Integrate iDRAC with Microsoft's Active Directory

This Dell technical white paper explains how to integrate and test iDRAC with Microsoft's Active Directory authentication, Single Sign-On, and Smart Card Logon

Dell Engineering
August 2014

Author:
Doug Roberts

Dell | Enterprise Solutions Group

A Dell Technical White Paper

Table of contents

Executive Summary

Using Active Directory to manage Dell's Integrated Dell Remote Access Controller (iDRAC) allows an administrator to manage all the iDRAC user accounts and privileges from a central location and provides better access control through the security group management. It also allows you to use Single Sign-On (SSO) or Smart Card Logon (SCL) for authentication.

There are a few mechanisms used to configure iDRAC Directory Services to communicate with Microsoft's Active Directory. This paper explores those mechanisms and helps Dell customers understand the integration process.

1 Introduction

Integrating a client with Microsoft's Active Directory for authentication can be complex. This paper provides step-by-step instructions to configure user authentication through Active Directory to log in to iDRAC. Once this integration is complete, you can configure Single Sign-On and Smart Card Logon.

The integration steps provided in this document is for iDRAC8 but also applies to iDRAC7. When referring to iDRAC, it applies to both iDRAC7 and iDRAC8 unless otherwise specified.

Configuring iDRAC is a four step process:

1. Importing a certificate for secure communications.
2. Setting the domain parameters.
3. Selecting a schema.
4. Configuring that schema.

This document uses the Web interface to configure iDRAC for use with Active Directory. This can also be accomplished using RACADM.

1.1 Standard and Extended Schemas

iDRAC supports two methods of integration with Active Directory, Standard Schema and Extended Schema.

Standard Schema uses Microsoft's default group objects. Using this method, the Active Directory group names and privileges must be defined on each iDRAC.

Extended Schema uses customized Active Directory objects. The customized objects are obtained by extending the Active Directory schema. It provides centralized management to define user access and privileges of each iDRAC.

See *Integrated Dell Remote Access Controller User's Guide* for more information about *Supported Active Directory Authentication Mechanisms*.

1.2 Active Directory Login Syntax

There are three login formats allowed for authenticating as an Active Directory user:

- *<username@domain>*
- *<domain>\<username>*
- *<domain>/<username>*

Where, *username* is an ASCII string of 1–256 bytes.

White space and special characters (such as \, /, or @) cannot be used in the user name or the domain name.

Note: The domain name must be a Fully Qualified Domain Name. For example **test.lab/admin** is a valid Active Directory user; **test/admin** is not valid.

1.3 Supported Active Directory Configurations

iDRAC supports an Active Directory configuration in mixed mode and across multiple domains in a single forest. The standard and extended schemas have guidelines that should be followed when configuring the user group types and user groups in different configurations. See Integrated *Dell Remote Access Controller User's Guide* for more information supported Active Directory configurations.

1.4 Test Environment

The test environment described in this paper resides on an isolated node. For simplicity, the test environment is constructed as follows:

- **Domain Controller:** Microsoft's 2012 Enterprise Server.
- **Managed system**: PowerEdge R730 Server with iDRAC8.
- **Management Station**: Windows 7 system.

The 2012 Server is the Domain Controller and has Active Directory, certificate service, DHCP, and DNS installed. The Active Directory infrastructure consist of a single domain, ***test.lab***, within a single forest. The name of the Domain Controller is ***Harpo***. The Fully Qualified Domain Name (FQDN) is ***harpo.test.lab*** .

The iDRAC has an Enterprise license installed. To use Directory Services on iDRAC, an Enterprise license is required.

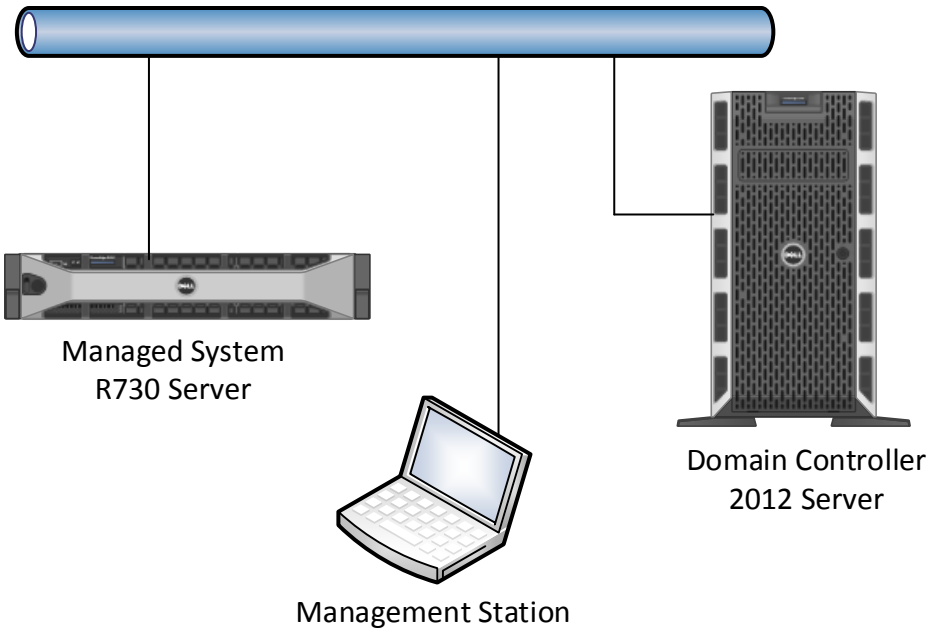

Figure 1 Test Environment

1.5 Before You Begin

Before you configure iDRAC to use with Active Directory, you must have:

- Working knowledge of networking, Microsoft's Active Directory, and Certificate service.
- Knowledge to add Users and Groups in Active Directory.
- Experience working with SSL certificates and access to root CA certificate exported from the Certificate Authority.

See the Microsoft's website for more details regarding Microsoft's 2012 Server and Active Directory. Use Google to search topics that may be unfamiliar.

2 Integrate iDRAC with Microsoft's Active Directory

To start configuring iDRAC using the web interface, log into iDRAC Web interface with administrative privileges. The first step is to configure the network setting properly, and then configure the Active Directory settings. The default settings remains unchanged where appropriate.

2.1 iDRAC Network Settings

You must configure the network DNS setting so that the iDRAC is able to communicate with the Domain Controller using its Fully Qualified Domain Name (FQDN). Set the DNS DRAC Name, if not already defined, and set the DNS Domain Name. It is recommended that iDRAC register with the DNS (required for use with Kerberos).

To configure the network settings, go to **Overview > iDRAC Settings > Network > Common Settings**. Enter the details as shown and click **Apply**.

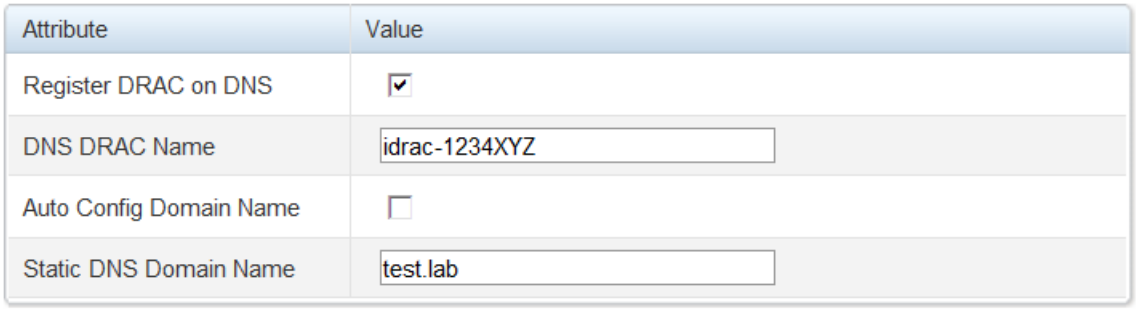

Figure 2 Network Common Settings

2.2 Enabling Active Directory Services

Go to **Overview > iDRAC Settings > User Authentication > Directory Services.** Select the **Microsft Active Directory** option and click **Apply.**

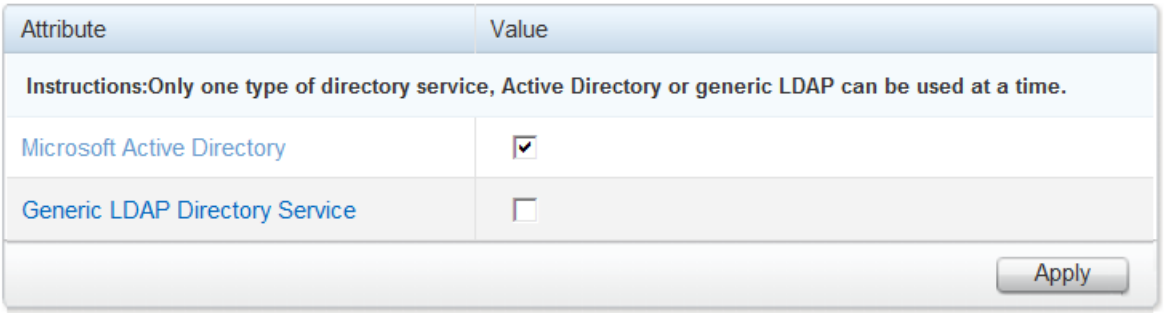

Figure 3 Directory Service

The Active Directory Configuration and Management page is displayed that contains the current Active Directory Configuration and Management settings. To configure Active Directory, scroll down to bottom of the page and click **Configure Active Directory**.

2.3 Configure Digital Certificate

Enable the digital certificate validation to be used during initiation of SSL connections when communicating with the Active Directory server.

Figure 4 Certificate Settings

After enabling certificate validation, a certificate from the Certificate Authority CA must be uploaded to iDRAC. This certificate is used by the Active Directory server during initiation of SSL connections. The CA's certificate is used to validate the authenticity of the certificate provided by the Active Directory.

Click **Choose File**, select the CA certificate, and click **Upload**.

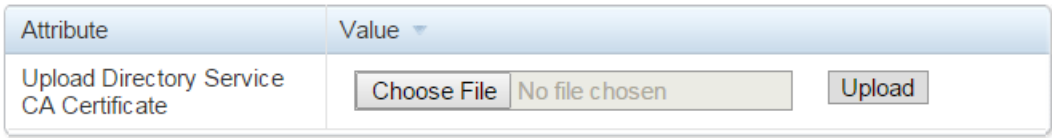

Figure 5 Upload Directory Service CA Certificate

After the certificate the uploaded, it is displayed in the **Current Directory Service CA Certificate** section.

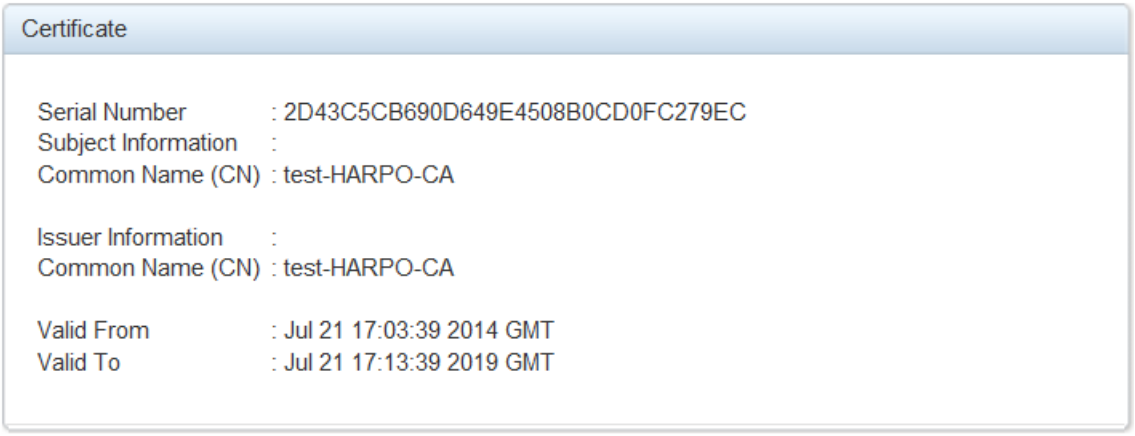

Figure 6 CA certificate

Click **Next**.

2.4 Configure Active Directory Domain Information

Enter the location information about the Active Directory server. Optionally, specify the User Domain Name. If specified, it helps simply the user login syntax. The configured domain name will be added to the drop-down list in the **Login** page. The defined Active Directory domains contain the iDRAC user accounts. When specifying the Domain Controllers, the iDRAC provides two options:

- **Lookup Domain Controllers with DNS:** Use DNS lookup to obtain the Active Directory Domain Controller. The DNS lookup uses the user Domain from Login or user specified.
- **Specify Domain Controller Addresses:** Use the Fully Qualified Domain Name (FQDN) or IP address of the Domain Controller. This option does not use DNS lookup.
  At least one of the three addresses is required to be configured. iDRAC attempts to connect to each of the configured addresses one-by-one until a successful connection is made.

If Extended Schema is selected, these are the addresses of the domain controllers where the iDRAC device object and association objects are located.

If Standard Schema is selected, these are the addresses of the domain controllers where the user accounts and the role groups are located.

Note: The FQDN or IP address that is specified for Domain Controller Server Address field must match the Subject or Subject Alternative Name field of your domain controller certificate if you have enabled certificate validation.

Now configure the location information about the Active Directory server and click **Next**.

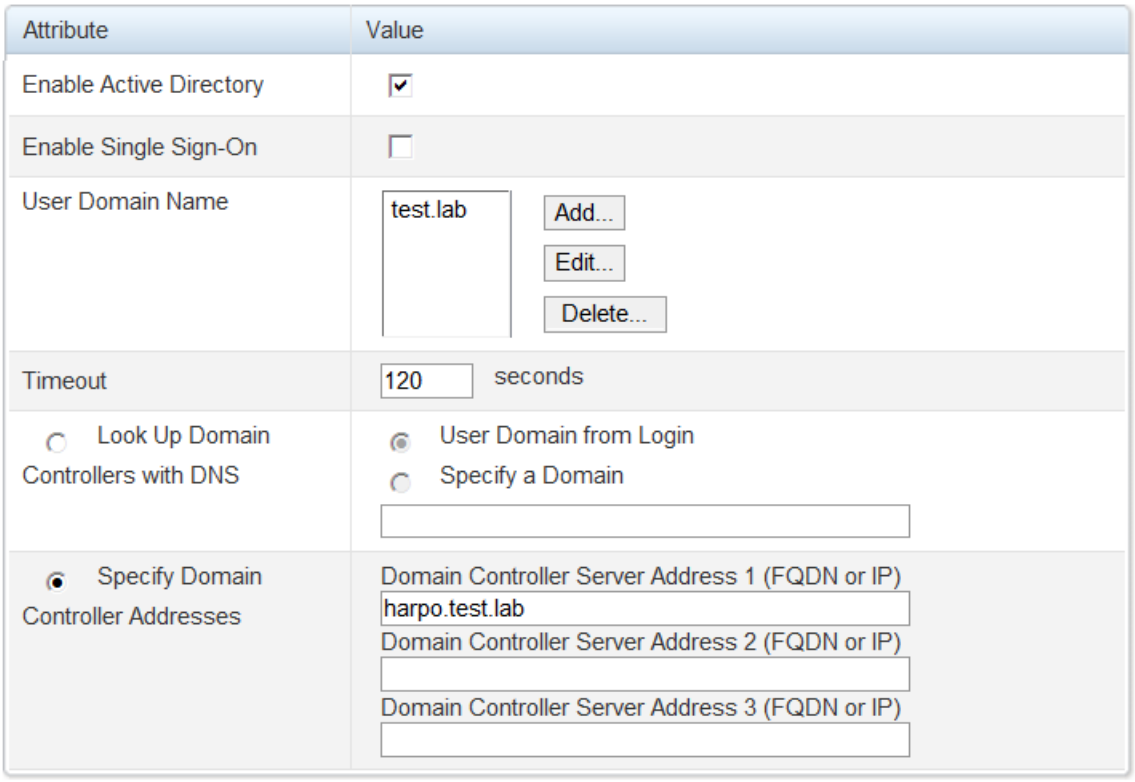

Figure 7 Domain Common Settings

2.5 Configure Standard Schema

Select the Schema mode as **Standard Schema** and click **Next**.

Figure 8 Standard Schema Selection

2.5.1 Standard Schema Users and Groups on AD Server

When using standard schema mode, all the necessary object classes are provided by Microsoft's default configuration of the Active Directory schema. The Role Groups defined in the **Active Directory Configuration and Management** page on iDRAC should be defined as Groups on the Active Directory server.

On the Active Directory server, create the following Groups and Users. Make each user a member of its corresponding group.

Groups	Users
iDRACAdministrators	admin
iDRACOperators	operator
iDRACGuests	guest

2.5.2 Standard Schema Settings

Under **Standard Schema Settings**, configure the location of the Active Directory Global Catalog server. There are 2 options for selecting a Global Catalog Server:

- **Look Up Global Catalog Servers with DNS:** Use DNS lookup to obtain the Active Directory Global Catalog Server. DNS lookup uses the specified Root Domain Name. iDRAC attempts to connect to each of the addresses returned by the DNS lookup, until a successful connection is made.
- **Specify Global Catalog Server Addresses:** Use the Fully Qualified Domain Name (FQDN) or IP address of the Domain Controller. This option does not use DNS lookup. At least one of the three addresses is required to be configured. iDRAC attempts to connect to each of the configured addresses one-by-one until a successful connection is made.

Note: The FQDN or IP Address that is specified for the Global Catalog Server Address field must match the Subject or Subject Alternative Name field of your Domain Controller certificate if certificate validation is enabled.

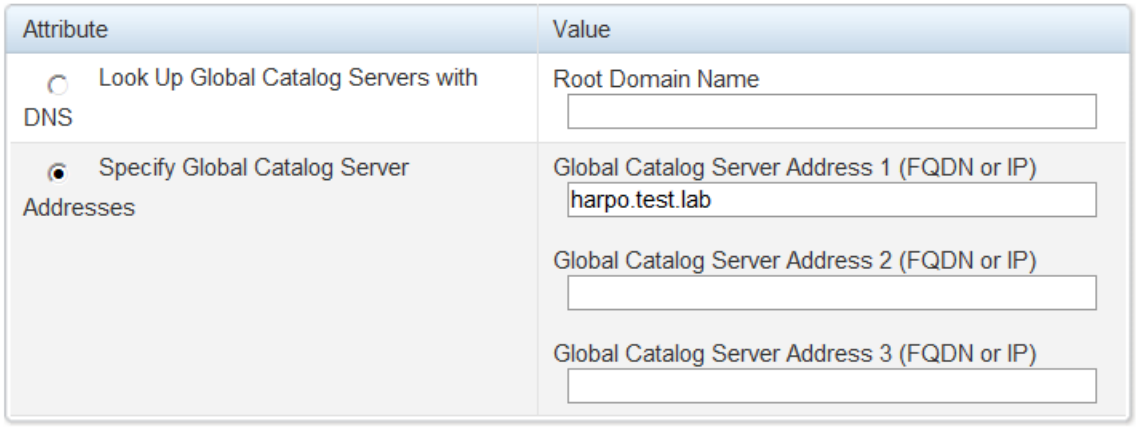

Figure 9 Standard Schema Settings

Note: A Global Catalog Server is required only for standard schema when the user accounts and role groups are in different domains.

Now configure the Role Groups. The Standard Schema Role Groups are used to specify authorization policy for iDRAC users. Each group can enforce authorization policy regarding access to iDRAC features.

In the **Role Groups** column, click the link(s) to configure the role group name, domain and the role group privileges. Up to five role groups can be defined in each iDRAC. The Group Names should match the Groups defined on the Active Directory server earlier.

Role Groups	Group Name	Group Domain	Group Privilege
Role Group 1	iDRACAdministrators	test.lab	Administrator
Role Group 2	iDRACOperators	test.lab	Operator
Role Group 3	iDRACGuests	test.lab	Read Only
Role Group 4			None
Role Group 5			None

Figure 10 Standard Schema Role Groups

Click **Finished**.

2.5.3 Testing Standard Schema Settings

Use the test feature in iDRAC to validate the Active Directory configuration. Click **Test Settings** at the bottom of page.

Enter username of user in **iDRACAdministrators** group along with password.

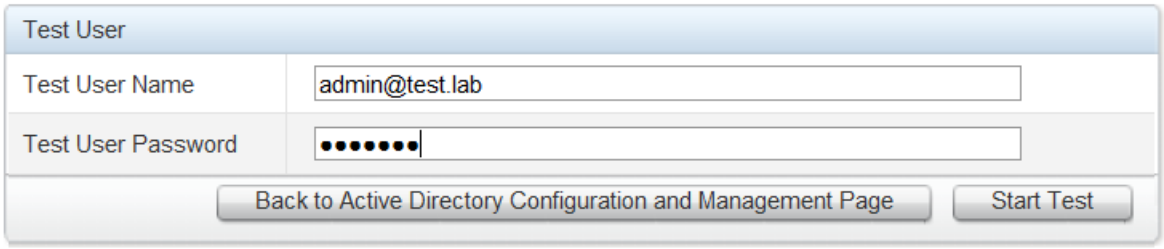

Figure 11 Test admin User

Click **Start Test**.

All tests must pass (including certificate validation) or be marked Not Applicable/Not Configured. The Test Log at the bottom of the page should be error-free and list all the nine privileges in the cumulative privilege gained section.

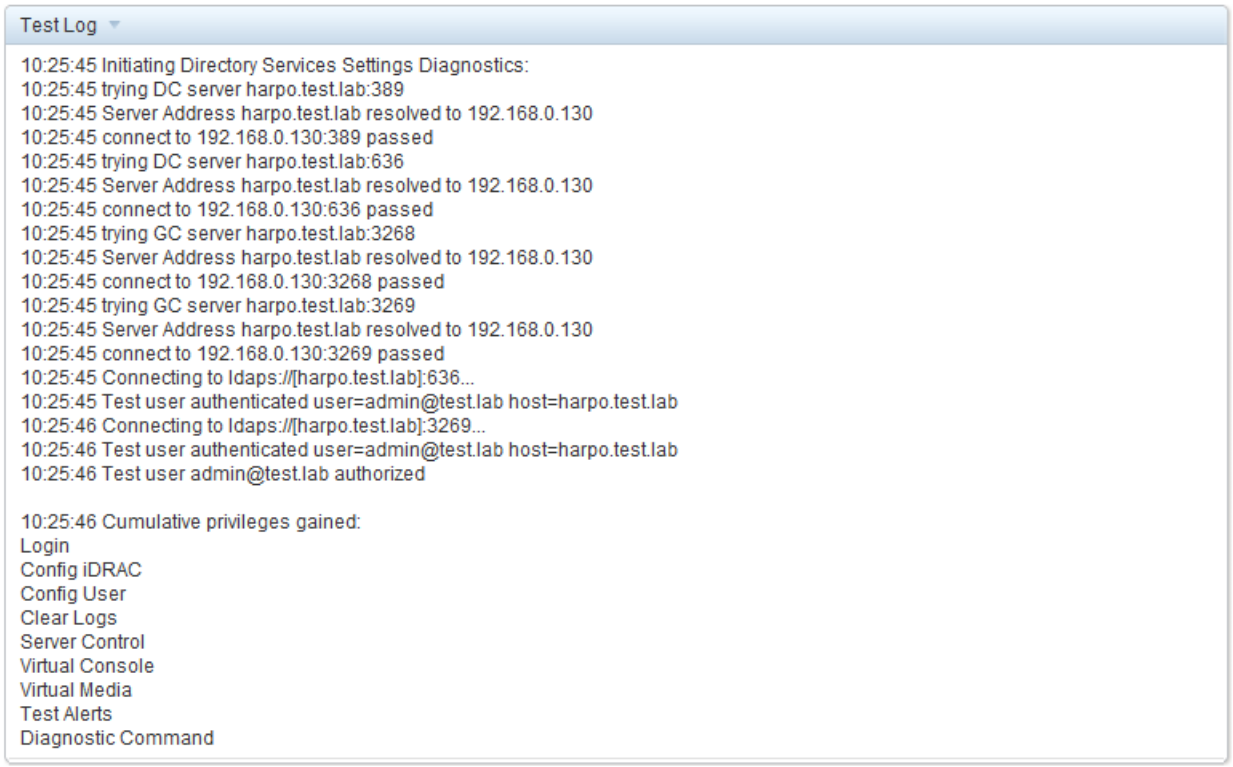

Figure 12 Test Log

Repeat the test using other users created, notice privileges gained on operator and guest users.

2.6 Configure Extended Schema

Select the Schema mode as **Extended Schema** and click **Next**.

Attribute	Value
Extended Schema	◉
Standard Schema	○

Figure 13 Extended Schema Selection

2.6.1 Extended Schema Users and Groups on AD Server

To use the extended schema mode, a new object class must be added to the Active Directory schema. Dell has extended the schema to include n *Association, Device and Privileges*. To extend the schema, install Dell's Active Directory Snap-In Utility on the Active Directory server.

The Dell Active Directory Snap-In Utility can be downloaded from the following link.

http://www.dell.com/support/drivers/us/en/19/driverdetails?driverid=H4P8Y

Follow the instructions to complete the installation. Once completed, open the Active Directory Users and Computers tool. A new **Dell** Organizational Unit (OU) should have been created as shown. Inside the new OU are predefined Association objects and Privilege objects as shown.

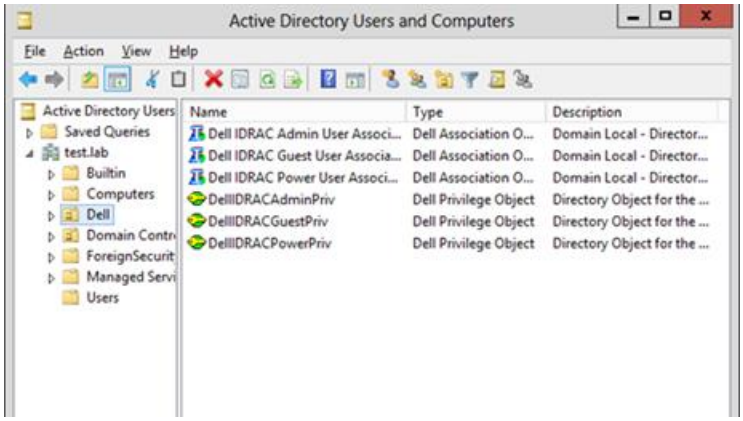

Figure 14 Predefined Association and Privilege Objects

An iDRAC object is required to represent each physical iDRAC device.

To create a device and associate the device to a set of predefined privileges:

1. Select the **Dell** Container. Right-click, go to **New > Dell Remote Management Object Advanced**.
2. Enter the iDRAC device name.

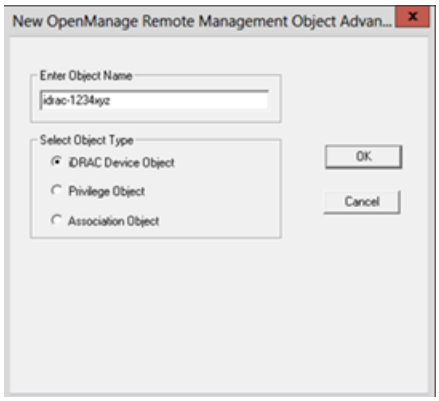

Figure 15 New OpenManage Remote Management Object Advanced

3. Click **OK**.

To add the iDRAC device to the predefined Admin association object.

1. Click the **Dell** container under ***test.lab***.
2. Select **Dell iDRAC Admin User Association > Properties**.
3. Click the **Products** tab; **Add >** type **iDRAC Name > Check Names** (it should be found).

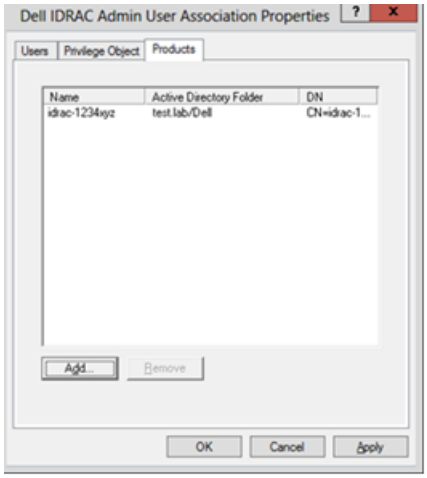

Figure 16 Dell iDRAC Admin User Association Properties

4. Click **OK.**

To add iDRAC device to Dell iDRAC Power User Association and Dell iDRAC Guest User Association, repeat the previous steps

Finally, add the users to the Association objects:

1. Click on the Dell container under ***test.lab***.
2. Select **Dell iDRAC Admin User Association > Properties**.
3. Click on **Users** tab.

4. Click **Add**; then type **admin > Check Names** (it should be found). Name should appear in list with other user names.

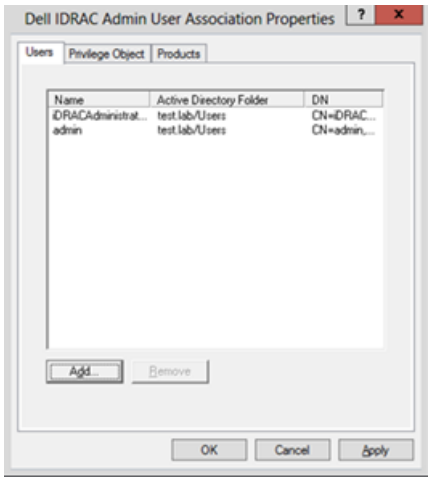

Figure 17 Dell iDRAC Admin User Association Properties

5. Click **OK**.

To add user **operator** to Dell Power User Association object and the **guest** to the iDRAC Guest User Association, repeat the previous step.

2.6.2 Configure iDRAC Device Name on iDRAC

Now that the schema has been extended and association objects defined on the Active Directory server, the iDRAC device name needs to be configured on iDRAC. First enter the iDRAC Name that uniquely identifies iDRAC in Active Directory. Second, enter the domain name where the iDRAC object is defined in Active Directory.

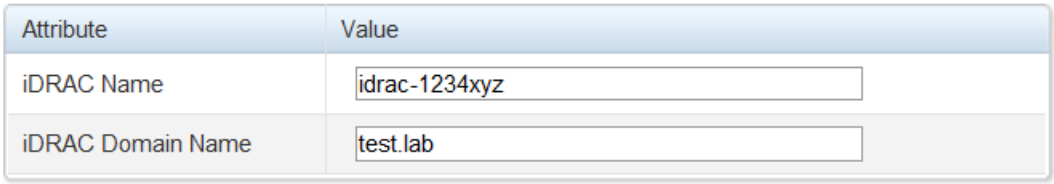

Figure 18 Extended Schema settings

Click **Finished**.

2.6.3 Testing Extended Schema Settings

Use the test feature in iDRAC to validate the Active Directory configuration. Click **Test Settings** at the bottom of page.

Enter username of user along with password.

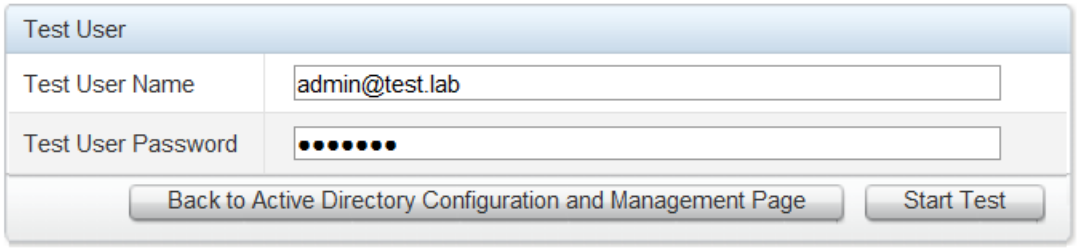

Figure 19 Test User

Click **Start Test**.

All tests must pass (including certificate validation) or be marked Not Applicable/Not Configured. The Test Log should be error-free and list all 9 privileges in the cumulative privilege gained section.

Repeat the test using the other users created, notice privileges gained on operator and guest users.

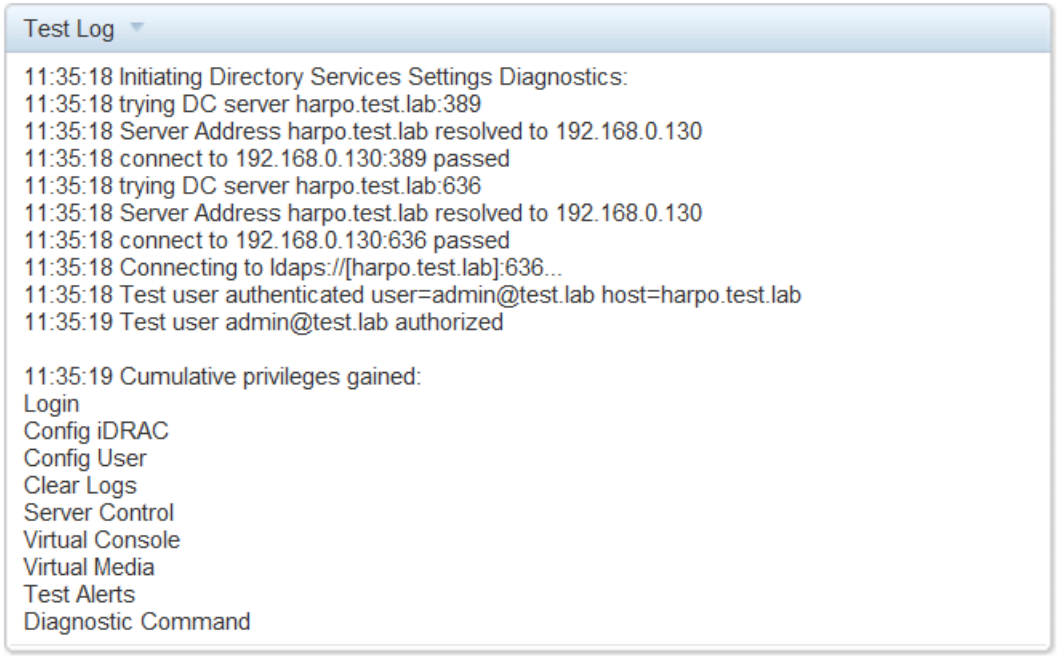

Figure 20 Test Log

3 Configure Single Sign-On and Smart Card Logon

iDRAC supports Kerberos authentication via Single Sign-On (SSO) and Smart Card Two Factor Authentication (SC-TFA) logon through the web interface. This section provides steps to configure iDRAC to use Single Sign-On and Smart Card Logon. This section assumes iDRAC is configured and tested with Active Directory.

Time Synchronization

The iDRAC time needs to be synchronized with the Active Directory Domain Controller time (plus or minus 5 minutes).

NOTE: If the time is not synchronized, Kerberos authentication on iDRAC is not successful.

DNS Forward and Reverse lookup

For Kerberos to operate properly, the iDRAC's Fully Qualified Domain Name (FQDN) must be registered in the DNS Forward and Reverse Lookup Zones. On the Domain Controller, open the DNS manager. Expand the Forward Lookup Zone and Reverse Lookup Zone to verify the iDRAC device name is in the table.

NOTE: If the FQDN does not match the reverse DNS lookup, Kerberos authentication is not successful.

Management Station

To use Single Sign-On, the management station must be a member of the Active Directory domain and the browser must be configured for SSO logon.

3.1 Integrate iDRAC With Kerberos KDC

3.1.1 Create Kerberos Keytab file on Active Directory Server

Before creating a keytab, the iDRAC user account must be created on the Active Directoy server. Each iDRAC device needs a unique user account in Active Directory. The iDRAC principal name will be mapped to this user account in the keytab file.

Open **Active Directory Users and Computers**. Expand ***test.lab***; Right-click on **User** container, go to **New > Users.** Enter a name and password for the user, select the **Password never expires** option and clear the **Change password on next reboot** option.

Select **Properties** of the new iDRAC user account, Click the **Account** tab, scroll through **Account** options and select the **This account supports Kerberos AES 256 bit encryption** option. This is the encryption type used when generating keytab. If a different encryption type is required, such as DES or AES128, select that option.

Figure 21 Create User for Device Keytab

Click **Apply > OK**.

Generate a Kerberos keytab file, which can be uploaded to the iDRAC server. Each iDRAC will have its own unique keytab file. On the Active Directory server, the **ktpass.exe** utility is used to create the file. The command syntax is:

```
ktpass -princ HTTP/idrac-1234xyz.test.lab@TEST.LAB -mapuser TEST\idrac-1234xyz-key  -mapop set –pass ******** -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -out c:\temp\idrac-1234xyz.keytab
```

Using the Fully Qualified Domain Name (FQDN) for the principal name and the iDRAC user account created earlier, generate a Kerberos keytab file.

NOTE: The keytab contains an encryption key and should be secured.

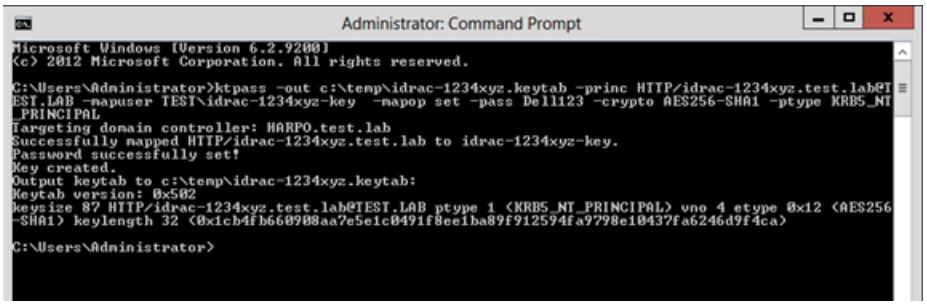

Figure 22 Generate a Kerberos Keytab File

Now that the keytab file has been created, the iDRAC user account needs to be configured for delegation. Right-click on iDRAC user and select **Properties**. Click the **Delegation** tab and select the **Trust this user for delegation to any service (Kerberos only)** option.

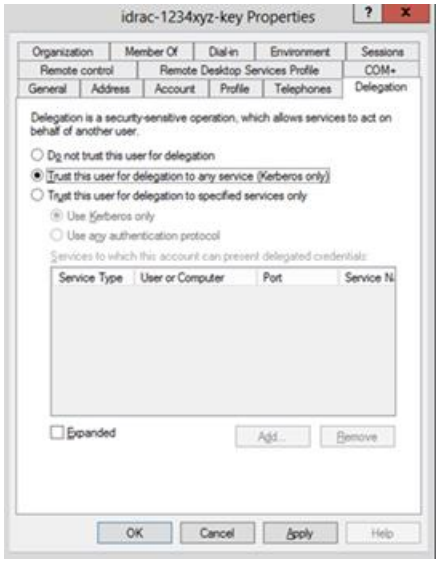

Figure 23 Trust User for Delegation

Click **Apply > OK**.

3.1.2 Upload Kerberos Keytab File in iDRAC

Go to **Overview > iDRAC Settings > User Authentication > Directory Services > Configure Active Directory**.

On the **Active Directory Management** page, click **Browse** and select the Kerberos keytab file.

Attribute	Value
Upload Kerberos Keytab	Browse... Upload
Current Kerberos Keytab	A valid Kerberos Keytab file is available in iDRAC.

Figure 24 Upload Kerberos Keytab File

Click **Upload > Next**.

3.2 Configure iDRAC for Single Sign-On

3.2.1 Enable Single Sign-On

Go to **Overview > iDRAC Settings > User Authentication > Directory Services > Configure Active Directory > Next.**

Now enable Single Sign-On in Common Settings

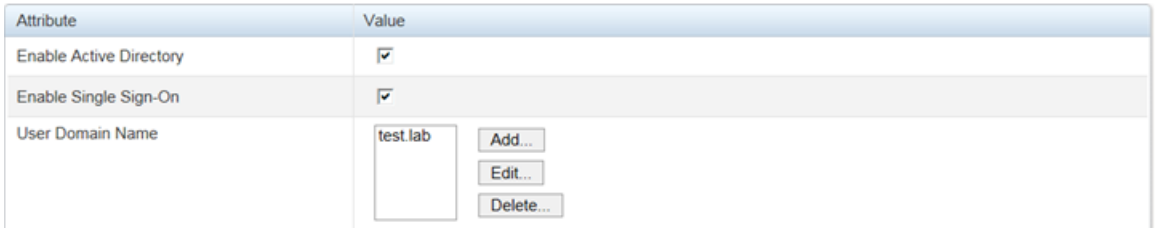

Figure 25 Enable Single Sign-On

Click **Next > Next > Finished**.

3.2.2 Configure and Test Single Sign-On on Management Station

For the management station to use Single Sign-On (SSO) to authenticate to iDRAC, the web browser(s) must be configured to support SSO.

3.2.2.1 Windows IE Browser

To enable Single Sign-On (SSO) support in Windows IE browser, go to **Tools > Internet Options > Security** and select the **Local Intranet**. Click **Sites**. Add the FQDN of the iDRAC or use a wildcard (*) to the trusted list. SSO only works using trusted URLs. Click **Add > Close > OK**.

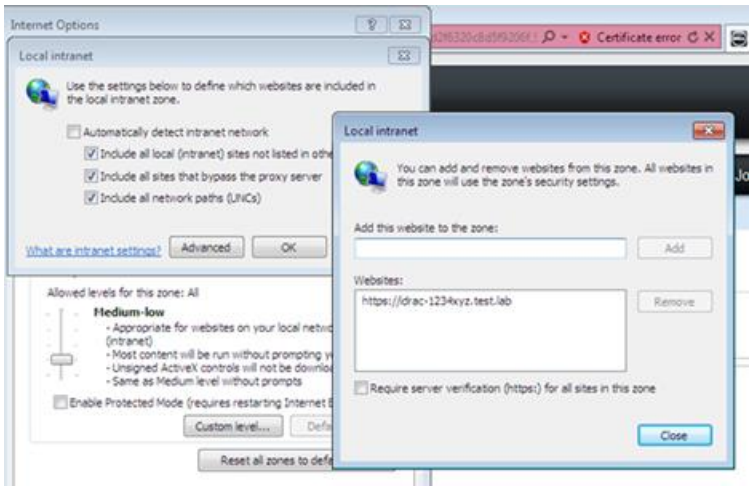

Figure 26 Configure IE for Single Sign-On

To configure the automatic authentication in the browser, from the **Security** tab, click **Custom level...**. Scroll to the bottom. Under **User Authentication > Logon**, verify that **Automatic logon only in Intranet zone** is selected. SSO only works on intranet sites. Click **OK** and restart the browser.

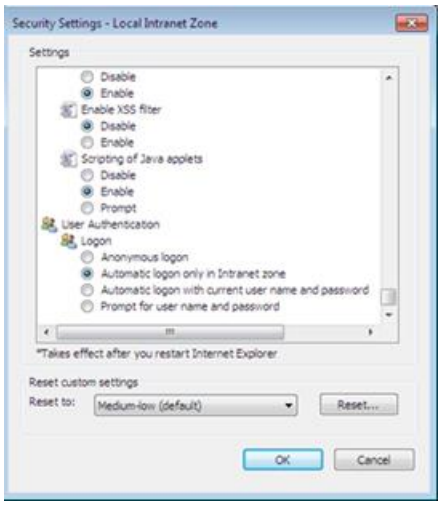

Figure 27 Security Setting – Local Intranet Zone

To test SSO authentication on the client, log onto Active Directory domain from the management station. Launch the IE browser window, use iDRAC's Fully Qualified Domain Name (FQDN) to connect with iDRAC. (Example: **idrac-1234xyz.test.lab**).

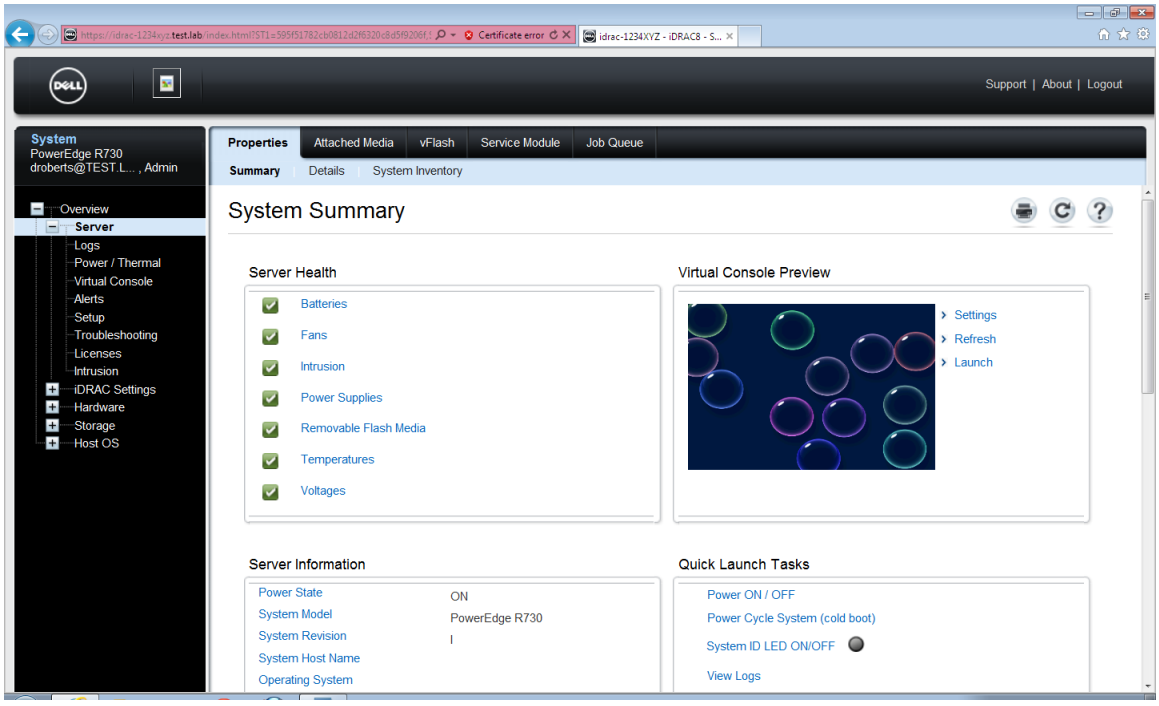

Figure 28 Single Sign-On

If the browser is configured correctly, the browser does not prompt for a name or password.

3.2.2.2 Mozilla Firefox Browser

To enable Single Sign-On (SSO) support in Firefox browser, launch Firefox. Type **about:config** in the URL. Type **negotiate** in the filter box. From filtered result, set the value of **auth.delegation-uris** and **auth.trusted-uris** to the domain name.

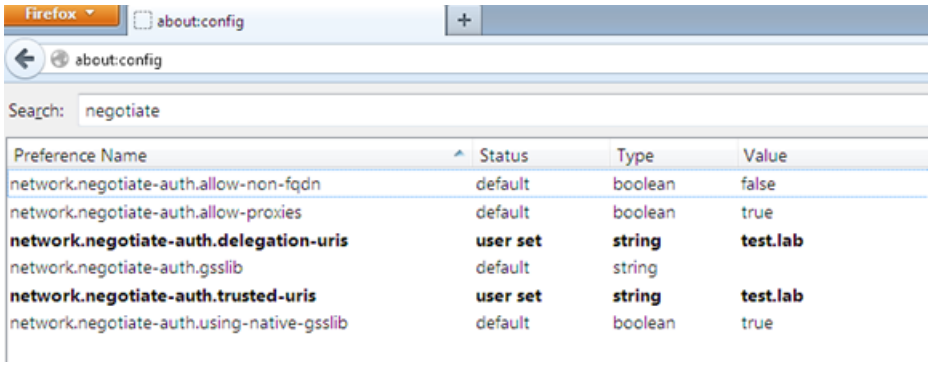

Figure 29 Configure Firefox for delegation and trust

To test SSO authentication on the management station, log onto Active Directory domain from the management station. Launch the Firefox browser window, use iDRAC's Fully Qualified Domain Name (FQDN) to connect with iDRAC. (Example: **idrac-1234xyz.test.lab**).

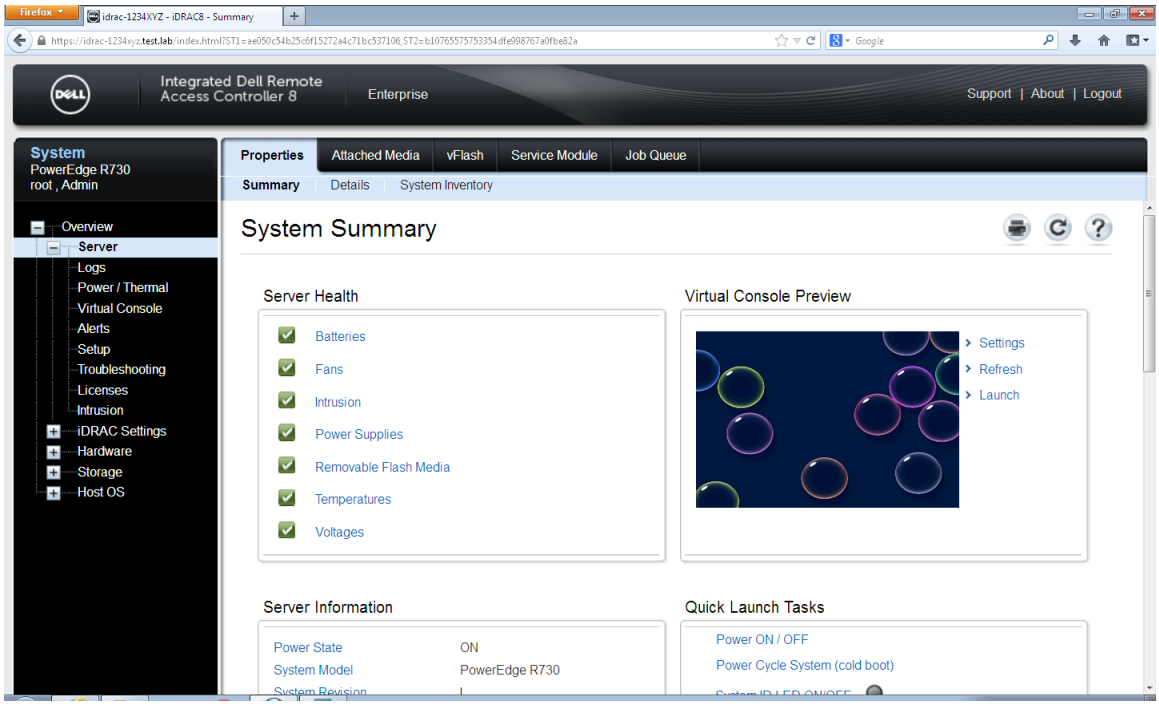

Figure 30 Single Sign-On

If the browser is configured correctly, the browser does not prompt for a name or password.

3.3 Configure iDRAC for Smart Card Logon

3.3.1 Enable Smart Card Logon

Go to **Overview > iDRAC Settings > User Authentication > Smartcard**

Select **Enable with Remote RACADM**. By enabling Smart Card Logon with this option, it provides an easy way to disable feature if it fails and if debugging is required.

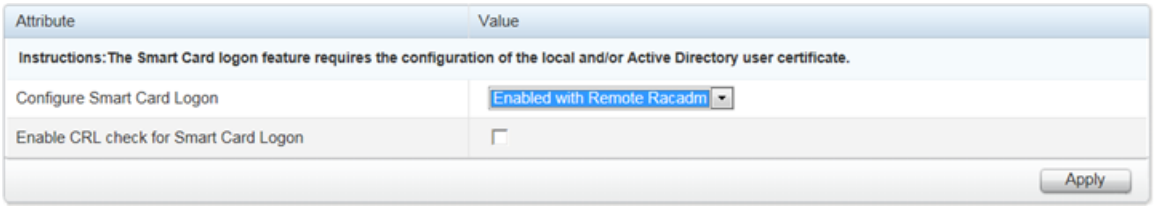

Figure 31 Enable Smart Card Logon

3.3.2 Test Smart Card Logon on Management Station

To test Smart Card setup, log into Active Directory domain using the management station that has a Smart Card. Launch the IE browser window, use iDRAC's Fully Qualified Domain Name (FQDN) to connect with iDRAC. (Example: **idrac-1234xyz.test.lab**).

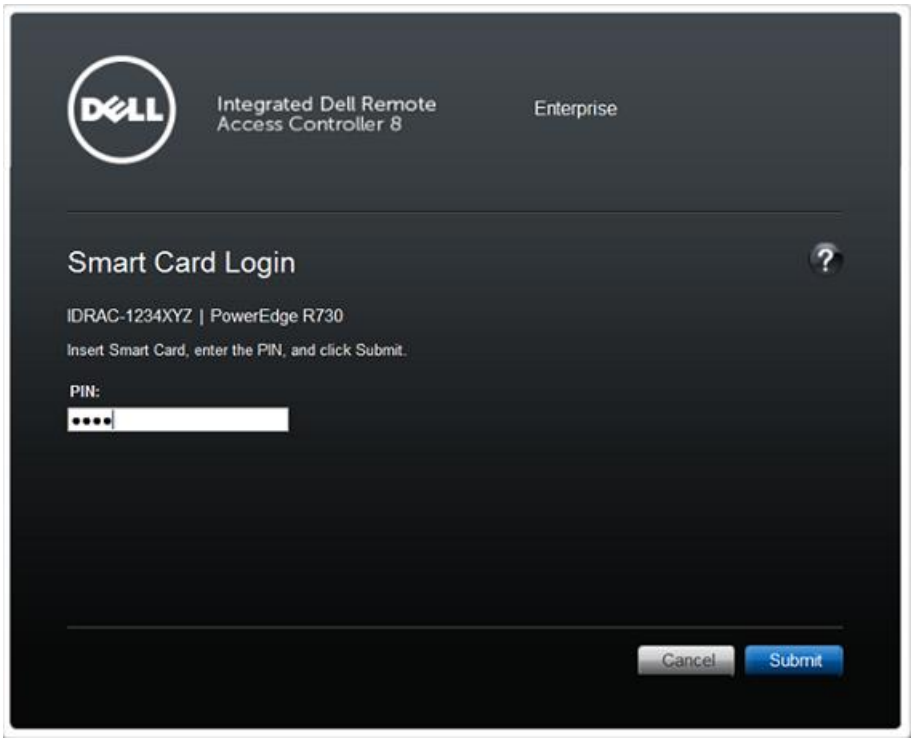

Figure 32 Smart Card Logon

Note: Enabling Smart Card Logon disables all command line interfaces that includes SSH, Telnet, Serial, Remote RACADM and IPMI over LAN. Disabling this feature sets all the command line interfaces to their default setting.

Enter the Smart Card Pin number.

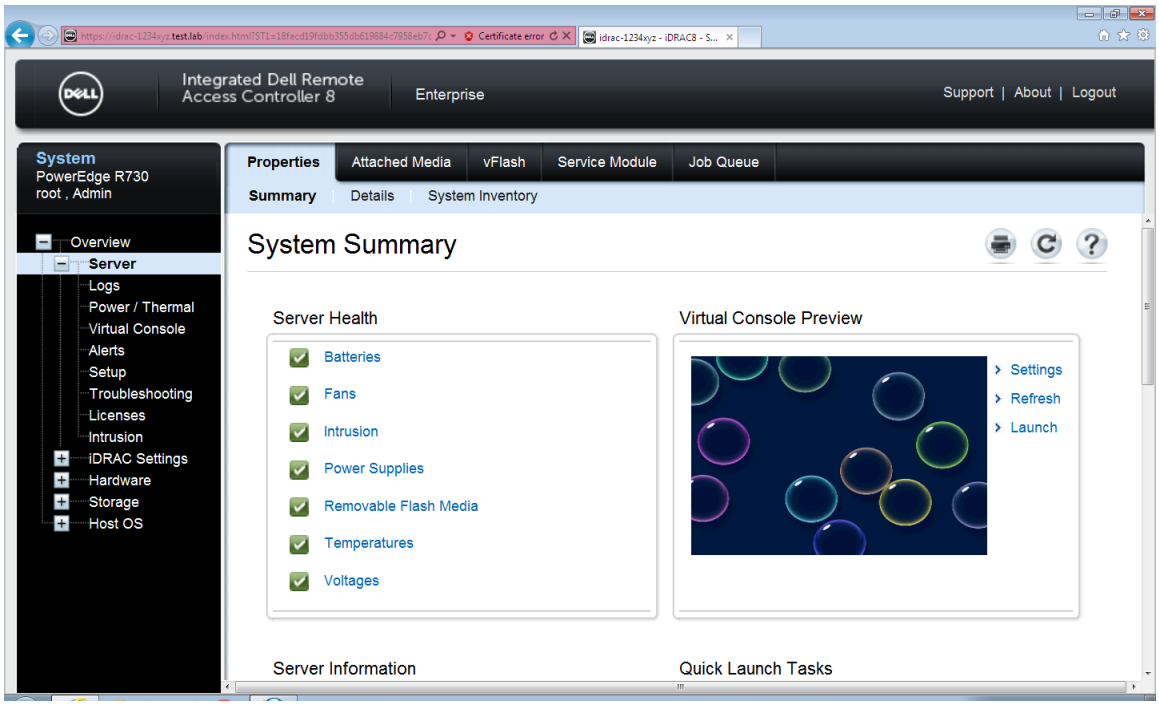

Figure 33 Smart Card Logon

A Configure iDRAC Using RACADM

A.1 Configure Digital Certificate

```
$racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
$racadm sslcertupload -t 0x2 -f harpo.rootCA
```

A.2 Configure Active Directory Domain Information

```
$racadm set iDRAC.ActiveDirectory.Enable 1
$racadm set iDRAC.ActiveDirectory.DomainController1 harpo.test.lab
$racadm set iDRAC.ActiveDirectory.GlobalCatalog1 harpo.test.lab
```

Note: A Global Catalog Server is required only for standard schema when the user accounts and role groups are in different domains.

A.3 Configure Standard Schema

```
$racadm set iDRAC.ActiveDirectory.Schema 2
```

A.3.1 Configure Standard Schema Settings

```
$racadm set iDRAC.ADGroup.1.Name iDRACAdministrators
$racadm set iDRAC.ADGroup.1.Domain test.lab
$racadm set iDRAC.ADGroup.1.Privilege 0x1ff
$racadm set iDRAC.ADGroup.2.Name iDRACOperators
$racadm set iDRAC.ADGroup.2.Domain test.lab
$racadm set iDRAC.ADGroup.2.Privilege 0x1f3
$racadm set iDRAC.ADGroup.3.Name iDRACGuest
$racadm set iDRAC.ADGroup.3.Domain test.lab
$racadm set iDRAC.ADGroup.3.Privilege 0x1
```

A.4 Configure Extended Schema

```
$racadm set iDRAC.ActiveDirectory.Schema 1
```

A.4.1 Configure Extended Schema Settings

```
$racadm set iDRAC.ActiveDirectory.RacName idrac-1234xyz.test.lab
$racadm set iDRAC.ActiveDirectory.RacDomain harpo.test.lab
```

B Additional Resources

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell Customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and installations.

Referenced or recommended Dell publications:

- Dell EqualLogic Configuration Guide: http://en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/19852516/download.aspx

Referenced or recommended Microsoft publications:

- Microsoft SQL Server 2008: Disk Partition Alignment Best Practices for SQL Server: http://msdn.microsoft.com/en-us/library/dd758814.aspx