Integrating iDRAC7 With Microsoft Active Directory

Whitepaper

Author: Jim Slaughter

April 2013| Rev 1.1

Contents

Overview

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 the best method. Once set up, you can switch between standard and extended schema method using the same Domain Controller with minimal configuration changes.

It is strongly recommended that you first perform these steps in a test environment. 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 you 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.dell.com/esmmanuals.

Benefits of Integrating iDRAC7 With Microsoft Active Directory

Using the Integrated Dell Remote Access Controller 7 (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 the iDRAC7 to use Active Directory authentication. See Confirming iDRAC7 Enterprise License Installation for more information.

Standard Schema Versus Extended Schema

You can integrate the iDRAC with Active Directory using two options: Standard Schema or Extended Schema, with different advantages and requirements for each.

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

In Standard Schema, you do not have to extend the Active Directory schema. However, you must enter Active Directory group names and privileges on each iDRAC.

Extended Schema 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.

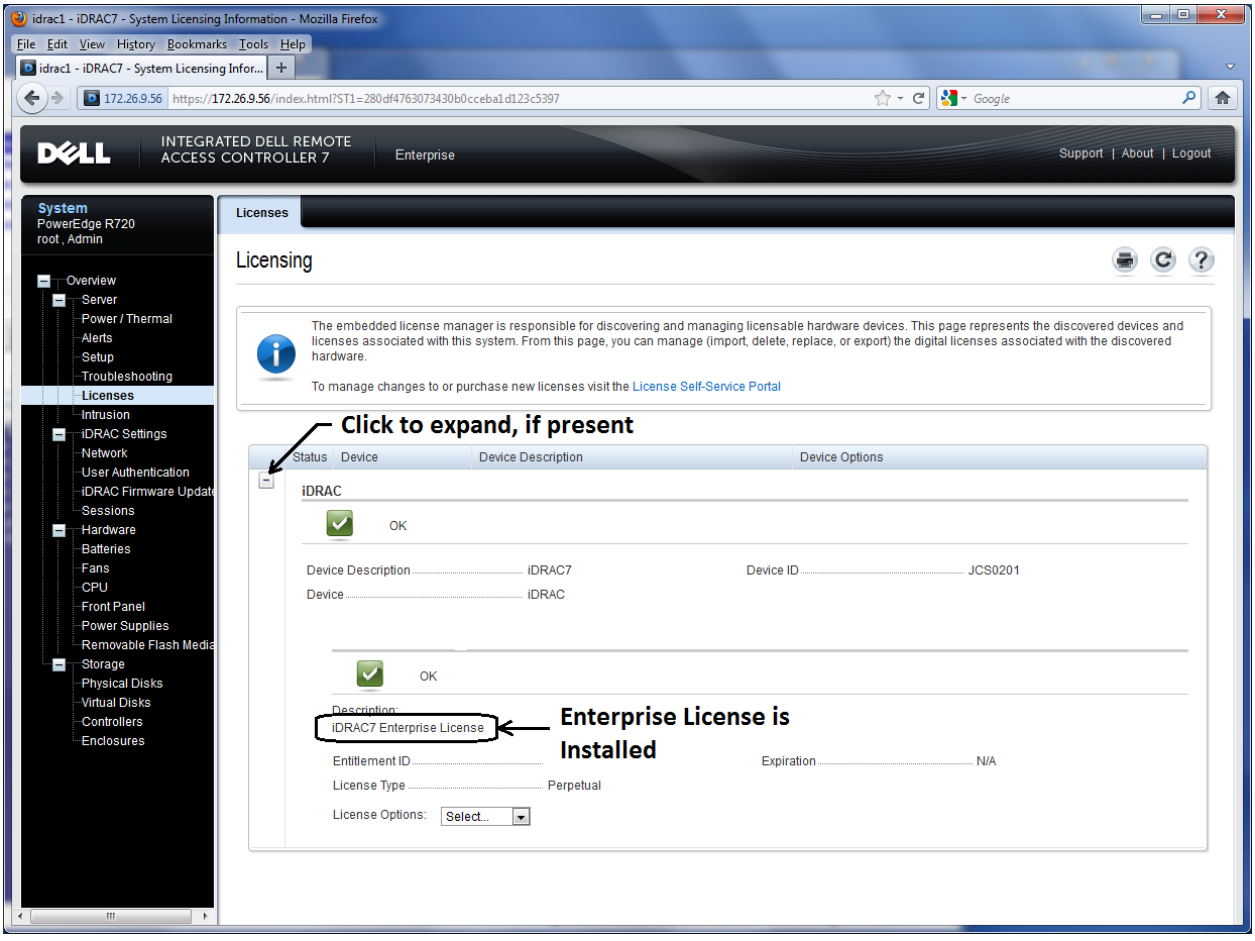
Confirming iDRAC7 Enterprise License Installation

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

To check the installed license level:

1. Browse to **https://<idrac_ip_address>** and log into the iDRAC GUI of the system as an administrative user (default username is root, password is calvin.)
2. Go to **Overview > Server > Licenses** page.
3. Expand the "**+**" in the left column of the license table to view the license (as shown in the following figure). 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 using the License Self-Service Portal (linked on the **Licensing** page) or by contacting your Dell Sales representative.

Figure 1. Viewing 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

- **Domain Controller** - A system running Windows Server 2008 Enterprise 32-bit Service Pack 1.
- **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 *iDRAC7 Readme* at **www.dell.com/esmmanuals**, 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.
- DCHP is running on the network on a different server. It is used to assign an IP address to the iDRAC. (DHCP is optional).
- The iDRAC is 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 the steps in this section are performed 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 required, change the Windows computer name of the Domain Controller before performing the next steps.

Promoting Server To Domain Controller and Installing DNS

The steps in this section are for Windows Server 2008 Enterprise. The 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**.

Figure 2. Active Directory Domain Services Installation Wizard.

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** twice.

   If DNS is not 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. After the installation is complete, reboot the system when prompted.

    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.

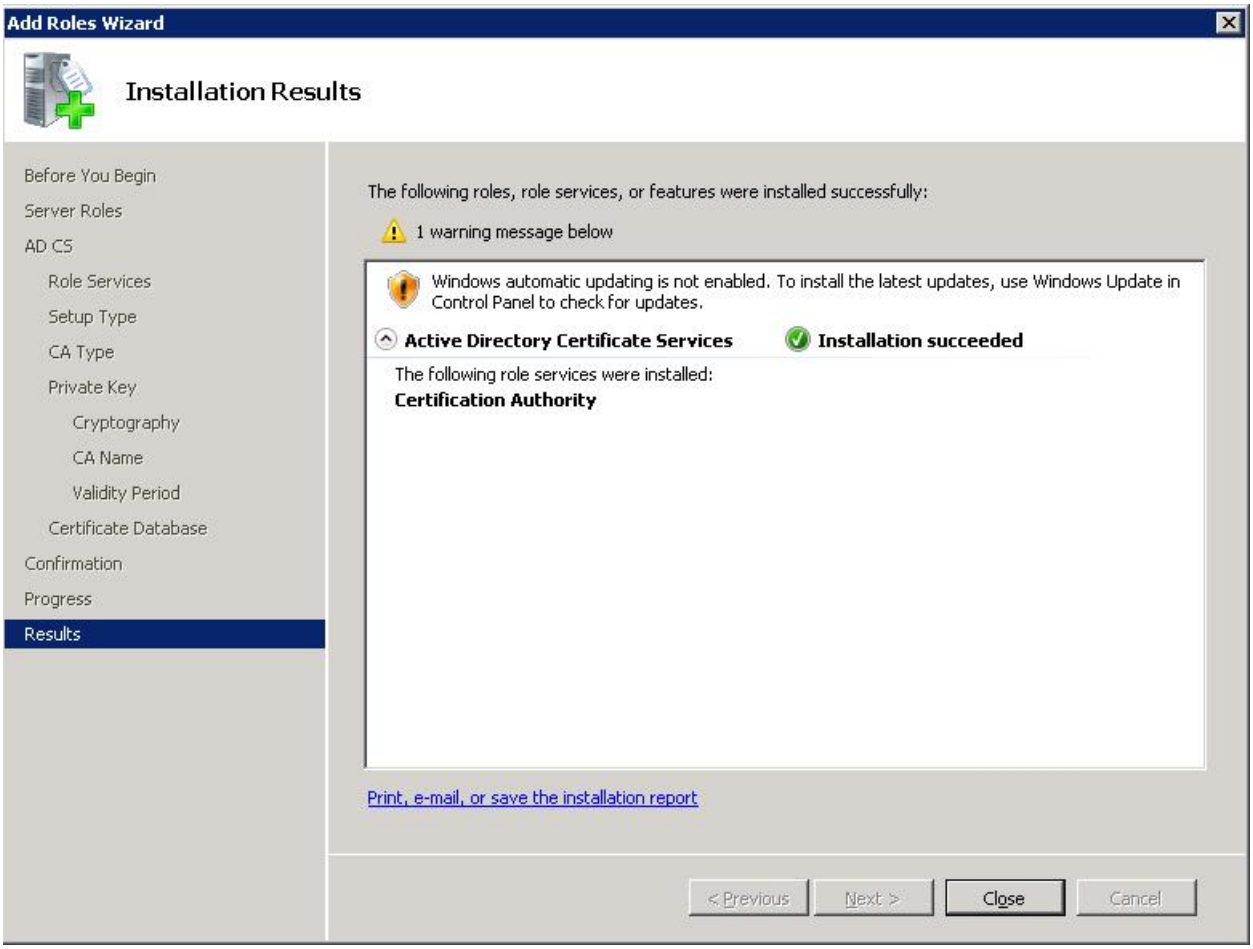
Installing and Configuring Active Directory Certificate Services

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 selected, and then click **Next** > **Enterprise** > **Next** > **Root CA** > **Next** > **Create a New Private Key** > **Next.**
5. Accept the default values for CSP, key character length, hash algorithm, and then click **Next.**
6. Accept the default CA name and 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, a successful message is displayed as shown.

Figure 3. Installation Succeeded Message screen



Adding Certificates Snap-in to Microsoft Management Console

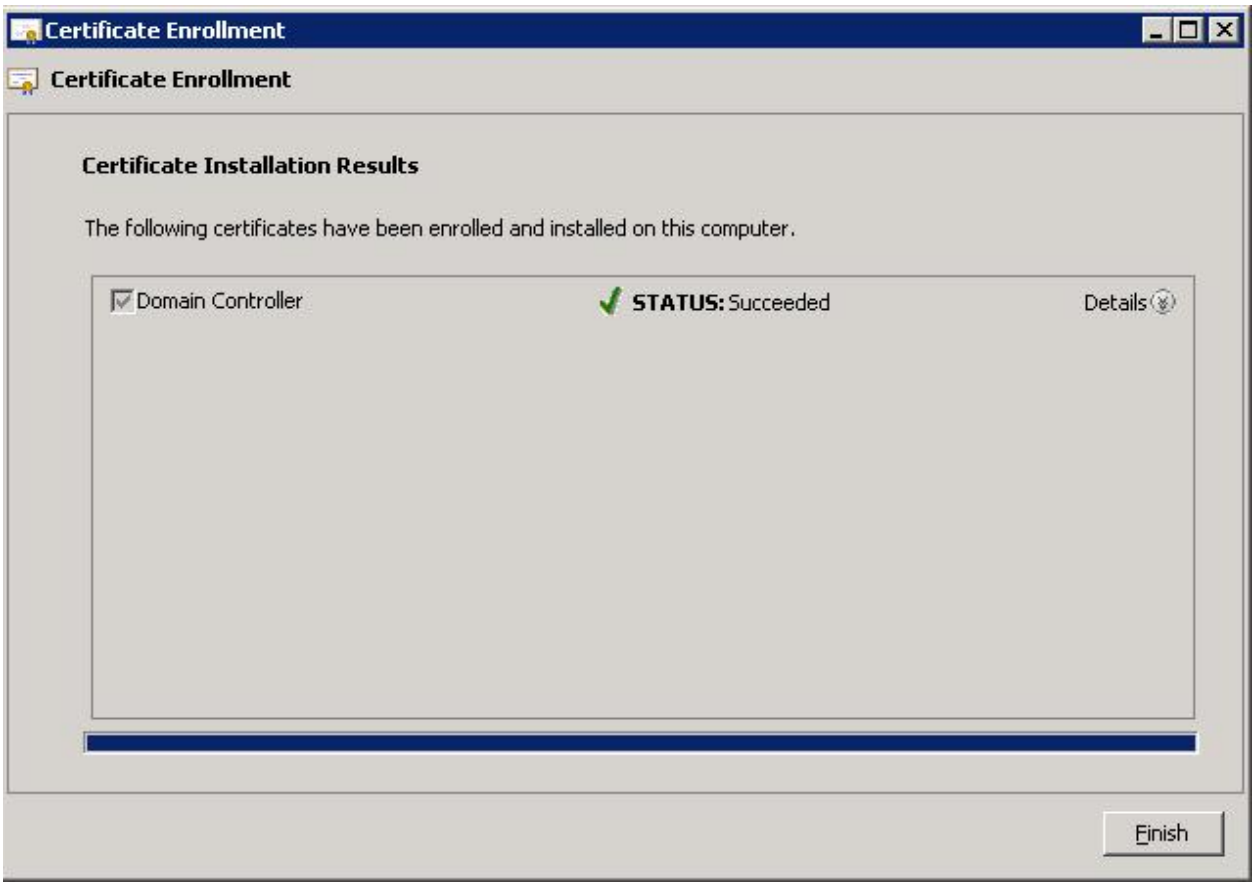
1. Click **Start** > **Run** > **MMC** > **OK**.
2. In the **Console 1** window, click **File** > **Add/Remove Snap-in** > select **Certificates** > **Add** > select **Computer Account** > **Next** > **Local Computer** > **Finish** > **OK**.

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

Installing the CA certificate for Client Authentication to the Domain Controller

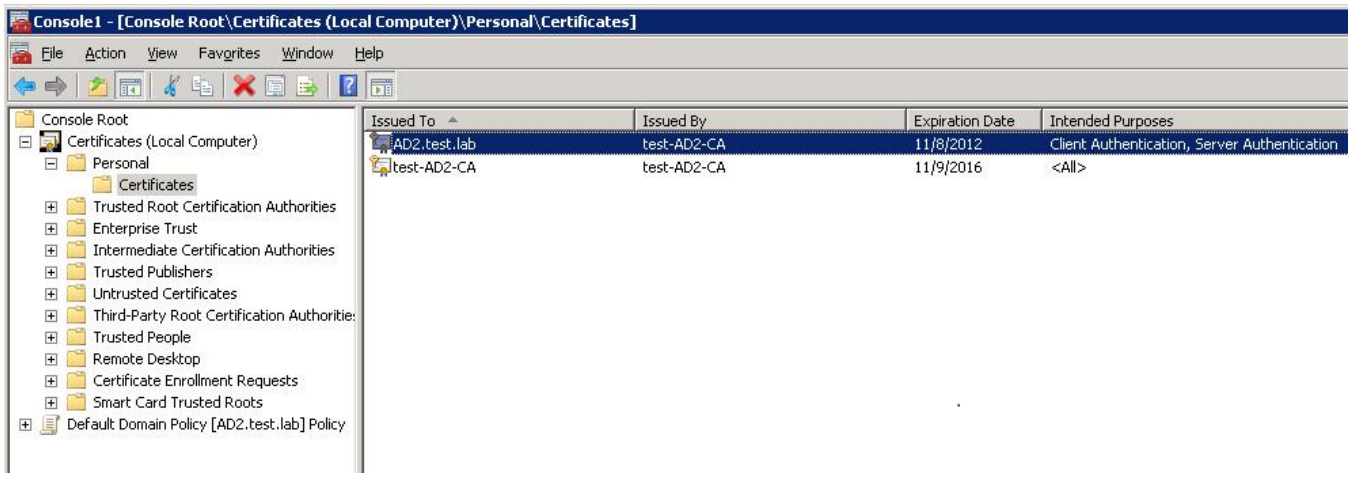
1. Open **Console1,** expand **Certificates**, expand **Personal**, click **Certificates**.
2. Right-click **Certificates**, then click **All Tasks** > **Request New Certificate.**
3. In the **Certificate Enrollment** wizard, click **Next**.
4. Select **Domain Controller**, and click **Enroll** > **Finish**. A successful message similar to the following is displayed.

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.

Figure 5. Certificate folder contents.



Exporting CA Certificate

Note: You must 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** > select **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 required path and specify a file name (for example, **ad2.cer**), and then click **Next.**

Figure 6. Completing the Certificate Export Wizard.

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

Creating iDRAC Users and Groups

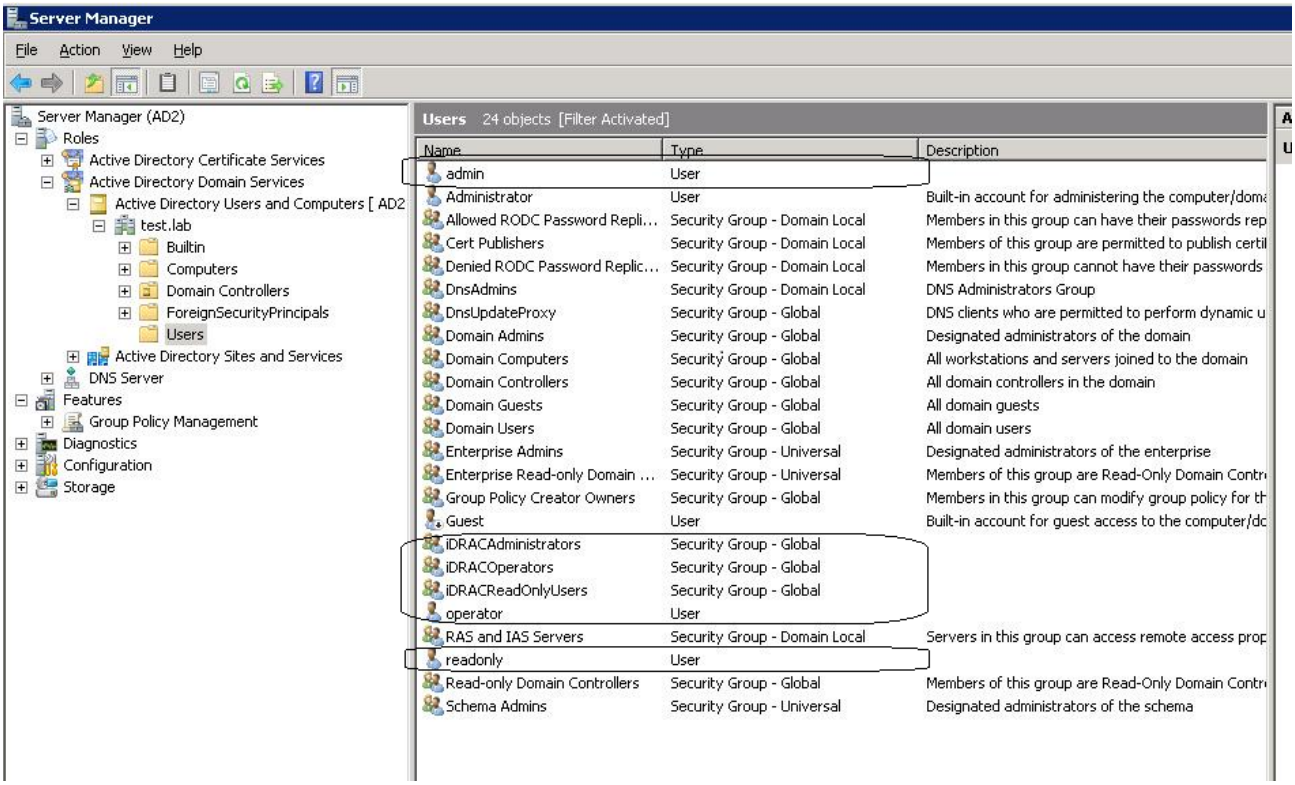
1. In the left pane of **Server Manager**, expand **Roles** > **Active Directory Domain Services** > **Active Directory Users and Computers** > your domain name (**test.lab**).
2. In the **Users** container, create users that will be provided the three different iDRAC privilege levels. (Right-click on **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. Do not use white space and special characters (such as \, /, or @) for the user name.

    - For each user, assign a password and clear the **User must change password at next logon** option.
    - 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 must display the new users similar to the following figure.

Figure 7. iDRAC Users and Groups



Assigning the users to their corresponding groups

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

Configuring iDRAC7 For Use With Active Directory Standard Schema

At the management station, browse to **https://<idrac_ip_address>** using your Internet Explorer or Firefox Web browser and log into the iDRAC GUI as an administrator (default username is **root**, password is **calvin**). You will do the following in the next sections:

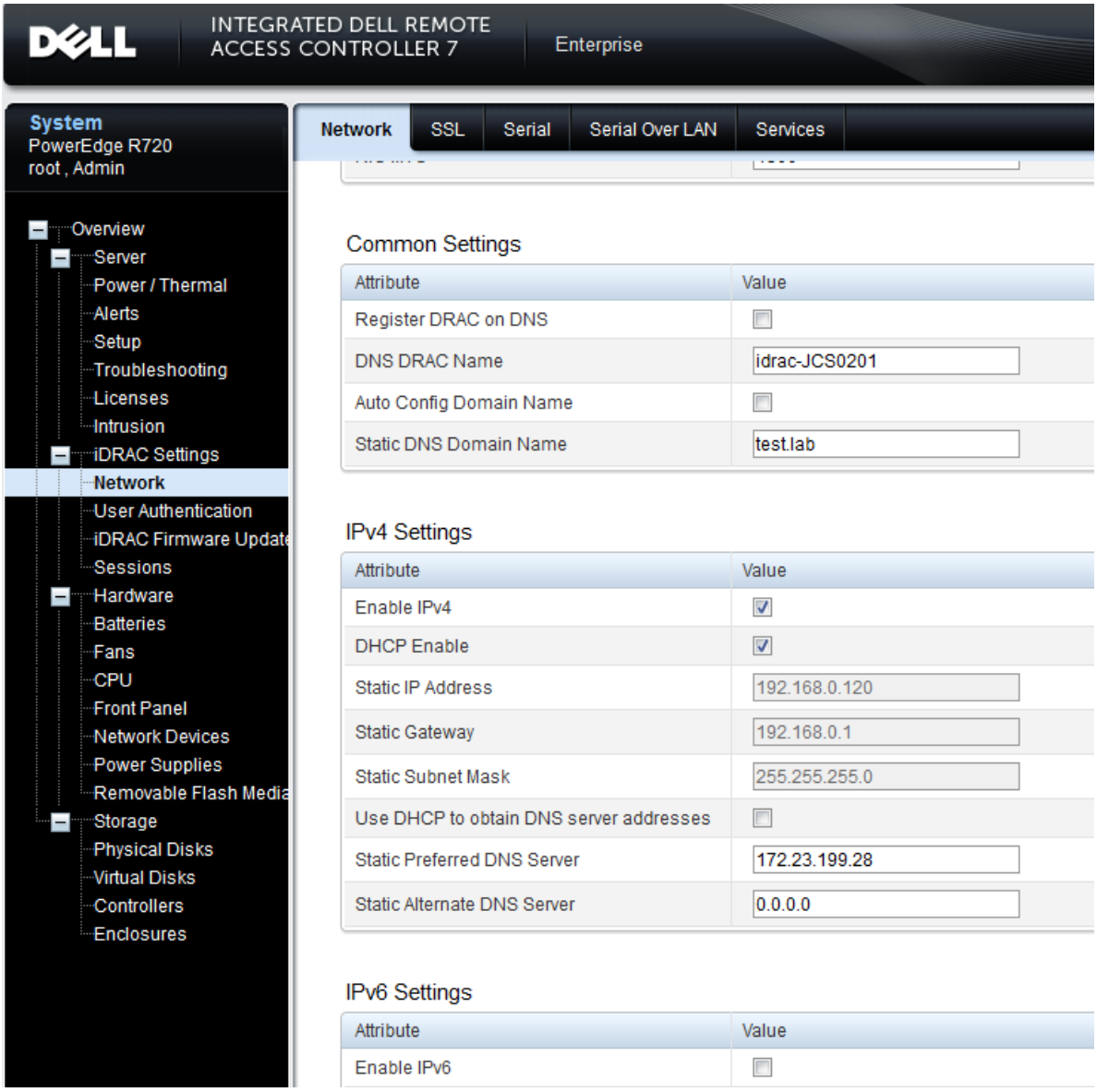
- Configure the iDRAC7 Network Settings
- Configure the iDRAC Directory Services Settings
- Test the Standard Schema Configuration

Configuring the iDRAC7 Network Settings

1. In the iDRAC GUI, go to **iDRAC Settings** > **Network**.
2. Under **Common Settings**:
    - **Register DRAC on DNS** – (Optional, this can be selected if your DNS server is configured for dynamic updates)
    - **DNS DRAC name** (optional) - The default is **idrac-<Dell service tag #>.**
    - **Auto config domain name** - Select this option only if the DCHP server provides the domain name.
    - **Static DNS Domain Name –** If you did not select the **Auto config domain name** option, specify the FQDN of your domain. For example, **test.lab**.
3. Under **IPv4 Settings**:
    - **Enable IPv4** – Select this option.
    - **DHCP enabled** - (optional, depending on your network configuration). This is selected for the Dell test environment.
    - **Use DHCP to obtain DNS server address** – Select this option only if you are using a DHCP server *and* it is configured to point to the Active Directory Server running DNS. This is not selected for the Dell test environment.
    - **Static Preferred DNS Server** - Specify the IP address of your domain controller running DNS if the **Use DHCP to obtain DNS server address** is not selected. For the Dell test environment, it is 172.23.199.28.
    - **Alternate DNS server** - Optional. The default is 0.0.0.0.
4. Click **Apply**. The iDRAC7 network settings are configured.

The following figure shows the iDRAC Network Settings for the Dell test environment set up.

Figure 8. iDRAC Network Settings



Configuring the iDRAC7 Directory Services Settings

Note: You must have an iDRAC7 Enterprise license to configure the directory services settings.

1. Go to **iDRAC Settings** > **User Authentication** > **Directory Services**.
2. Select **Microsoft Active Directory** and click **Apply**.
3. In the **Active Directory Configuration and Management** page, scroll down to the bottom of the page and click **Configure Active Directory**.
4. Select **Enable Certificate Validation**.
5. Upload the **Directory Service CA Certificate** - 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 to **Upload Directory Service CA Certificate**, click **Browse**, select the file, and click **Upload**.

   A message similar to the following is displayed.

   Figure 9. Upload Complete

   If you see 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 matches the date and time on the CA (the Domain Controller in this document) and try again.

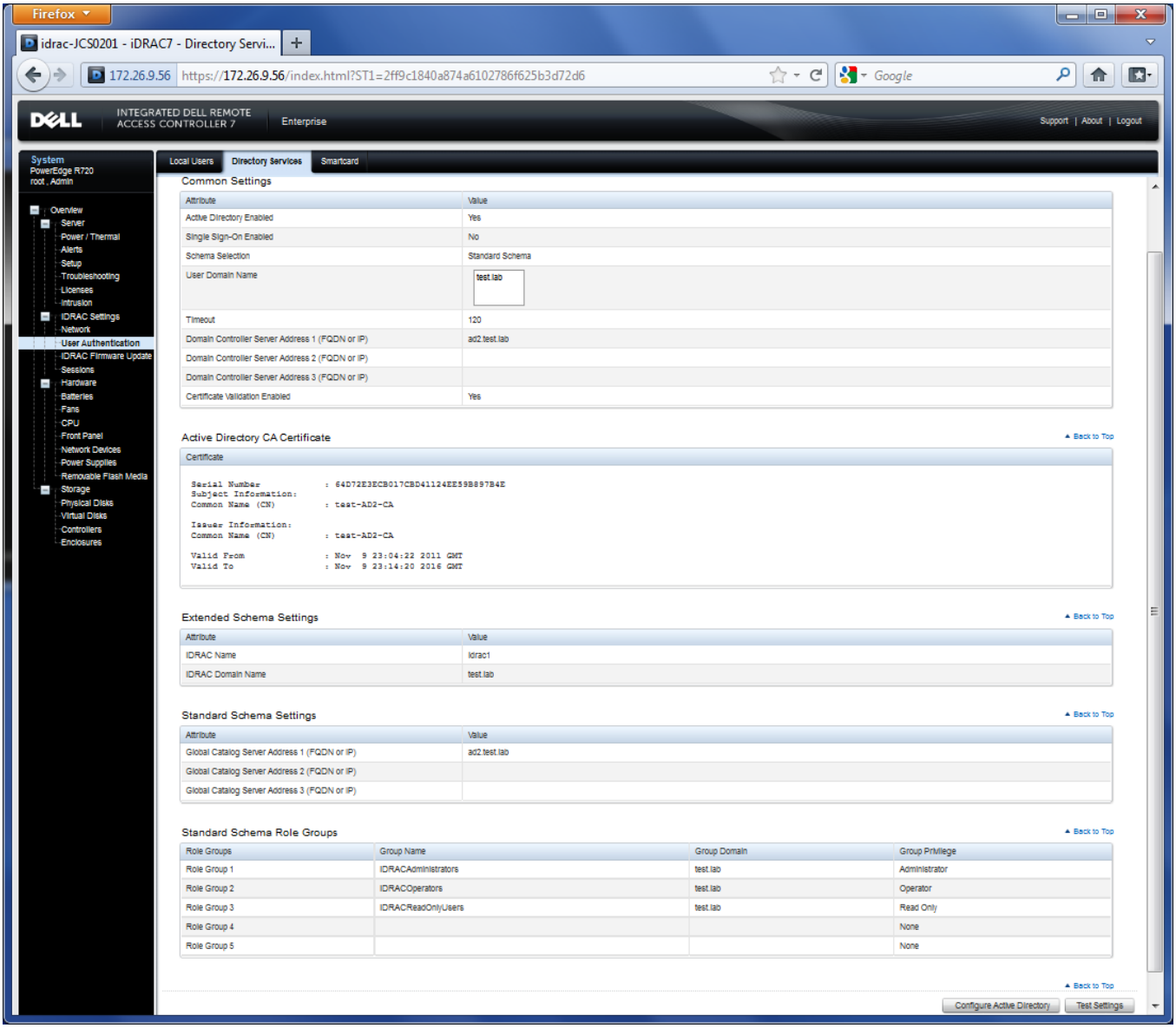
   Note: Applies to iDRAC firmware releases prior to 1.30.30 only. If the certificate was issued from a *newly created CA*, it may continue to be reported as not valid even though the iDRAC and CA server dates and times match. This is because the iDRAC treats its time as UTC (Coordinated Universal Time). 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 waiting until the time has passed. This issue has been fixed in iDRAC firmware 1.30.30 and later versions.

6. Click **OK** and then click **Next**.
7. Select **Enable Active Directory**.
8. Clear **Enable Single Sign-on**.
9. For **User Domain Name**, click **Add** and enter the FQDN of your domain. For example, **test.lab** and click **OK**.

10. Select **Specify Domain Controller Addresses** and enter the FQDN of your Domain Controller for **Domain Controller Server Address 1** (for example, **ad2.test.lab**).
11. Click **Next**.
12. Select **Standard Schema.**
13. Click **Next.**
14. 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).
15. Click **Role Group 1**.
    - **Group Name** - Enter **iDRACAdministrators**.
      Note: All group names must be an exact match to the group names you created earlier in Active Directory.
    - **Group Domain** - Enter your domain name. For example, **test.lab**.
    - **Role Group Privilege Level** - Select **Administrator** from the drop-down menu.
      Note: All the nine privilege options are selected. Even though these privileges can be customized, it is recommended that you use the default options selected for the Administrator and Read Only users. "Operator" can be used for customized privilege selections.
    - Click **Apply.**
16. Click **Role Group 2**.
    - **Group Name** - iDRACOperators
    - **Group Domain** -test.lab for example
    - **Privilege Level** - Select **Operator** from the drop-down menu.
      Note: Seven privileges are selected. Customize the privileges (if any) by selecting or clearing the appropriate boxes as required.
    - Click **Apply.**
17. Click **Role Group 3.**
    - **Group Name** - iDRACReadOnlyUsers
    - **Group Domain** - test.lab for example
    - **Privilege Level** - Select **Read Only** from the drop-down menu.
    - Click **Apply** and then click **Finish**.

A summary page similar to the following figure is displayed.

Figure 10. Directory Services Summary.



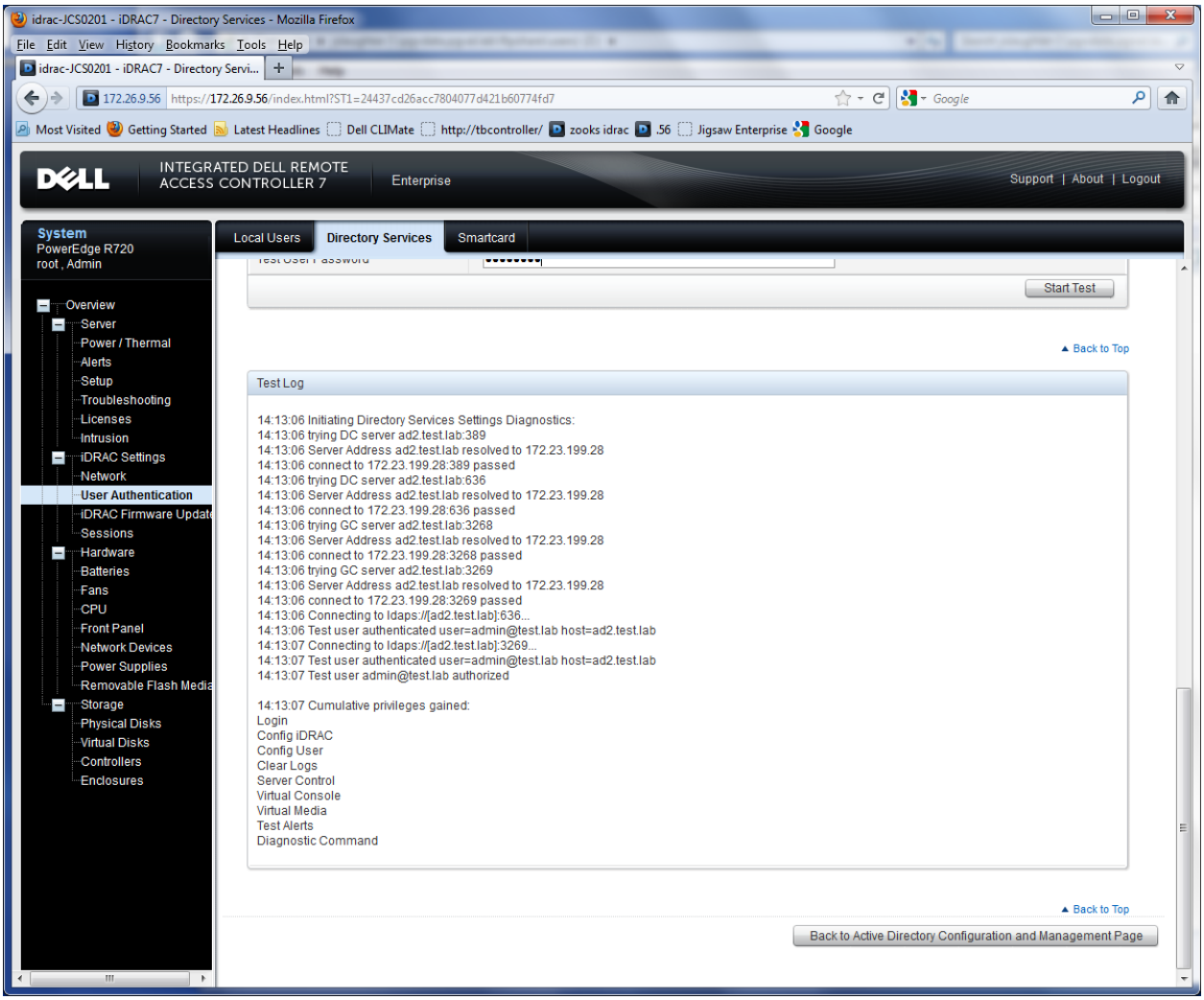
Testing Standard Schema Configuration Settings

1. Click **Test Settings** in the lower right part of the screen.
2. In the **Test User Name** field, type the administrative user in username@domain.com format. For example, **admin@test.lab**.
3. In the **Test User Password** field**,** 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 must be marked Not Applicable/Not Configured.

   The **Test Log** at bottom of page must have no errors and must list all the nine privileges in the **Cumulative privileges gained** section as shown in the following figure.

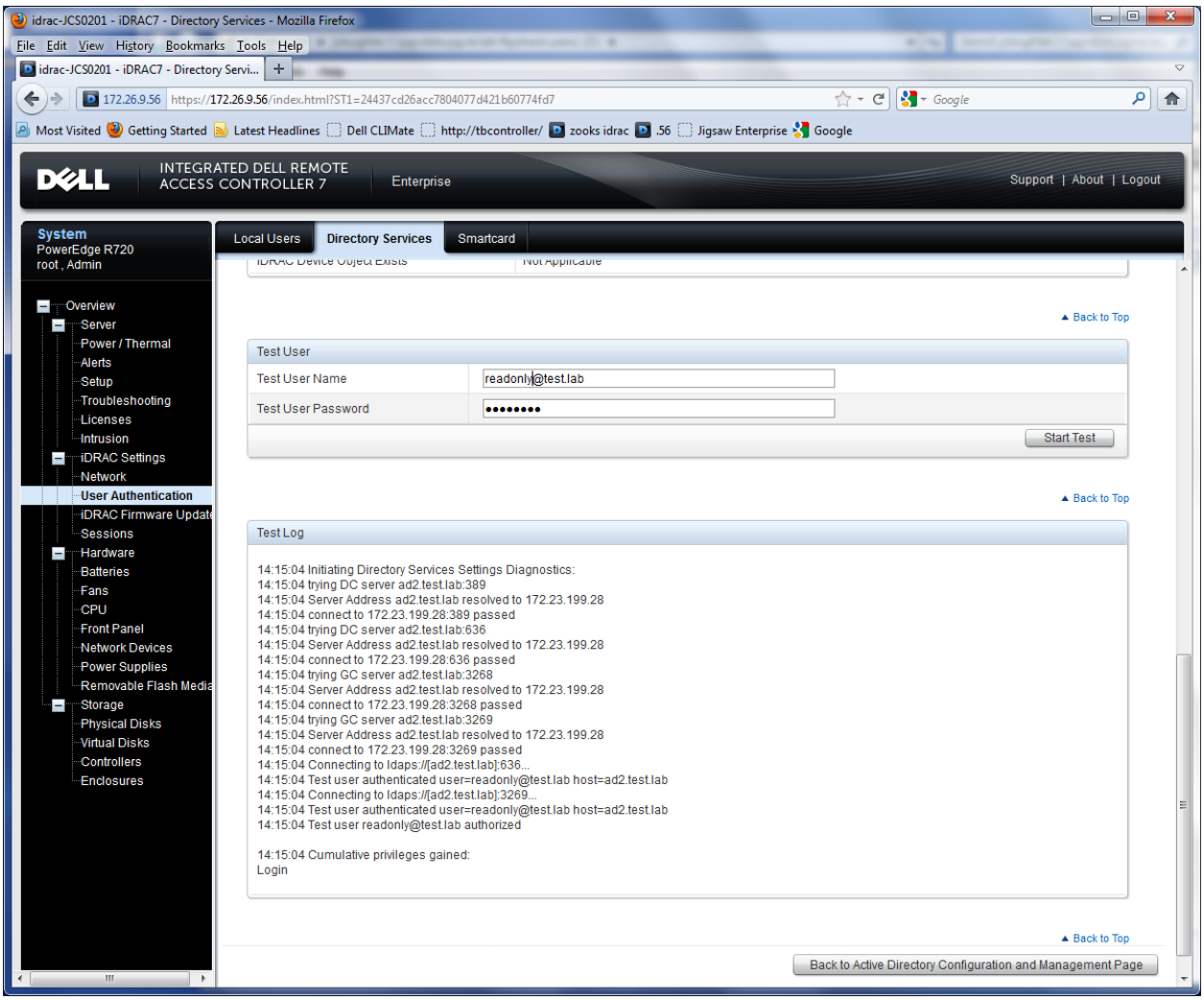
Figure 11. Administrative User Test Results



You can repeat the test with the other users you have created. The following figure shows the result from the read-only user.

Note: The only privilege listed is **Login** which is the correct behavior for this user.

Figure 12. Read-Only User Test Results.



Active Directory Login Syntax Options

There are different methods for authenticating as an Active Directory user. All the iDRAC interfaces (GUI, racadm, WSMAN, SSH, and Telnet) accept the following domain-username formats:

Table 1. Domain username formats

Format	Example
username@domain.com	admin@test.lab
domain.com/username	test.lab/admin
domain.com\username	test.lab\admin

Note: 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 for both standard and extended schema.

Authentication Examples

For the following examples:

- iDRAC7 IP address - 172.26.9.56
- Domain - test.lab
- User - admin
- Password - Dell1234

Authenticating with Active Directory Credentials in a RACADM Command

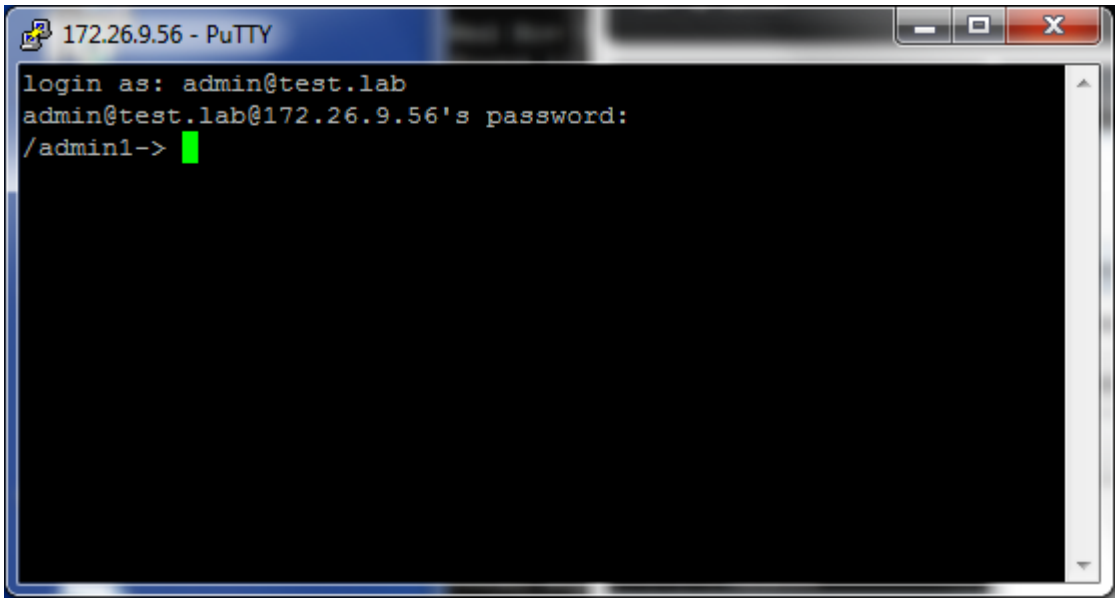
```
racadm -r 172.26.9.56 -u test.lab\admin -p Dell1234 getsysinfo
```

Authenticating with Active Directory Credentials in a WSMAN (WinRM) Command

```
winrm e cimv2/root/dcim/DCIM_PhysicalDiskView -u:test.lab/admin -p:Dell1234 -
r:https://172.26.9.56/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -
a:basic
```

Authenticating with Active Directory Credentials Using SSH login

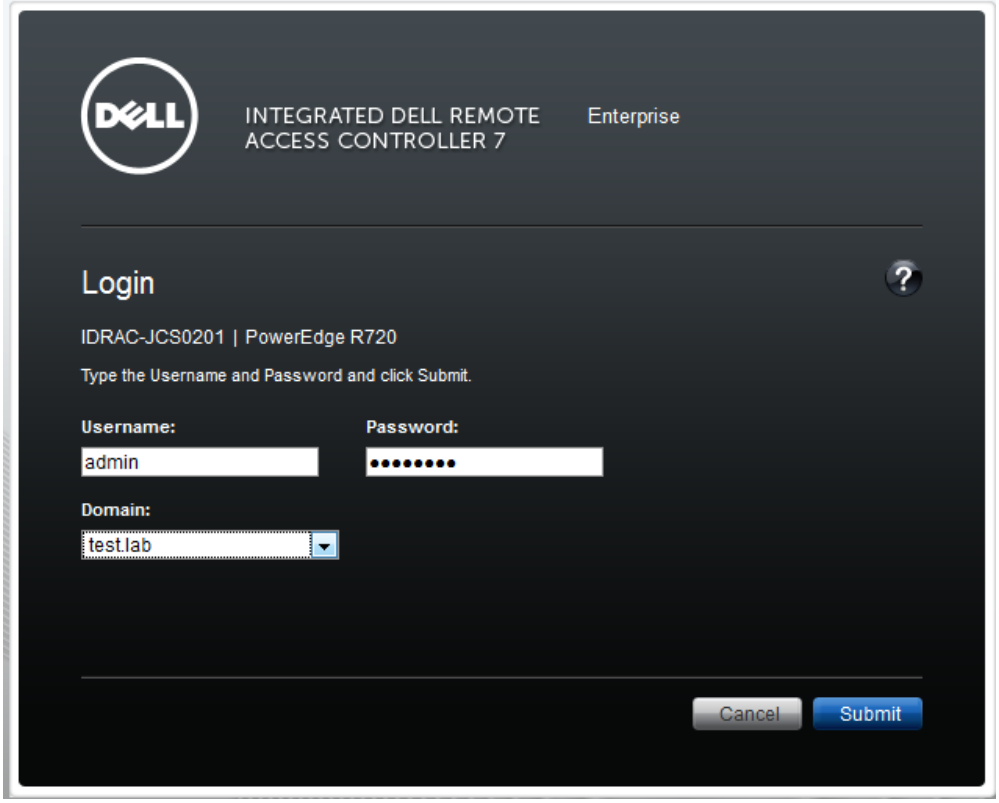
Figure 13. SSH login



Authenticating with Active Directory Credentials in the iDRAC GUI

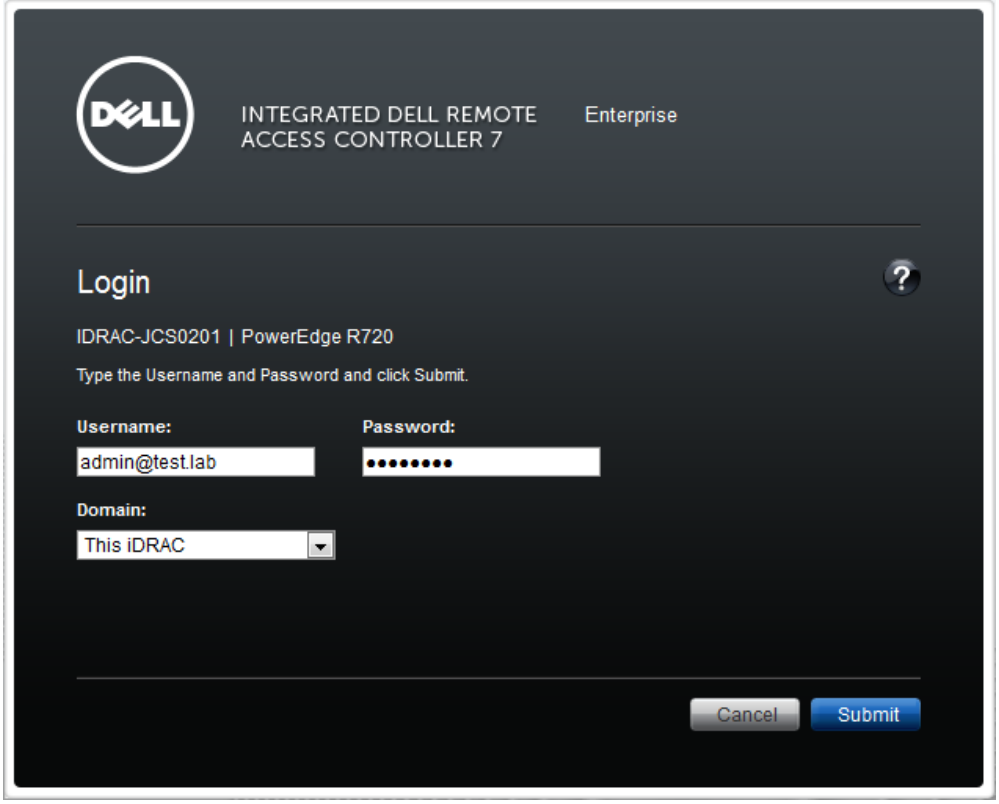
There is one additional option when logging into the iDRAC GUI. You can select the domain from the drop-down list and enter only the username and password as shown

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:

Figure 15. iDRAC GUI login option 2.



Configuring Domain Controller 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:

   32 Bit:

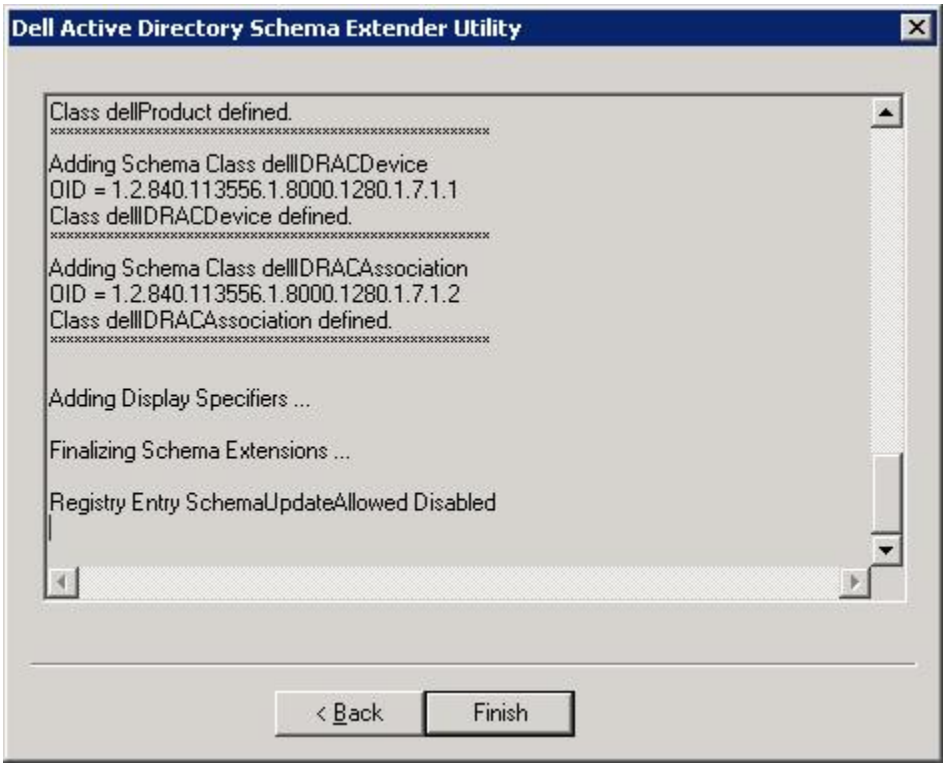
   ```
   DVD_DRIVE:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema_Extender\SchemaExtender.exe
   ```

64 Bit:

```
DVD_DRIVE:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema_Extender64\SchemaExtender.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**. The schema is extended and a message similar to the following is displayed.

Figure 16. Schema Extension Complete



8. Click **Finish**.

Viewing Active Directory Schema Changes (Optional)

To view the changes made by extending the schema, install the Microsoft Active Directory Schema snap- in utility. To do this:

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

   ```
   regsvr32 schmmgmt.dll
   ```

2. A message is displayed indicating that the command is successful. Click **OK**.
3. Open the 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**, and then click **OK**.
6. Expand **Active Directory Schema** and expand **Classes**. In the right pane, you can locate the added classes prefixed with "dell".
7. Under Active Directory Schema, click the **Attributes** folder. In the right pane, you can locate the added attributes prefixed with "dell".

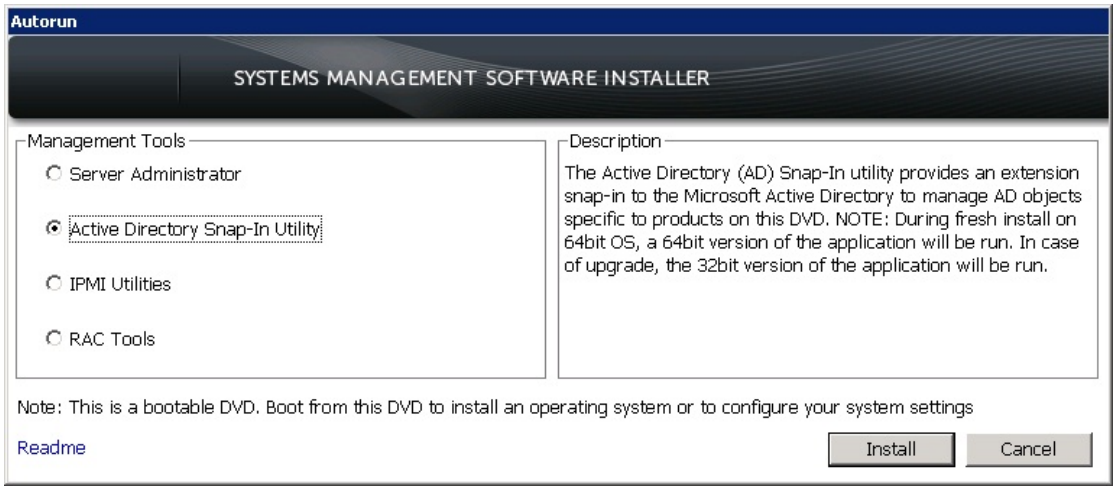
Installing Dell Extension to Active Directory Users and Computers Snap-In

Note: If your domain controller is running 64-bit Windows and you are using the *Systems Management Tools and Documentation* DVD version 7.0.0 or 7.1.0, see the next section. If you are using the DVD version 7.2.0 or later, this section applies to both 32-bit and 64-bit operating systems. This section also applies if you are using version 7.0.0 or 7.1.0 of the DVD and a 32-bit operating system.

Install the Dell extension to the Active Directory Users and Computers Snap-In as follows:

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

Figure 17. Installing the Active Directory Snap-In



Note: If you are using a Remote Desktop to connect to the Domain Controller and if an error is displayed that installation is not permitted from Remote Desktop, map a drive letter to the DVD instead of using a Universal Naming Convention (UNC) share name and try again.

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

Installing Dell Extension to Active Directory Users and Computers Snap-In for 64-bit Windows Using System Management Tools and Documentation DVD Version 7.0.0 or 7.1.0.

Note: If you are using the *Systems Management Tools and Documentation* DVD version 7.2.0 or later see the preceding section.

If the Domain Controller is running a 64-bit version of Windows and you are using the *Systems Management Tools and Documentation* DVD version 7.0.0 or 7.1.0, install the Dell extension to the Active Directory Users and Computers Snap-In as follows:

1. From the Systems Management Tools and Documentation DVD, run:

```
DVD_DRIVE:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64\suppo
rt\vcredist_x64.exe (This is the Visual C++ redistributable package).

DVD_DRIVE:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64\sampl
e_install_activedirectory_snapins_64bit.bat
```

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

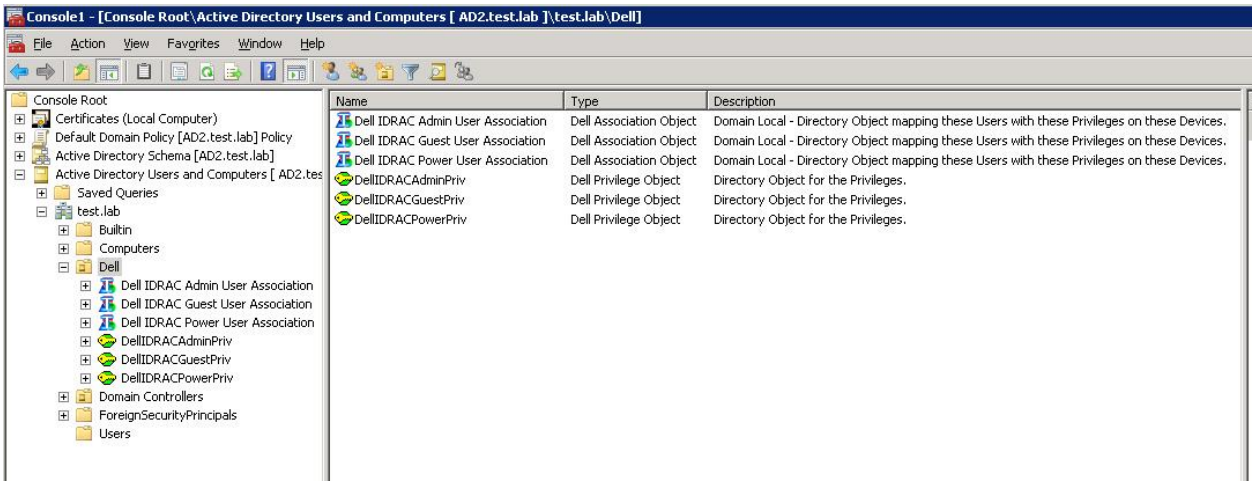
The Dell Active Directory Snap-in extension is not fully functional in the Server Manager console. For full functionality, use Microsoft Management Console as per the following steps.

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

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

1. Go to **File** > **Add/Remove Snap In**.
2. Select **Active Directory Users and Computers**, click **Add**, and then click **OK**.
3. Expand **Active Directory Users and Computers** and then expand the domain name (**test.lab**). A new container named Dell containing six iDRAC objects is displayed. There are three association objects (Admin, Guest, and Power User) and three levels of corresponding privilege objects as shown in the following figure.

Figure 18. Dell iDRAC Objects



Privilege and Role Names

The privilege names and role names are a different in Active Directory versus the iDRAC GUI as they are renamed for iDRAC7. The earlier names are retained in the Active Directory schema extension for backward compatibility.

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

Table 2. Role Names

Prior PowerEdge Generations (in Active Directory)	Current PowerEdge Generation (in iDRAC GUI)
Admin	Administrator
Power User	Operator
Guest	Read Only

Table 3. Privilege names

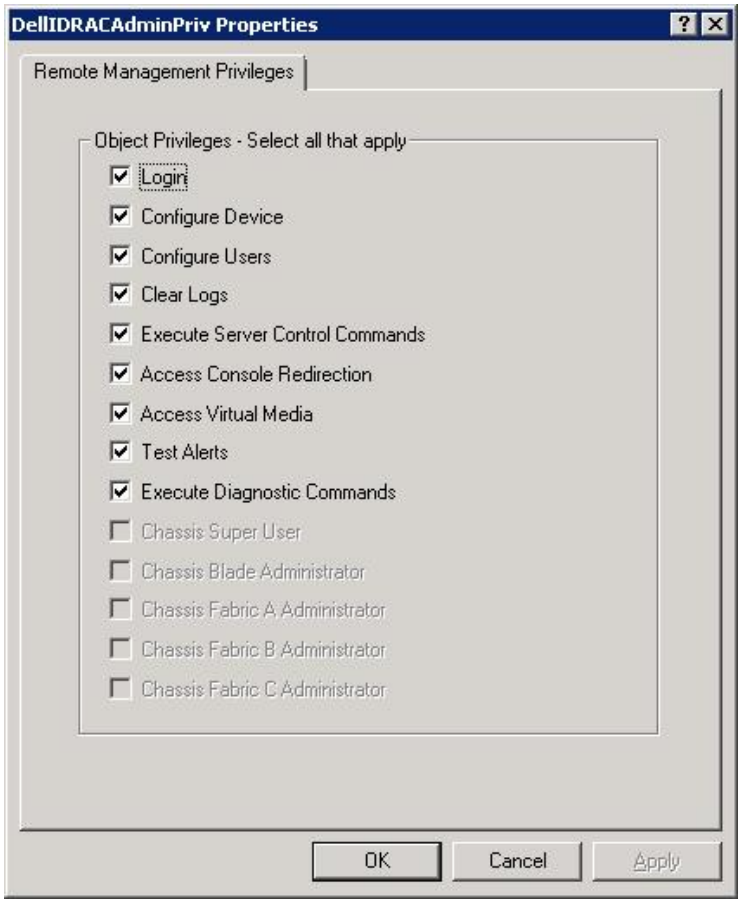
Prior PowerEdge Generations (in Active Directory)	Current PowerEdge Generation (*Local User* Privileges in iDRAC GUI)
Login	Login
Configure Device	Configure
Configure Users	Configure Users
Clear Logs	Logs
Execute Server Control Commands	System Control
Access Console Redirection	Access Virtual Console
Access Virtual Media	Access Virtual Media
Test Alerts	System Operations
Execute Diagnostic Commands	Debug

Active Directory Objects

Privilege Objects

Right-click on **DellIDRACAdminPriv** and select **Properties**. The **DellIDRACAdminPriv Properties** dialog box is displayed.

Figure 19. DellIDRACAdminPriv Propertied Dialog Box



The privilege object lists all the privilege names. In this example, all the options are selected since this object controls the Administrator's privileges.

If it is DellIDRACGuestPriv object, only the Login option is selected. Similarly, DellIDRACPowerPriv has by default all but two options selected.

To customize user privileges, it is recommended to use the DellIDRACPowerPriv object by selecting the required options. This object represents the mid-level Power User (also known as the Operator) iDRAC role.

iDRAC Objects

An iDRAC object is created for each physical iDRAC that is integrated 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.

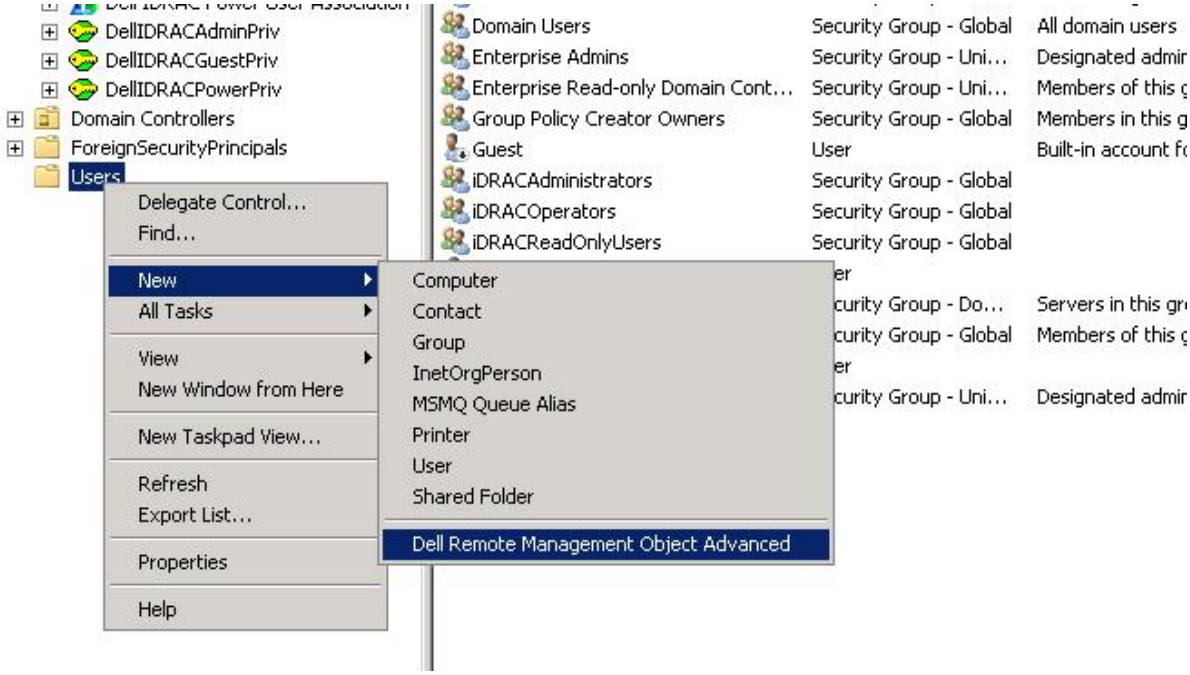
Configuring Active Directory

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 fewer privileges for the same iDRAC object.

1. In the **Console** window, in the left pane, right-click on **Users** and select **New** > **Dell Remote Management Object Advanced**.

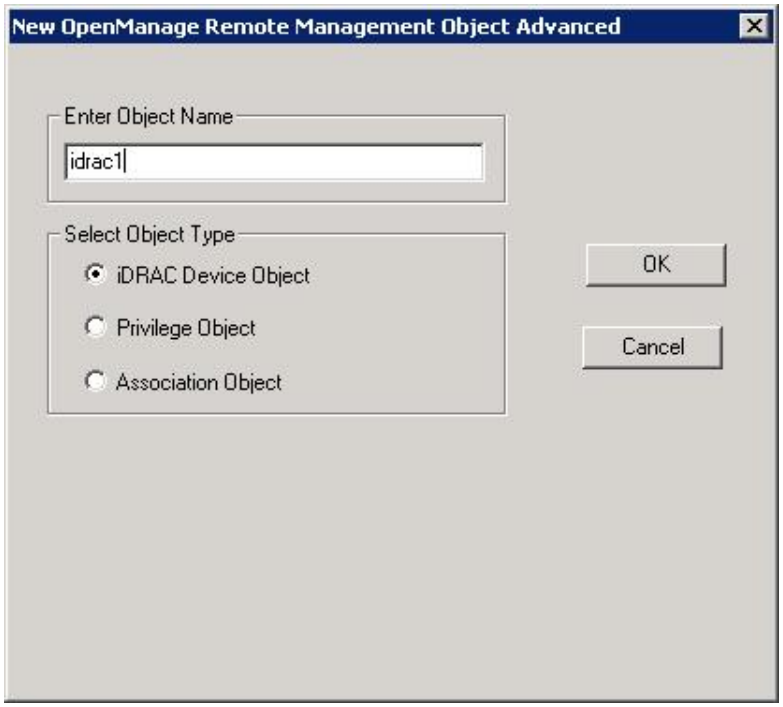
   Note: This option is not available if you are using the Server Manager console. Make sure you are using MMC.

Figure 20. Creating a New Dell Object



The **New OpenManage Remote Management Object Advanced** window is displayed.

Figure 21. Entering Object Name



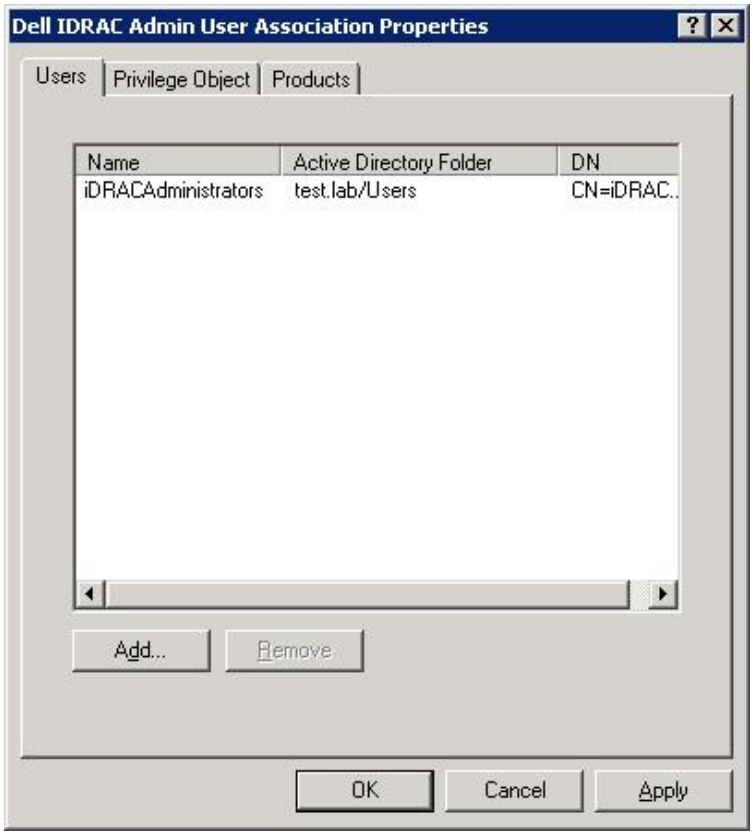
2. In the **Enter Object Name field**, type a unique name for the iDRAC object. For example, **idrac1**.
3. Select the **iDRAC Device Object** option and click **OK**. The iDRAC device object appears in the Users container in Active Directory.

Figure 22. iDRAC Device Object

4. Expand the Dell Container under yourdomain.com (**test.lab**), right-click on **Dell iDRAC Admin User Association** and select **Properties**.

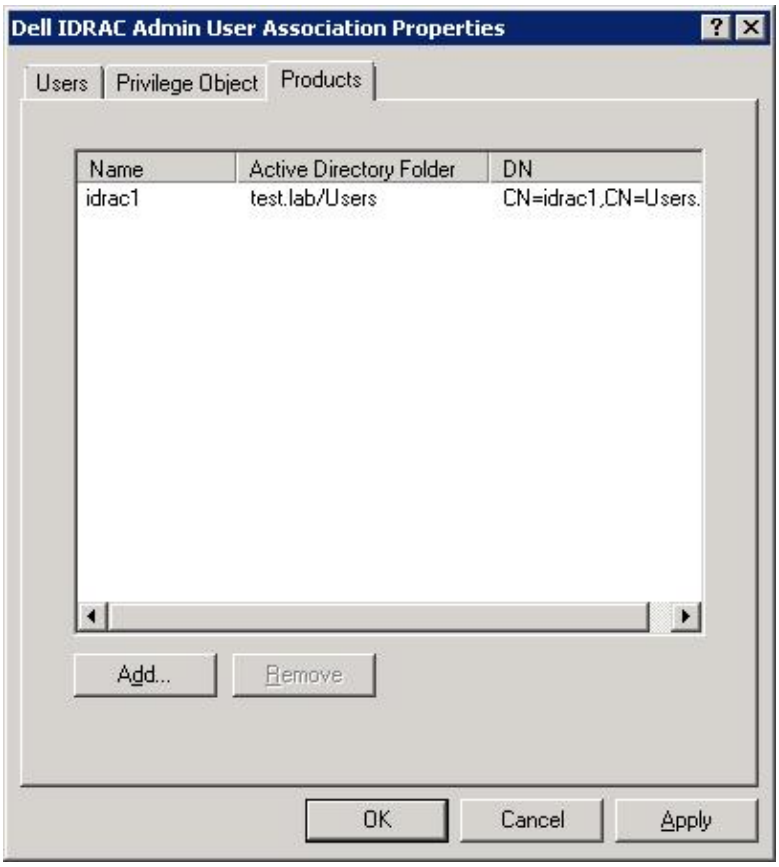
    - On the **Users** tab, click **Add** > **Object Types** > select **Groups**, and then click **OK**.
    - Under **Enter the object names to select**, enter **iDRACAdministrators**, click **Check Names**. The object should be found as shown by an underline, and then click **OK**.

Figure 23. Configuring the Admin User Association Object



5. Click the **Privilege Object** tab. It is pre-populated with the **DellAdminPriv** object.
6. On the **Products** tab, click **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**.

Figure 24. Configuring the iDRAC Admin User Association Object (continued)



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** field, enter **iDRACReadOnlyUsers** and click **Check Names** (it must display the object). Click **OK**.
    - The **Privilege Object** tab is pre-populated with the **DellGuestPriv object**.
    - On the **Products** tab, click **Add**.
    - Enter the **iDRAC name** (idrac1) and click **Check Names** (it must display the object). Click **OK** and again click **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**. Click **OK**.
    - In the **Enter the object names to select** field, enter **iDRACOperators** and click **Check Names** (it must display the object). Click **OK**.
    - The **Privilege Object** tab is pre-populated with the **DellPowerPriv object**.
    - On the **Products** tab, click **Add.**

- Enter the DRAC name (**idrac1**) and click **Check Names** (it must display the object). Click **OK** and again click **OK**.

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 need to set up additional iDRACs, create a new iDRAC object with a unique name for each object (such as idrac2, idrac3, and so on). 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** field 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** option.

Configuring iDRAC For Use With Active Directory Extended Schema

On the management station, log into the iDRAC GUI of the managed system using a browser:

https://<idrac_ip_address>

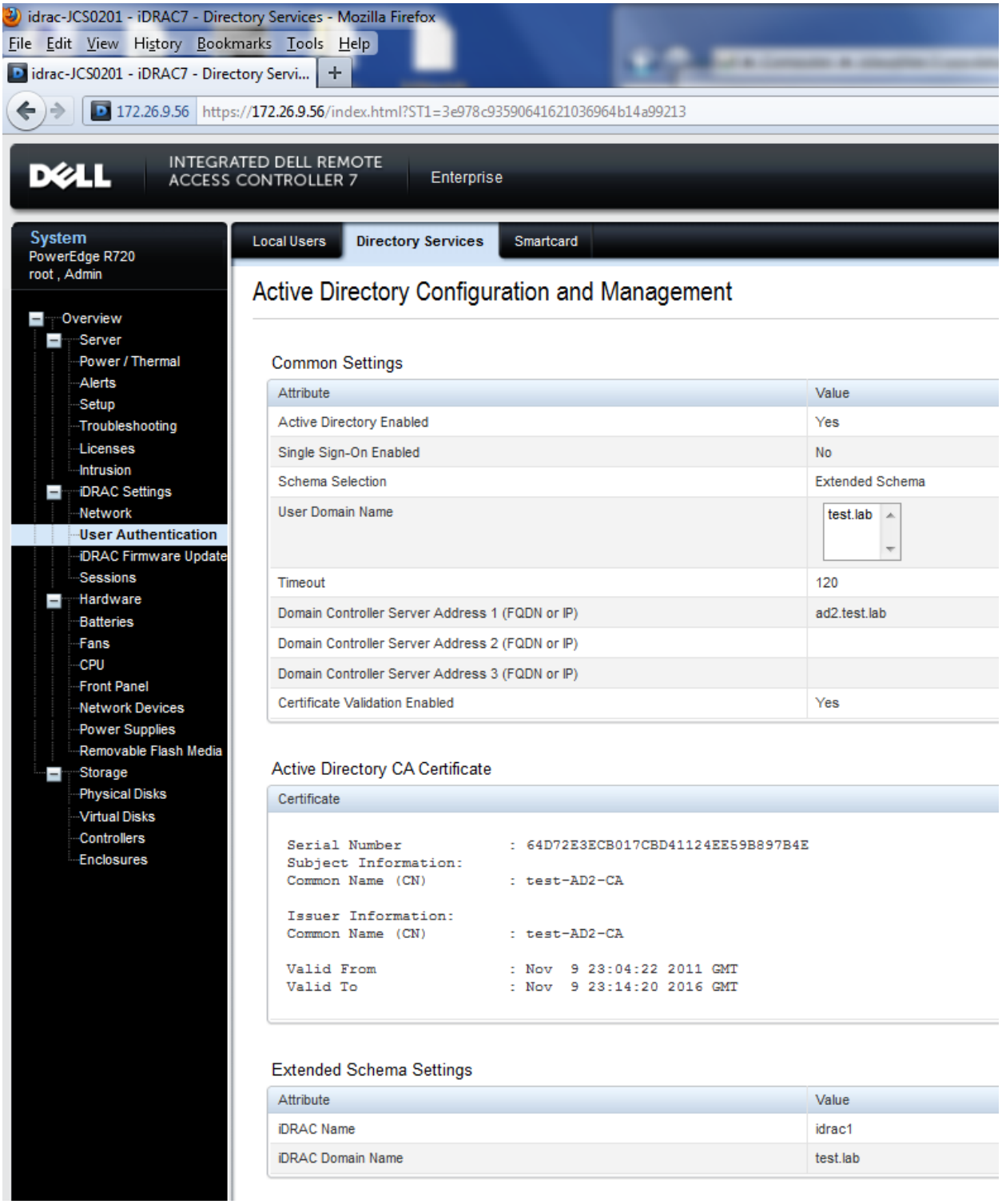
The iDRAC Network Settings can remain as previously configured for Standard Schema authentication. To review these settings, see Configuring the iDRAC7 Network Settings in the Standard Schema configuration section.

1. Go to **iDRAC Settings** > **User Authentication** > **Directory Services:**
    a. Make sure **Microsoft Active Directory** is selected and click the **link** or **Apply**.
    b. Scroll Down to bottom of page and click **Configure Active Directory**.
    c. Make sure **Enable Certificate Validation** is selected and the certificate uploaded during Standard Schema configuration is shown under **Current Directory Service CA Certificate**.
    d. Click **Next**.
    e. Make sure **Enable Active Directory** is selected.
    f. Make sure **Enable Single Sign-On** is not selected.
    g. For **User Domain Name**, make sure the **FQDN of your domain name** is specified (for example, test.lab).
    h. Make sure **Specify Domain Controller Addresses** is selected and the **FQDN of your Domain controller** is present for **Domain Controller Server Address 1**. (For example, ad2.test.lab).
    i. Click **Next.**
    j. Select **Extended Schema,** and then click **Next.**
    k. For **iDRAC Name**, use the name of the iDRAC object you created in Active Directory (for example, **idrac1**).

l. Specify the **iDRAC Domain Name** (for example, **test.lab).**

m. Click **Finish**. A summary page similar to the following is displayed.

Figure 25. Active Directory Configuration and Management summary page



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

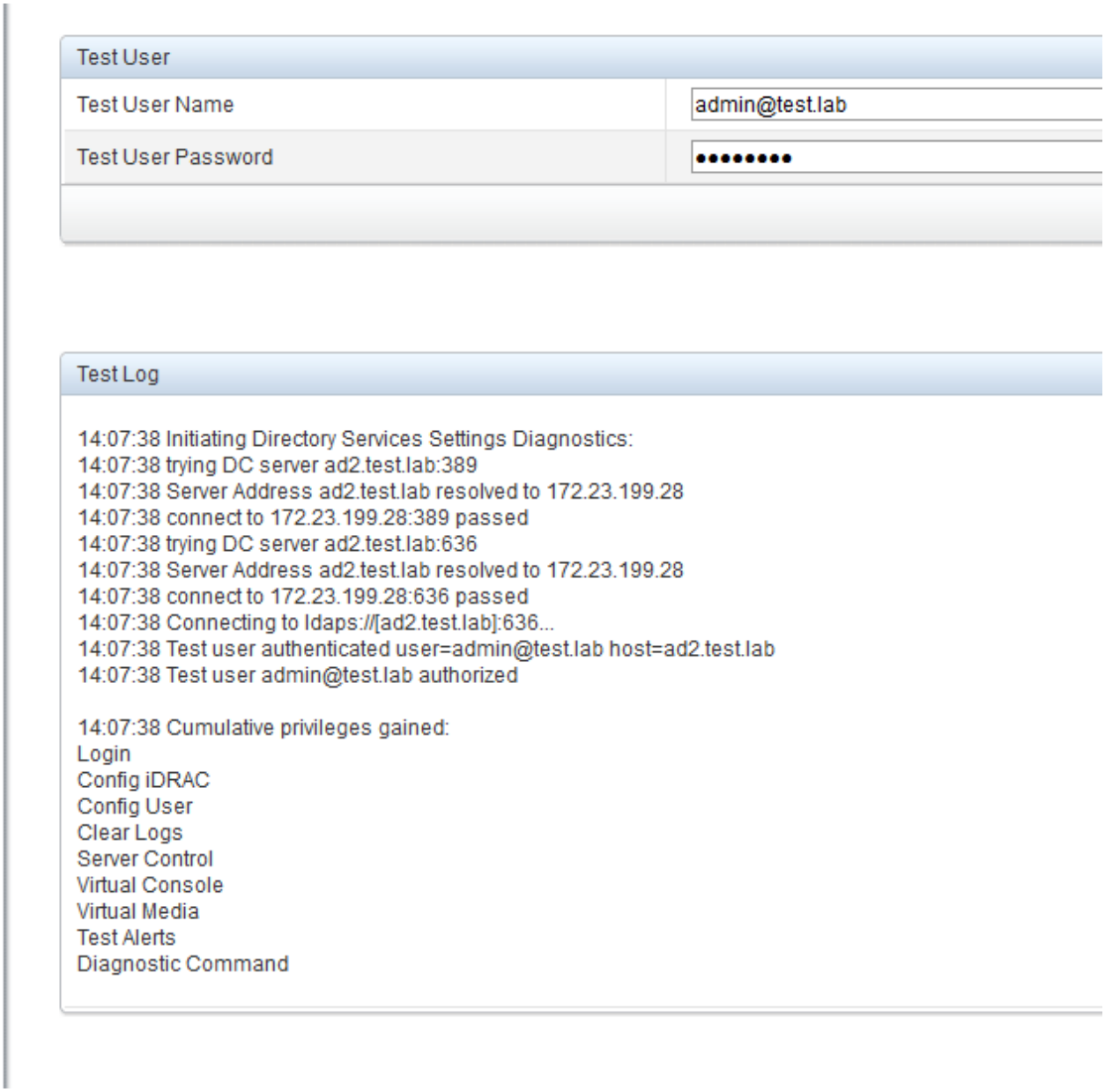
Testing Extended Schema Configuration

1. Scroll down to the bottom of the **Active Directory Configuration and Management Summary** page, and click **Test Settings**.
2. In **Test User Name** field, type the administrative user in username@domain.com format. For example, **admin@test.lab**.
3. In the **Test User Password** field**,** 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 must be marked Not Applicable/Not Configured/Not Run.

The **Test Log** at the bottom of page must have no errors and must list all nine privileges in the **Cumulative privileges gained** section as shown in the following figure.

Figure 26. Test Results for Administrative User.



It is recommended that you also run the test for users with lower privilege levels (the users that were named readonly and operator earlier) to confirm everything is configured correctly.

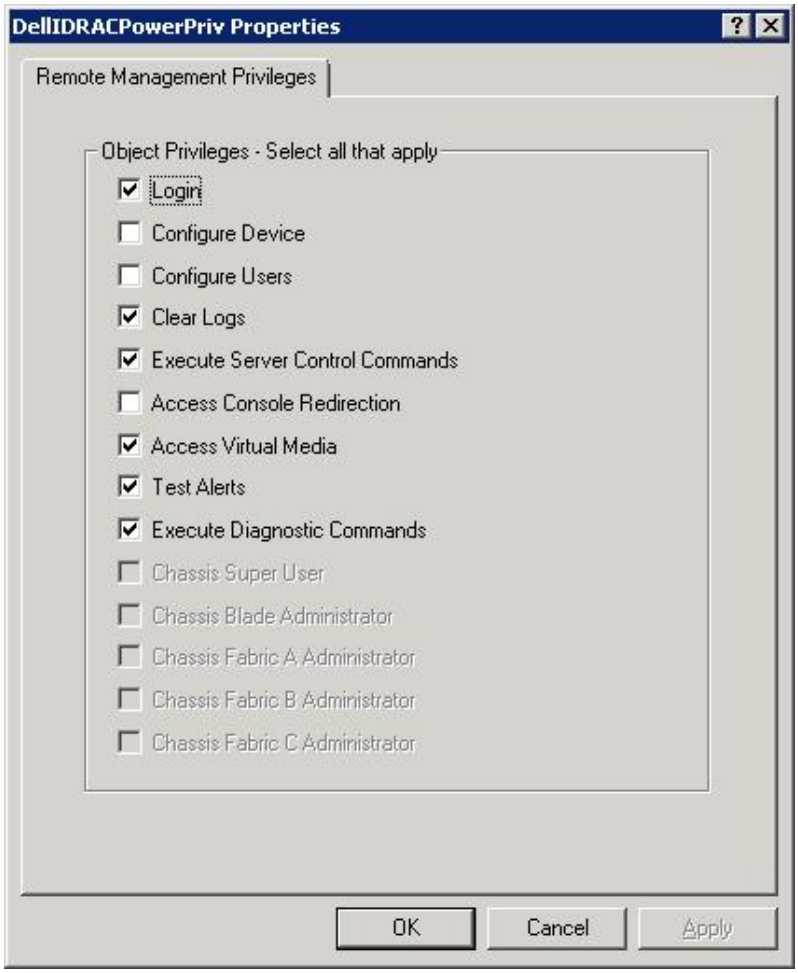
You can now authenticate to the iDRAC for all services (RACADM, WSMAN, SSH, Telnet, and the GUI) as shown earlier in the Authentication Examples section.

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.

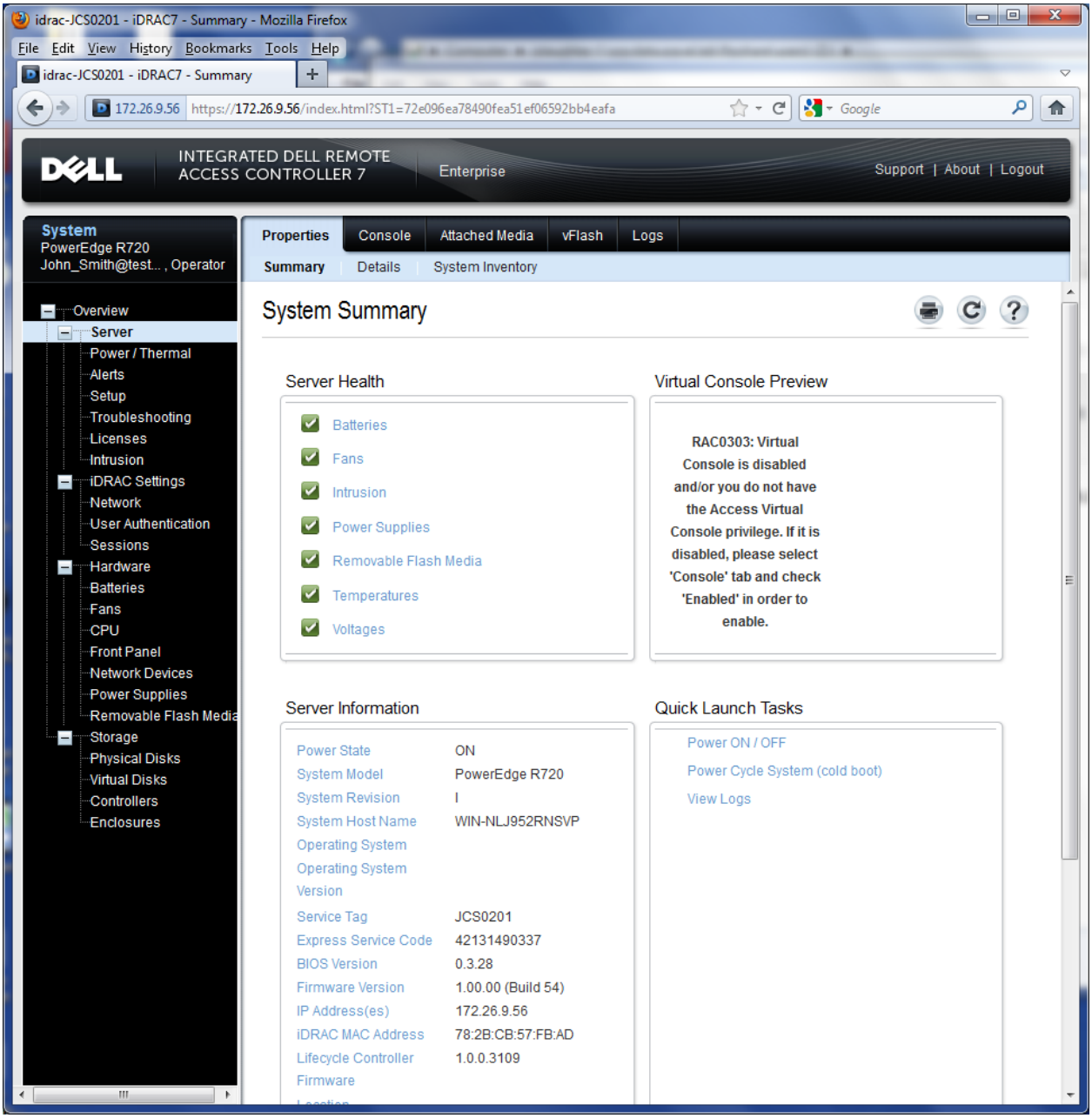
1. At the Domain Controller, under **Active Directory Users and Computers** create a new user with the login name **John_Smith**. Assign a password and clear the **User must change password at next logon** option.
2. Add **John_Smith** to the **iDRACOperators** group.
3. Customize the privileges John_Smith (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 **DellIDRACPowerPriv** and select **Properties**.
5. Clear the **Access Console Redirection** option as shown in the following figure.

Figure 27. Configuring Custom Privileges.



6. Click **OK**.
7. At the **management station**, log out of the iDRAC GUI.
8. Log into the iDRAC GUI as John_Smith. Make sure to specify the domain (**test.lab**). A **System Summary** page similar to the following figure is displayed.

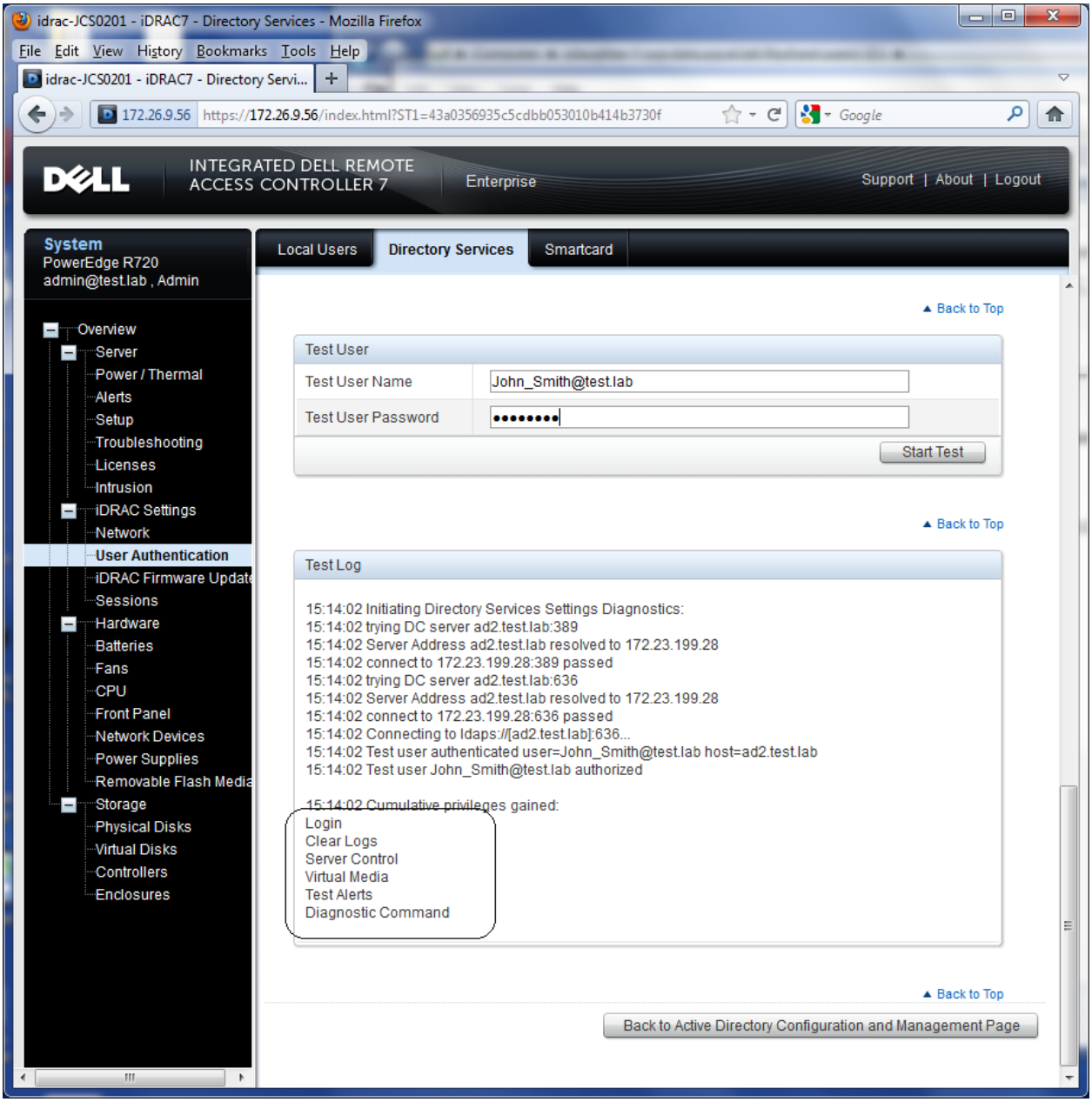
Figure 28. John Smith's System Summary page



Notice the **Virtual Console Preview** section (upper right of Summary Page) is not shown and is replaced with a message indicating that 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 previous step.

9. Test the settings for John_Smith's privileges to confirm everything is configured properly:
    a. Log out and log back in as an *administrative* user in the iDRAC GUI.
    b. Go to **iDRAC Settings** > **User Authentication** > **Directory Services** > **Microsoft Active Directory** > **Test Settings**.
    c. Enter **John_Smith@yourdomain.com** (John_Smith@test.lab), John's password, and then click **Start Test**.
    d. The results must match the privileges configured in the earlier steps 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.