Integrating iDRAC7 with Active Directory

Configuring iDRAC for use with Active Directory Extended Schema ........................................... 29
   Test your Extended Schema configuration .............................................................................. 31
   Creating an Active Directory user with customized iDRAC privileges .................................... 33
Summary ........................................................................................................................................ 36
Benefits of integrating iDRAC7 with Microsoft Active Directory

Using your integrated Dell Remote Access Controller v7 (iDRAC7) with Microsoft Active Directory simplifies user account and privilege management. It eliminates configuring each individual user and their associated privileges on every iDRAC. Once configured, users provide their Active Directory credentials to authenticate to all iDRACs. You can use these credentials to log into the iDRAC GUI, SSH and Telnet consoles, and for running racadm, and WSMAN commands from the CLI.

**Note:** You must have an Enterprise License installed on your iDRAC7 to use Active Directory authentication. See [Confirming the iDRAC7 has an Enterprise License Installed](#) for more information.

Standard Schema versus Extended Schema

There are two options when integrating your iDRAC: Standard Schema or Extended Schema, with different advantages and requirements for each.

With either Standard or Extended Schema, existing Active Directory you can easily assign users to groups that have predefined privilege levels for the iDRACs.

Standard Schema has the advantage of not having to extend the Active Directory schema. However, you must enter Active Directory group names and privileges on each iDRAC.

Extended Schema by definition requires an extension to the Active Directory schema, which is an irreversible process. However, this provides the additional benefit of only having to configure the Active Directory group names and privileges once for all iDRACs on the Domain Controller.

This document

Integrating iDRAC with Active Directory can be complex, and this document simplifies the process with step-by-step instructions. There are multiple ways to achieve the same results and steps vary with different operating systems and in different network environments.

This document covers a standard schema setup, then adds extended schema. This lets you get hands-on experience with each option and determine which method is best for you. Once set up, you can switch from either schema method using the same Domain Controller with minimal configuration changes.

It is strongly recommended that you do these steps in a test environment first. Then you can determine the level of integration that works best for you, along with the steps required to implement Active Directory in your environment.

This document assumes you have some experience working in Active Directory on a Domain Controller and are familiar with IP addressing, DNS, and DHCP.

For additional information on integrating iDRAC7 with Active Directory, see the *iDRAC7 User's Guide* on [www.support.dell.com](http://www.support.dell.com).

Confirming the iDRAC7 has an enterprise license installed

You must have an Enterprise License installed on your iDRAC7 to use Active Directory authentication.

To check the license you have:
Integrating iDRAC7 with Active Directory

1. Browse to https://<idrac_ip_address> and log into the iDRAC GUI of your system as an administrative user (default username is root, password is calvin.)

2. Go to the Overview > Server > Licenses page.

3. Expand the “+” in the left column of the license table to view the license (pictured below). If you have no “+” to expand, or if the license displayed is “Basic” or “Express”, you cannot use the Active Directory feature. However, you can quickly upgrade to an Enterprise License electronically by using the License Self-Service Portal (linked on the Licensing page) or by contacting your Dell Sales representative.

Figure 1. Viewing the license.

Dell test environment
To help you transfer the steps outlined in this document to your environment, the Dell test environment set up is as follows:

Systems Used in the Dell test environment

Integrating iDRAC7 with Active Directory

- **Managed System** - A Dell PowerEdge R720 with iDRAC7 and an Enterprise License installed.
- **Management Station** - A system running Windows 7 and Firefox 7. (Internet Explorer is also supported).

**Note:** See the Systems Management Tools and Documentation DVD version 7.0.0 or later, or www.support.dell.com, for the full list of supported PowerEdge Systems, Operating Systems, and Browsers.

**Additional Information about the Dell test environment**

- The Active Directory domain name is test.lab.
- The FQDN of the Domain Controller is ad2.test.lab and it has a static IP address of 172.23.199.28.
- DHCP is running on the network on a different server. It is being used to assign an IP address to the iDRAC. (DHCP is optional).
- The iDRAC has been assigned a dynamic IP address of 172.26.9.56.
- DNS and Certificate Services will be running on the Domain Controller (described in *Building the domain controller*).
- The Dell Systems Management Tools and Documentation DVD, version 7.0.0, is used.

**Building the domain controller**

All of the steps in this section take place on the server used as the *Domain Controller*.

- Install a supported Windows Server operating system, such as Windows Server 2008 Enterprise.
- Make sure the date, time, and time zone on the server are correct. This is critical for Active Directory authentication with iDRAC.
- Configure a static IP address (recommended since it also is the DNS server).
- If desired, change the Windows computer name of the Domain Controller before running the next steps.

**Promoting the server to a domain controller and installing DNS**

The steps that follow are from Windows Server 2008 Enterprise. Steps for other supported Windows Server operating systems are similar.

1. Promote the server to a Domain Controller. Click **Start > Run > dcpromo**.
2. In the *Active Directory Domain Services Installation Wizard*, click **Next**.
3. In the Operating System Compatibility page, click **Next**.

4. Select **Create a new domain in a new forest**, and then click **Next**.

5. Provide the **FQDN of the forest root domain** (for example, test.lab).

6. For both Forest & Domain functional levels, choose either **Windows Server 2003** or **Windows Server 2008**, and then click **Next** two times.

   If DNS is not already installed, you are prompted to install it. Accept the default options and install DNS.

7. Accept the default locations for the Database, Log files, and SYSVOL, and then click **Next**.

8. Assign a **Directory Services Restore Mode Administrator Password**, and then click **Next**.

9. In the **Summary** page, click **Next**.

10. Allow the installation to complete and reboot the system when prompted.

11. Your system is now a Domain Controller running DNS.

**Note:** If DHCP is not already running on your network, you can optionally install it on the Domain Controller at this time or use static IP addresses on your network.
Installing and configuring Active Directory Certificate Services

Installing Certificate Services as an Enterprise Root CA

1. Open Server Manager, and then click Roles > Add Roles, and then click Next.
2. Select Active Directory Certificate Services, and then click Next.
3. Click Next.
4. Make sure Certification Authority is checked, then click Next > Enterprise > Next > Root CA > Next > Create a New Private Key > Next.
5. Accept the defaults for CSP, key character length, and hash algorithm, and then click Next.
6. Accept the default CA name, and then click Next.
7. Select the default validity period, and then click Next.
8. Select the default database and log locations, and then click Next.
9. Click Install.

When installation is complete you should get an Installation Succeeded message similar to this:

**Figure 3.** Installation succeeded message screen.

![Add Roles Wizard](image-url)
Integrating iDRAC7 with Active Directory

Adding the certificates snap in to Microsoft Management Console

1. Click Start > Run > MMC > OK.
2. In the Console 1 window, click File > Add/Remove Snap-in > select Certificates > Add > select Computer Account > Next > Local Computer > Finish > OK.

It is recommended that you save Console1.msc to your Desktop at this point. You will use this console for other snap-ins later in this document.

Installing the CA certificate for Client Authentication to the Domain Controller

1. Open Console1, expand Certificates, expand Personal, click Certificates.
2. Right click Certificates, then click All Tasks > Request New Certificate.
3. In the Certificate Enrollment wizard, click Next.
4. Select Domain Controller, and click Enroll > Finish.
5. You will get the following success message:

   ![Certificate Enrollment](image)

   **Figure 4.** Certificate Enrollment success message.

The contents of your certificate folder should now look similar to the following, with the newly created certificate highlighted below.
Integrating iDRAC7 with Active Directory

Figure 5. Certificate folder contents.

Exporting the CA Certificate (You install this certificate on iDRAC later).

1. Locate the CA certificate. This is the certificate issued to your CA, (named test-AD2-CA in this example).
2. Right click the CA Certificate and select All Tasks > Export.
3. In the Certificate Export Wizard click Next > No, do not export the private key, and then click Next.
4. Select Base-64 encoded X.509 (.CER), and then click Next.
5. Browse to the desired path and give it a file name (For example, ad2.cer), and then click Next.

Figure 6. Completing the Certificate Export Wizard.
Integrating iDRAC7 with Active Directory

6. Click Finish.
7. View the success message and then click **OK**.

Creating iDRAC users and groups

1. In the left pane of **Server Manager**, expand **Roles > Active Directory Domain Services > Active Directory Users and Computers >** your domain name (**test.lab**).

2. In the **Users** container, create users that will be provided the three different iDRAC privilege levels. (Right click on **Users** and select **New > User**). For example, create three users and name them:
   - admin
   - operator
   - readonly

   **Note:** usernames must be an ASCII string of 1-256 bytes. White space and special characters (such as \, /, or @) cannot be used in the user name.

   • Assign each user a password and uncheck **User must change password at next logon** as each user is created.
   • In addition, in the **Users** container, create groups based on iDRAC privilege levels that the iDRAC users will belong to (Right click on **Users** and select **New > Group**). Keep the default group type of **Global, Security**. For example, create three groups and name them:
     - iDRACAdministrators
     - iDRACOperators
     - iDRACReadOnlyUsers

When complete, it should look something like this:
Integrating iDRAC7 with Active Directory

Assigning the users to their corresponding groups

1. Double click on the admin user, and then on the Member Of tab, click Add.
2. Under Enter the object names to select, type iDRAC (or part of the group name you used) > Check Names > select the iDRACAdministrators group > OK > OK > OK.
3. Repeat for the operator and readonly users. (Assign them to iDRACOperators and iDRACReadOnly groups respectively.)

Configure iDRAC for use with Active Directory Standard Schema

At the management station, in your Internet Explorer or Firefox web browser, browse to https://<idrac_ip_address> and log into the iDRAC GUI of your system as an administrative user (default username is root, password is calvin.)

Configure the iDRAC network settings

1. In the iDRAC GUI, go to iDRAC Settings > Network > Common Settings.
   - Register DRAC on DNS (unchecked, optional)
   - DNS DRAC name (optional), the default is idrac<-Dell service tag #>
   - Auto config domain name (not checked). (Only check this if your DCHP server will provide the domain name).
Integrating iDRAC7 with Active Directory

- **Static DNS Domain Name** - specify the FQDN of your domain, for example `test.lab`, if the box above was not checked.
- Click **Apply**.

2. On the same page under **IPv4 Settings**:
   - Select **Enable IPv4**.
   - **DHCP enabled** - (optional, depending on your network configuration). This box is checked for the Dell test environment.
   - **Use DHCP to obtain DNS server address** - only check this box if you are using a DHCP server and it is configured to point to the Active Directory Server running DNS. This is not checked for the Dell test environment.
   - **Static Preferred DNS Server** - Specify the IP address of your domain controller running DNS if the box above was left unchecked. For the Dell test environment, it is 172.23.199.28.
   - **Alternate DNS server** - optional, can leave at 0.0.0.0.
   - Click **Apply**.

This is how the iDRAC Network Settings look for the Dell test environment set up:
Configure the iDRAC Directory Services settings

1. Go to iDRAC Settings > User Authentication > Directory Services (Reminder that an Enterprise License is required to get the Directory Services option).
   - Select Microsoft Active Directory, and then click Apply.
   - In the Active Directory Configuration and Management page, scroll down to bottom of page and click Configure Active Directory.
   - Select Enable Certificate Validation.
   - Upload the Directory Service CA Certificate - For this, you upload the certificate file generated earlier (named ad2.cer in this example) to iDRAC. First, copy this file from the Domain Controller to your management station. Second, in the iDRAC Web GUI next
Integrating iDRAC7 with Active Directory

To Upload Directory Service CA Certificate, click Browse, point to the file, and click Upload.

You should get a message similar to the following:

Figure 9. Upload complete.

If you get a message indicating the Certificate is not valid, there may be a date/time discrepancy between your CA and the iDRAC. Make sure the date and time on the iDRAC match the date and time on the CA (the Domain Controller in this document) and try again.

Note: If the certificate was issued from a newly created CA, it may continue to be reported as not valid even though the iDRAC and CA server dates and times match. This is because the iDRAC treats its time as UTC (Coordinated Universal Time). For example, if your CA server was created today at 2:00 pm Central Standard Time, the iDRAC views this as 2:00 pm UTC, a difference of 6 hours. As a result, the ‘valid from’ timestamp on the certificate is not considered valid by the iDRAC until 8:00 pm on the day the CA was created. You can work around this by temporarily moving the time on the Managed System containing the iDRAC ahead by the appropriate amount for your time zone and resetting the iDRAC, or by simply waiting until the time has passed. Dell is aware of this issue and is developing a fix for a later release.

2. After you receive the Upload complete message pictured above, click OK.
3. Click Next.
4. Select Enable Active Directory.
5. Clear Enable Single Sign-on.
6. User Domain Name. Click Add and enter the FQDN of your domain. For example, test.lab, and click OK.
7. Select Specify Domain Controller Addresses and enter the FQDN of your Domain Controller for Domain Controller Server Address 1 (For example, ad2.test.lab).
8. Click Next.
10. Click Next.
11. Select Specify Global Catalog Server Addresses and enter the FQDN of your Domain Controller for Global Catalog Server Address 1 (For example, ad2.test.lab).
12. Click Role Group 1.
   - For the Group Name, enter iDRACAdministrators (Note: all group names must be an exact match to the group names you created earlier in Active Directory).
Integrating iDRAC7 with Active Directory

- **Group Domain** - enter your domain name. For example, test.lab.
- **Role Group Privilege Level** - Select Administrator from the drop down box. Note that all nine of the privilege check boxes are checked. Even though these privileges can be customized, it is recommended that you keep the default boxes checked for the Administrator and Read Only users. "Operator" is the correct user level to make customized privilege selections.

  - Click **Apply**.

13. Click **Role Group 2**.

- **Group Name** - iDRACOperators
- **Group Domain** - test.lab for example
- **Privilege Level** - Select Operator from the drop-down list. Note that seven of the nine privilege boxes are checked. This is where customized privileges (if any) should be made by checking/unchecking the appropriate boxes as desired.

  - Click **Apply**.

14. Click **Role Group 3**.

- **Group Name** - iDRACReadOnlyUsers
- **Group Domain** - test.lab for example
- **Privilege Level** - Select Read Only from the drop-down list.

  - Click **Apply**
  - Click **Finish**. You are taken to a summary page that looks similar to this:
Test your Standard Schema configuration

1. Click the **Test Settings** button in the lower right part of the screen.
2. In the **Test User Name** text box, type your administrative user in username@domain.com format, for example, admin@test.lab.
3. In the **Test User Password** text box, type the user’s password for the domain.
4. Click **Start Test**.
5. At the top of the results page, all tests must pass (including Certificate Validation) or be marked Not Applicable/Not Configured.
6. The Test Log at bottom of page should have no errors and list all 9 privileges in the Cumulative privileges gained section as shown below.

**Figure 11.** Administrative User Test Results.

![Administrative User Test Results](image)

You can repeat the test with the other users you've created. The screenshot below shows the result from the read-only user. Note that the only privilege listed is Login which is the correct behavior for this user.
Active Directory login syntax options

Now that you have Active Directory authentication functional with your iDRAC, you need to know the different methods for authenticating as an active directory user. All of the iDRAC interfaces (GUI, racadm, WSMAN, SSH, and Telnet) accept the following domain-username formats:

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:username@domain.com">username@domain.com</a></td>
<td><a href="mailto:admin@test.lab">admin@test.lab</a></td>
</tr>
<tr>
<td>domain.com/username</td>
<td>test.lab/admin</td>
</tr>
<tr>
<td>domain.com\username</td>
<td>test.lab\admin</td>
</tr>
</tbody>
</table>

Note that the domain name must be fully qualified. For example, test/admin does not work; it must be test.lab/admin.

The login syntax is the same regardless of the schema option (standard or extended) used.
**Authentication examples**

For the following examples, the IP address of the iDRAC is 172.26.9.56. The domain is test.lab, and the user is admin with a password of Dell1234.

**Example Racadm Command using Active Directory credentials**

```
racadm -r 172.26.9.56 -u test.lab\admin -p Dell1234 getsysinfo
```

**Example WSMAN (WinRM) Command using Active Directory credentials**

```
```

**Example SSH login using Active Directory credentials**

![SSH login](image)

Figure 13. SSH login
iDRAC GUI login examples using Active Directory credentials

There is one additional option when logging into the iDRAC GUI. You can select the domain from the drop-down list and enter only the username and password in the boxes provided as shown below:

Figure 14. iDRAC GUI login option 1.

Or you can use one of the formats provided for the user name as long as you leave the Domain set to *This iDRAC* as follows:
Integrating iDRAC7 with Active Directory

Figure 15.  iDRAC GUI login option 2.

Configuring the domain controller for use with Active Directory

Extended Schema

This section builds on the standard schema setup illustrated above. It uses the users, groups, certificates, and some of the iDRAC settings made above. Keep in mind that schema extensions cannot be undone. If you are using a virtual server it is a good idea to take a snapshot of the image before proceeding.

Extending the schema

1. Obtain the Dell Systems Management Tools and Documentation DVD, version 7.0.0 or later, provided with your Dell PowerEdge system.
2. Log in to your Domain Controller as an Administrator.
3. Run the Schema Extender from the DVD:
   DVD_DRIVE:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema_Extender.exe
4. If a Security Warning message is displayed, click Run.
5. A Welcome Message is displayed, click Next.
6. A Warning Message is displayed indicating Schema Extensions cannot be undone, click Next.
7. Accept the default option to use current credentials, and then click Next.
Integrating iDRAC7 with Active Directory

8. The schema will be extended and you get a message similar to the following when complete:

![Schema Extension Complete](image)

---

9. Click Finish.

Optional - View the changes made to the Active Directory Schema

If you would like to see the changes made by extending the schema, you need to install the Microsoft Active Directory Schema snap in. You can do so as follows:

1. At the **command prompt**, type the following command, and then press **ENTER**:

    ```
    regsvr32 schmmgmt.dll
    ```

2. A message indicates that the command succeeded. Click **OK**.

3. Open your saved **Console1.msc** (or create a new one by running mmc).

4. Click **File** > **Add/Remove Snap In**.

5. Select **Active Directory Schema**, click **Add**, then **OK**.

You can now view the changes as follows:

6. Expand **Active Directory Schema** and expand **Classes**. In the right pane, you can locate the added classes prefixed with “dell”.

---
Integrating iDRAC7 with Active Directory

7. Under Active Directory Schema, click the Attributes folder. In the right pane, you can locate the added attributes prefixed with "dell".

**Install the Dell Extension to the Active Directory Users and Computers Snap-In for 32-bit Windows**

**Note:** For Domain Controllers running 64-bit windows see the next section.

If your Domain Controller is running a 32-bit version of Windows, install the Dell extension to the Active Directory Users and Computers Snap-In as follows:

1. Run **Autorun.exe** from the root of the Systems Management Tools and Documentation DVD.
2. If a Security Warning message is displayed, click Run.
3. Select **Install Active Directory Snap-In Utility**, and then click Install.

**Figure 17. Installing the 32-bit version.**

![Dell OpenManage Install](image)

**Available options**
- Dell OpenManage Server Administrator
  - (Standalone Server Management)
- Tools
  - Active Directory Snap-In Utility
- BMC Utilities
- DRAC Tools

**Dell OpenManage Power Center**

**Documentation**

View **Readme**

**Note:** This is a bootable DVD. Boot from this DVD to install an operating system or to configure your system settings.

| Install | Cancel |

**Note:** If you are using a Remote Desktop connection to connect to your Domain Controller and get an error that installation is not permitted from Remote Desktop, map a drive letter to the DVD rather than using a UNC share name and try again.

4. Click **Next**.
Integrating iDRAC7 with Active Directory

5. Accept the License agreement, and then click Next.
6. Click Install.
7. A success message is displayed when complete. Click Finish.

Install the Dell Extension to the Active Directory Users and Computers Snap-In for 64-bit Windows

**Note:** For Domain Controllers running 32-bit Windows see the preceding section.

If your Domain Controller is running a 64-bit version of Windows, install the Dell extension to the Active Directory Users and Computers Snap-In as follows.

1. Obtain the Systems Management Tools and Documentation DVD and run:
   
   DVD_DRIVE:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64\support\vcredist.exe (This is the Visual C++ redistributable package).

   DVD_DRIVE:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64\sample_install_activedirectory_snapins_64bit.bat

Install the Active Directory Users and Computers Snap-In to MMC

**Note:** The Dell Active Directory Snap-in extension is not fully functional in the Server Manager console. For full functionality use Microsoft Management Console per the following steps.

Use your saved Console1.msc file or create a new console by running mmc.

Add the Active Directory Users and Computers Snap-In to your console as follows:

1. Click File > Add/Remove Snap In.
2. Select Active Directory Users and Computers, click Add, then OK.
3. Expand Active Directory Users and Computers > expand the domain name (test.lab). Note that there is a new container named Dell containing six iDRAC objects. There are three Association objects (Admin, Guest, and Power User) and three levels of corresponding Privilege objects, as shown below.
Integrating iDRAC7 with Active Directory

Figure 18. Dell iDRAC Objects.

Privilege and role name changes
The privilege names and role names are a little different in Active Directory versus the iDRAC GUI as they have been renamed for iDRAC7. The old names have been retained in the Active Directory schema extension for backwards compatibility.

The following tables map the prior generation privilege names and role names to the current generation.

Table 2. Role Names.

<table>
<thead>
<tr>
<th>Prior PowerEdge Generations (Seen in Active Directory)</th>
<th>Current PowerEdge Generation (Seen in the iDRAC GUI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Administrator</td>
</tr>
<tr>
<td>Power User</td>
<td>Operator</td>
</tr>
<tr>
<td>Guest</td>
<td>Read Only</td>
</tr>
</tbody>
</table>

Table 3. Privilege names.

<table>
<thead>
<tr>
<th>Prior PowerEdge Generations (Seen in Active Directory)</th>
<th>Current PowerEdge Generation (Local User Privileges seen in the iDRAC GUI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Login</td>
</tr>
<tr>
<td>Configure Device</td>
<td>Configure</td>
</tr>
<tr>
<td>Configure Users</td>
<td>Configure Users</td>
</tr>
<tr>
<td>Clear Logs</td>
<td>Logs</td>
</tr>
<tr>
<td>Execute Server Control Commands</td>
<td>System Control</td>
</tr>
<tr>
<td>Access Console Redirection</td>
<td>Access Virtual Console</td>
</tr>
<tr>
<td>Access Virtual Media</td>
<td>Access Virtual Media</td>
</tr>
<tr>
<td>Test Alerts</td>
<td>System Operations</td>
</tr>
<tr>
<td>Execute Diagnostic Commands</td>
<td>Debug</td>
</tr>
</tbody>
</table>

Active Directory objects
Privilege Objects

Right click on DellIDRACAdminPriv and select Properties.

You will see the following:

*Figure 19. Dell Admin Privilege Object.*

The privilege object lists all privilege names. All boxes are checked in this example since this is the DellIDRACAdminPriv, which controls the Administrator's privileges.

If you repeat the above with the DellIDRACGuestPriv, you will see only the Login box has been checked. Likewise, DellIDRACPowerPriv has by default all but two boxes checked.

If you want to customize user privileges it is recommended that you do so in the DellIDRACPowerPriv object by checking/unchecking the appropriate boxes. This represents the mid-level Power User (also known as the Operator) iDRAC role.

**iDRAC objects**

An iDRAC object is created below for each physical iDRAC that is integrated with Active Directory.
Integrating iDRAC7 with Active Directory

**Association objects**

An Association object is used to link iDRAC objects to Active Directory users (or groups) to Privilege objects. The Association object effectively bundles the three items together.

**Configure Active Directory**

In the following steps, an iDRAC object representing the physical iDRAC in the Managed PowerEdge server is created. Using the Admin User Association object, the iDRAC object is associated with the iDRACAdministrators group and the DellIDRACAdminPriv object. These steps are repeated for other groups requiring lesser privileges for the same iDRAC object.

1. Right Click on the **Users** Container and select **New > Dell Remote Management Object Advanced**.  
   **Reminder** - this option is not available if you are using the Server Manager console - be sure you are using MMC.

   ![Adding a New Dell Object](image)

   **Figure 20. Adding a New Dell Object.**

2. For **Enter Object Name**, put the name to be used for the iDRAC. This name must be unique for each iDRAC object in Active Directory. For example, use **idrac1**.
Integrating iDRAC7 with Active Directory

3. Make sure the iDRAC Device Object option button is selected and click OK. The iDRAC device object now appears in the Users container in Active Directory.

4. Expand the Dell Container under yourdomain.com (test.lab), right click on Dell iDRAC Admin User Association and select Properties.
   - On the Users tab, click Add > Object Types > select Groups, and then click OK.
   - Under Enter the object names to select enter iDRACAdministrators, click Check Names.
   - The object should be found as shown by an underline, and then click OK.
5. Leave the window open and click the **Privilege Object** tab. It will be pre-populated with the **DellAdminPriv** object.

6. On the **Products** tab, select **Add**.

7. Under **Enter the object names to select**, enter the iDRAC object name used earlier (**idrac1**) and then click **Check Names** (it should be found as shown by an underline), click **OK**.

Your window should look something like this:
8. Repeat for the Guest User (also known as the Read Only User)
   - Right click on Dell iDRAC Guest User Association and select Properties.
   - On the Users tab, click Add > Object Types > select Groups, and then click OK.
   - In the Enter the object names to select box enter iDRACReadOnlyUsers > Check Names (it should be found) > click OK.
   - The Privilege Object tab will be pre-populated with the DellGuestPriv object.
   - On the Products tab, click Add.
   - Enter your iDRAC name (idrac1) > Check Names (it should be found) > OK > OK.

9. Repeat for the Power User (also known as the Operator)
   - Right click on Dell iDRAC Power User Association and select Properties.
   - On the Users tab, click Add > Object Types > select the Groups box > OK > in the Enter the object names to select text box enter iDRACOperators > Check Names (it should be found) > OK.
   - The Privilege Object tab will be pre-populated with the DellPowerPriv object.
   - On the Products tab, click Add.
   - Enter your iDRAC name (idrac1) > Check Names (it should be found) > OK > OK.
Integrating iDRAC7 with Active Directory

Adding users
You can add new users to the appropriate Active Directory group (iDRACAdministrators, and so on) with no further configuration necessary.

Adding iDRACs
If you have additional iDRACs you wish to set up, create a new iDRAC object with a unique name for each (such as idrac2, idrac3, and so on). You can then follow the steps above to add the additional iDRAC objects to the Products tab in each of the three Association objects. You can add multiple iDRACs at the same time by separating their names with semicolons in the **Enter the object names to select** box or by typing the first few letters in their names (assuming they all start with the same few letters), clicking **Check Names**, and selecting the iDRAC objects from the **Multiple Names Found** box.

Configuring iDRAC for use with Active Directory Extended Schema
In your browser at the management station, log into the iDRAC GUI of your managed system.

`https://<idrac_ip_address>`

The iDRAC Network Settings can remain as previously configured for Standard Schema authentication. If you would like to review them please see Configure the iDRAC Network Settings in the Standard Schema configuration section here.

   - Make sure **Microsoft Active Directory** is checked and click the link or **Apply**.
   - Scroll Down to bottom of page and click **Configure Active Directory**.
   - Make sure **Enable Certificate Validation** is checked and the certificate uploaded for during Standard Schema configuration is shown under **Current Directory Service CA Certificate**.
   - Click **Next**.
   - Make sure **Enable Active Directory** is checked.
   - Make sure **Enable Single Sign-On** is unchecked.
   - For **User Domain Name**, make sure the **FQDN of your domain name** is present (for example, test.lab).
   - Make sure **Specify Domain Controller Addresses** is selected and the **FQDN of your Domain controller** is still present for **Domain Controller Server Address 1**. (For Example, ad2.test.lab).
   - Click **Next**.
   - This is where the changes start. Select **Extended Schema**, and then click **Next**.
   - For **iDRAC Name**, use the name of the iDRAC object you created in Active Directory (for example, idrac1).
- Specify your **iDRAC Domain Name** (For example, `test.lab`).
- Click **Finish**. You are taken to a summary page that looks similar to the following:

**Figure 25.** Active Directory Configuration and Management summary page.
Integrating iDRAC7 with Active Directory

Note: At the bottom of the page (not visible above) you see sections labeled Standard Schema Settings and Standard Schema Role Groups. These are still retained in the iDRAC configuration but are not used when Extended Schema is selected. This lets you easily switch back and forth between the two schema options with minimal additional configuration.

Test your Extended Schema configuration

1. Scroll down to the bottom of the Active Directory Configuration and Management summary page, and click Test Settings.

2. In Test User Name text box, type your administrative user in username@domain.com format, for example, admin@test.lab.

3. In the Test User Password text box, type the user’s password for the domain.

4. Click Start Test

At the top of the results page, all tests must Pass (including Certificate Validation) or be marked Not Applicable/Not Configured/Not Run.

The Test Log at bottom of page should have no errors and list all 9 privileges in the Cumulative privileges gained section as shown below.
It is recommended that you also run the test for your users with lower privilege levels (readonly and operator for example) at this time to confirm everything is configured correctly.

You can now authenticate to the iDRAC for all services (racadm, WSMAN, SSH, Telnet, and the GUI) as shown earlier in the Authentication Examples section.
Creating an Active Directory user with customized iDRAC privileges

This example creates a new user, assigns the user to the iDRACOperators group, modifies the default privileges held by the Power User role (also known as the Operator role), and then tests the configuration.

1. At the Domain Controller, under Active Directory Users and Computers create a new user with a login name of John_Smith. Assign a password and uncheck User must change password at next logon.
2. Add John_Smith to the iDRACOperators group.
3. Now customize the privileges John_Smith (and the iDRACOperators group) receives by removing the ability to use Console Redirection.
4. Under Active Directory Users and Computers in the Dell container, right-click on DellIDRACPpowerPriv and select Properties.
5. Uncheck Access Console Redirection. The window should look like this:

Figure 27. Configuring Custom Privileges.
6. To close, click **OK**.

7. At the **management station**, log out of the **iDRAC GUI**.

8. Log back in to the **iDRAC GUI** as **John_Smith**. Be sure to specify your domain (**test.lab**). You should see a **System Summary Page** similar to this:

![John Smith's System Summary page](image)

Note that the **Virtual Console Preview** (upper right of Summary Page) is not shown and was replaced with a message indicating the user does not have access. This feature is part of the **Access Console Redirection** privilege that was removed from the group that the user belongs to in the prior step.
Integrating iDRAC7 with Active Directory

9. Do a full Test of John_Smith’s privileges to confirm everything is configured properly as follows:
   - Log out and log back in as an *administrative* user in the iDRAC GUI. Go to iDRAC Settings > User Authentication > Directory Services > Microsoft Active Directory > Test Settings.
   - Enter John_Smith@yourdomain.com (John_Smith@test.lab) and John’s password, and then click *Start Test*.
   - The results should match the privileges configured above and appear as follows:

   **Figure 29. Privilege Test Results for John Smith.**
Summary
Active Directory integration with iDRAC7 can greatly simplify management of your iDRAC users and privileges. This document simplifies the set up process and enables you to evaluate the Standard Schema and Extended Schema options for use with the Dell iDRAC.