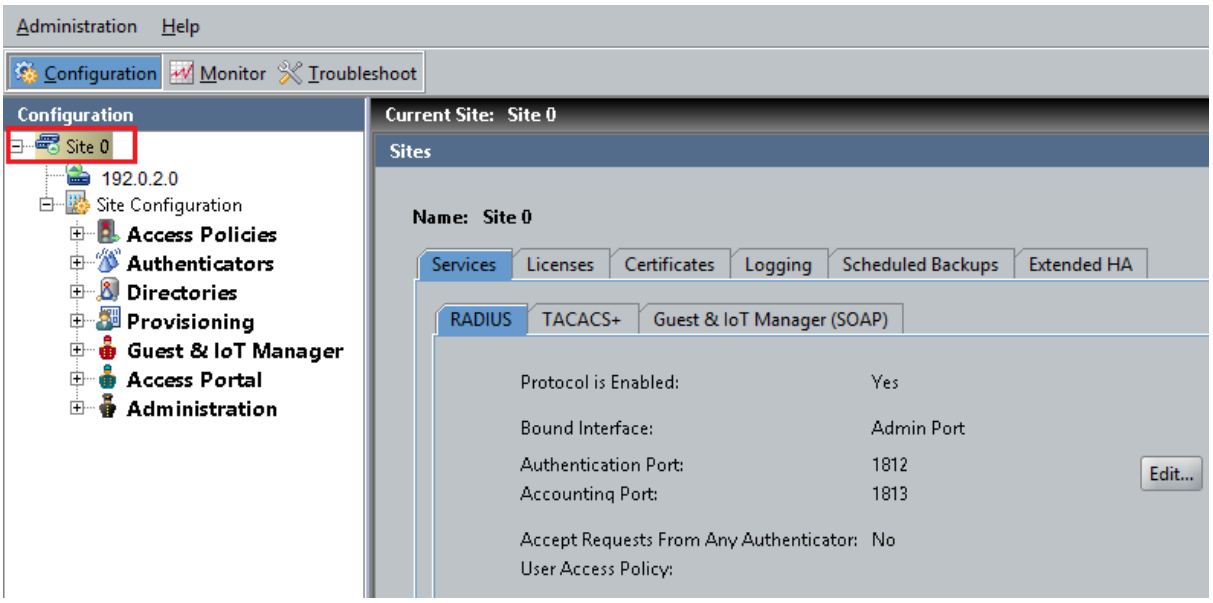
- Select the **Enable Port** checkbox.
- Enter the port address in the **IP Address** field, and enter the subnet mask in the field to the right. You must enter the subnet using network prefix notation (an integer between 0 and 32 representing the number of bits in the address is used in the comparison).

Setting the Admin Password and User, Site, and Node Names

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

Procedure

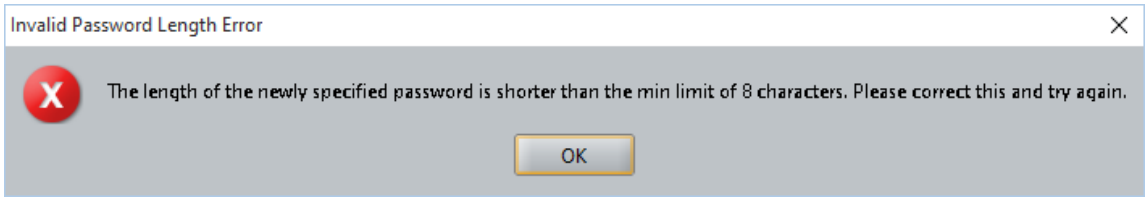
1. In Dashboard's Configuration tree, click the name of your site.



2. From the **Actions** menu (at the upper right), select
   - **Change User Name** to change the administrator login name
   - **Change Password** to change the administrator password

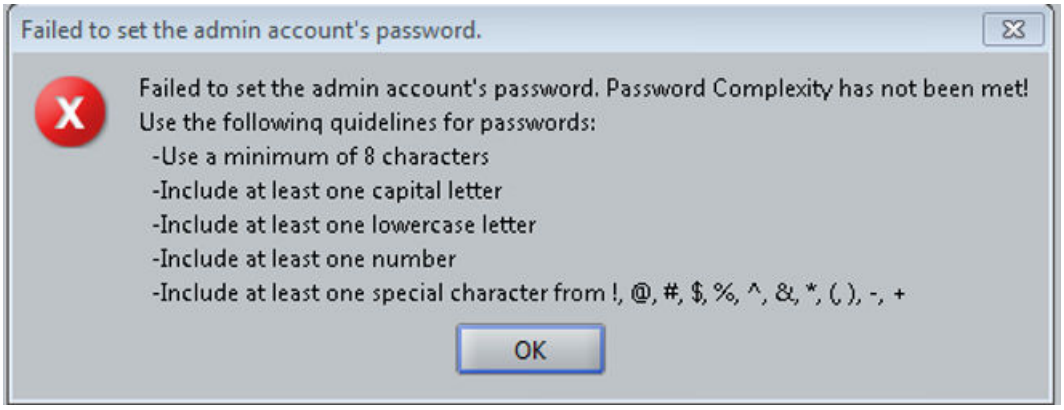
   The new password must meet the following complexity checks:
   - Use minimum of eight characters in the password.

     Following error message is displayed if the above rule is not followed:



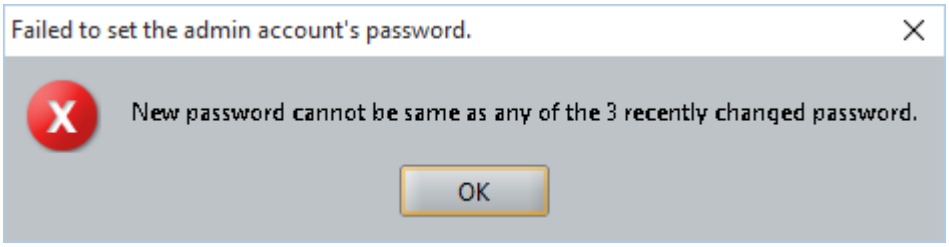
   - Password must be a combination of the following character types:
     - Include at least one lowercase letter
     - Include at least one uppercase letter
     - Include at least one number
     - Include at least one special character from `!, @, #, $, %, ^, &, *, (, ), -, +`.

     Following error message is displayed if the password does not consist of the above characters:



- New password cannot match the three recently used passwords.

  The following error message is displayed if the new password matches the previously used password:



- **Rename Site** to rename the site. A site is typically a pair of Ignition Servers, but it may consist of just one server.

3. To rename your node (your Ignition Server appliance), in Dashboard's main navigation tree, right-click on the IP address or name of your node and select **Rename Node**.

Next steps

Your basic set-up is complete. For more information on your next steps, see Further Configuration on page 35.

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 36. For more information on Ignition Server features, see *Identity Engines Ignition Server Configuration document*.

Note:

Analytics server related configuration in Ignition Dashboard is documented in *Identity Engines Ignition Network Analytics document*.

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 11.

The following features describes how to configure Ignition Server for providing Network Access Control:

Make sure you have a copy of the following documents:

- *Identity Engines Ignition Server Getting Started document*
- *Identity Engines Ignition Server Configuration document*

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 11
   - 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 40.) Use UDP port 1812 as the RADIUS server port.
3. **802.1X settings:** If you 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 connects 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 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 use IPSec for VPN access, make sure that client machines (those 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.

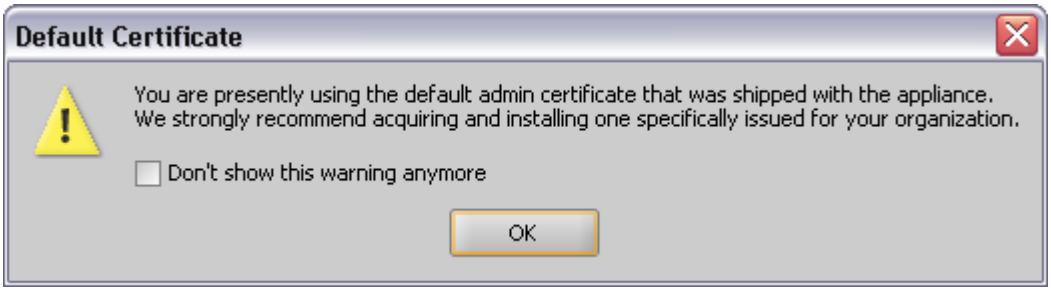
Configuring the Ignition Server Appliance

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

Procedure

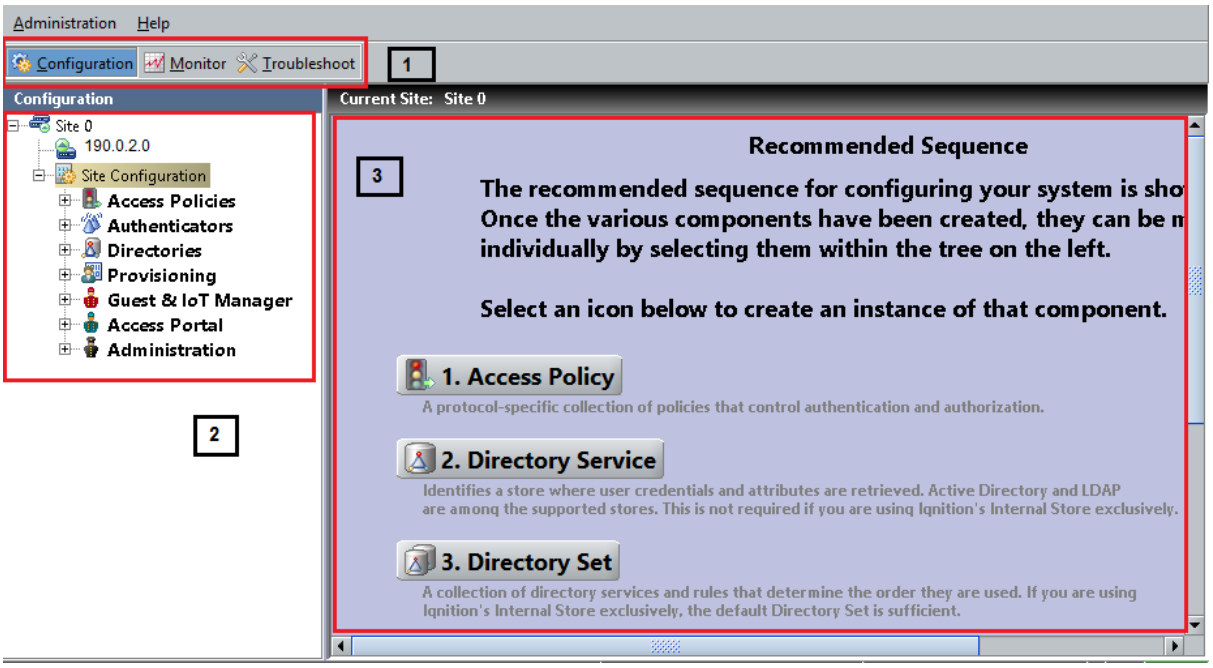
1. Start Ignition Dashboard: Double-click Ignition Dashboard icon on your **Start** > **Programs** > **Ignition Dashboard** > **Ignition Dashboard**. The Login window is displayed.

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**.



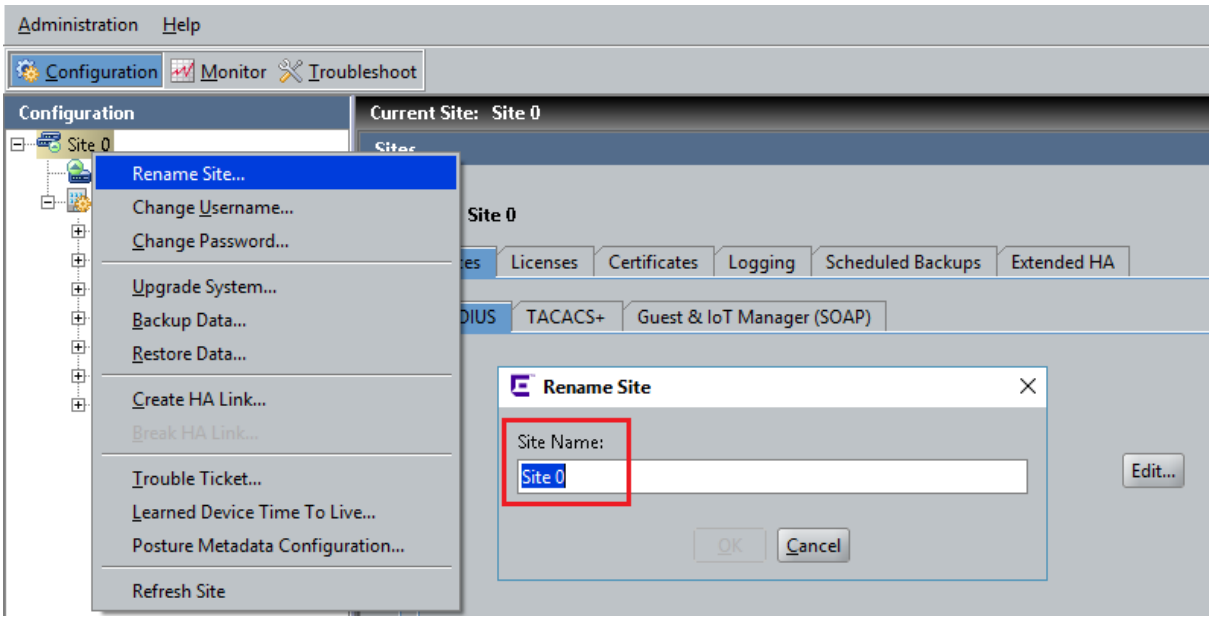
Initially, the Default Certificate window displays alerting you that you are using the default Ignition Dashboard-to-Ignition Server certificate (“admin certificate”) that was shipped with Ignition Dashboard. Click **OK** to dismiss the window. (**Configuring the Ignition Server appliance** recommends that you later consult the “Certificates” chapter of the *Identity Engines Ignition Server Configuration document*Guide and replace the certificate as explained there.)

Dashboard displays its main window, which consists of three tabs as below:



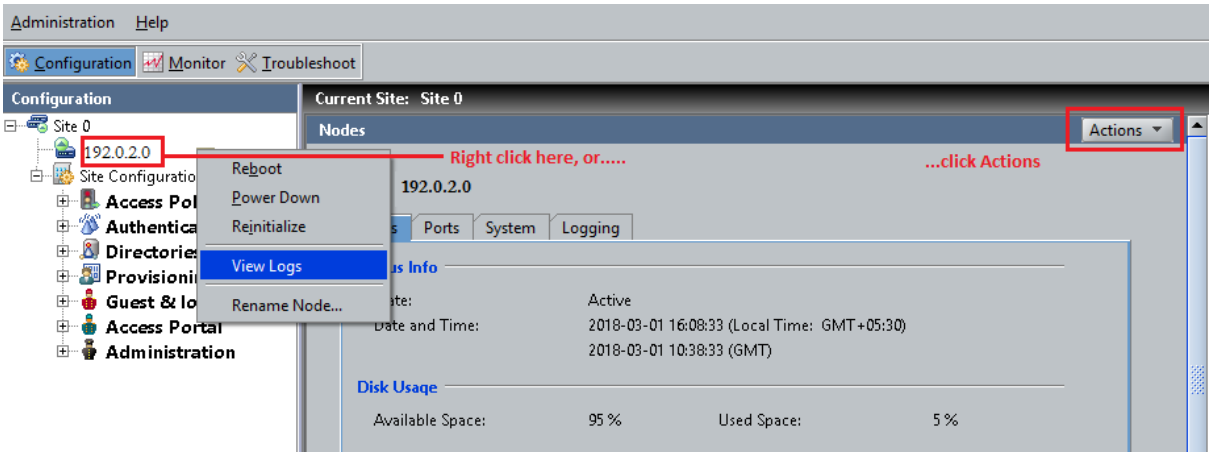
Serial No.	Description
1	Configuration, Monitor, and Troubleshooting tabs
2	Navigation Tree
3	Reading and editing panel

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 use the name Sunnyvale Campus. Click **OK** to accept the new name.

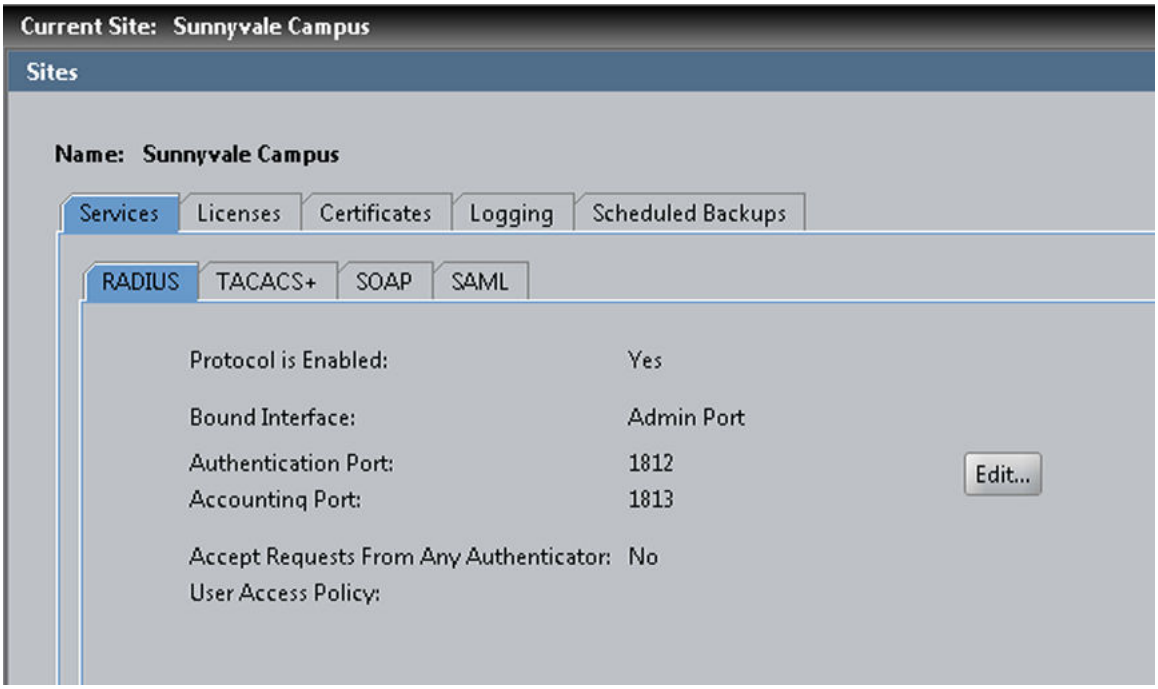


4. In the navigation tree, click on the machine name or IP address of the Ignition Server appliance you wish to configure. The application displays the Nodes panel, which allows you to manage network settings on the appliance, and check its current status.

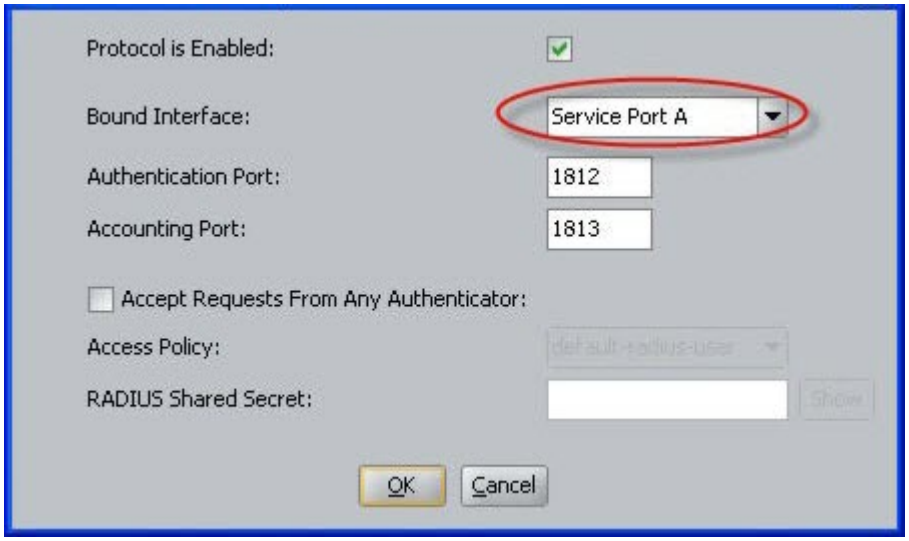
   Hint: The **Actions** menu allows you to manage the appliance hardware (actions such as rebooting and shutting down). To use the Actions menu, right-click the IP address of your Ignition Server in the navigation tree, or, with the IP address selected, click the Actions menu at the upper right.



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**. Select the **Enable** checkbox 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 Servers 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 you authentication network is separate from your management network: Make sure you have plugged in the cable connecting the Ignition Servers* **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.

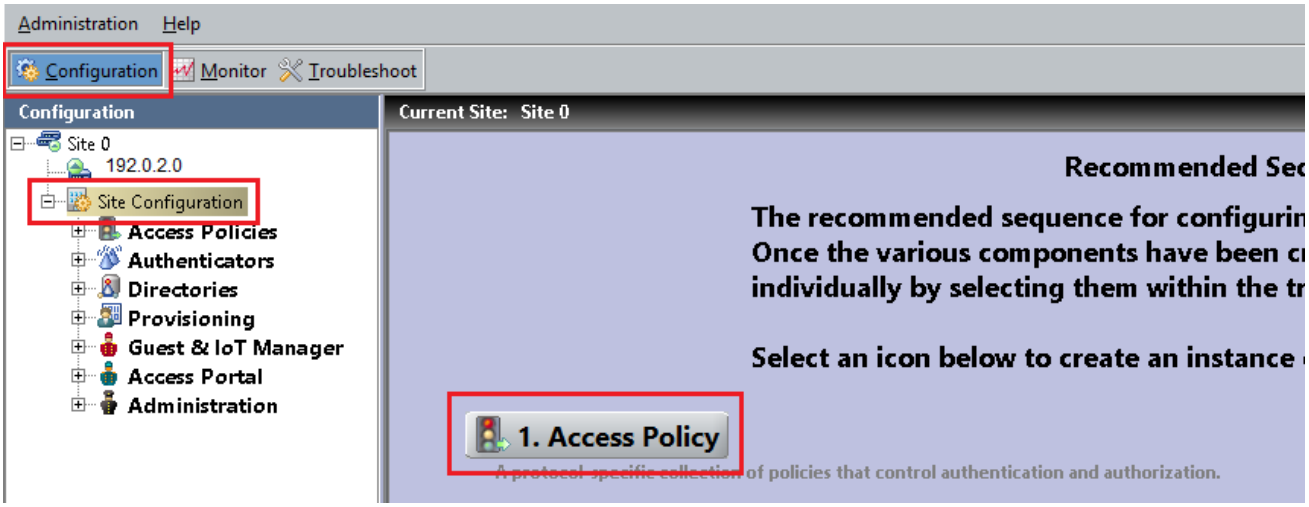
Next steps

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

Creating a RADIUS Access Policy

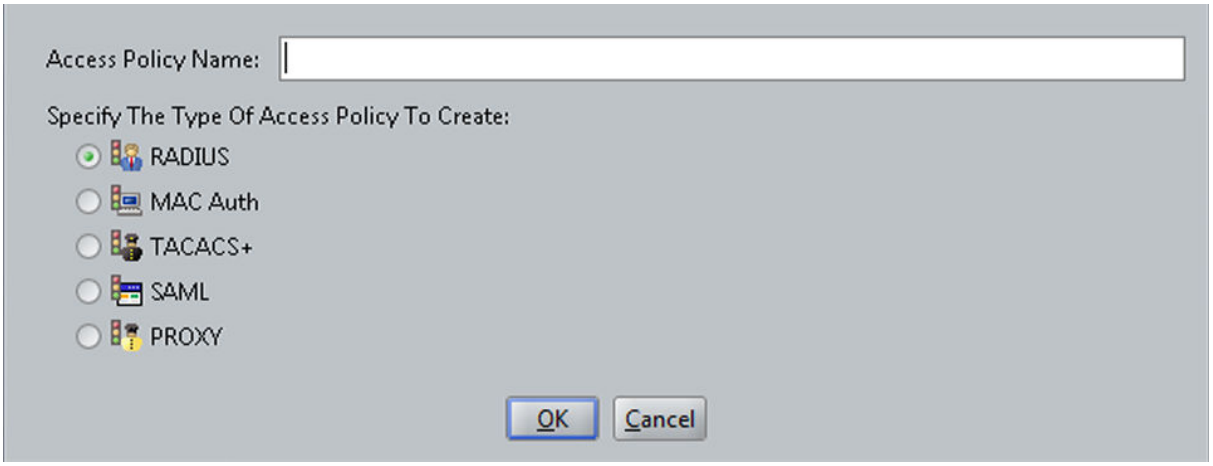
Your RADIUS access policy contains the rules that determine how a user must authenticate and, based on the user's identity, what network the user is allowed to use.

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.



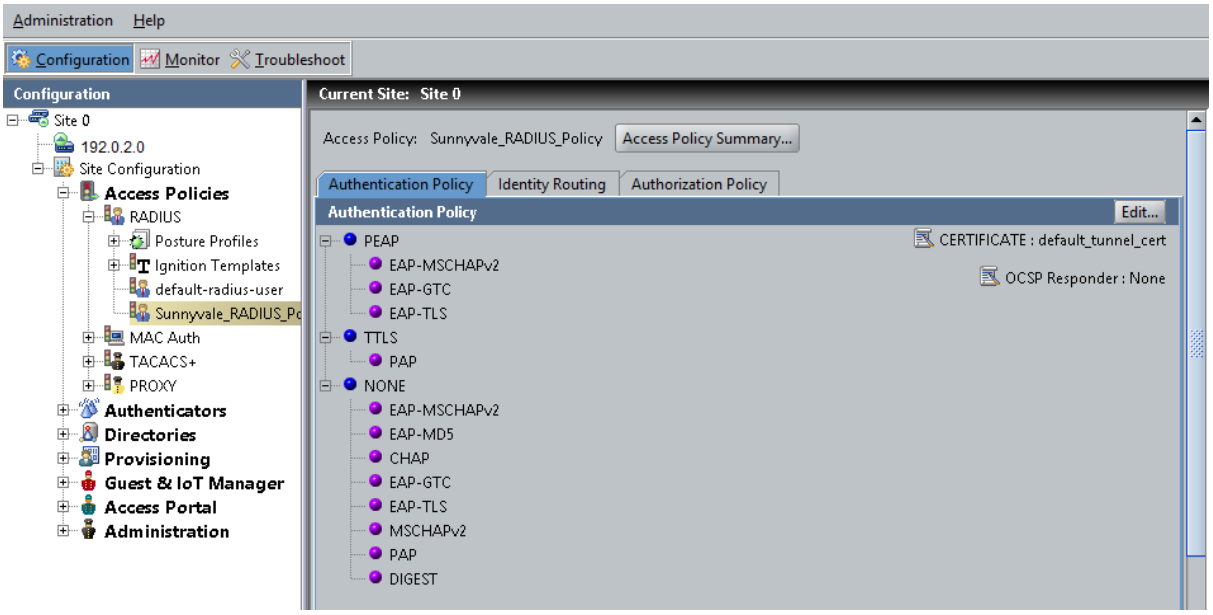
Procedure

1. If Dashboard is not connected to your Ignition Server, select **Administration** > **Login**, and provide the necessary credentials.
2. In the Dashboard's Configuration tree, click **Site Configuration**, and click **Access Policy** in the main window.
3. In the New Access Policy window, type a name for your policy and select the **RADIUS** checkbox. The name typically offers a clue as to which authenticators uses this policy. For example, the name may indicate the location of the authenticators.



4. Click **OK**.

   Your access policy has been saved. For now, leave the policy empty. (Later, you can add rules to it in the Dashboard Configuration tree by expanding **Site Configuration** > **Access Policies** > **RADIUS** , selecting your policy and using the tabs and **Edit** buttons in the main panel to edit the policy.)



Add rules to your access policy later. For more information, see Setting your Authentication Policy on page 85.

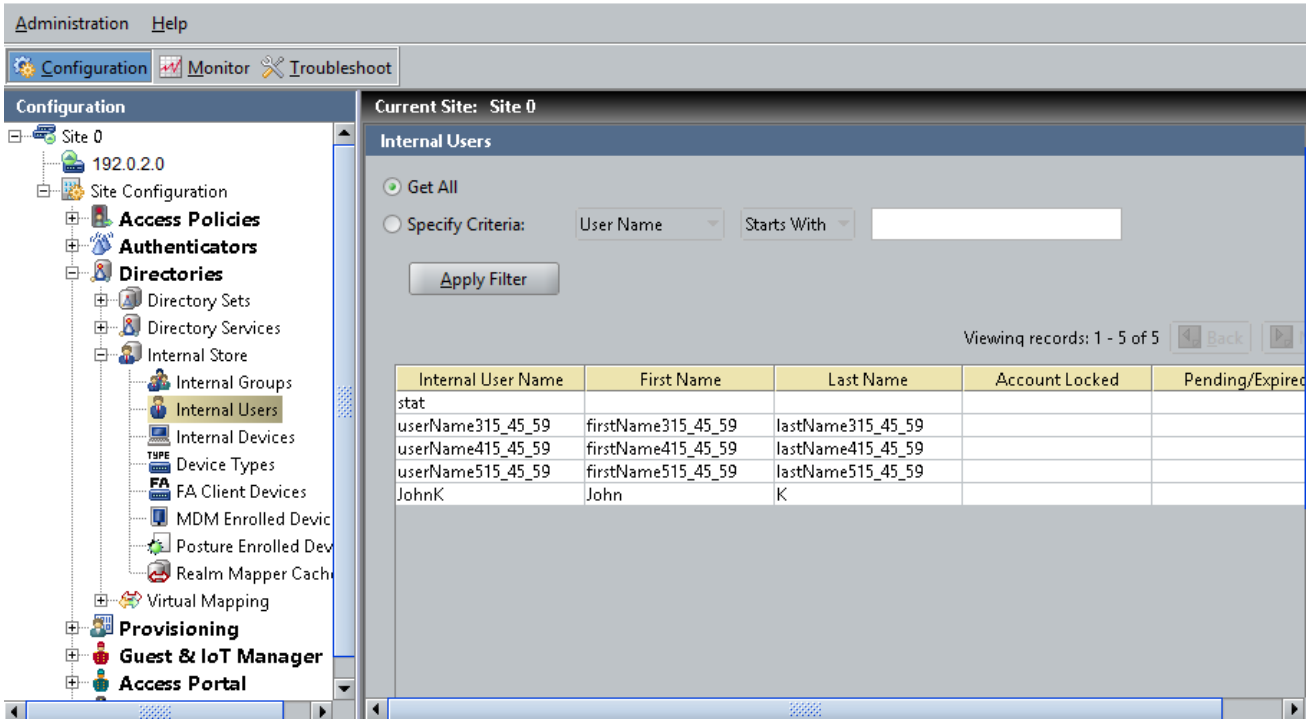
Next steps

Create a user account. For more information, see Creating a User in the Internal User Store on page 43.

Creating 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 Setting up your Connection to a User Store on page 45.

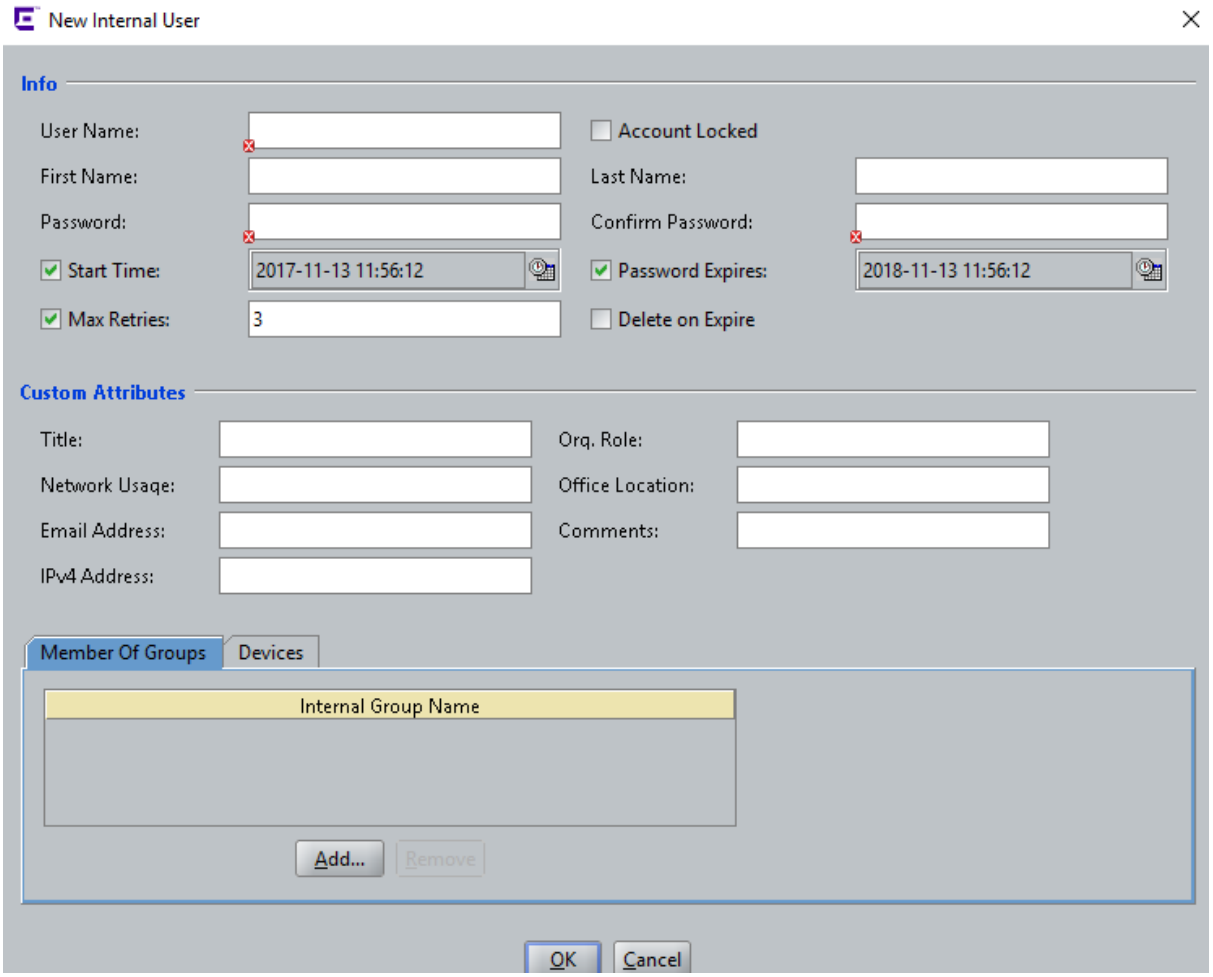
Ignition Server typically authenticates users against your corporate user store (for example an Active Directory or LDAP store), but the Ignition Server appliance also contains a local store, called the internal user store. You can use the embedded store to complement your corporate AD or LDAP store. 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 describes to create a user account in the internal user store. Later, build the access policy to determine this user's access rights.

Procedure

1. In the Dashboard's Configuration tree, expand **Site Configuration** > **Directories** > **Internal Store** and click **Internal Users**. At the bottom of the window, click **New**.
2. In the **User Name** field, 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 Setting up your Connection to a User Store on page 45.

Setting up your Connection to a User Store

The 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 describes how to create a directory service. For each store you wish to use, you can define one directory service. After you define your directory services, 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 Creating a Directory Set on page 76.

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

- Preparing to Connect to Active Directory on page 48
- Connecting to LDAP on page 61

Connecting to Active Directory

The following section describes 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.

Gather Active Directory 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 authenticates users.

Setting name	Setting value
AD Domain Name	The Active Directory domain that holds your user accounts. Domain names typically carry a domain suffix like ".COM" as in, for example, "COMPANY.COM".
Service Account Name	The name of the AD administrator account that the Ignition Server uses 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. For more information, 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

Table continues…

Setting name	Setting value
	is usually the user id of the user without the domain prefix. For example, the sAMAccountName for the user COMPANY.COM/Administrator usually be Administrator. For more information, see Creating the Service Account in AD on page 49 and Setting the AD Permissions of the Service Account on page 52.
Service Account Password	The password for the AD service account. *Do not record the password here.*
Security Protocol	Specifies whether Ignition Server should SSL-encrypt traffic to the directory service. 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). *Use the LDAP ports (389 and 636) only!*
Name	The Name you use in Ignition Server to identify this AD data store. This can be any name.
NetBIOS Domain	The NetBIOS Domain name (pre-Windows 2000 domain name) of your AD data store. This setting is typically written in all uppercase letters, as in, “COMPANY”. This setting applies only to Active Directory stores. For information on using Microsoft tools to find this name, see Looking up AD Settings to Find Domain and NetBIOS Names on page 69.
NETBIOS Server Name	Optional. Allows Ignition Server to find the NETBIOS server where Ignition Server performs 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. It is recommended 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 helps you determine the NETBIOS server name by retrieving a list of domain controllers in the domain.
Directory Root DN	The root of the AD tree containing your groups and schema, expressed using X.500 naming. For example, dc=company,dc=com. When you connect the directory service, the Ignition Server Create Service wizard attempts to choose a Directory Root DN for you. For more information on finding this DN, see Looking up AD Settings to Find Root DNs on page 68.
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 attempts to choose a User Root DN for you. For more information on

Table continues…

Setting name	Setting value
	finding this DN, see Looking up AD Settings to Find Root DNs on page 68.
Netlogon Account Root DN	The container in AD where the Ignition Server creates its own machine account when joining the AD domain. This setting is optional. If specified, Ignition Server only attempts 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 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 more information, see Setting the AD Permissions of the Service Account on page 52.

Preparing 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 46.
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:

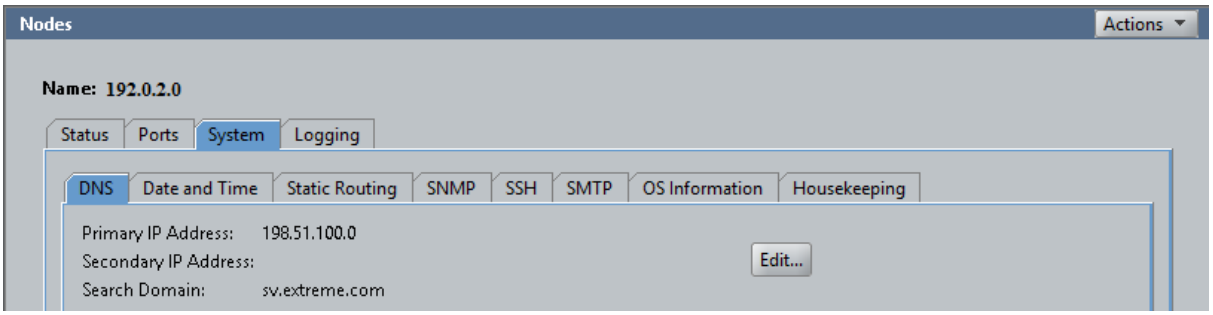
     `HKLM\System\CurrentControlSet\LSA\DisallowMsvChapv`

- Make sure that the following key is set to a value of 1, 2, 3, or 4. A setting of 5 causes Ignition Server 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 Creating the Service Account in AD on page 49.
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 Setting the AD Permissions of the Service Account on page 52.
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, it is recommended 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 main Dashboard 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 Connecting Ignition Server to AD on page 56.

Creating 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

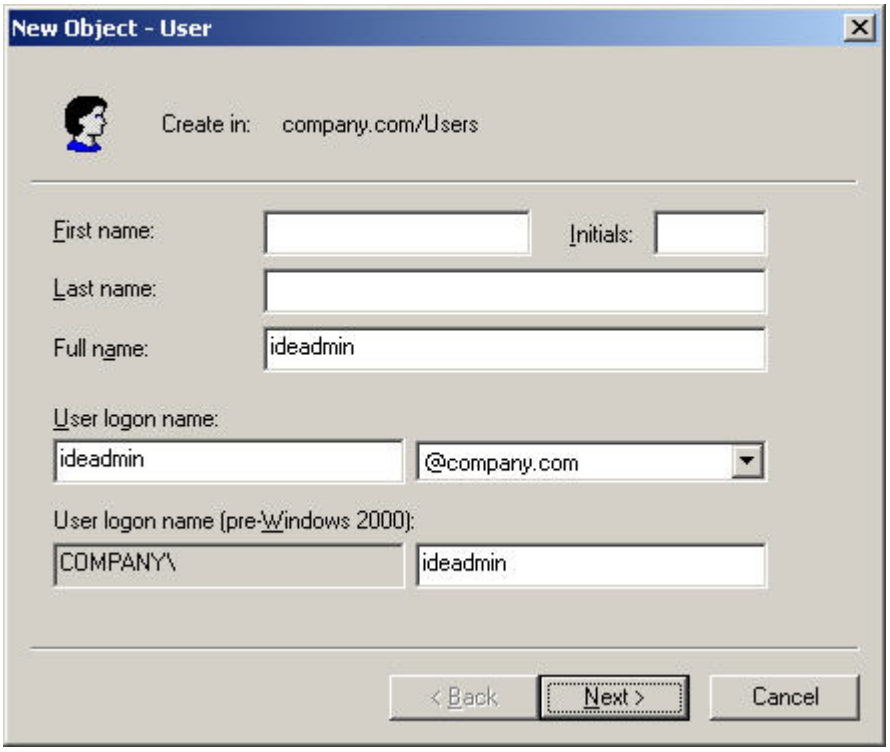
service account must have write and delete permissions in the Netlogon account root of your AD service. The location of the service account in AD does not matter.

If you have a suitable account already, you may skip this section and go to Setting the AD Permissions of the Service Account on page 52. Use this procedure to create an account.

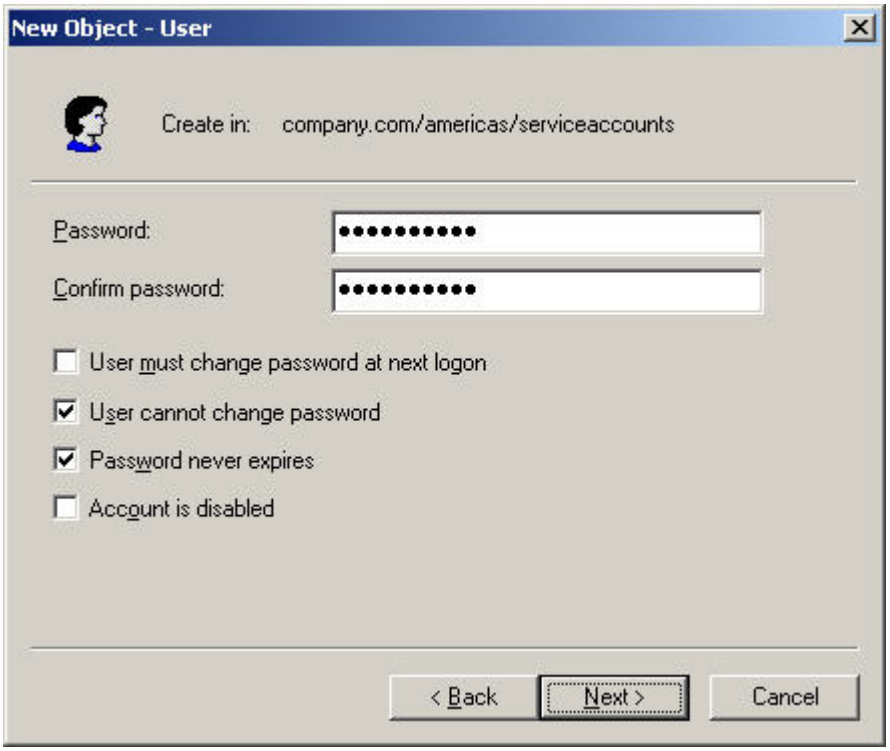
Procedure

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 create the new user. For this example we'll use the **Users** container.

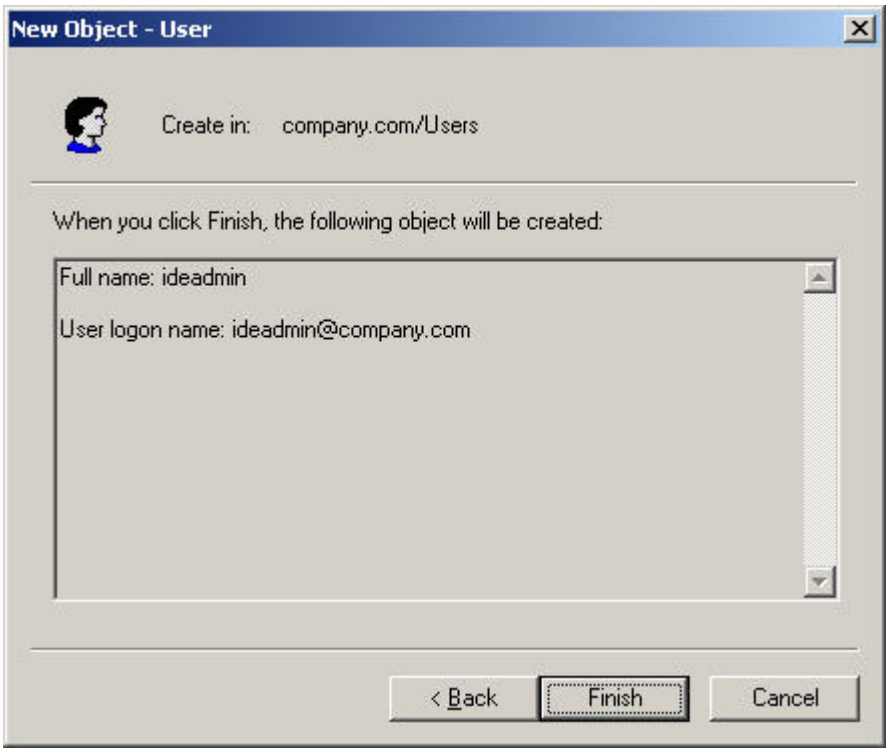
4. Select **Action** > **New** > **User**.
5. In the New Object - User window, create the Ignition Server service account. It is recommended that you create an account that is used exclusively by the Ignition Server appliance. For this example, we use the account name, "ideadmin". Click **Next** after specifying the name.



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



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



Setting 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 more information on Netlogin Account Root DN, see Settings for connecting to an AD Store on page 46.

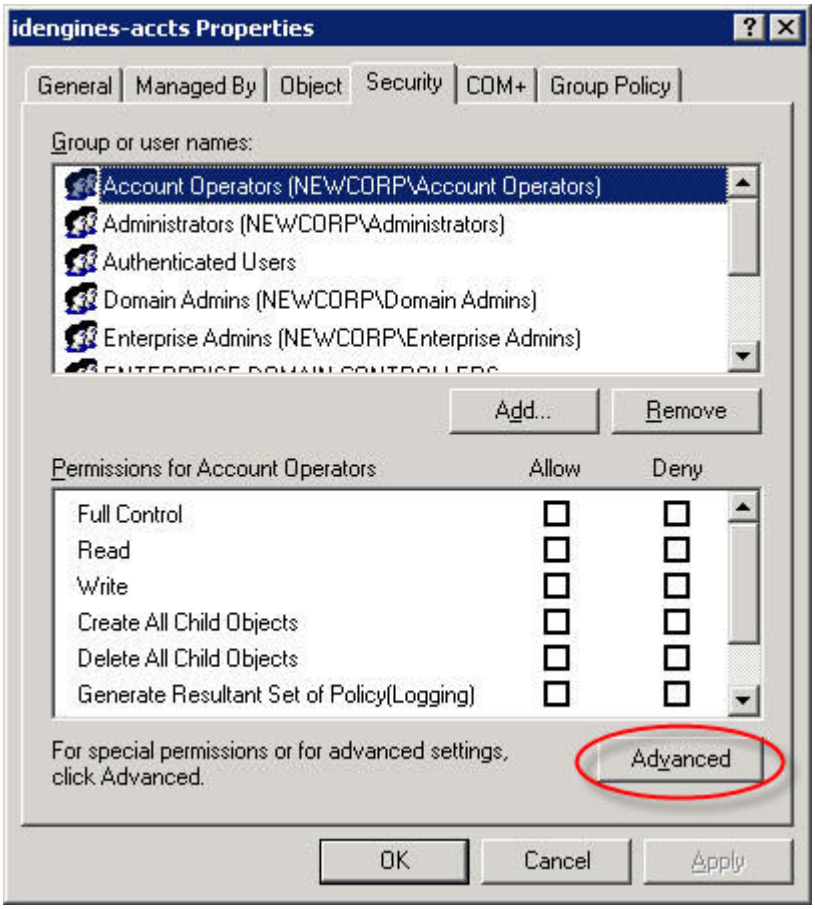
This section describes how to grant the minimal required permissions to your service account. If your service account already has the right permissions, for more information, see Gather Active Directory Connection Settings on page 46.

Procedure

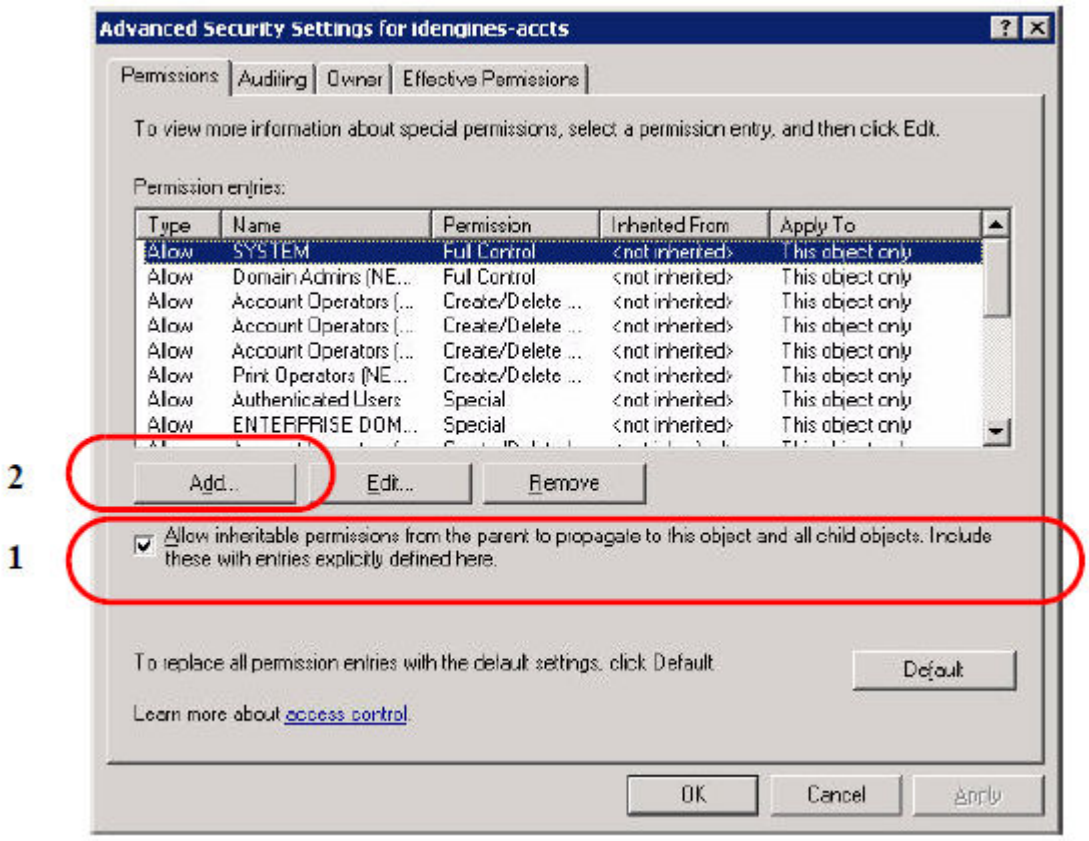
1. Log into your AD server machine as the Domain Administrator.
2. Open the Active Directory Users and Computers snap-in from the Administrative Tools or the Windows Control Panel. Under **View**, enable **Advanced Features**.
3. In the object tree on the left side, click on the container that serves as your Netlogon account root. You may configure the location Ignition Server is used as the Netlogon account root. For more information on Netlogin Account Root DN, see Settings for connecting to an AD Store on page 46.

   If you want to create a new container that serves as the Netlogon account root, click on the root domain in the tree and create the new OU there.

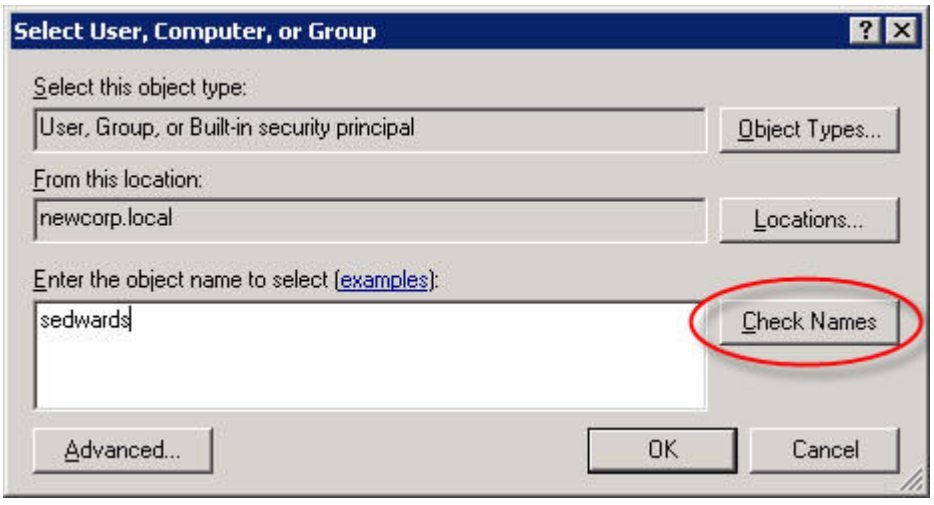
4. Right-click your Netlogon account root container, select the **Security** tab, and, under the **Permissions for Account Operators** list, click **Advanced**.



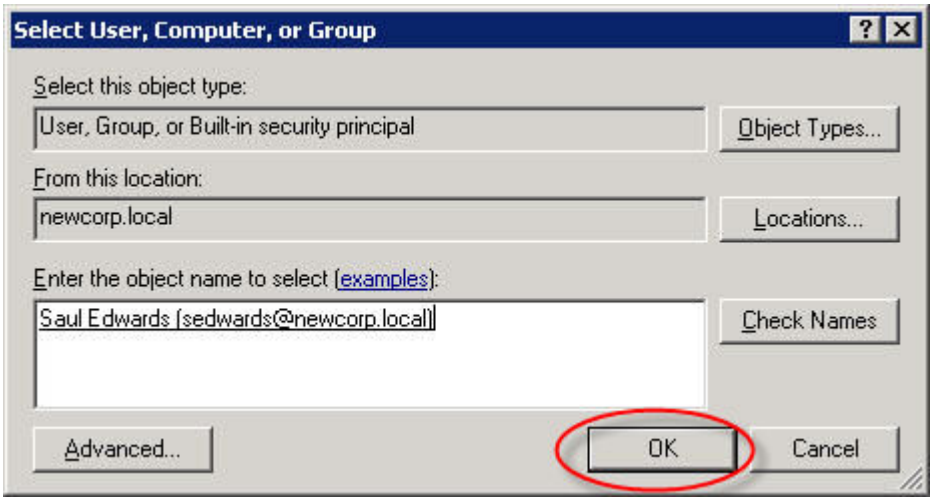
5. In the Advanced Security Settings window, click the **Permissions** tab and:
   - Make sure the **Allow inheritable permissions from the parent to propagate...** checkbox is selected.
   - Click **Add**.



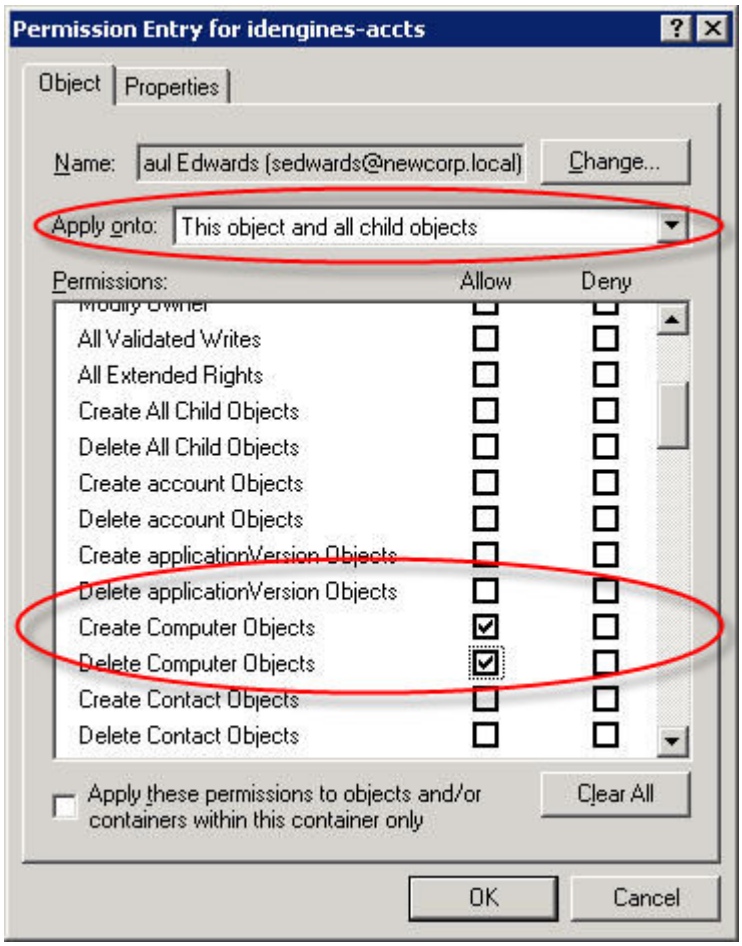
6. In the **Enter the object name** field, type the name or partial name of your Ignition Server service account and click **Check Names**.



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



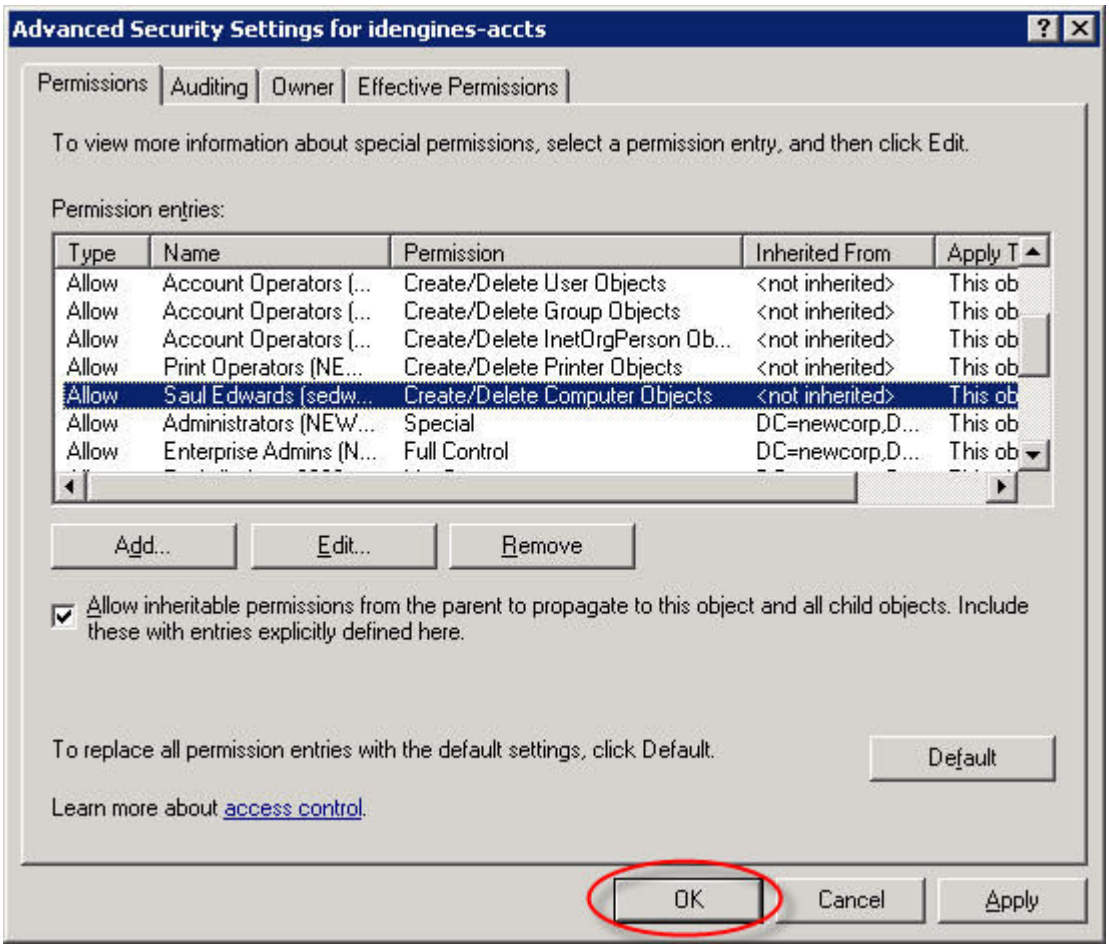
8. In the Permission Entry window, click the **Object** tab and:
   - In the **Apply onto** field, choose **This object and all child objects**.



   - In the permissions table, scroll to find the rows, **Create Computer Objects** and **Delete Computer Objects**, and select 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 46

Connecting Ignition Server to AD

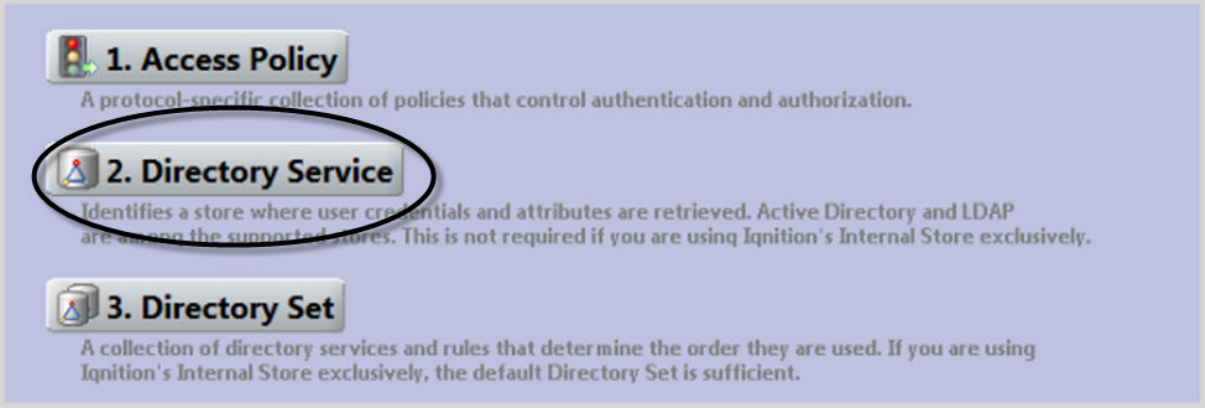
To connect Ignition Server to your Active Directory data store, save the AD store as a directory service in Ignition Server. The *directory service* specifies the connection settings that Ignition Server uses to connect to AD. Create one directory service for each AD domain you wish to connect to. You can search across multiple directory services by grouping them into a directory set as explained in Creating a Directory Set on page 76.

This sections describes 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, go to Creating the Service Account in AD on page 49.

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

Procedure

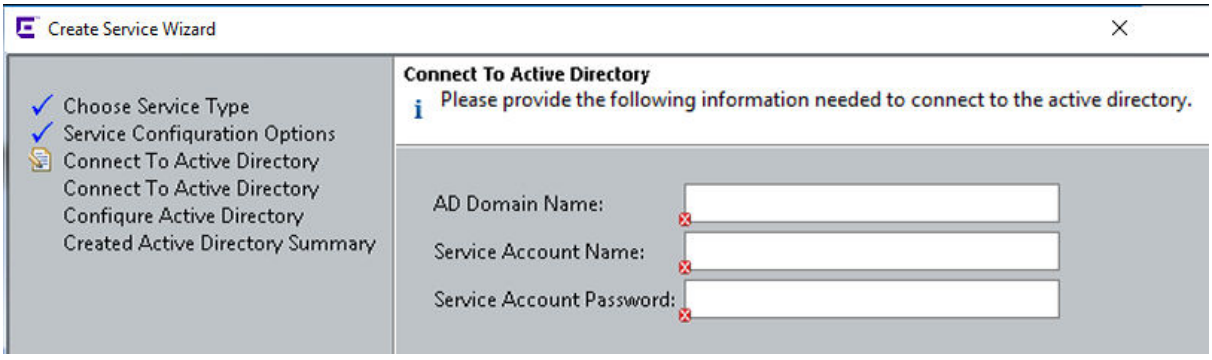
1. In Dashboard's Configuration tree, click **Site Configuration**.
2. Click the **Directory Service** link in the main panel.



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. For more information, see Troubleshooting AD and LDAP Connections on page 66.

5. In the Connect to Active Directory window, enter the connection settings you gathered in Gather Active Directory Connection Settings on page 46, or use the login you created in Creating the Service Account in AD on page 49 and click **Next**.



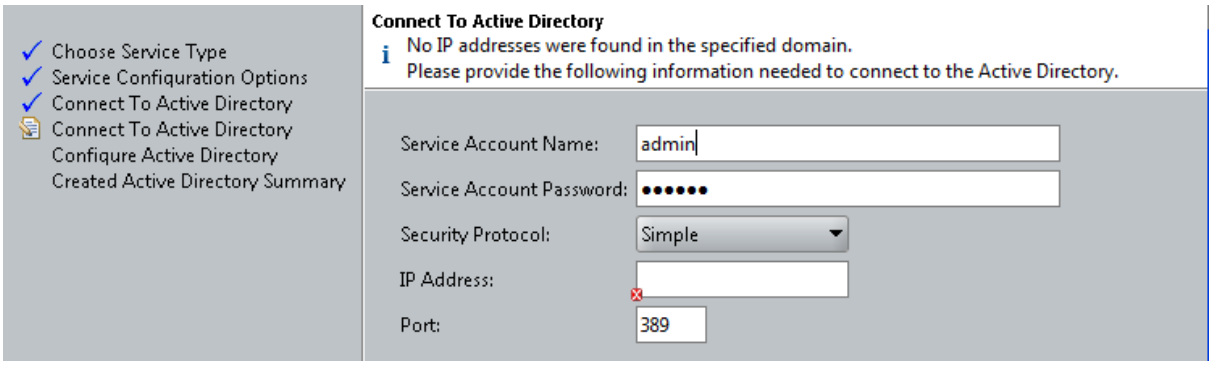
6. In the next Connect to Active Directory window, do the following:
   a. Enter the AD service account credentials in the **Service Account Name** and **Password** fields.

b. Select the **Security Protocol**: choose **Simple** for unencrypted communication with AD, or choose **SSL** for encrypted communication.

c. In the **IP Address** field, type the address of your desired AD server.

d. Check the **Port** setting and edit it if needed. Ignition Server defaults to the port number used by most AD servers.

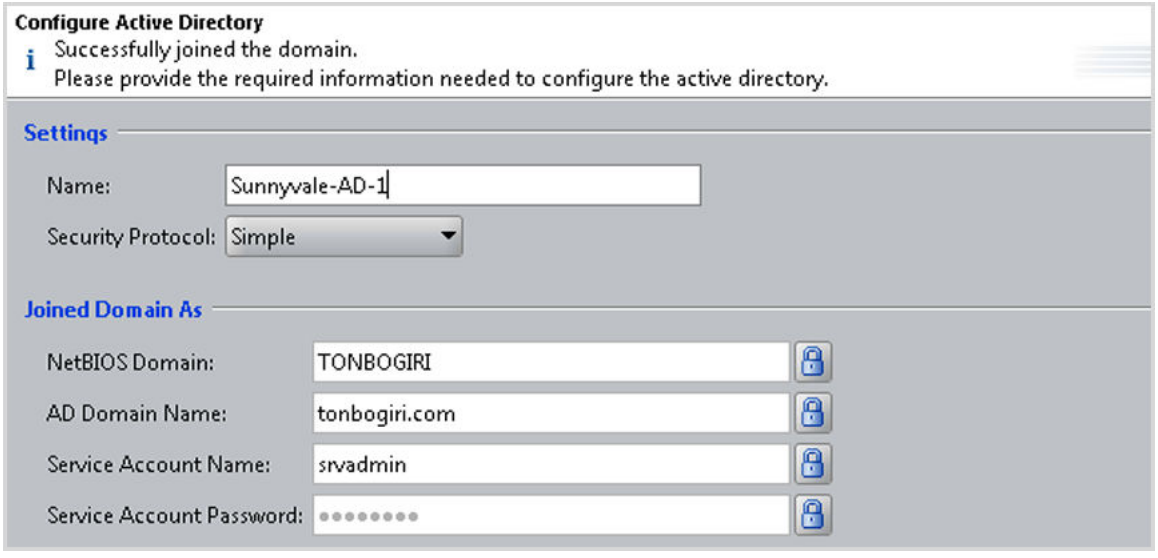
e. Click **Next**.



7. In the Configure Active Directory window, do the following:

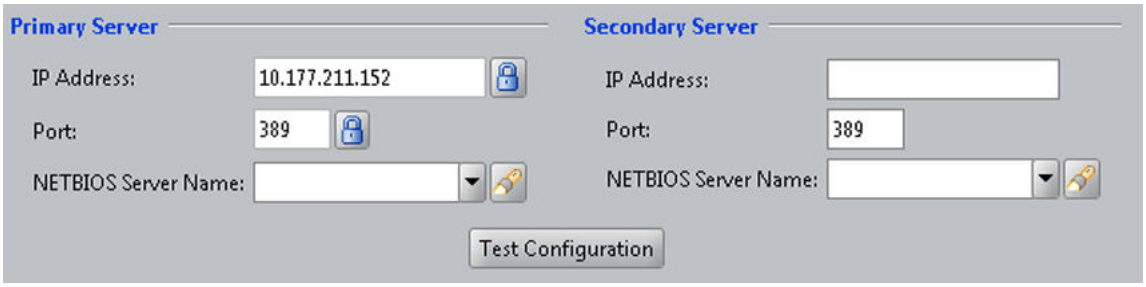
a. In the **Settings** section, type a **Name** for this directory service. For this example, enter `Sunnyvale-AD-1`.

b. In the **Joined Domain As** section, the settings are already populated by the wizard. If you need to change a setting, click the lock/unlock button and edit the field. For an explanation of each field, see the table in Gather Active Directory Connection Settings on page 46.



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

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



e. The **DN Configuration** fields are populated by the wizard; if necessary, edit them. The Directory Root, User Root, and Netlogon Account Root are explained in Settings for connecting to an AD Store on page 46. 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.

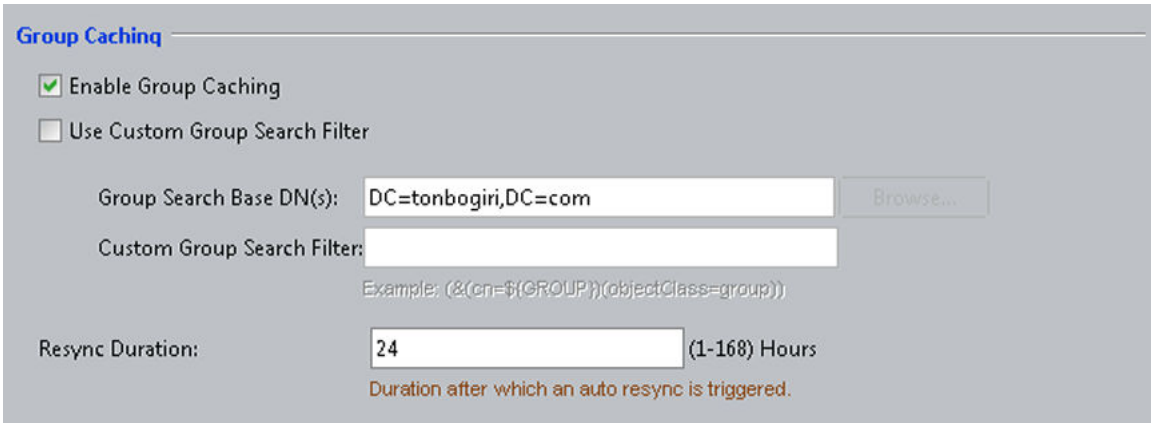
Selecting the **Accept all users in the forest** checkbox allows Ignition Server to look up users in the global catalog of your AD.

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

g. 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.

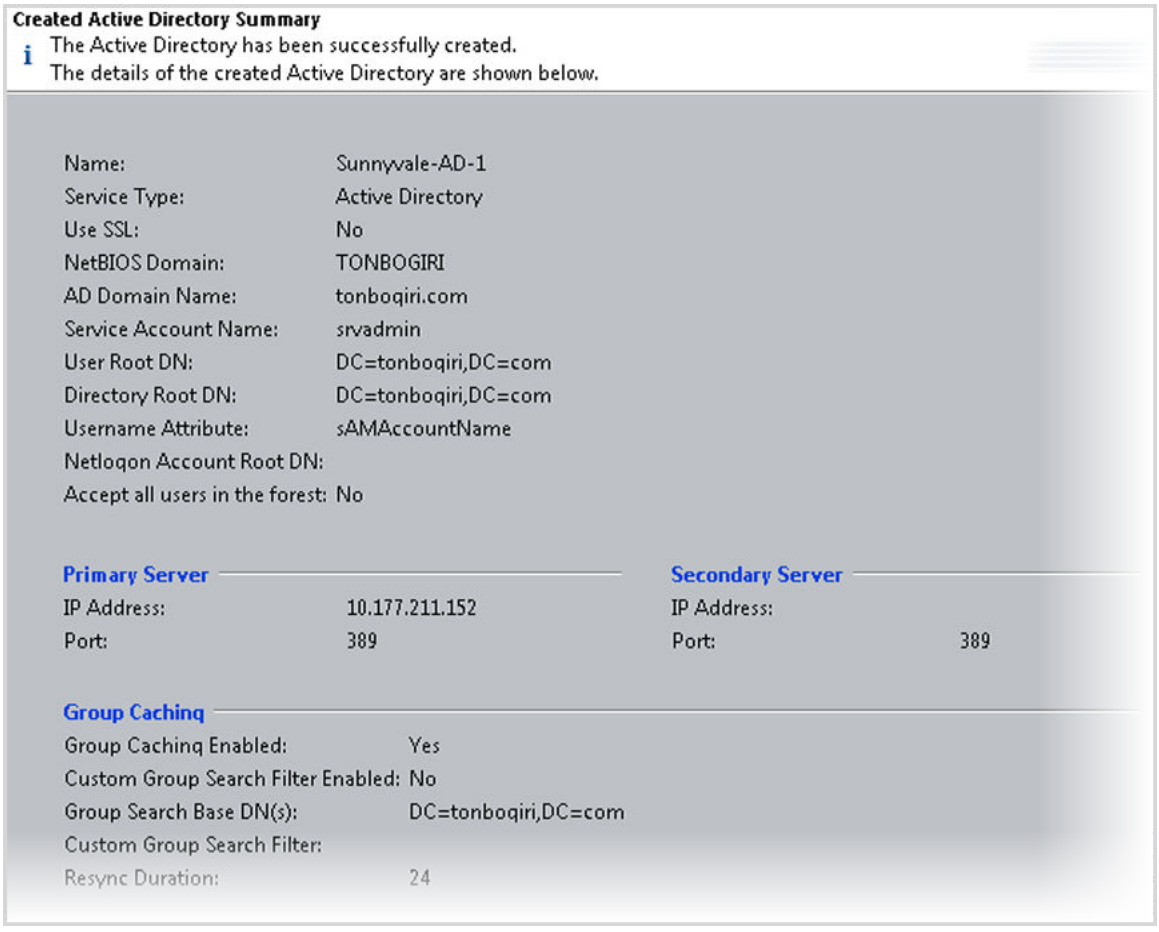
h. Enter the sync interval between Ignition Server and Active Directory, in hours, in **Resync Duration**.

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



8. Click **Next**.

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



9. If the settings are correct, click **Finish** to create the directory service.

Next steps

Do one of the following:

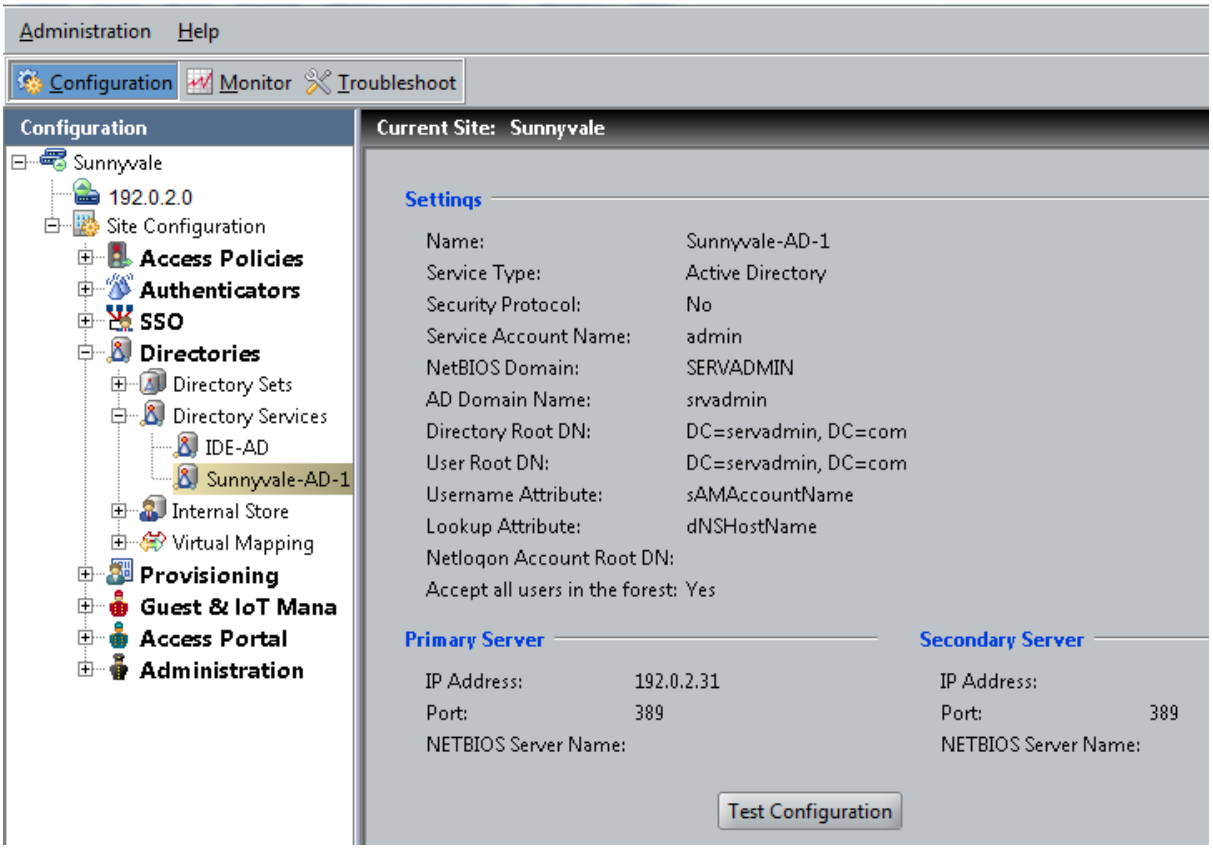
- If the connection attempt succeeded, continue with Creating a Directory Set on page 76.
- If your connection attempt failed. For more information, see Troubleshooting AD and LDAP Connections on page 66.

Editing a Directory Service

Use this procedure to edit your directory service.

Procedure

1. In the Dashboard Configuration tree, expand **Site Configuration** > **Directories** > **Directory Services**, and click the name of your directory service.



2. The main panel displays the connection details of the service. To test the connection, click the **Test Configuration** . To edit the connection, click **Edit**.

Connecting to LDAP

To connect Ignition Server to your LDAP store, you have to 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 have to 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. For more information, see Creating a Directory Set on page 76.

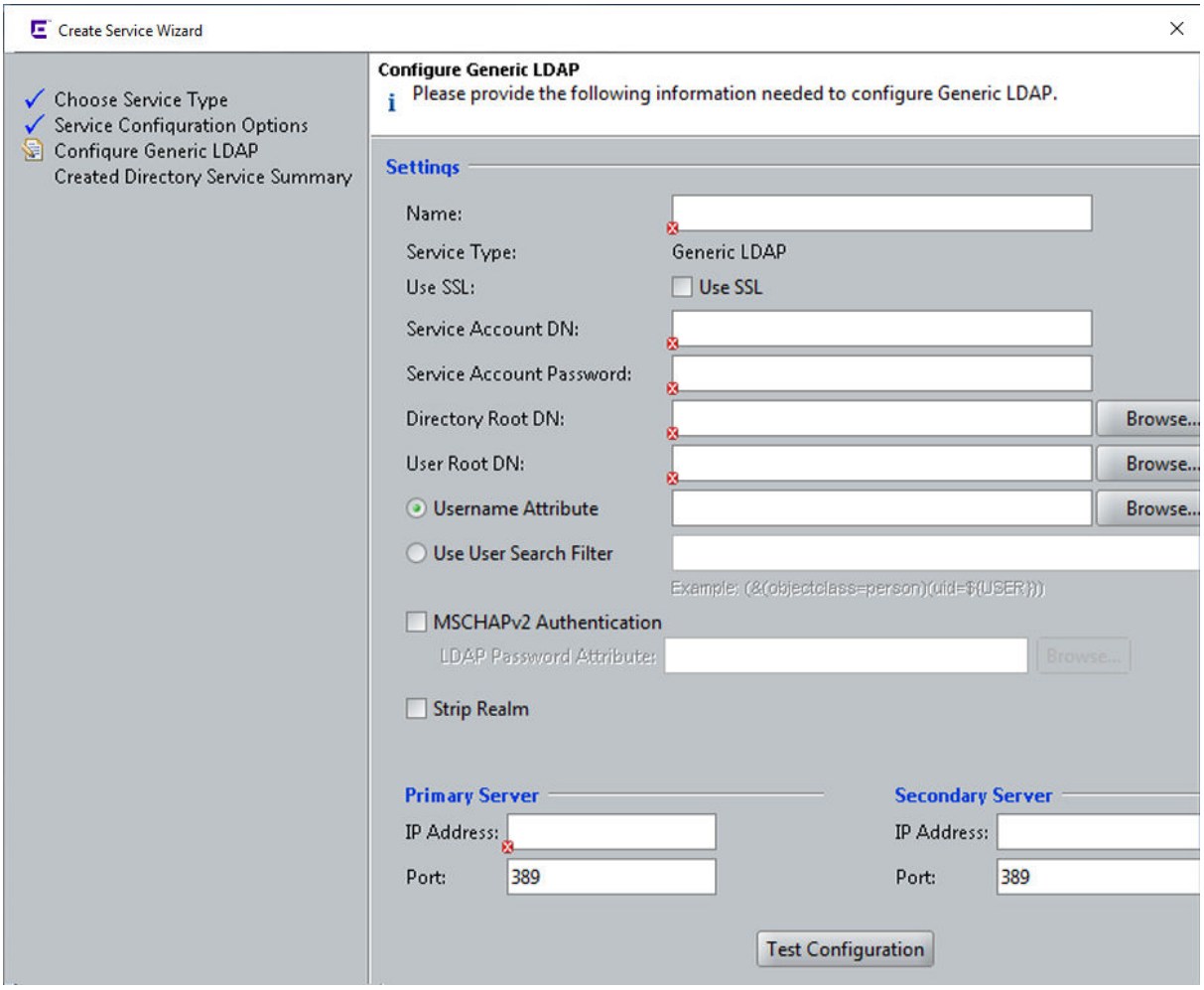
This sections describes with the assumption that your user data resides in LDAP and that you have an LDAP administrator account that you can use as the Ignition Server service account.

You can connect using Ignition Server LDAP connection wizard in *automatic connection* mode.

Procedure

1. In Dashboard's Configuration 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, Generic LDAP) and click **Next**.
4. In the Service Configuration Options window, click **Automatically configure** and click **Next**.

   If your LDAP connection attempt fails while you are carrying out the steps below. For more information, see Troubleshooting AD and LDAP Connections on page 66.
5. In the Connect to LDAP window (specific to the type of LDAP store that you selected), do the following:



a. In the **Service Account DN** field, enter the DN of the LDAP administrator account. Ignition Server connects as this administrator. For example, cn=Directory Manager.

b. In the **Service Account Password** field, enter the password of the LDAP administrator.

c. **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 travels over the network in unencrypted form. It is recommended that you use an SSL connection to connect to your directory server.

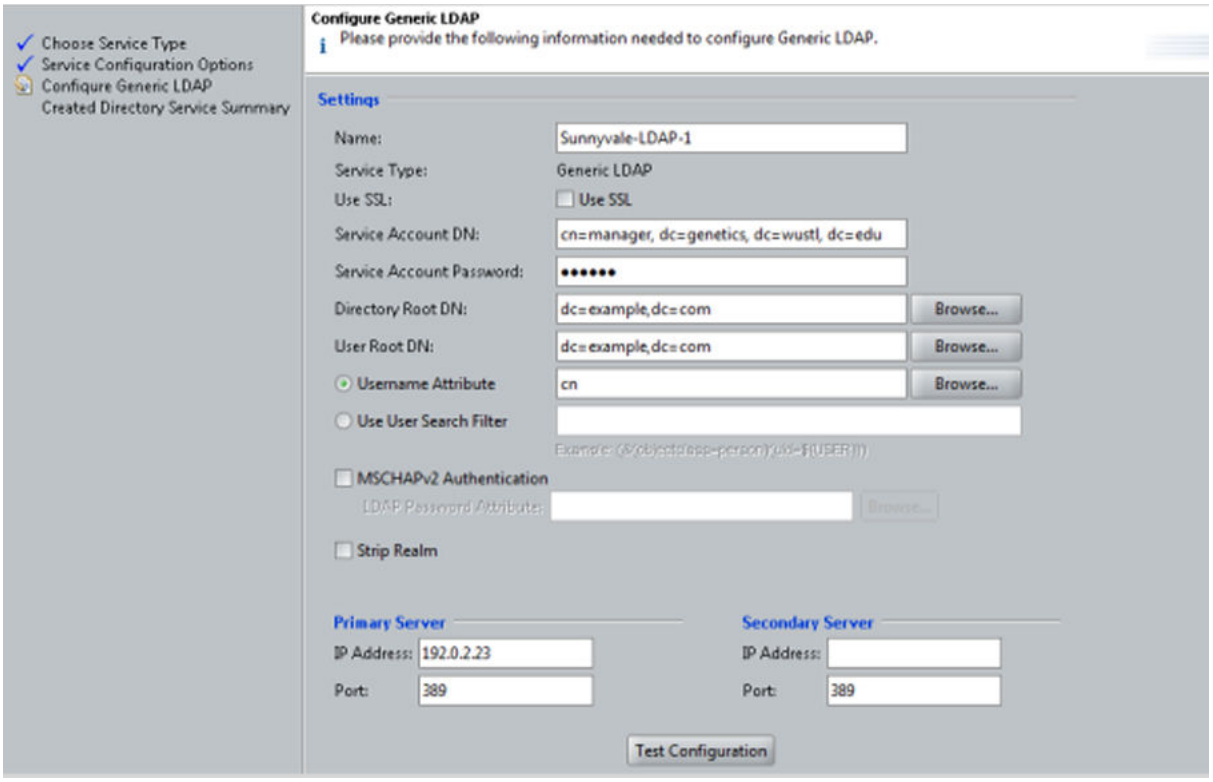
d. In the **IP Address** field, enter the IP address of the primary LDAP server.

e. In the **Port** field, enter the 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 LADP window is displayed.

7. In the **Settings** section, type a **Name** for this directory service. For this example, `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 does not display auxiliary classes; those you must type directly. The fields are:

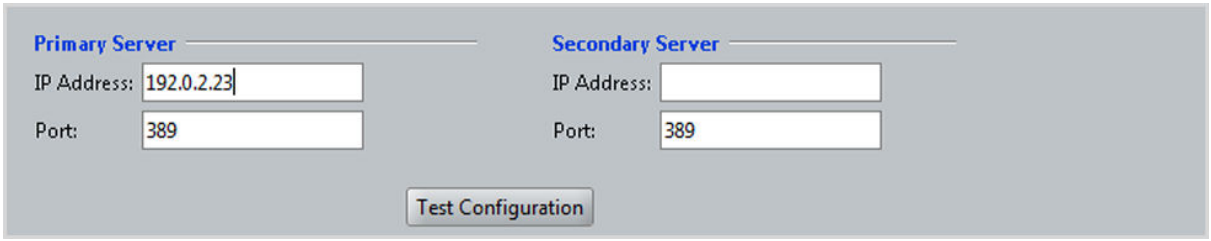
- **Directory Root DN**: DN where the LDAP schema containing your users and groups may be found. For example, dc=company,dc=com. When you connect the directory service, the Ignition Server Create Service wizard attempts to choose a Directory Root DN for you.
- **User Root DN**: DN of the LDAP container Ignition Server from where it loads user records. For example, cn=users,dc=starironinc,dc=com. When you connect the directory service, the Ignition Server Create Service wizard attempts to choose a User Root DN for you.
- **Username Attribute**: An LDAP attribute that stores the user name.

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

  Optional: If this LDAP store supports MSCHAPv2 authentication, select the **MSCHAPv2 authentication** checkbox and, in the **LDAP Password Attribute** field, set the name of LDAP attribute that stores the hash of the user's MSCHAPv2 password. For more information, see "Setting up MSCHAPv2 Authentication on LDAP" in *Identity Engines Ignition Server Configuration document*.

8. 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.



9. In the Group Caching section
   a. 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** checkbox.
   b. 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 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.
   c. Enter the sync interval between Ignition Serverand the LDAP service, in hours, in **Resync Duration**.

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

10. Click **Next**.

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

11. Review the settings. If the settings are correct, click **Finish** to create the directory service.

    Your directory service has been saved in Ignition Server.

Next steps

Do one of the following:

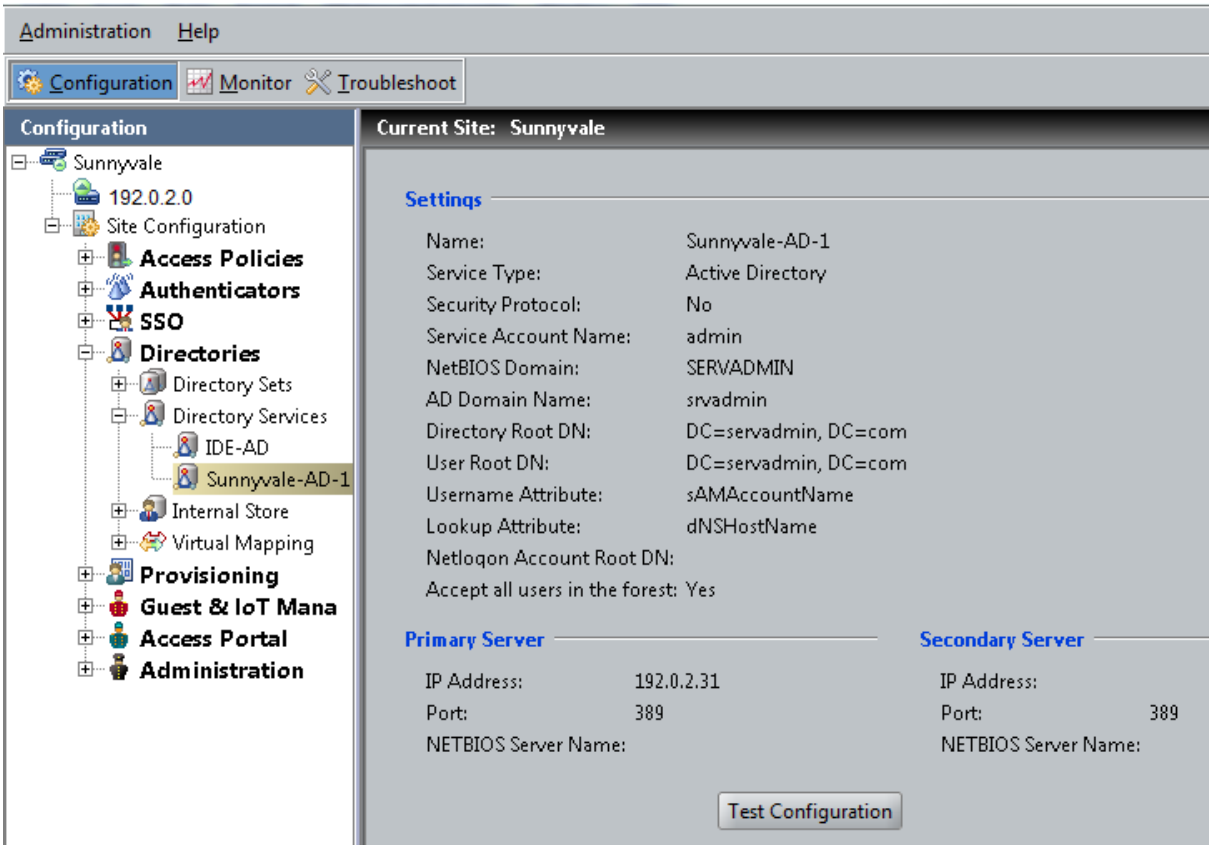
- If the connection attempt succeeded, continue with Creating a Directory Set on page 76.
- If your connection attempt failed. For more information, see Troubleshooting AD and LDAP Connections on page 66.

Editing a Directory Service

Use this procedure to edit your directory service.

Procedure

1. In the Dashboard Configuration tree, expand **Site Configuration** > **Directories** > **Directory Services**, and click the name of your directory service.



2. The main panel displays the connection details of the service. To test the connection, click the **Test Configuration** . To edit the connection, click **Edit**.

Troubleshooting AD and LDAP Connections

This section describes tips to troubleshoot AD and LDAP connections.

Checking a Directory Connection

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

Procedure

1. In Dashboard's Configuration tree, expand **Site Configuration** > **Directories** > **Directory Services**, and click the name of your directory service.
2. 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.

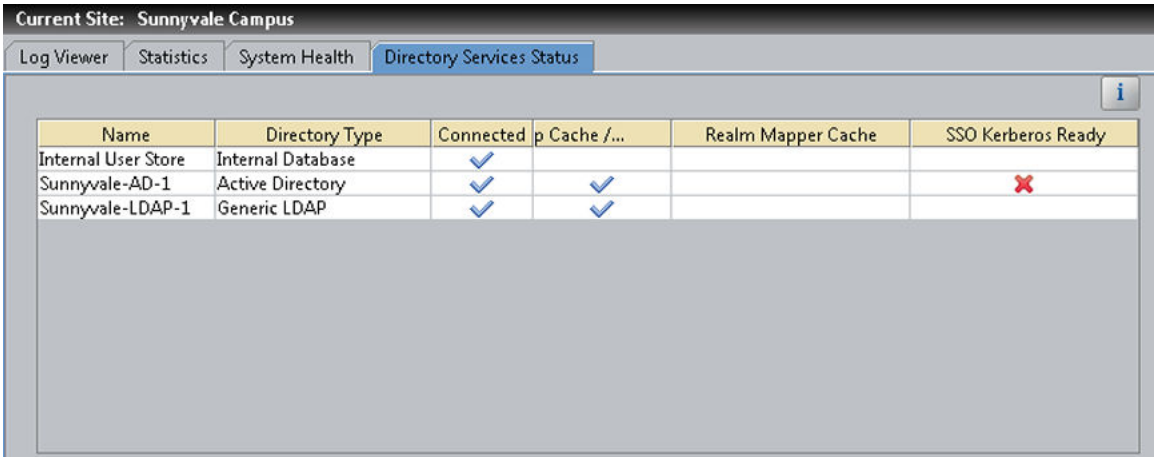
   The Test Connection Results window displays the test outcome, displaying one success/failure line for the primary server and one line for the secondary server, if configured.

Checking Directory Connections and Cache Status

Use this 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.



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

Use this 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 more information, see "Advanced Troubleshooting for Directory Services and Sets" in *Identity Engines Ignition Server Configuration document*.

Looking up AD Settings to Find Root DNs

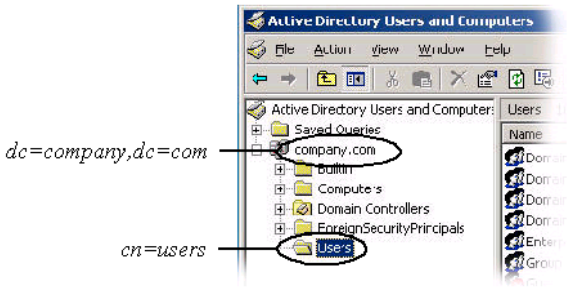
Use this procedure to find your **User Root DN** and **Directory Root DN**.

Procedure

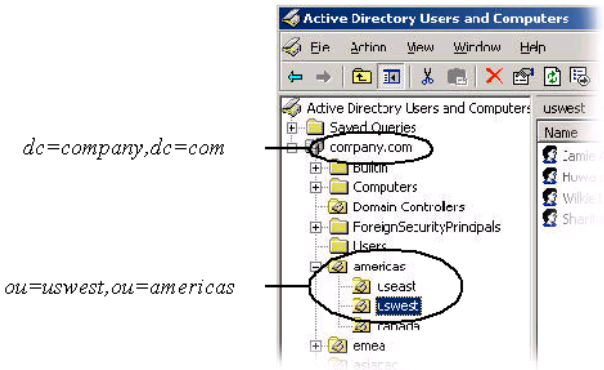
1. Enter the names of containers in your AD data store using X.500 naming.
   - **User Root DN** points to the AD container that stores your user records.
   - **Directory Root DN** points to the root of your AD tree and is used to obtain schema and group information.
2. To determine the X.500 names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

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

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



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



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

Looking up AD Settings to Find Domain and NetBIOS Names

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

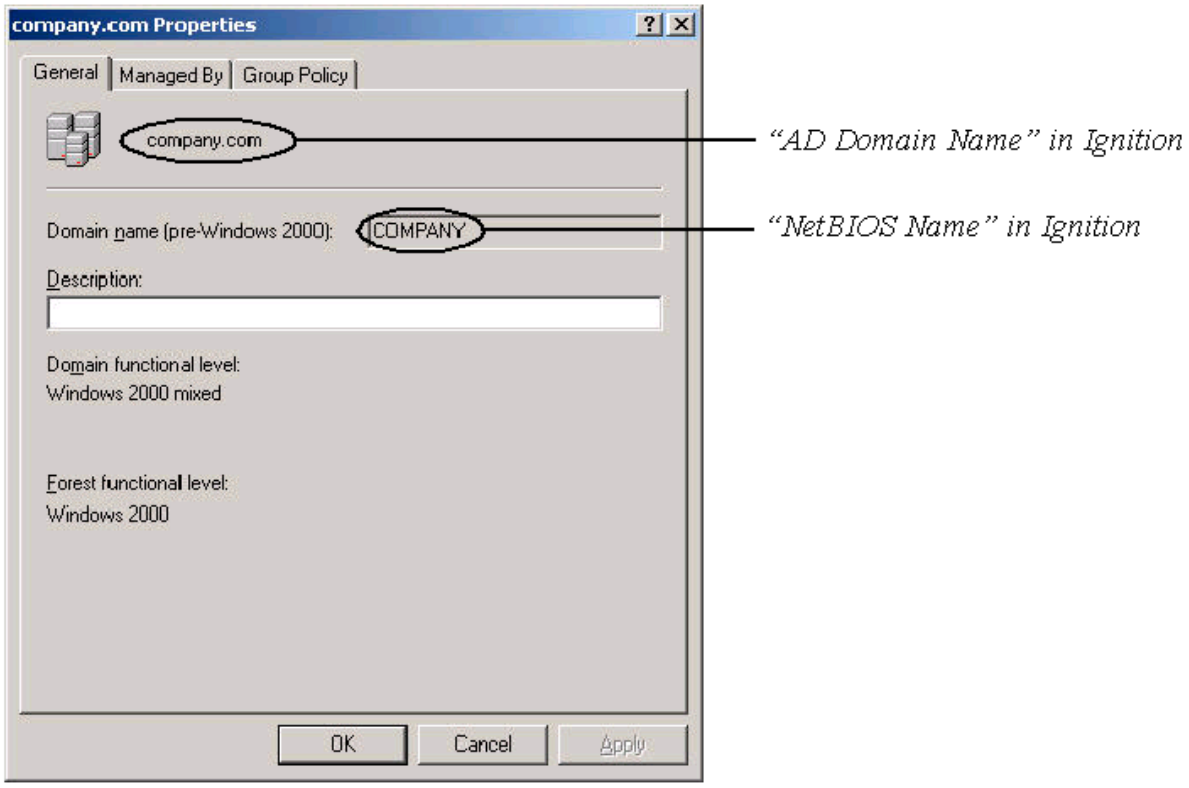
Procedure

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

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

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

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



Looking up AD Settings to Find AD Server IP Address

Use this 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**.

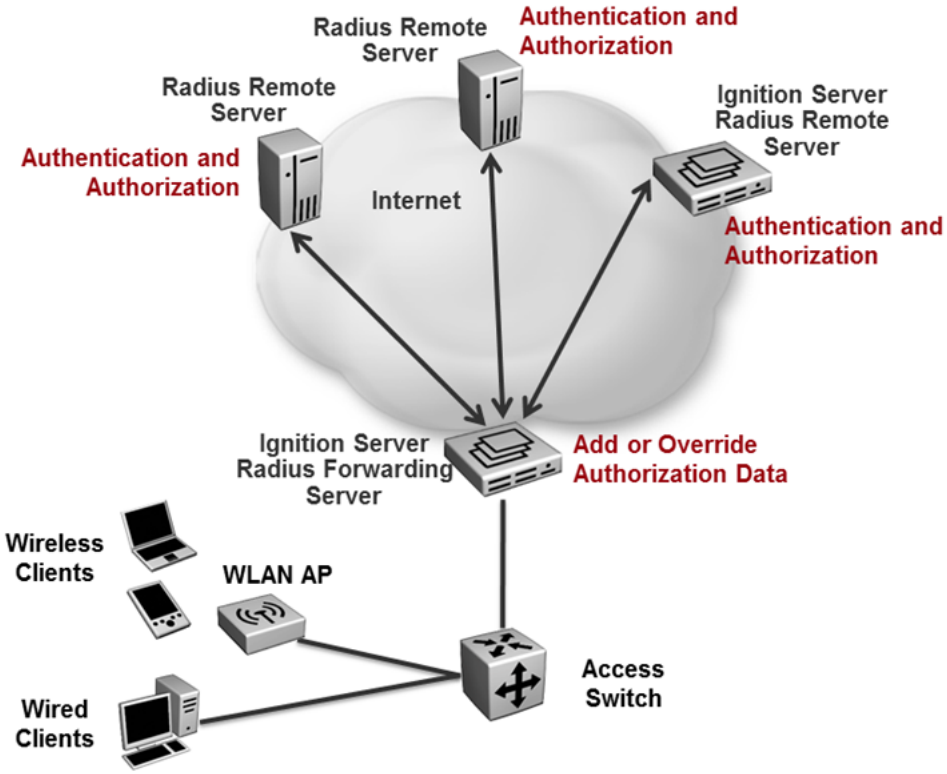
  Read the **IP address** from the TCP/IP Properties window.

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.

The forwarding server performs local authorization after receiving a response from the remote server to suit the local network deployment. After the forwarding server completes authentication, the information is logged for both success and failure.

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



Adding the RADIUS Proxy Server to a Directory Set

After you create a RADIUS proxy authentication service, create a directory set. For more information, see Creating a Directory Set on page 76. 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.

Creating a RADIUS Access Policy for 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. For more information, see Setting your Identity Routing Policy on page 88.

Creating a New RADIUS Proxy Policy

Use this procedure to create a new RADIUS Proxy Policy and add authorization policy rules.

Each rule consists of one or more constraints. Each constraint tests the value of an attribute. If there are multiple constraints, you can join them into separate logical statements to ensure the proper order of authorization as required.

The rule action determines whether the user is denied or granted access based on the defined constraints.

Procedure

1. In Dashboard's **Configuration** hierarchy tree, expand **Access Policies** and click **PROXY**. Click **New**.
2. Enter the **Access Policy Name** and click **OK**.
3. Highlight the new access policy name, and click **Edit**.

   The Edit Authorization Policy window is displayed.
4. Do one of the following:
   - To add a new rule, click **Add** in the Rules panel, enter a **Name** for the new rule and click **OK**.
   - To copy an existing rule, click **Copy** in the Rules panel, select the desired rule, and click **OK**.
5. To set up rule details, highlight the rule name in the **Rules** list.

   The rule details are shown in the **Selected Rule Details** pane. Any existing constraints for the selected rule are listed in the **Constraints** list.
6. Do one of the following:
   - To add new constraints, click **New**.
   - To edit existing constraints, highlight the constraint and click **Edit**.
7. From the **Attribute Category** drop-down list, select the category.

   All of the valid attributes for the category are listed.
8. Select the desired attribute.

The configurable details for the selected attribute are displayed.

9. Configure the attribute details as applicable:
   - Select the comparison operator.
   - Select the format.
   - To compare the attribute value with a fixed value, select the **Static Value** radio button and type or choose the comparison value in the field below.
   - To compare the attribute value with a value retrieved from another attribute, select the **Dynamic Value of Attribute** radio button. In the drop-down list below, choose the Attribute Category. In the second drop-down list, choose the attribute that should provide the comparison value. The list of comparison attributes contains only those attributes whose data type matches the data type of the constraint attribute.
10. Click **OK**.
11. Repeat Steps 6 through 10 for each constraint.
12. To logically group multiple constraints, in the **Constraint** list, highlight the first and last constraints to be grouped and use the opening and closing parentheses drop-down lists to group the constraints. Use the **AND/OR** drop-down list to form a logical condition statement.
13. Do one of the following:
    - Select **Deny** for the **Action** and go to Step 15.
    - Select **Allow** for the **Action**.
14. If you chose **Allow** for the **Action**, do the following:
    - In the **Send Attributes** row, click the Edit icon, and use the left and right arrows to add or delete attribute values from the **Attribute List**.

      The forwarding server updates (if present) or adds (if not present) these attributes to the remote server response before sending to the authenticator.
    - In the **Delete Attributes** row, click the Edit icon, and use the left and right arrows to add or delete attribute values from the **Attribute List**.

      The forwarding server deletes these attributes from the remote server response before sending to the authenticator.

    Note that, when a forwarding server receives a response from a remote server, the first Delete Attribute is applied, and then the second, and so on. All of the attributes defined in the Delete Attribute List on the forwarding server are deleted first. After that, the first Send Attribute either adds the attribute or updates an existing attribute value that may be present in the remote server response. Then the second, and so on. After applying Delete, Send (in that order), the forwarding server sends a response back.
15. Check the **Summary** section to confirm the rule details, and click **OK**.

    The policy and associated rules is saved.

Creating a RADIUS Proxy Authentication Service

Use this procedure to create a RADIUS proxy authentication service. The Create Service Wizard guides you through the steps.

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 is used in your Ignition Server policy to specify that this RADIUS proxy server should be used.
4. Enter the **Shared Secret** for the RADIUS proxy server.
5. Select the **Proxy Policy** from the drop-down list.

   This policy determines how to update the RADIUS response from the remote server and change the authorization attributes to suit the local network deployment. This policy can only be associated with the Radius Proxy type of directory services and include only authorization.

   The list contains the proxy policies configured on the system. By default, it is associated with a default policy that has no local authorization.

   For more information on configuring the proxy policies, see Creating a New RADIUS Proxy Policy on page 72.
6. To send a regular “keepalive” ping, select 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.

   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 reachability.

   With Keepalive turned on, Ignition Server periodically looks up the supplied username/password on the remote server to determine reachability, and if successful, marks the service as *Connected* in the **Directory Services Status** tab. By default, Ignition Server uses a predefined username and 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.

   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 the Dashboard’s Troubleshoot view.

Note:

We recommend you to 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 that the remote server is always connected and the requests may get dropped if the remote server health status is not determined.

7. Specify the **IP Address** and **Port** for the primary RADIUS proxy server and optionally for the secondary RADIUS proxy server.

   If both the primary and secondary servers are configured and the Keepalive is not enabled, RADIUS proxy authentication attempts 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.

8. Click the **Test Keepalive** button.

   Testing the connection may take a few minutes. If a configuration setting is incorrect, Ignition Server warns you.

9. Click **Next**.

   The next window displays the connection settings of the service.

10. Click **Finish**.

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

Configuring the Remote RADIUS Server

After you set up the RADIUS proxy server, you must perform some configuration tasks on the remote RADIUS server.

Creating an Authenticator

For the remote RADIUS server, the proxy (forwarding) server acts as an authenticator. Create an authenticator similar to creating a regular authenticator, that points to the proxy server. From the Dashboard, go to **Configuration** > **Site Configuration** > **Authenticators** and click **New**.

Creating an Access Policy

Assign an Access Policy that is capable of handling authentication requests from the proxy server. Create a regular Access Policy as you would for any regular authenticator and configure the necessary authentication and authorization policies. Make sure that the shared secret configured here matches the shared secret as configured at the forwarding server's proxy service.

Proxying of MAC Authentication Requests

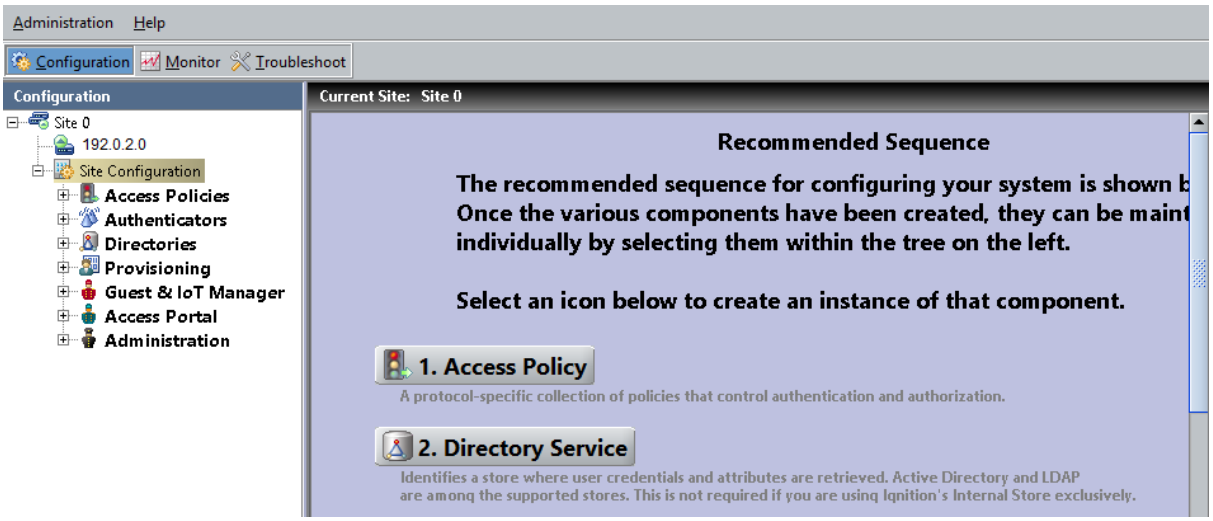
MAC authentication is typically used for devices that are incapable of performing 802.1X authentication. MAC authentication requests are also RADIUS requests. MAC authentication verifies that the MAC address submitted by a connecting client device matches an entry on your list of known MAC addresses. 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.

Creating a Directory Set

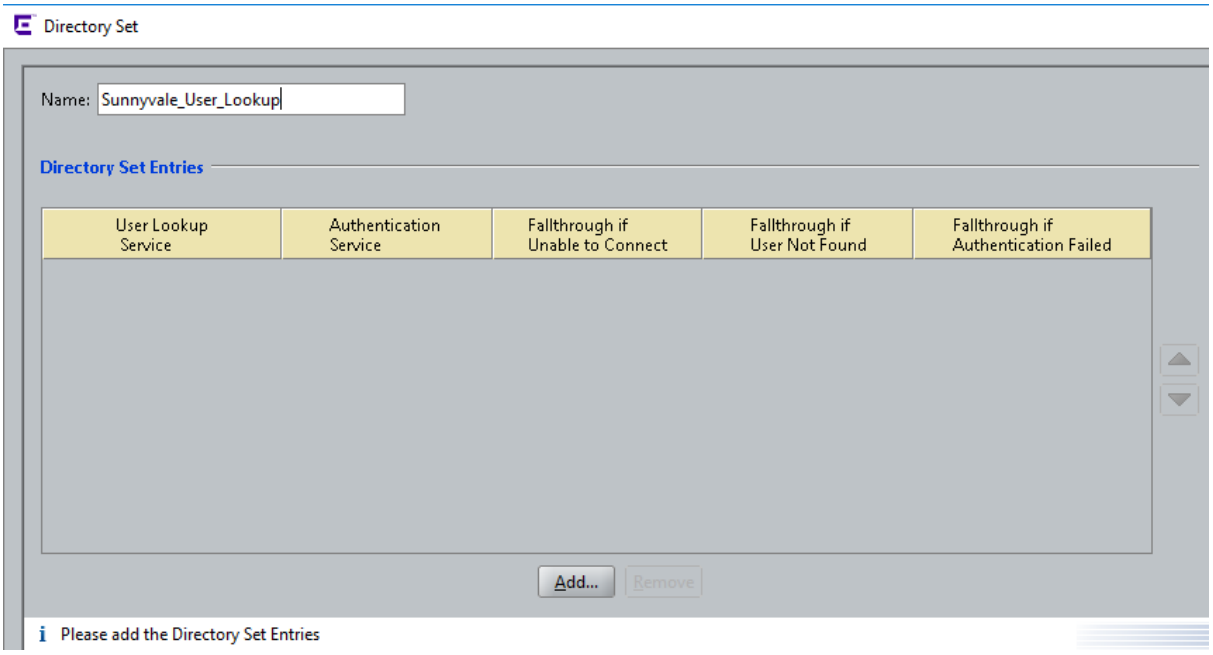
A directory set is the mechanism Ignition Server uses to scan multiple directories for a user account. You can define each user data store (that is, each AD data store, LDAP data store, and the embedded store) as a directory service in Ignition Server, and you can group those directory services into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

Procedure

1. In the Dashboard's Configuration tree, click **Site Configuration** , and click **Directory Set** in the main panel.



2. 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.
3. Click **Add** to start adding directory services to the set.

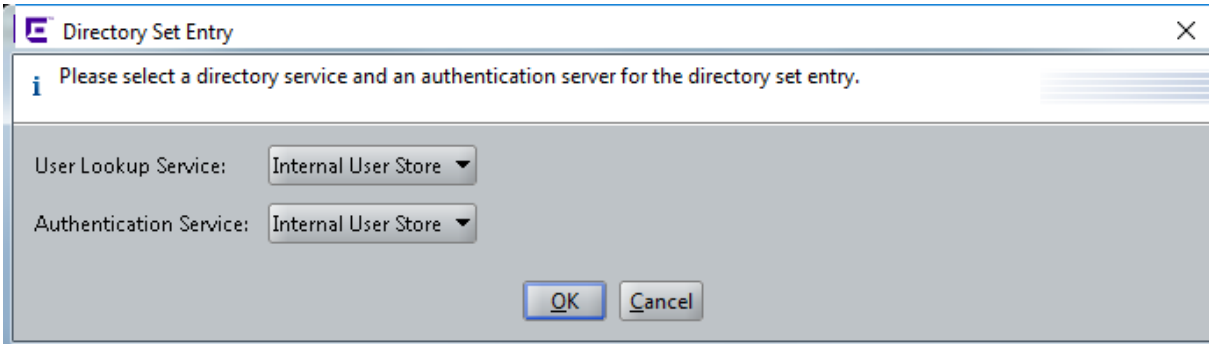


4. In the Directory Set Entry window, specify the directory that provides user account data and group memberships (**User Lookup Service**) and the directory that authenticates users (**Authentication Service**).

   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.

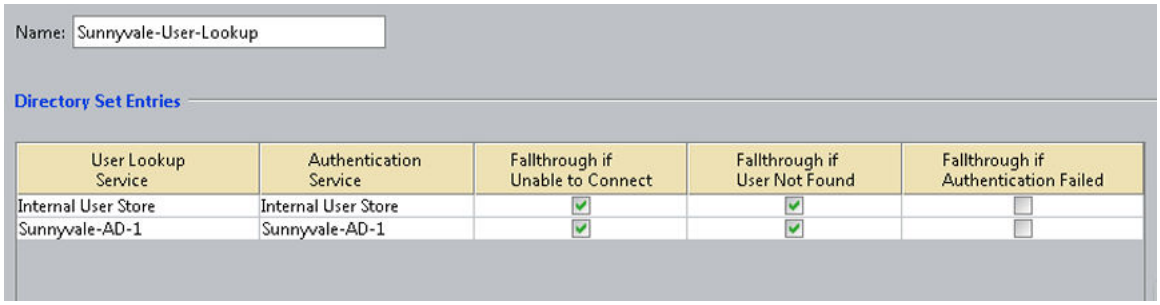
   For this example, we use the internal user store so that we can later demonstrate an authentication of the user account we created earlier. If you have an LDAP or AD user you can test with, you may use your AD or LDAP store instead.

   - 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**.



5. 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, select the **Fallthrough** checkboxes in the top row of the table to specify how you want Ignition Server to handle directory failover. By selecting these boxes, you can, for example, specify that Ignition Server attempts authentication against *ActiveDirectory1* if the user's lookup in the *Internal User Store* fails.



6. Click **OK** to save the set.

Next steps

Map user groups. For more information, see Creating Virtual Groups on page 78.

Creating Virtual Groups

Virtual groups are Ignition Servers 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.

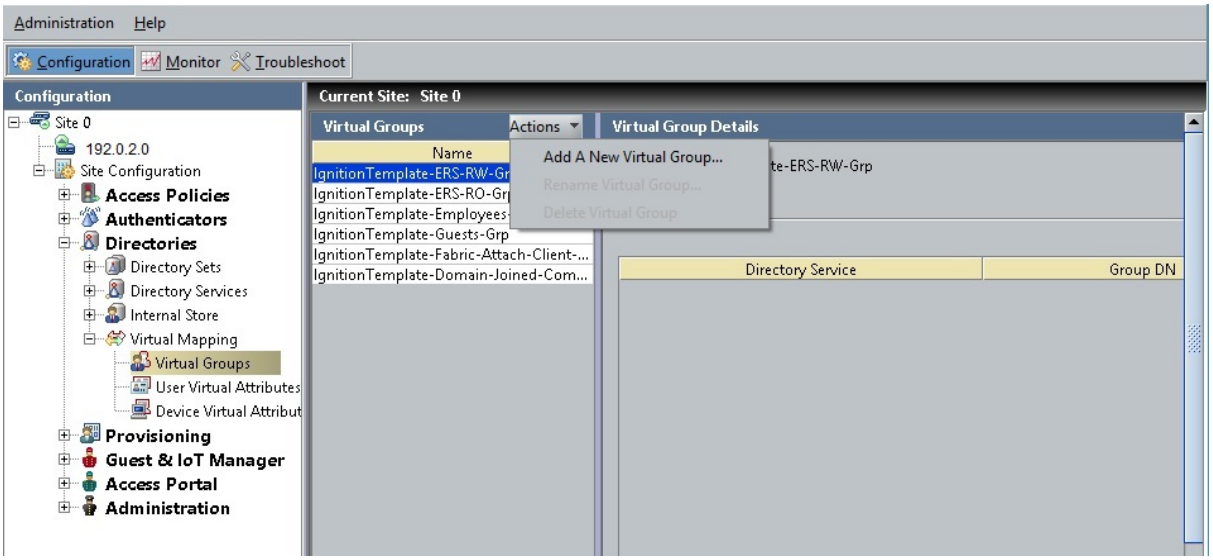
For example, you might create an Ignition Server virtual group called, *"Administrators"* and map it to the DN, *"ou=admin,ou=Users,dc=company,dc=com"* in the user database of your Fresno office, and also map it to the nsRole value *"AdminGroup"* in the user database in your Irvine office. Your access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

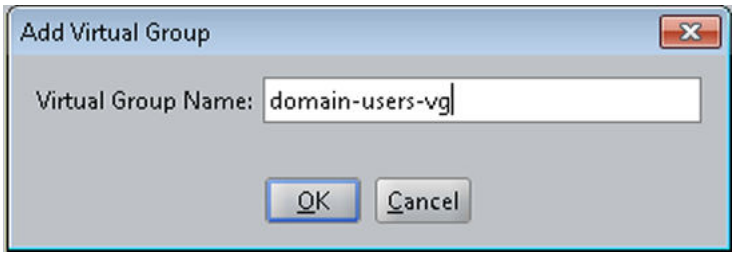
This example shows a virtual group that maps to the Domain Users group in the AD store.

Procedure

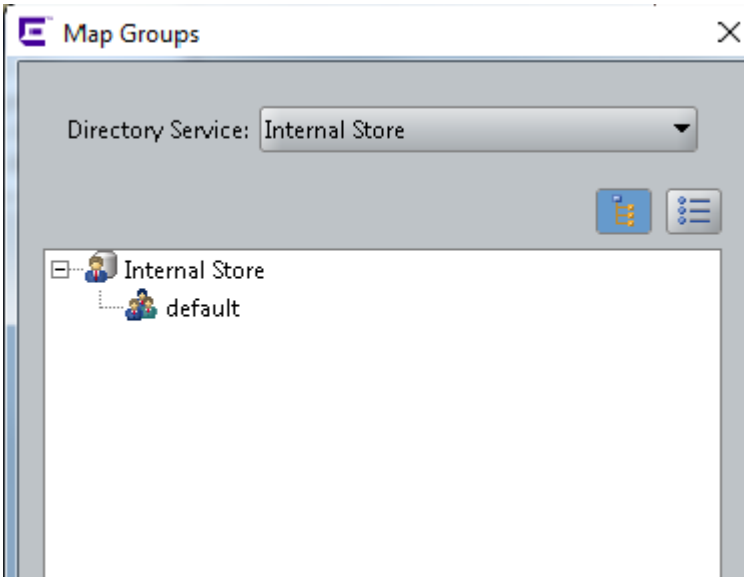
1. In the Dashboard's Configuration tree, expand **Site Configuration** > **Directories** > **Virtual Mapping**, and click **Virtual Groups**.
2. In the Virtual Groups panel, click **Actions** > **Add A New Virtual Group**.



3. Type the virtual group name and click **OK**. In this example, the virtual group name is `domain-users-vg`. This group contains the members of the “Domain Users” group of the AD server.

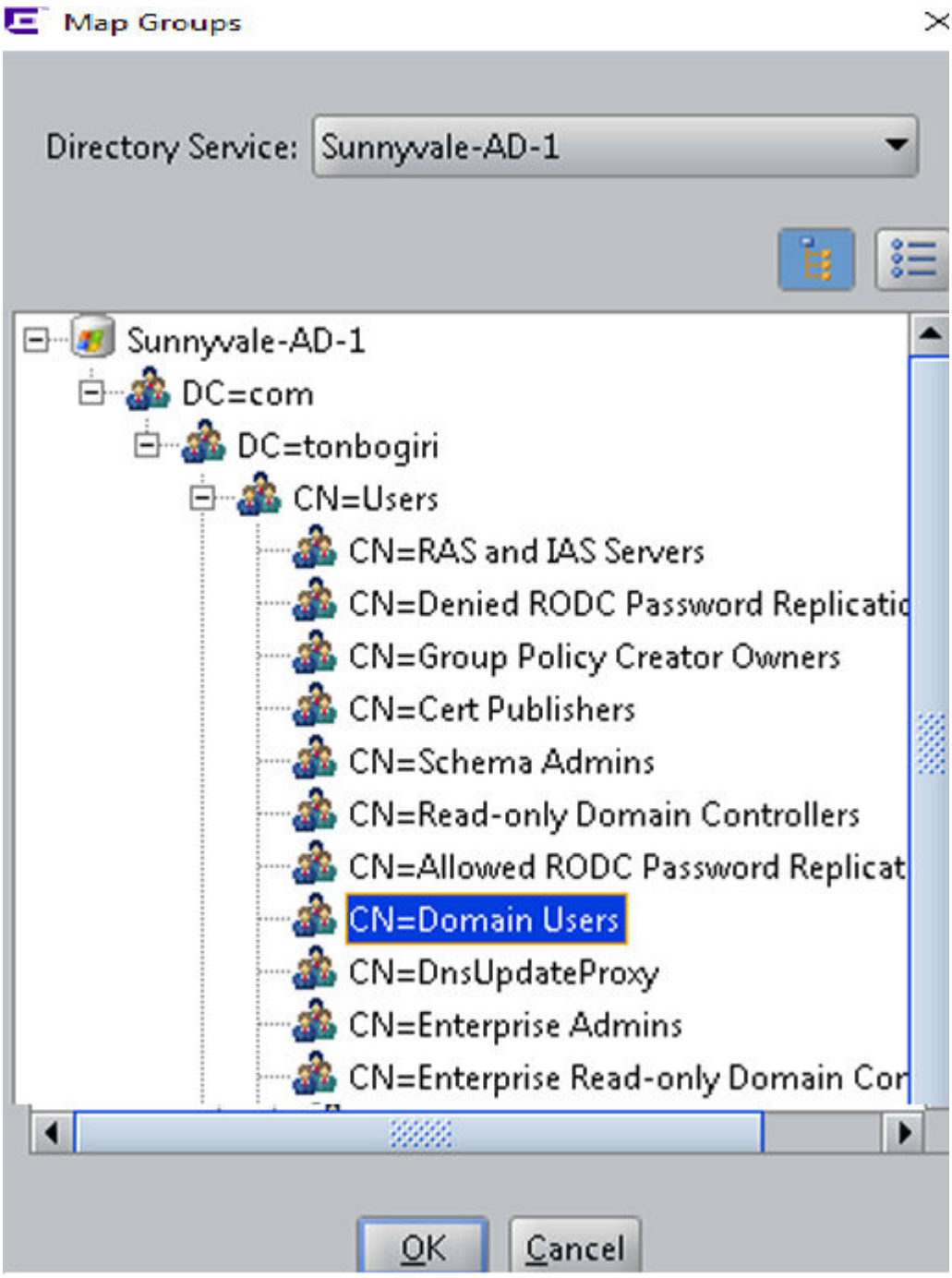


4. In the Virtual Groups list, select the group name you just created. At the bottom of the Virtual Group Details panel, click **Add**.
5. In the Map Groups window, click in the Directory Service drop-down list and select the name of your Directory Service.



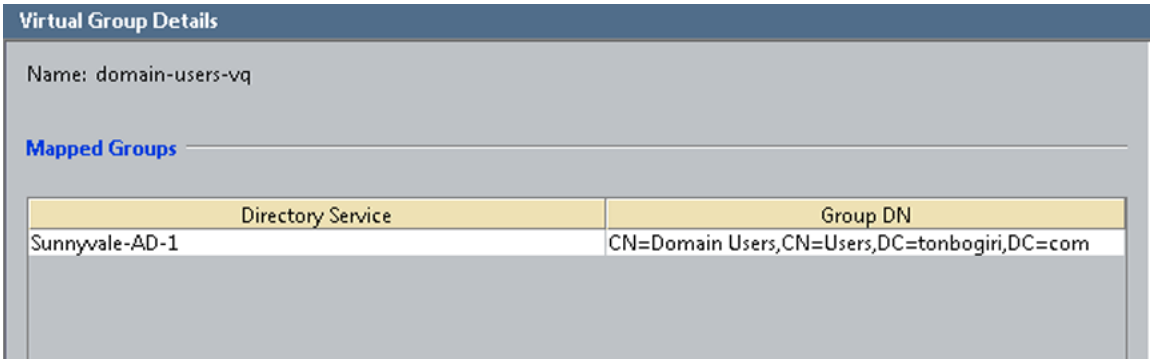
6. Use the tree list to find the group (AD container) you wish to map. In this example, the Active Directory group is “CN=Domain Users”. This enables us to create an Ignition Server authorization rule that grants access to any user who is a member of *Domain Users*.

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



7. Click **OK**.

   The new mapping is displayed in the Mapped Groups list.



Now that you have created 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 Creating Authenticators on page 82.

Creating 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 apply your authentication, authorization, and provisioning policies to it.

Create an authenticator for each switch and/or access point that authenticates against Ignition Server.

Procedure

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

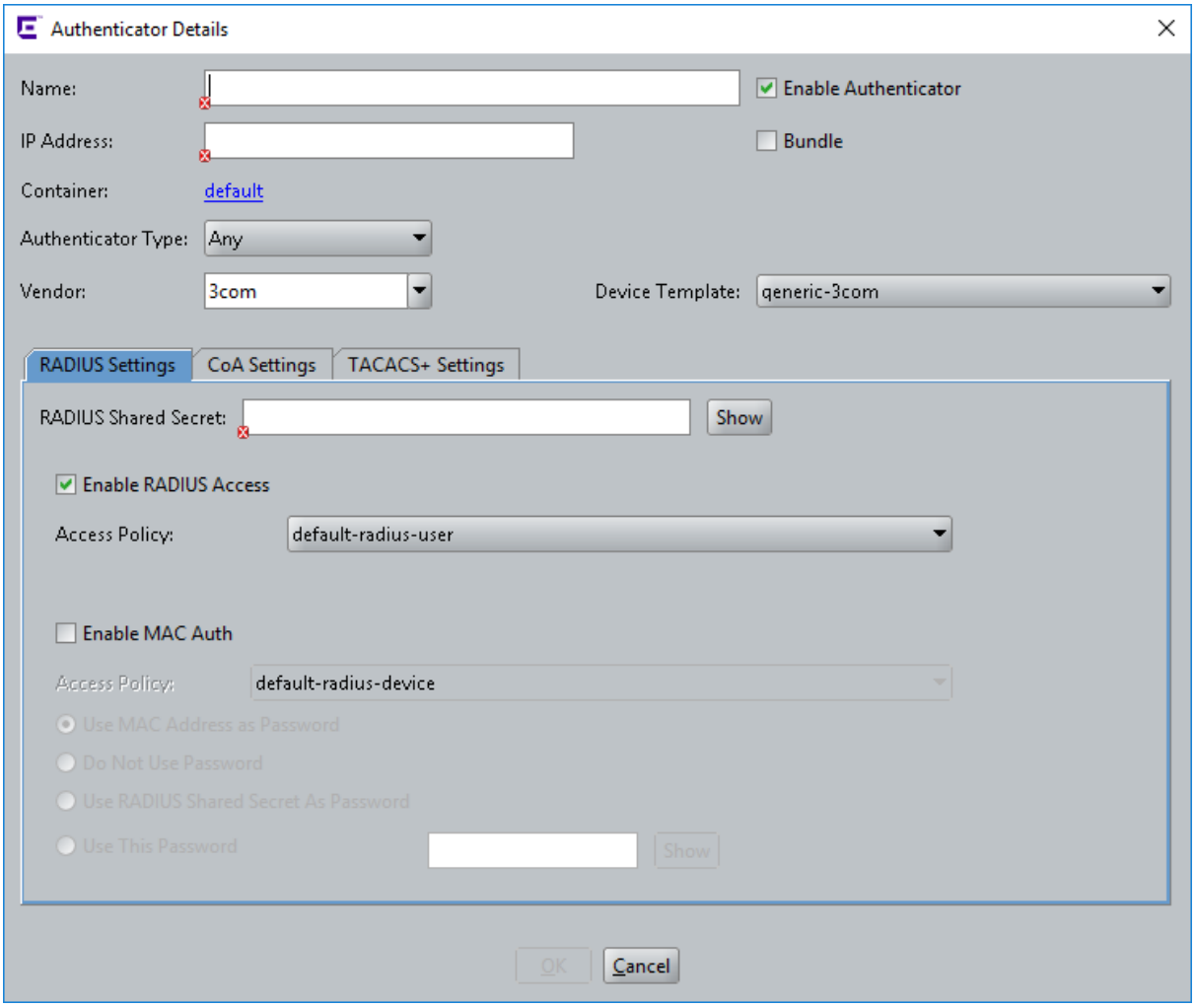
	Authenticator 1	Authenticator 2	Authenticator 3
Authenticator Name	_____	_____	Choose a name to identify the authenticator. This name is used to refer to the authenticator within Ignition Server.
IP Address	_____	_____	IP address of authenticator.
Subnet Mask	_____	_____	*Optional*: If you wish to create one record (a “bundle”) to represent a

Table continues…

	Authenticator 1	Authenticator 2	Authenticator 3
			number of authenticators, this field holds the mask describing the subnet in which all authenticators are treated as one authenticator.
Container	_____	_____	Optional: If you are grouping your authenticators using Ignition Server “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 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 Configuration tree, click **Site Configuration**.
3. Click the **Authenticator** link in the main panel.

   The Authenticator Details window is displayed.



4. Do the following:
   - Fill in the fields using the information you collected in Step 1.
   - Make sure the **Enable RADIUS Access** checkbox is selected.
   - For **Access Policy**, choose the name of the policy you created in Step 3 on page 42.

   For an explanation of the rest of the fields, see *Identity Engines Ignition Server Configuration document*.
5. Click **Save** to save the settings.

Next steps

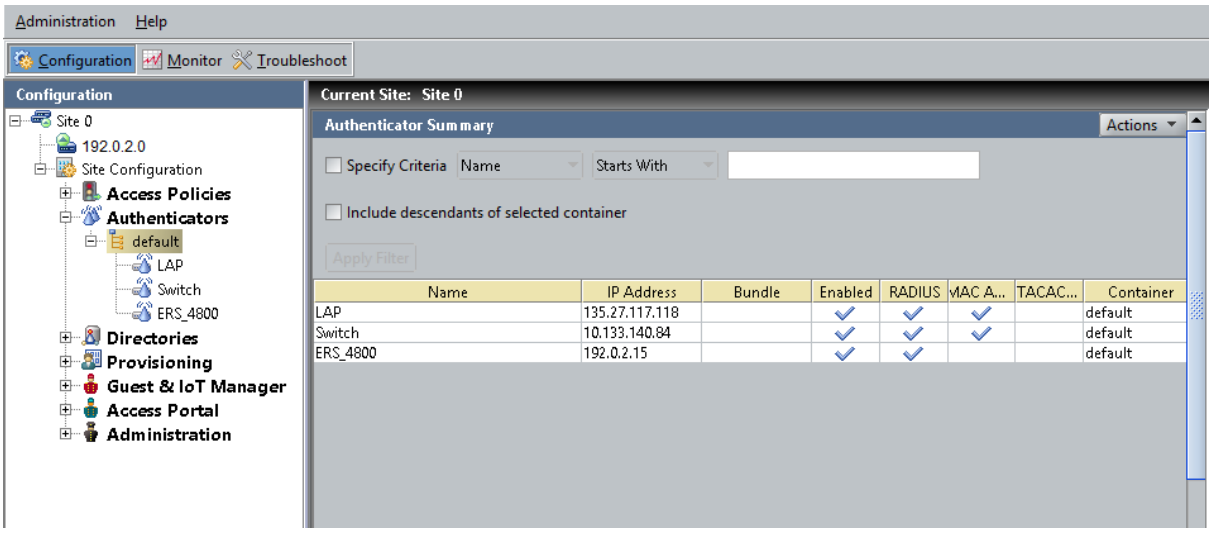
Set your credential verification rules as shown in Setting your Authentication Policy on page 85.

Editing Authenticators

Use this procedure to edit authenticators.

Procedure

1. In Dashboard's Configuration tree, expand **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.

Setting your Authentication Policy

You created an empty access policy in the section Creating a RADIUS Access Policy on page 41. In this section and the ones that follow, use the Access Policy panel to add an authentication policy and add the various rules that make up your access policy.

An 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. The access policy controls whether and how that user is permitted to use the network, as well as how the authentication transaction is to be done.

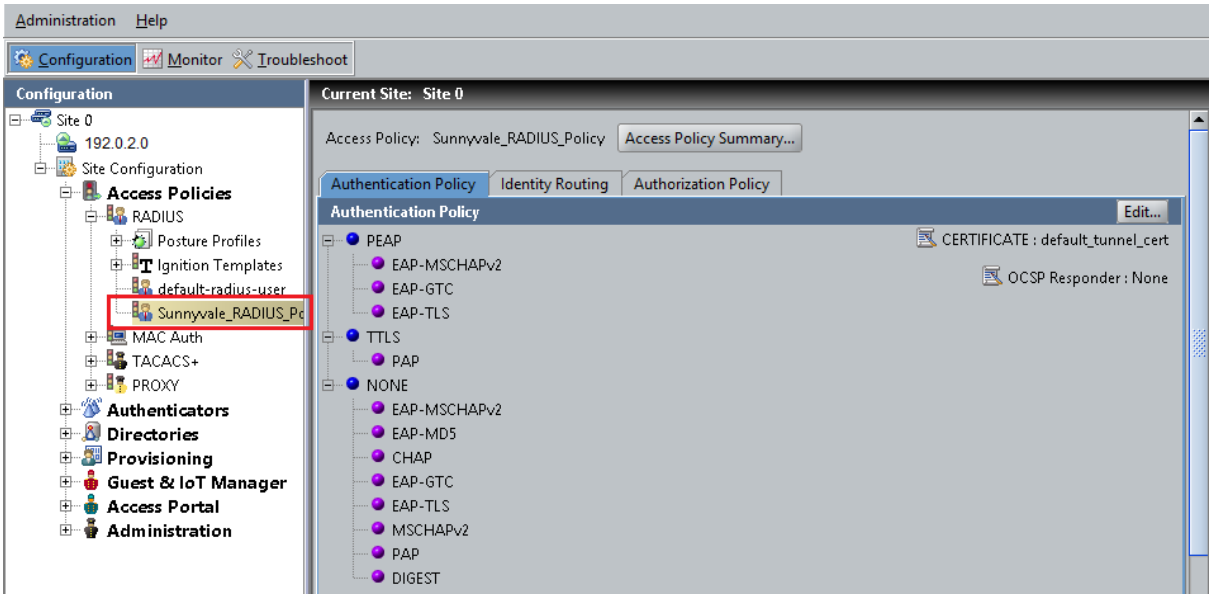
In your Ignition Server system you may define many access policies for the many different segments of your organization, but assign only *one* RADIUS access policy to each authenticator. This means that all users connecting through that authenticator are governed by that RADIUS access policy. You may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

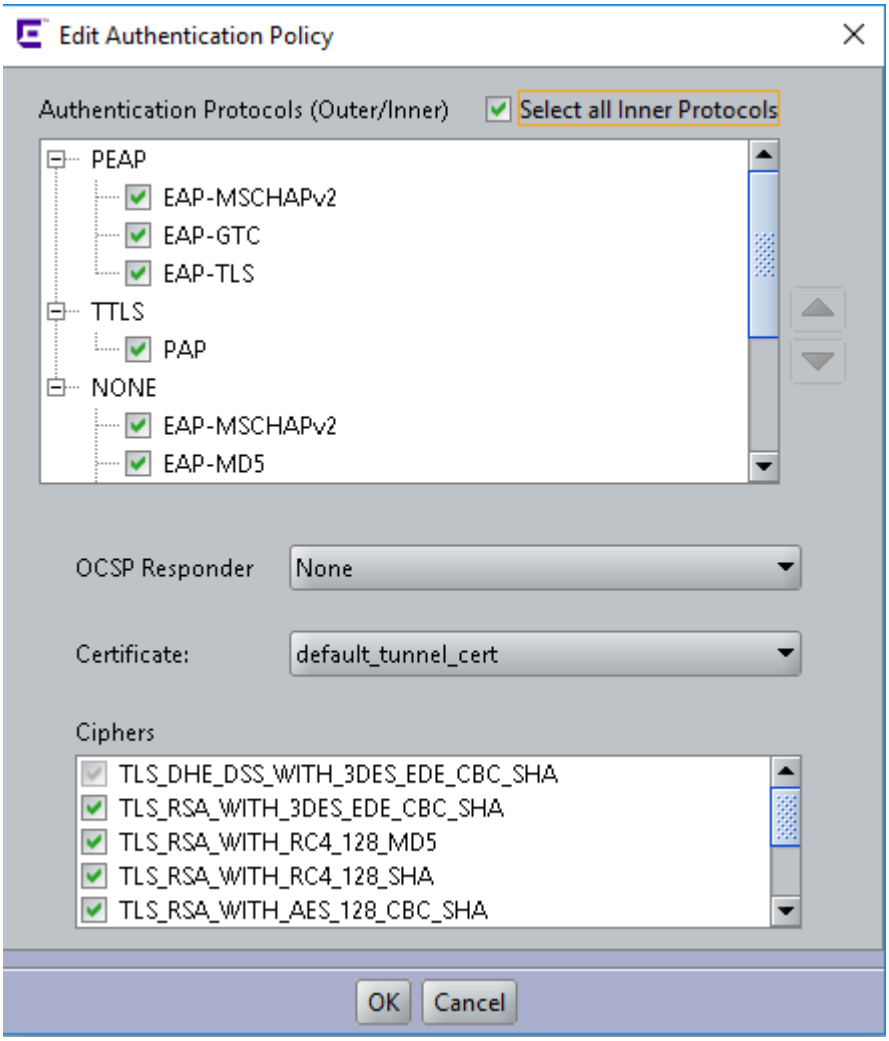
supplicant and the Ignition Server appliance, and the inner tunnel secures the connection from the supplicant to the user store if an external user store (like AD) is used.

Procedure

1. In the Dashboard **Configuration** tree, expand **Site Configuration** > **Access Policies** > **RADIUS**, and click the policy name.



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, select the **EAP-MSCHAPv2** checkbox.
   - In the **NONE** section, select the **PAP** checkbox.



If you want to verify that an authentication protocol is compatible with your data store. For more information, see the section, “Supported Authentication Types” in *Identity Engines Ignition Server Configuration document*.

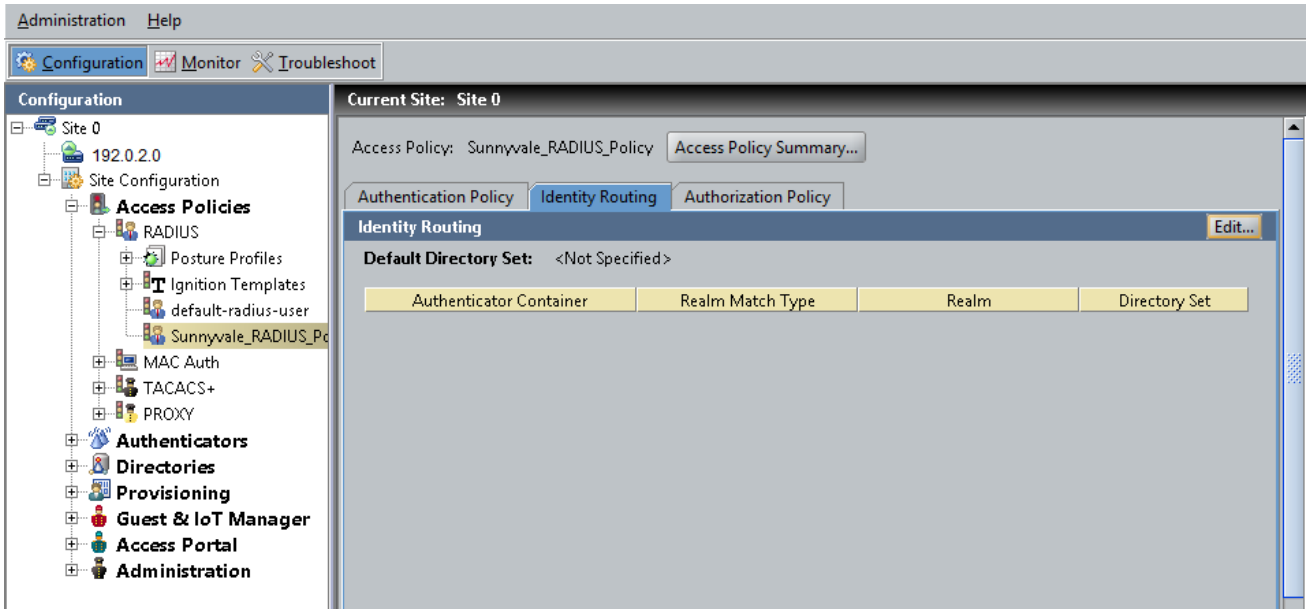
You can sort the order in which Ignition Server attempts to apply the authentication types to an authentication request by clicking the name of the authentication type or tunnel type and clicking the up/down arrows to sort the list.

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

4. Click **Save**.

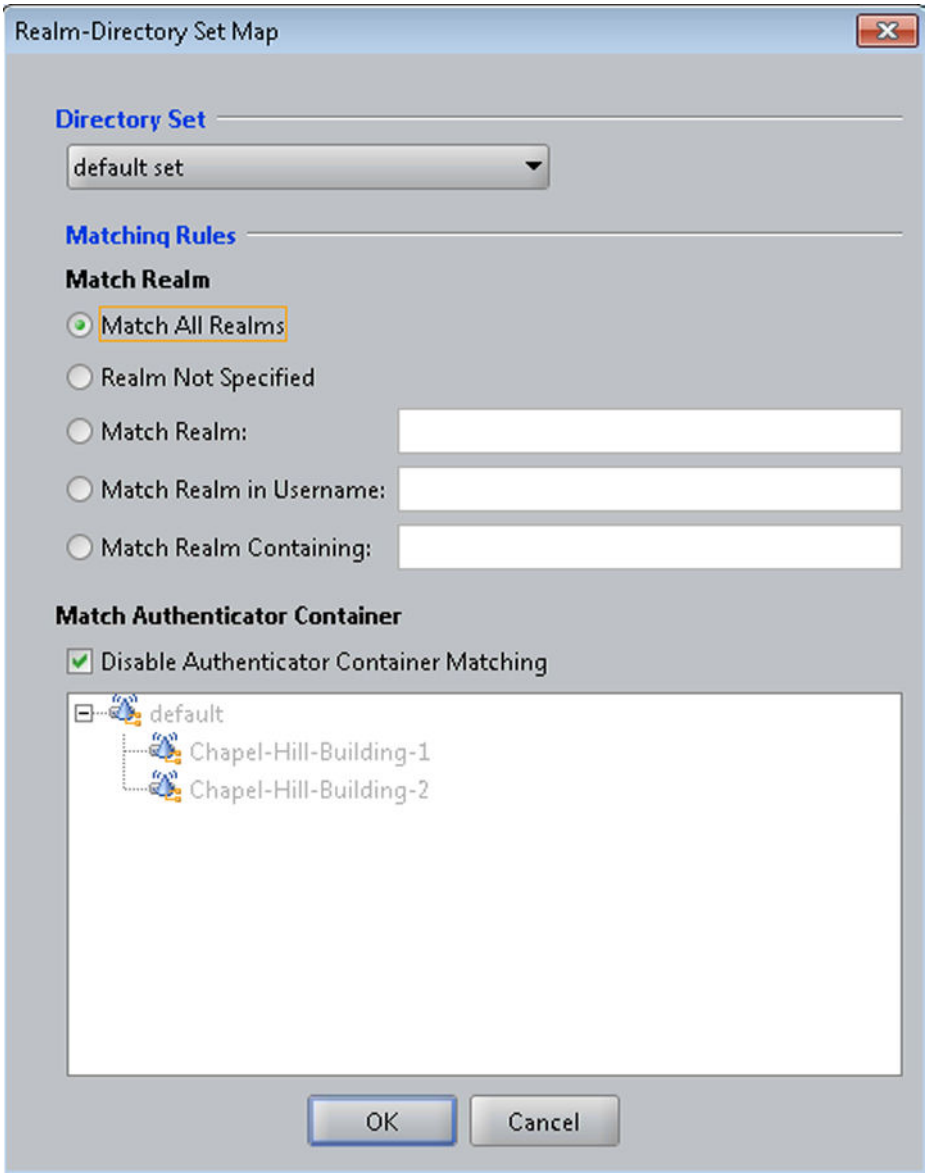
Setting your Identity Routing Policy

The next policy to be set in your access policy is the identity routing policy. This is the prescribed sequence for searching in a set of user stores to find a user account when attempting authentication. This example sets a catch-all policy that uses a single directory set for all users.



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 list, select the directory set you created in Step 3 on page 76. If you are using the example names, this set is called *Sunnyvale-User-Lookup*.



b. Select the **Match All Realms** checkbox.

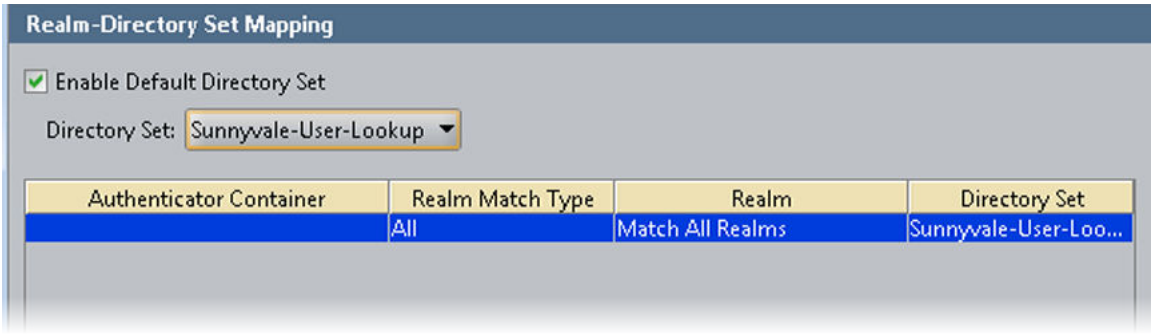
c. Select the **Disable Authenticator Container Matching** checkbox.

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**, use the down arrow control 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, choose *Sunnyvale-User-Lookup*.

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



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

Setting 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 *Administering Identity Engines Ignition Server*, 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*. For more information, see Creating an Authorization Policy — Example for Embedded Store Users on page 90.
- If your user accounts reside in an *AD user store*. For more information, see Creating an Authorization Policy — Example for AD Users on page 93.

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 (For more information, see Setting your Identity Routing Policy on page 88).

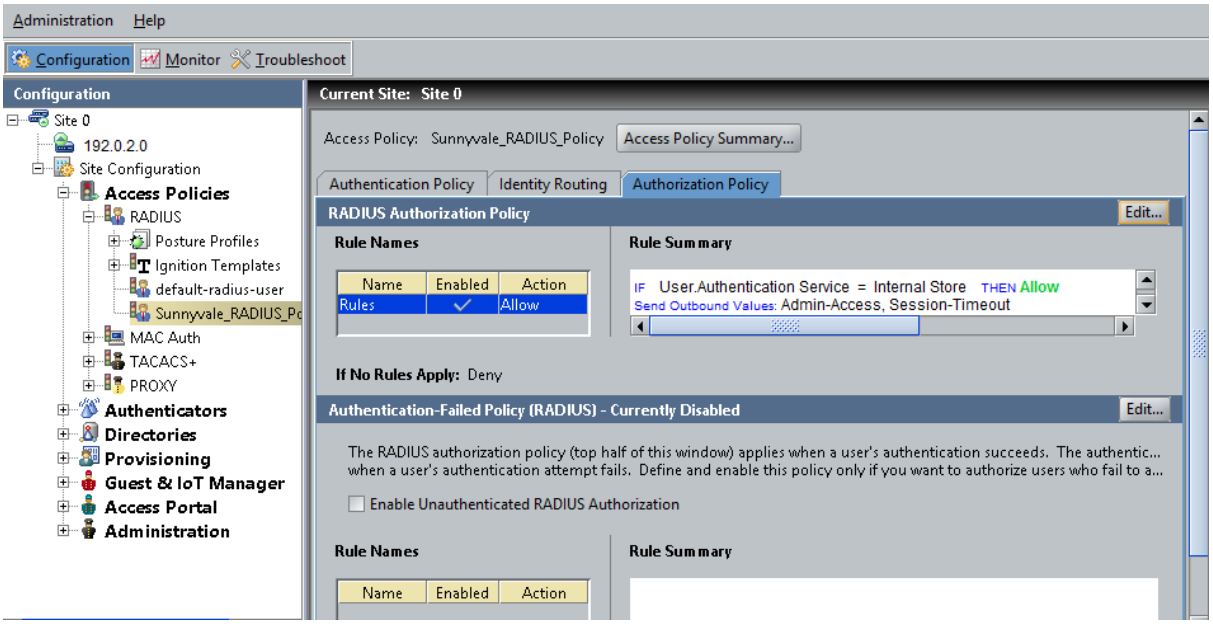
Creating an Authorization Policy — Example for Embedded Store Users

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

This section describes 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.

Procedure

1. In the Dashboard **Configuration** tree, expand **Site Configuration** > **Access Policies** > **RADIUS**, click the policy name, and click the **Authorization Policy** tab.

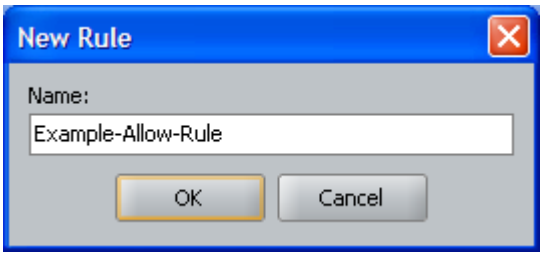


2. The top half of the **Authorization Policy** tab contains your RADIUS authorization policy. Click the top **Edit** button to edit it.

   The Edit Authorization Policy window is displayed.

3. In the **Rules** section, click **Add**.

   The New Rule window is displayed, where you name the new rule.



4. Type *Example-Allow-Rule* and click **OK**.

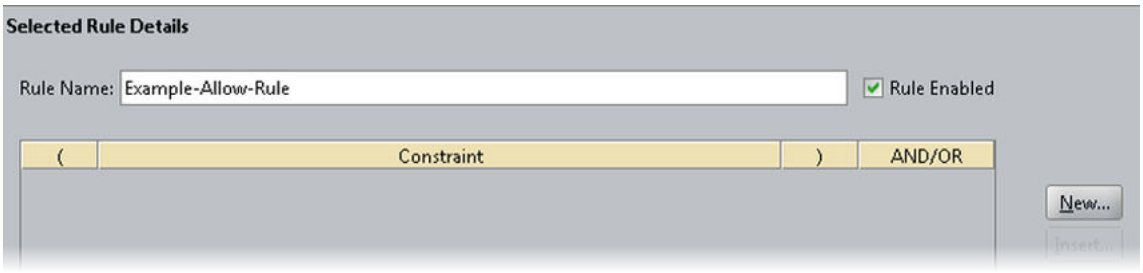
   The New Rule window closes. In the Edit Authorization Policy window, the rule you just created is displayed in the **Rules** list that occupies the left side of the window.

   The **Rules** list 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.

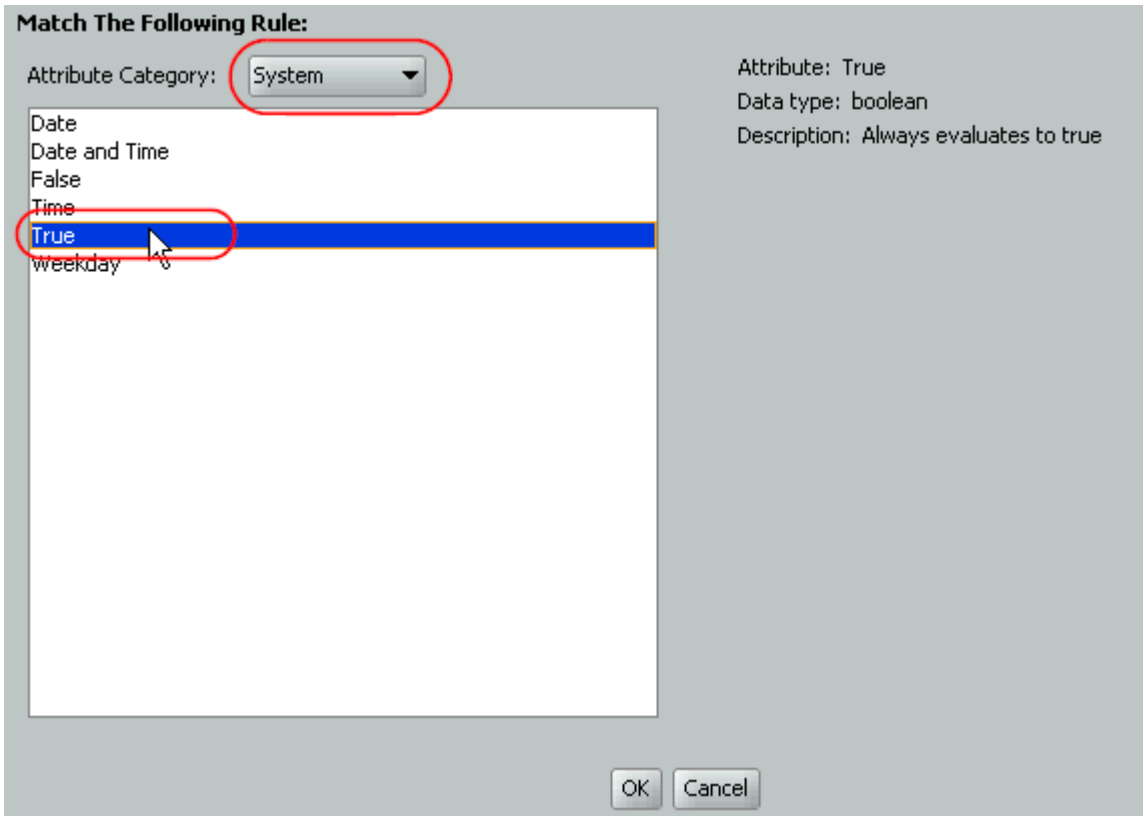
5. In the **Rules** list, click the rule you just created.

   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**.

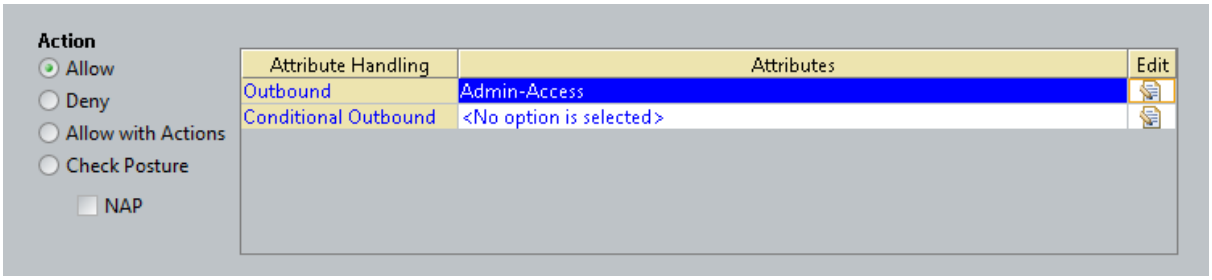


7. In the Constraint Details window, do the following. The steps below create a rule that always evaluates to true. Such a rule is not practical in a production system, but it demonstrates rule setting in this exercise. Bear in mind that, even if you have an *always-allow* rule like this, the authenticating user must still *authenticate successfully* and *pass all* DENY *rules* before triggering 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**.



   - 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.



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.

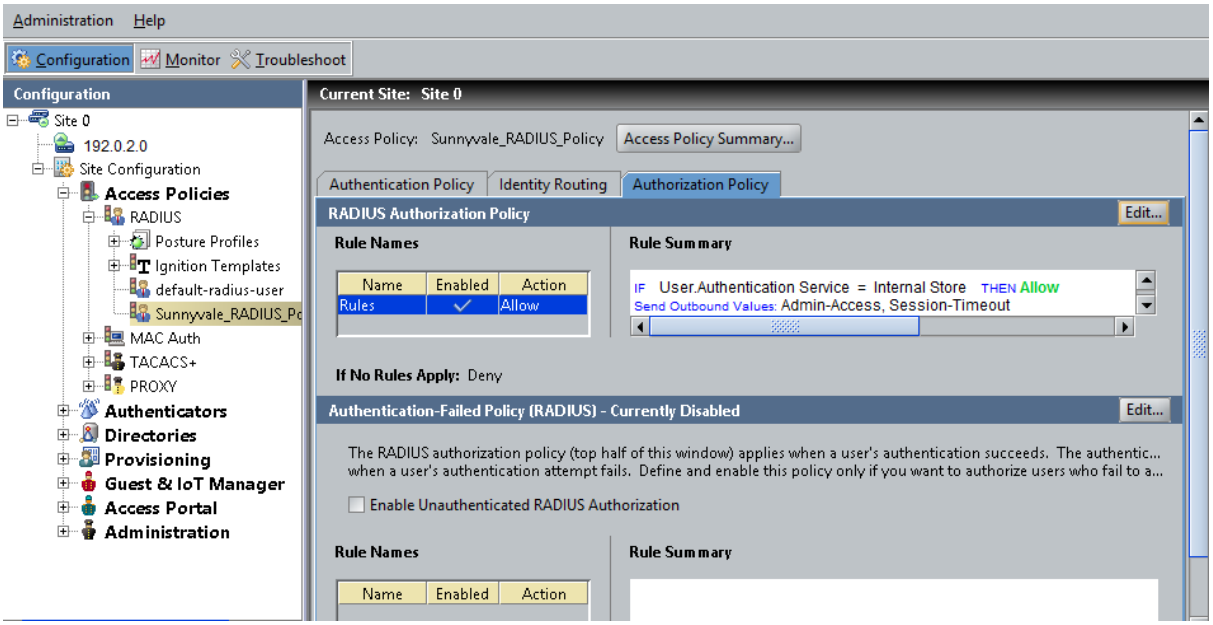
Creating an Authorization Policy — Example for AD Users

You can create a policy that authorizes access for any user who has a user account on the AD domain (that is, if the user has an account in the Domain Users group). Upon authentication, the user is provisioned based on their virtual group name. Note that the virtual group may map to a single AD workgroup or multiple workgroups on one or more domain controllers.

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

Procedure

1. In the Dashboard **Configuration** tree, expand **Site Configuration** > **Access Policies** > **RADIUS**, click the policy name, and click the **Authorization Policy** tab. Click **Edit** 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 is displayed.

3. In the **Rules** section, in the lower left part of the window, click **Add**.

   The New Rule window is displayed, where you name the new rule.

4. Type `CheckHasADAccount` and click **OK**.

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

   The **Rules** list shows the rule sequence that forms your authorization policy. 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**.

   For more information on how Ignition Server evaluates sets of rules and constraints, see *Identity Engines Ignition Server Configuration document*.

6. In the Constraint Details window, create your constraint as follows:

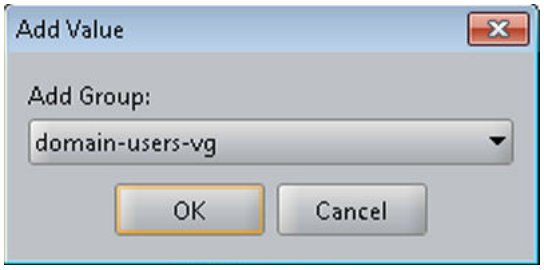
   a. In the drop-down list at the top of Constraint Details window, select the Attribute Category, *User*. The list just below this displays the names of attributes of type *User*.

   b. In the list, select the attribute named *group-member*.

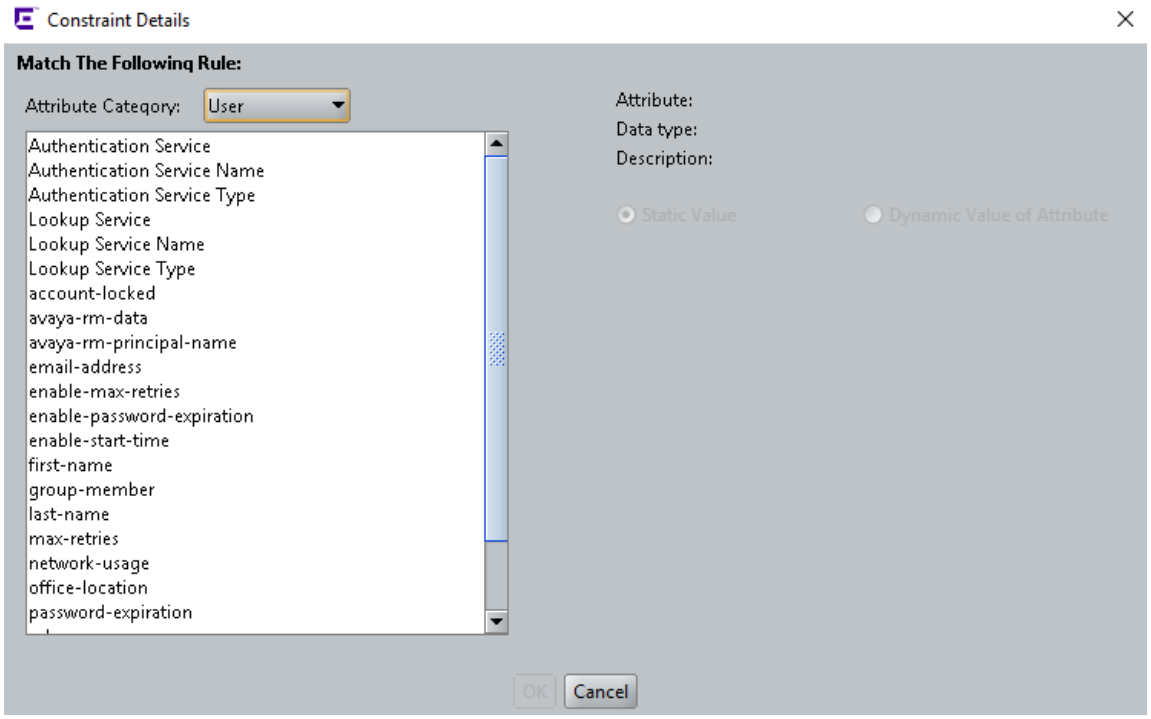
   c. In the drop-down list of the Phrase section, select **Contains Any** and click the **Static Value** radio button.

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

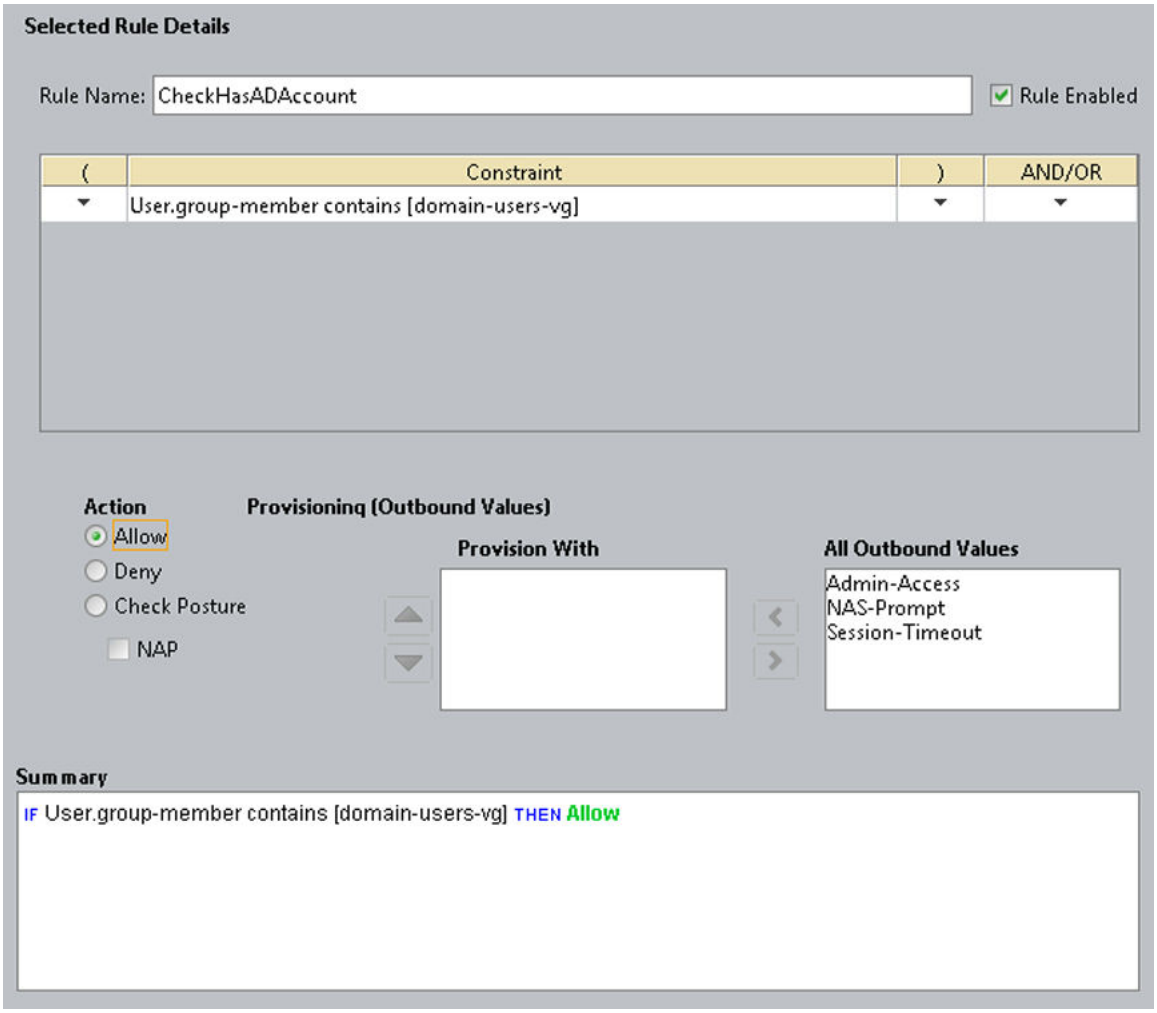


f. Click **OK** to close the Constraint Details window and return to the Edit Authorization Policy window.



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 checks 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 **OK** to close the Edit Authorization Policy window and return to the Policy Management window.

Testing your Configuration

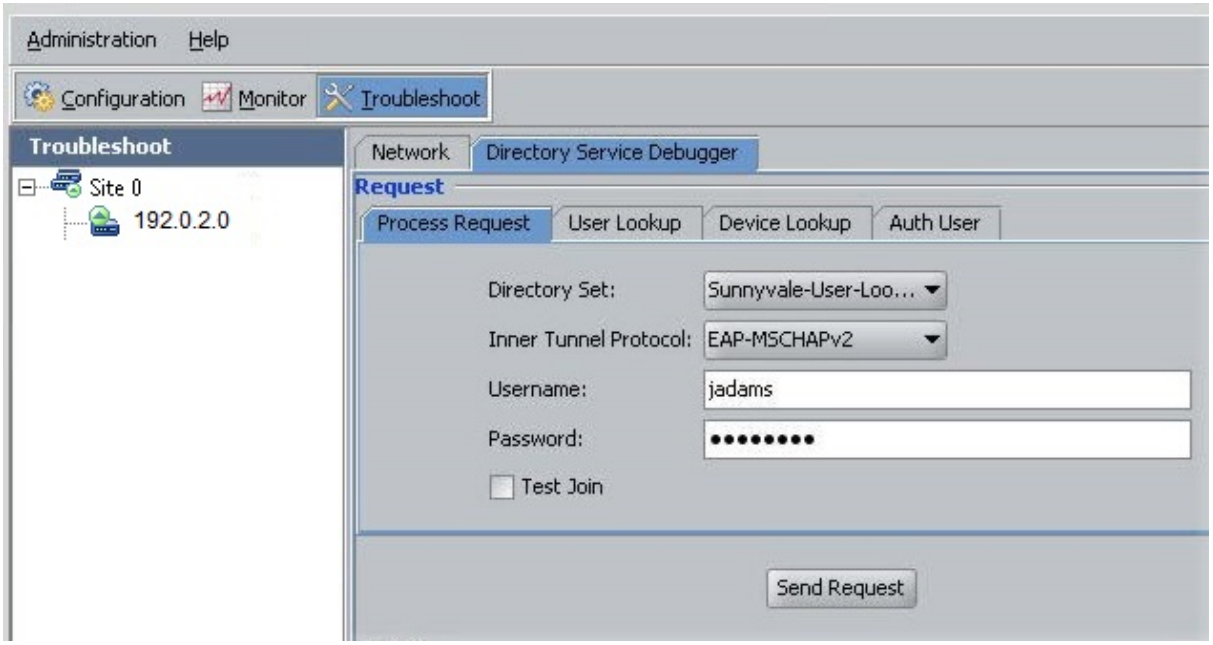
This section describes how to test your configuration by Checking User Lookup and Authentication on page 96 and Using NTRadPing as a Test Authenticator on page 97.

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.



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 is displayed in the **Results** panel.

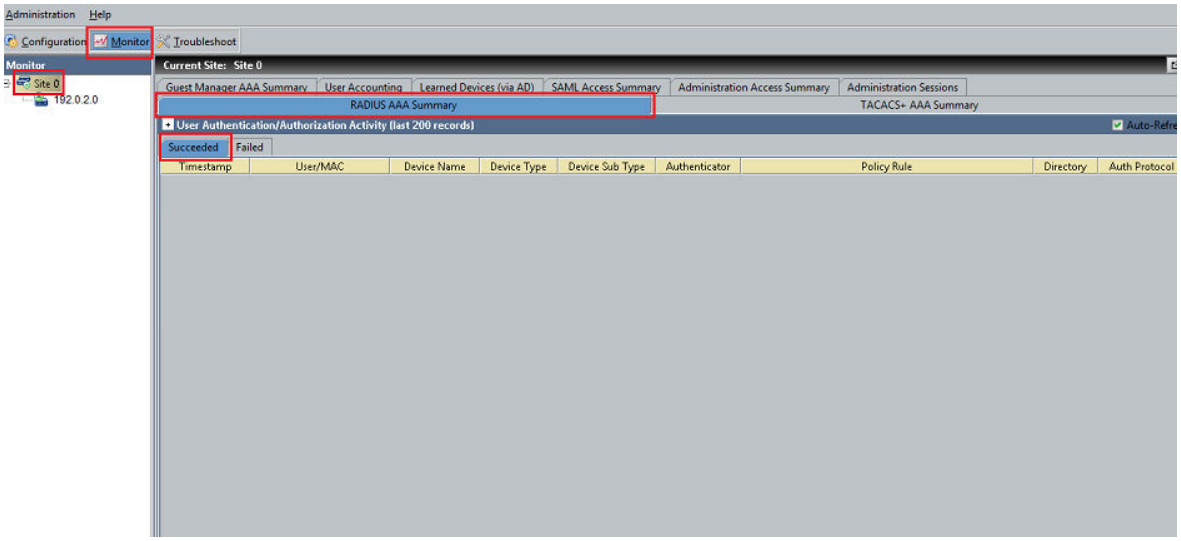
Using NTRadPing as a Test Authenticator

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 the Dashboard's Configuration 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 enabled 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 information, click the record and click the **Access Record Details** link near the bottom of the page.