

Configure iDRAC to use Active Directory Authentication

Abstract

This Dell technical white paper explains how to configure and test iDRAC with Microsoft's Active Directory authentication and Single Sign-On Logon.

July 2021

Revisions

Date	Description
July 2021	Initial release

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2021 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [07/01/2021] [Whitepaper] [495]

Contents

1	Introduction.....	4
1.1	Standard and Extended Schemas.....	4
1.2	Supported Active Directory Configurations	4
1.3	Active Directory Login Syntax.....	5
1.4	Test Environment.....	5
1.5	What You Need to Know	5
2	Integrate iDRAC with Microsoft's Active Directory.....	6
2.1	iDRAC Network Settings	6
2.2	Enable Active Directory	6
2.3	Configure the Digital Certificate.....	7
2.4	Configure Active Directory Domain Information	8
2.5	Configure Standard Schema Mode	9
2.5.1	Standard Schema Users and Groups on AD Server.....	9
2.5.2	Standard Schema Settings on iDRAC.....	9
2.5.3	Testing Standard Schema	11
2.6	Configure Extended Schema Mode.....	12
2.6.1	Extended Schema Users and Groups on AD Server	12
2.6.2	Extended Schema Settings	16
2.6.3	Testing Extended Schema	17
3	Configure iDRAC Single Sign-On	19
3.1	Integrate iDRAC with Kerberos KDC.....	19
3.1.1	Create Kerberos Keytab file on Active Directory	19
3.1.2	Upload Kerberos Keytab file in iDRAC.....	22
3.2	Configure iDRAC for Single Sign-On.....	23
3.3	Configure and Test Single Sign-On on Management Station	23
3.3.1	Windows IE Browser	23
3.3.2	Mozilla Firefox Browser	25
A	Configure Active Directory using RACADM	27
A.1	Configure Digital Certificate.....	27
A.2	Configure Active Directory Domain Information	27
A.3	Configure Standard Schema Settings	27
A.4	Configure Extended Schema Settings.....	27

1 Introduction

Using Microsoft Active Directory allows an administrator to manage Dell's Integrated Dell Remote Access Controller (iDRAC) user accounts and privileges from a central location and provides better access control through the security group management.

Integrating a client with Microsoft's Active Directory for authentication can be complex. This paper provides step-by-step instructions on how to configure iDRAC to use Active Directory for user authentication to iDRAC.

The steps that are described in this document were done using iDRAC9 but also applies to earlier generations of iDRAC. For the remaining document, when referring to 'iDRAC' it applies to both iDRAC7, iDRAC8 and iDRAC9 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 interface.

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 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 AD configurations.

Single Domain compare with Multiple Domain Scenarios

If all the login users and role groups, including the nested groups, are in the same domain, then only the domain controllers' addresses must be configured on iDRAC. In this single domain scenario, any group type is supported.

If all the login users and role groups, or any of the nested groups, are from multiple domains, then Global Catalog server addresses must be configured on iDRAC. In this multiple domain scenario, all the role groups and nested groups, if any, must be a Universal Group type.

1.3 Active Directory Login Syntax

There are three login formats that are allowed for authenticating as an active directory user.

1. `<username>@<domain>`
2. `<domain>\<username>`
3. `<domain>/<username>`

where `username` is an ASCII string of 1 through 256 bytes.

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

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

1.4 Test Environment

The test environment that is described in this paper resides on an isolated node; the test environment is constructed as follows:

- **Domain Controller:** Microsoft's 2019 Enterprise Server.
- **Managed system:** PowerEdge R640 Server with iDRAC9.
- **Management Station:** Windows 10 system.

The 2019 Server is the domain controller and has Active Directory, Certificate service, DHCP and DNS installed. The Active Directory infrastructure consist of a single domain, **`fwad.local`**, within a single forest. The Fully Qualified Domain Name (FQDN) is **`WIN-4RFKEQCK5CK.fwad.local`** .

The iDRAC has an Enterprise license installed which is required for Directory Services.

1.5 What You Need to Know

- Readers are expected to have a working knowledge of networking, Microsoft's Active Directory and Certificate service.
- Have some knowledge to add Users and Groups in Active Directory.
- Experience working with SSL certificates, access to root CA certificate exported from the Certificate Authority.

Go to Microsoft's website for more details regarding Microsoft's 2019 Server and Active Directory

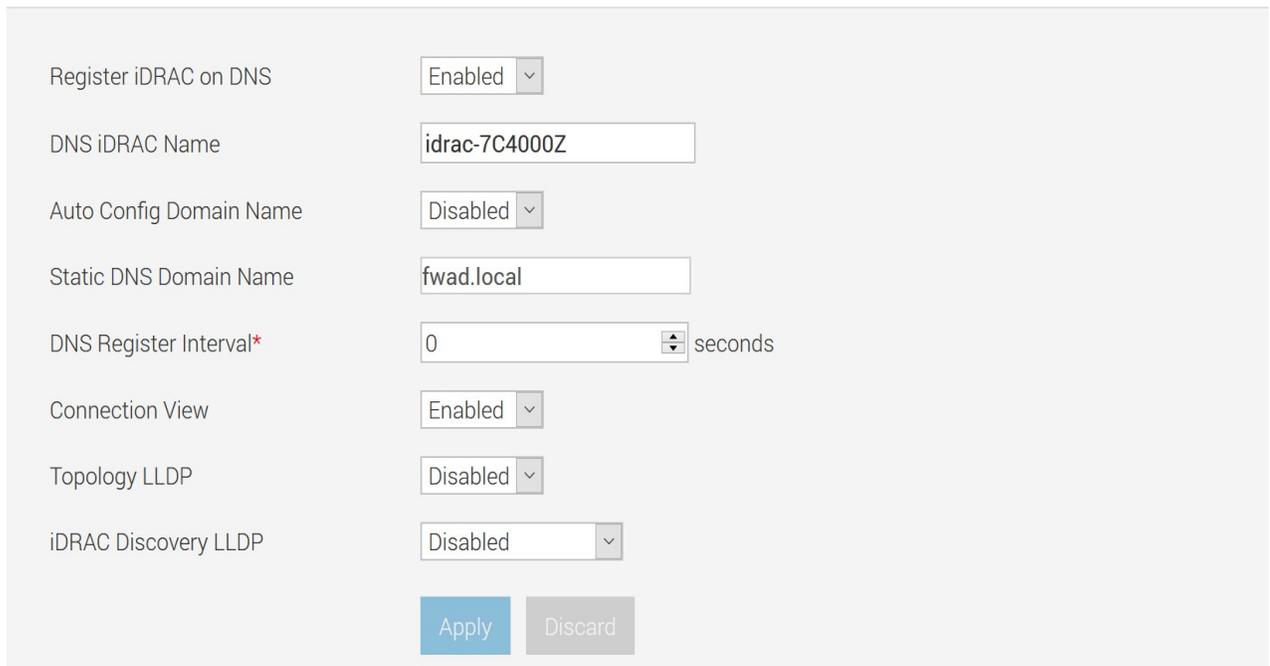
2 Integrate iDRAC with Microsoft's Active Directory

2.1 iDRAC Network Settings

Before configuring Active Directory settings on iDRAC, verify that network settings are configured properly. Configuring the network DNS setting is required so that iDRAC can communicate with the domain controller using its Fully Qualified Domain Name (FQDN). Set the DNS DRAC Name, if not already defined, and set the Static DNS Domain Name as shown below. Here it is recommended that iDRAC register with the DNS. Default settings remain unchanged where appropriate.

Go to **iDRAC Settings > Connectivity > Network > Common Settings**.

▼ Common Settings



The screenshot shows the 'Common Settings' configuration page for iDRAC network settings. It includes the following fields and options:

Register iDRAC on DNS	Enabled
DNS iDRAC Name	idrac-7C4000Z
Auto Config Domain Name	Disabled
Static DNS Domain Name	fwad.local
DNS Register Interval*	0 seconds
Connection View	Enabled
Topology LLDP	Disabled
iDRAC Discovery LLDP	Disabled

At the bottom of the form are two buttons: 'Apply' (highlighted in blue) and 'Discard'.

Figure 1: Network Common Settings

Also, ensure DNS IP address is configured correctly under IPv4/IPv6 settings.

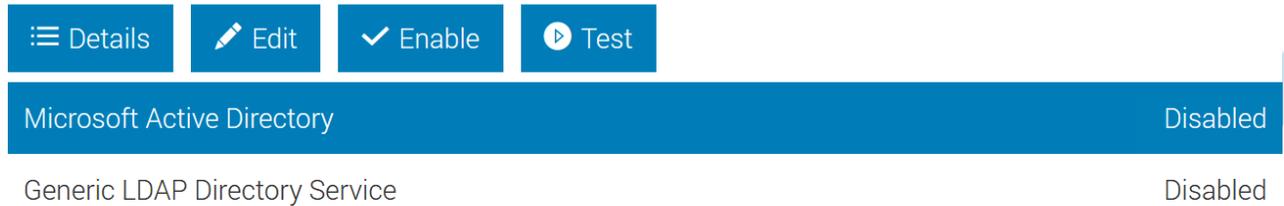
2.2 Enable Active Directory

To configure Active Directory settings this feature must be enabled, it is disabled by default. Default settings remain unchanged where appropriate.

To enable Microsoft's Active Directory services, go to **iDRAC Settings > Users > Directory Services**. Select the Microsoft Active Directory option, click **Enable** button.

Directory Services

Instructions: Only one type of directory service, Active Directory or generic LDAP can be used at a time.



The screenshot shows a configuration interface for Directory Services. At the top, there are four buttons: 'Details' (with a list icon), 'Edit' (with a pencil icon), 'Enable' (with a checkmark icon), and 'Test' (with a play icon). Below the buttons is a table with two rows. The first row is highlighted in blue and shows 'Microsoft Active Directory' with a status of 'Disabled'. The second row shows 'Generic LDAP Directory Service' with a status of 'Disabled'.

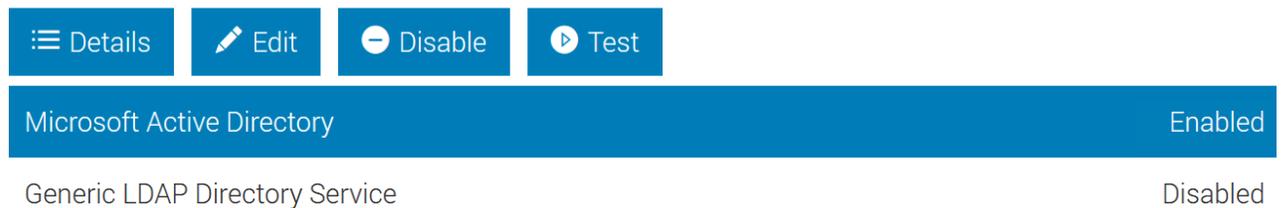
Microsoft Active Directory	Disabled
Generic LDAP Directory Service	Disabled

Figure 2: Enable Microsoft Active Directory

Now to edit Microsoft Active Directory settings click **Edit** button.

Directory Services

Instructions: Only one type of directory service, Active Directory or generic LDAP can be used at a time.



The screenshot shows the same configuration interface as Figure 2, but with the 'Enable' button replaced by a 'Disable' button (with a minus sign icon). The table below shows that 'Microsoft Active Directory' is now 'Enabled' and 'Generic LDAP Directory Service' remains 'Disabled'.

Microsoft Active Directory	Enabled
Generic LDAP Directory Service	Disabled

Figure 3: Edit Microsoft Active Directory Settings

2.3 Configure the Digital Certificate

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

By 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 **Browse**, select the CA certificate then **Upload**.

Certificate Settings

Certificate Validation: Enabled

Upload Directory Service CA Certificate* fwad-rootca.cer

Figure 4: Certificate Validation

After the certificate is uploaded, it is displayed in the current **Directory Service CA Certificate** section of **Details** page.

Directory Service CA Certificate			
Serial Number	75E9E0C70843D3824C0E115199DA0D10		
Subject Information		Issuer Information	
Common Name (CN)	fwad-WIN-4RFKEQCK5CK-CA	Common Name (CN)	fwad-WIN-4RFKEQCK5CK-CA
Valid From	Dec 17 17:03:58 2019 GMT	Valid To	Dec 17 17:13:58 2024 GMT

Figure 5: CA Certificate

2.4 Configure Active Directory Domain Information

Configure the location information about Active Directory servers and user accounts. Default settings remain unchanged where appropriate.

User Domain Name is optional, if specified it helps simplify the user login syntax. Domain names that are configured here will be added to the drop-down list in the login page. The AD domains defined here contain iDRAC useraccounts.

When specifying the Domain Controllers, iDRAC provides two options.

- **Lookup Domain Controllers with DNS:** Use DNS lookup to obtain the AD 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 are 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.

Common Settings

The screenshot displays the 'Common Settings' configuration page for iDRAC. It includes the following settings:

- Active Directory:** Enabled
- Single Sign-On:** Disabled
- User Domain Name:** fwad.local (with Add, Edit, and Delete buttons)
- Timeout*:** 120 seconds
- Lookup Domain Controllers with DNS:** Disabled
- Specify Domain Controller Addresses:**
 - Domain Controller Server Address 1 (FQDN or IP)*: WIN-4RFKEQCK5CK.fwad.local
 - Domain Controller Server Address 2 (FQDN or IP): (empty)
 - Domain Controller Server Address 3 (FQDN or IP): (empty)

Figure 6: Domain Common Settings

2.5 Configure Standard Schema Mode

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 AD 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
iDRACAdministrator	admin
iDRACOperator	operator
iDRACReadonly	readonly

2.5.2 Standard Schema Settings on iDRAC

Select the Standard Schema mode

Schema Selection

The screenshot shows a dropdown menu with the text 'Schema Selection' on the left and 'Standard Schema' with a downward arrow on the right.

Figure 7: Standard Schema Selection

The 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 Root Domain Name specified. 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.

Standard Schema Settings

The screenshot shows the following configuration options:

- Lookup Global Catalog Servers with DNS: Disabled (dropdown)
- Specify Global Catalog Server Addresses:
 - Global Catalog Server Address 1 (FQDN or IP): WIN-4RFKEQCK5CK.fwad.local
 - Global Catalog Server Address 2 (FQDN or IP): [Empty field]
 - Global Catalog Server Address 3 (FQDN or IP): [Empty field]

Figure 8: 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 15 role groups can be defined in each iDRAC. The Group Names should match the Groups defined on the Active Directory server earlier.

Standard Schema Role Groups

Role Groups	Group Name	Group Domain	Group Privilege
Role Group 1	iDRACAdministrator	fwad.local	Administrator
Role Group 2	iDRACOperator	fwad.local	Operator
Role Group 3	iDRACReadonly	fwad.local	Read Only
Role Group 4			None
Role Group 5			None

Figure 9: Standard Schema Role Groups

2.5.3 Testing Standard Schema

Use the test feature in iDRAC to validate the Active Directory configuration. Go to **iDRAC Settings > Users > Directory Services**, click **Test Settings**.

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

Test User

The screenshot shows a web form for testing user credentials. It contains two input fields: 'Test User Name*' with the text 'admin@fwad.local' and 'Test User Password*' with masked characters. Below the password field is a blue button labeled 'Test'.

Figure 10: Test Admin User

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 9 privileges in the cumulative privilege gained section.

Test Log

```

10:39:03 trying GC server WIN-4RFKEQCK5CK.fwad.local:3268
10:39:03 Server Address WIN-4RFKEQCK5CK.fwad.local resolved to 192.168.1.10
10:39:03 connect to 192.168.1.10:3268 passed
10:39:03 trying GC server WIN-4RFKEQCK5CK.fwad.local:3269
10:39:03 Server Address WIN-4RFKEQCK5CK.fwad.local resolved to 192.168.1.10
10:39:03 connect to 192.168.1.10:3269 passed
10:39:04 Connecting to ldaps://[WIN-4RFKEQCK5CK.fwad.local]:636...
10:39:04 Test user authenticated user=admin@fwad.local host=WIN-4RFKEQCK5CK.fwad.local
10:39:04 Connecting to ldaps://[WIN-4RFKEQCK5CK.fwad.local]:3269...
10:39:04 Test user authenticated user=admin@fwad.local host=WIN-4RFKEQCK5CK.fwad.local
10:39:04 Test user admin@fwad.local authorized

10:39:04 Cumulative privileges gained:
  Login
  Config iDRAC
  Config User
  Clear Logs
  Server Control
  Virtual Console
  Virtual Media
  Test Alerts
  Diagnostic Command
    
```

Figure 11: Test Log

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

2.6 Configure Extended Schema Mode

The extended schema uses Dell association objects to join iDRAC and permission. This allows you to use iDRAC based on the overall permissions granted. The default Access Control List (ACL) of Dell Association objects allows Self and Domain Administrators to manage the permissions and scope of iDRAC objects.

By default, the Dell Association objects do not inherit all permissions from the parent Active Directory objects. If you enable inheritance for the Dell Association object, the inherited permissions for that association object are granted to the selected users and groups. This may result in unintended privileges being provided to the iDRAC.

To use the Extended Schema securely, Dell Technologies recommends not enabling inheritance on Dell Association objects within the extended schema implementation.

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 an *Association*, *Device*, and *Privileges*. To extend the schema install [Dell's Active Directory Snap-In Utility](#) on to the Active Directory server.

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

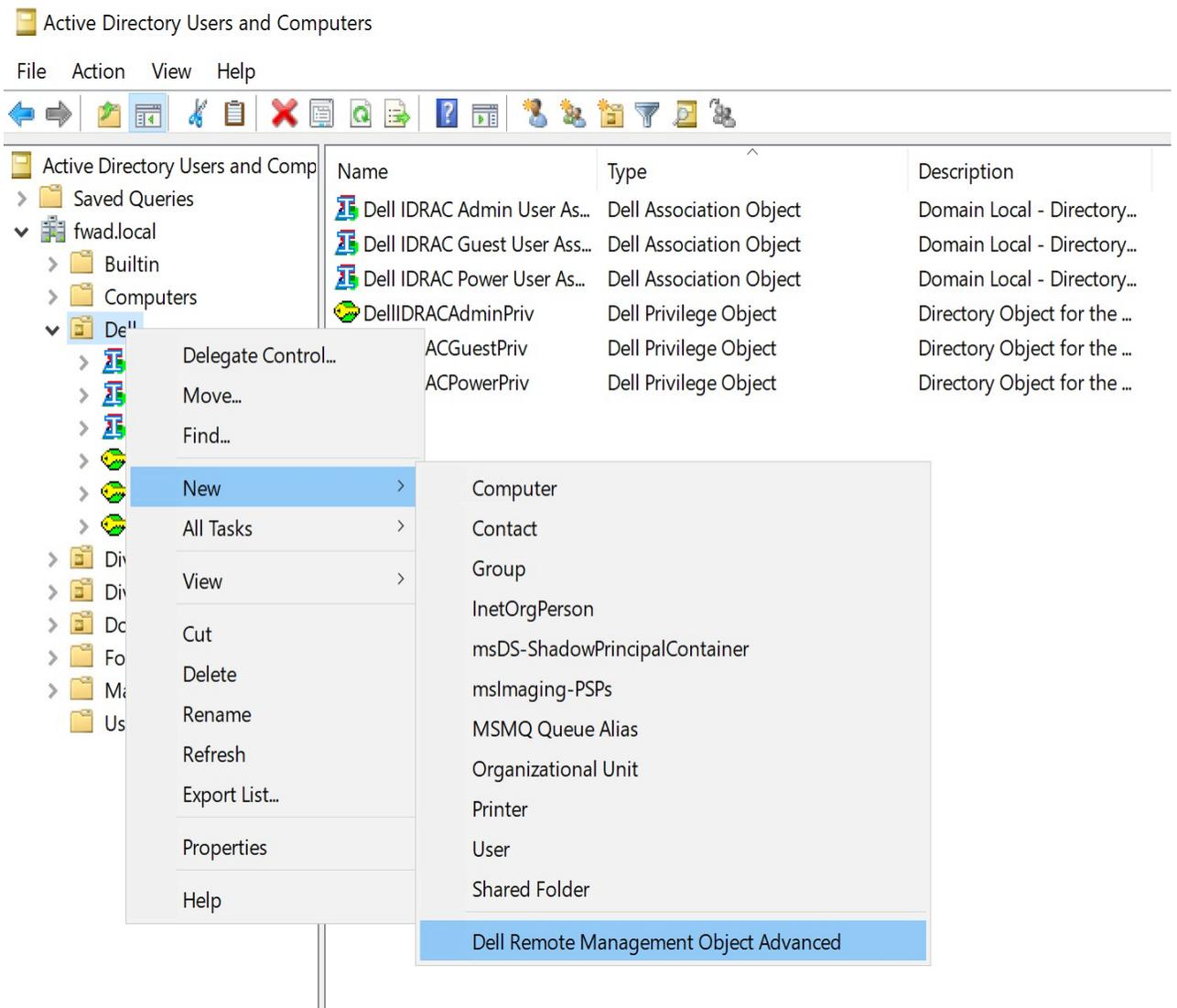


Figure 12: Predefined Association and Privilege Objects

An iDRAC object is required to represent each physical iDRAC device. Now create a device and associate the device to a set of predefined privileges. Select the **Dell** Container. Right-click, go to **New > Dell Remote Management Object Advanced**.

Enter the iDRAC device name.

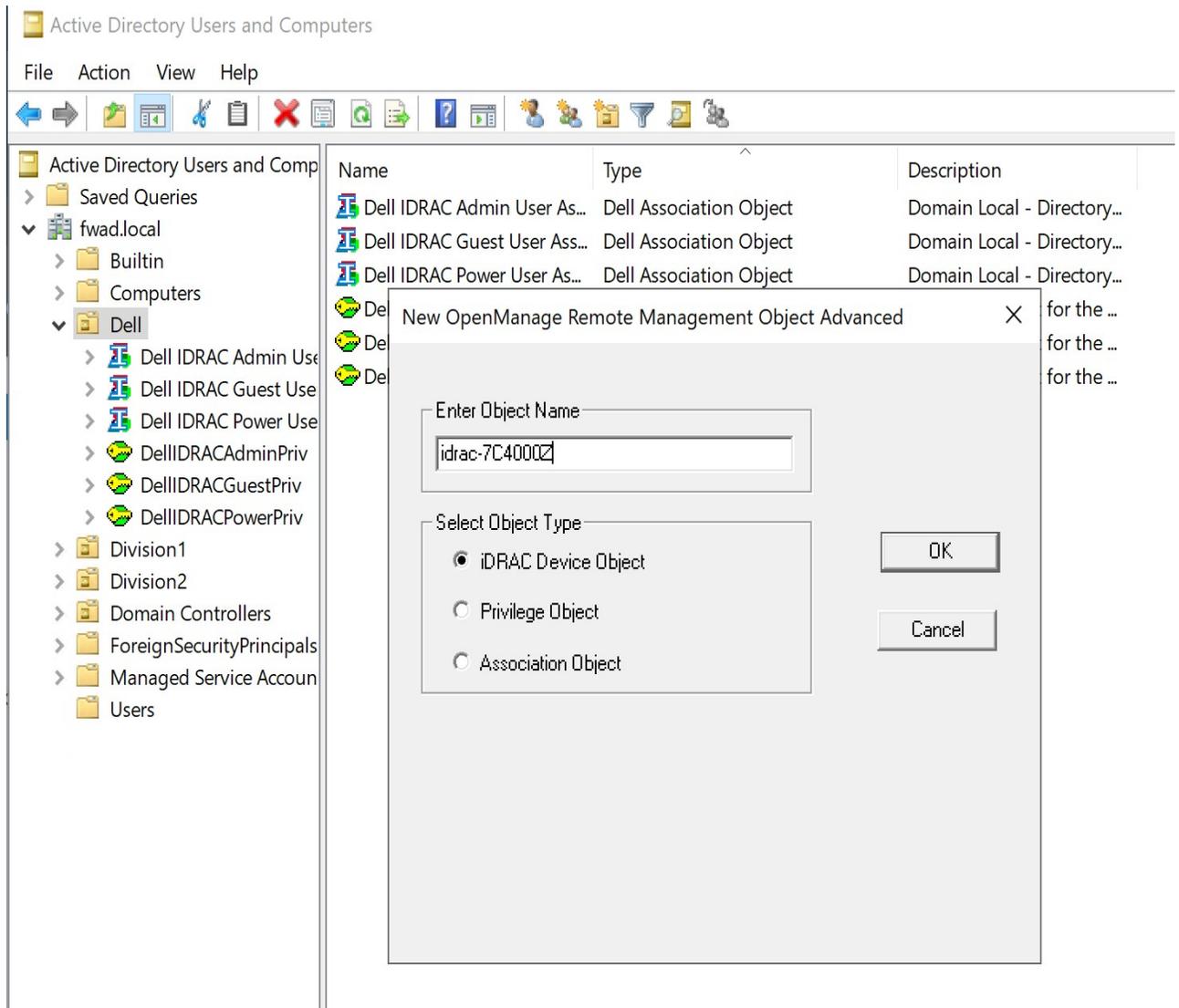


Figure 13: User Association Object

Next add the iDRAC device to the predefined Admin association object. Click the **Dell** container under **fwad.local**.

- Select **Dell iDRAC Admin User Association > Properties**.
- Click on Products tab; **Add > type iDRAC Name > Check Names** (it should be found).

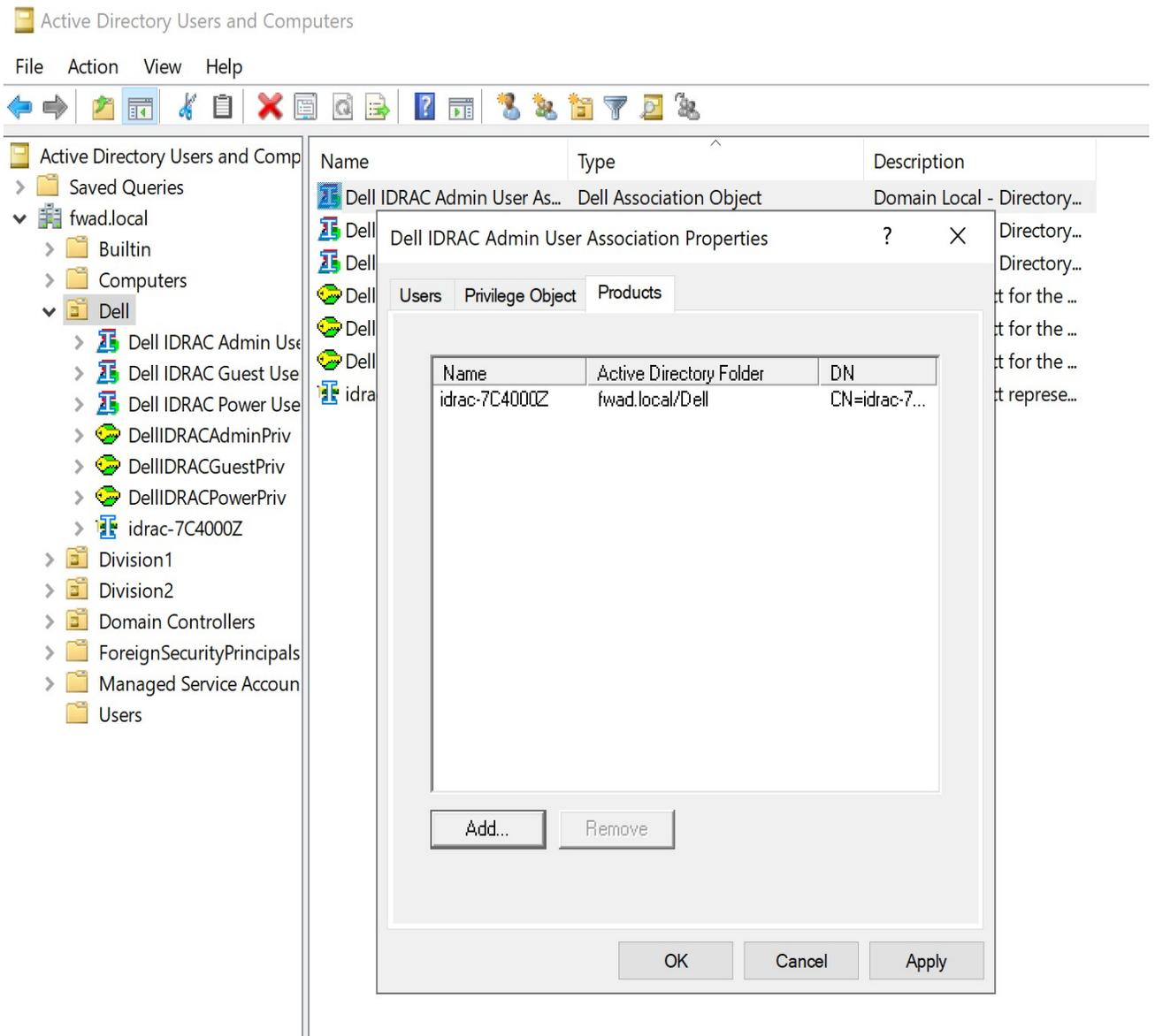


Figure 14: User Association Properties - Products

Repeat the steps above to add iDRAC device to Dell iDRAC Power User Association and Dell iDRAC Guest User Association.

Finally, add the users to the Association objects. Click the Dell container under **fwad.local**.

- Select **Dell iDRAC Admin User Association > Properties**.
- Click on **Users** tab.
- Click **Add**; then type **admin > Check Names** (it should be found). Name should appear in list with other usernames.

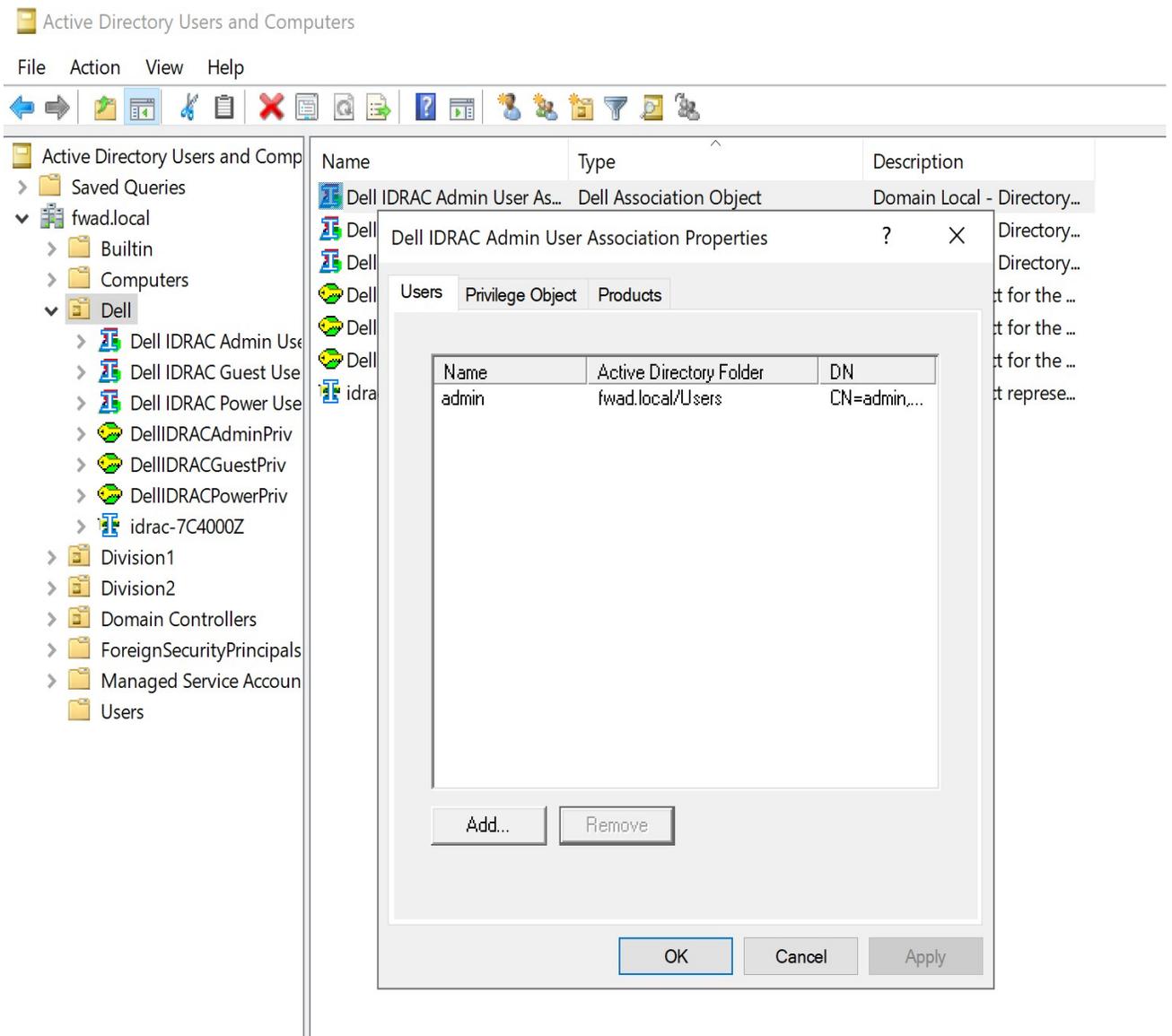


Figure 15: User Association Properties - Users

Repeat the above steps to add user **operator** to Dell Power User Association object and the **read-only** to the iDRAC Guest User Association.

2.6.2 Extended Schema Settings

Now that the schema has been extended and association objects that are defined on the Active Directory server, configure the schema selection on iDRAC.

Select the Extended Schema mode.

Schema Selection

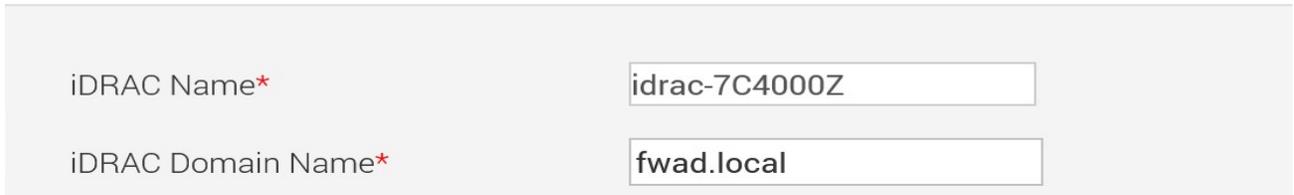


The screenshot shows a form titled "Schema Selection". On the left, the text "Schema Selection" is displayed. To its right is a dropdown menu with the text "Extended Schema" and a downward-pointing arrow.

Figure 16: Extended Schema Selection

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.

Extended Schema Settings



The screenshot shows a form titled "Extended Schema Settings". It contains two input fields. The first field is labeled "iDRAC Name*" and contains the text "idrac-7C4000Z". The second field is labeled "iDRAC Domain Name*" and contains the text "fwad.local".

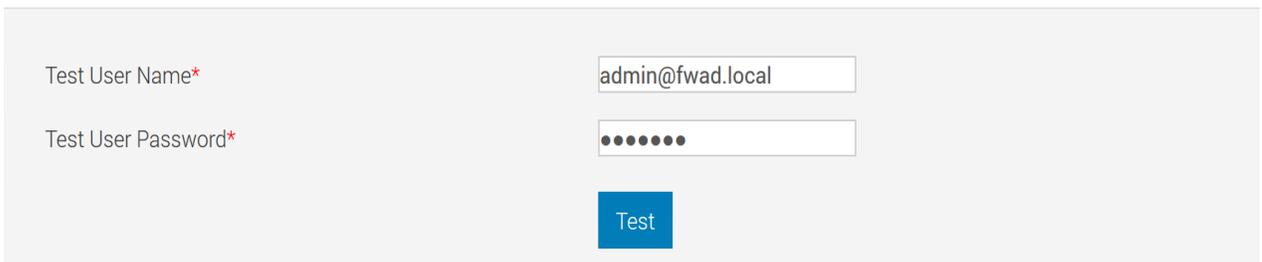
Figure 17: Extended Schema Settings

2.6.3 Testing Extended Schema

Use the test feature in iDRAC to validate the Active Directory configuration. Go to **iDRAC Settings > Users > Directory Services**, click **Test Settings**.

Enter username of user along with password.

Test User



The screenshot shows a form titled "Test User". It contains two input fields. The first field is labeled "Test User Name*" and contains the text "admin@fwad.local". The second field is labeled "Test User Password*" and contains a masked password represented by seven dots. Below the password field is a blue button labeled "Test".

Figure 18: Test Admin User

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

Repeat the test using the other users created, notice privileges on operator and read-only users.

Test Log

```
13:01:21 Initiating Directory Services Settings Diagnostics:
13:01:21 trying DC server WIN-4RFKEQCK5CK.fwad.local:389
13:01:21 Server Address WIN-4RFKEQCK5CK.fwad.local resolved to 192.168.1.10
13:01:21 connect to 192.168.1.10:389 passed
13:01:21 trying DC server WIN-4RFKEQCK5CK.fwad.local:636
13:01:21 Server Address WIN-4RFKEQCK5CK.fwad.local resolved to 192.168.1.10
13:01:21 connect to 192.168.1.10:636 passed
13:01:21 Connecting to ldaps://[WIN-4RFKEQCK5CK.fwad.local]:636...
13:01:22 Test user authenticated user=admin@fwad.local host=WIN-4RFKEQCK5CK.fwad.local
13:01:22 Test user admin@fwad.local authorized

13:01:22 Cumulative privileges gained:
  Login
  Config iDRAC
  Config User
  Clear Logs
  Server Control
  Virtual Console
  Virtual Media
  Test Alerts
  Diagnostic Command
```

Figure 19: Test Log

3 Configure iDRAC Single Sign-On

iDRAC supports Kerberos authentication by Single Sign-On (SSO) through the web interface. When Single Sign-On is enabled, users can log in to iDRAC using credentials that were cached in the operation system when user logged in using valid Active Directory account. This section provides steps to configure iDRAC to use Single Sign-On. This section assumes iDRAC is configured and tested with Active Directory.

Time Synchronization

The iDRAC time must 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 that 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

Before creating a keytab, the iDRAC user account must be created on the Active Directory 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 **fwad.local**; 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.

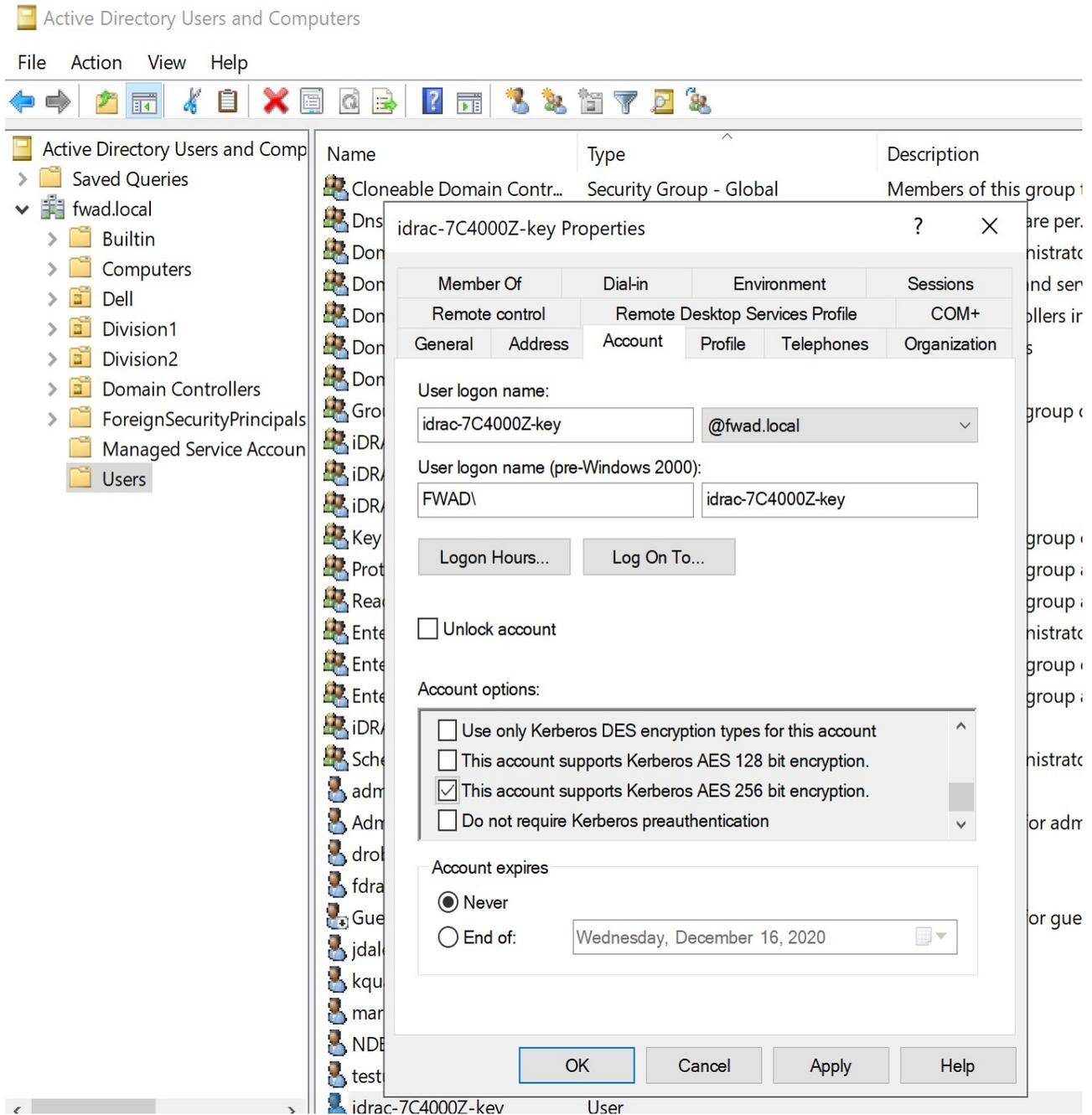


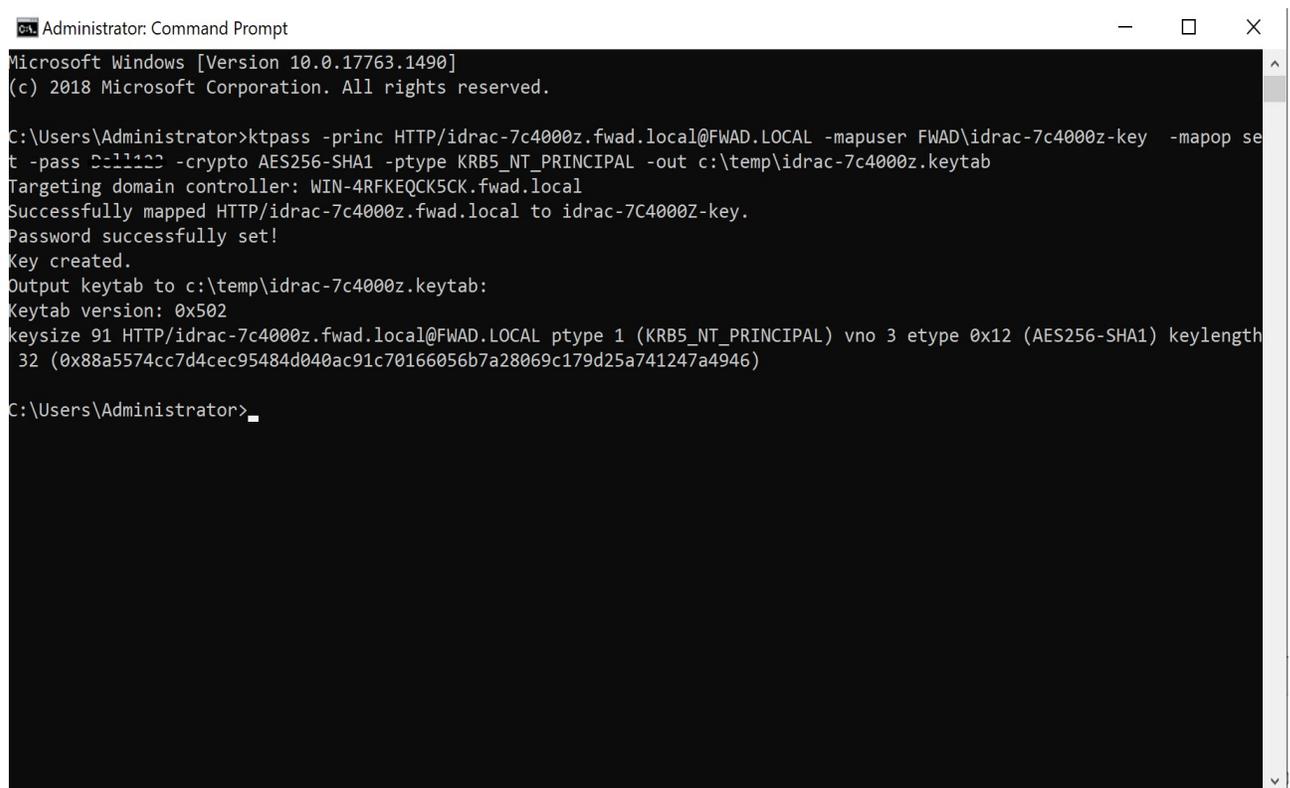
Figure 20: Create User for Device keytab

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-7c4000z.fwad.local@FWAD.LOCAL -mapuser FWAD\idrac-7c4000z-key -mapop set -pass ***** -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -out c:\temp\idrac-7c4000z.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.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1490]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ktpass -princ HTTP/idrac-7c4000z.fwad.local@FWAD.LOCAL -mapuser FWAD\idrac-7c4000z-key -mapop se
t -pass D:llllll -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -out c:\temp\idrac-7c4000z.keytab
Targeting domain controller: WIN-4RFKEQCK5CK.fwad.local
Successfully mapped HTTP/idrac-7c4000z.fwad.local to idrac-7C4000Z-key.
Password successfully set!
Key created.
Output keytab to c:\temp\idrac-7c4000z.keytab:
Keytab version: 0x502
keysize 91 HTTP/idrac-7c4000z.fwad.local@FWAD.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x12 (AES256-SHA1) keylength
32 (0x88a5574cc7d4cec95484d040ac91c70166056b7a28069c179d25a741247a4946)

C:\Users\Administrator>
```

Figure 21: Generate a Kerberos Keytab File

Now that the keytab file has been created, the iDRAC user account must 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.

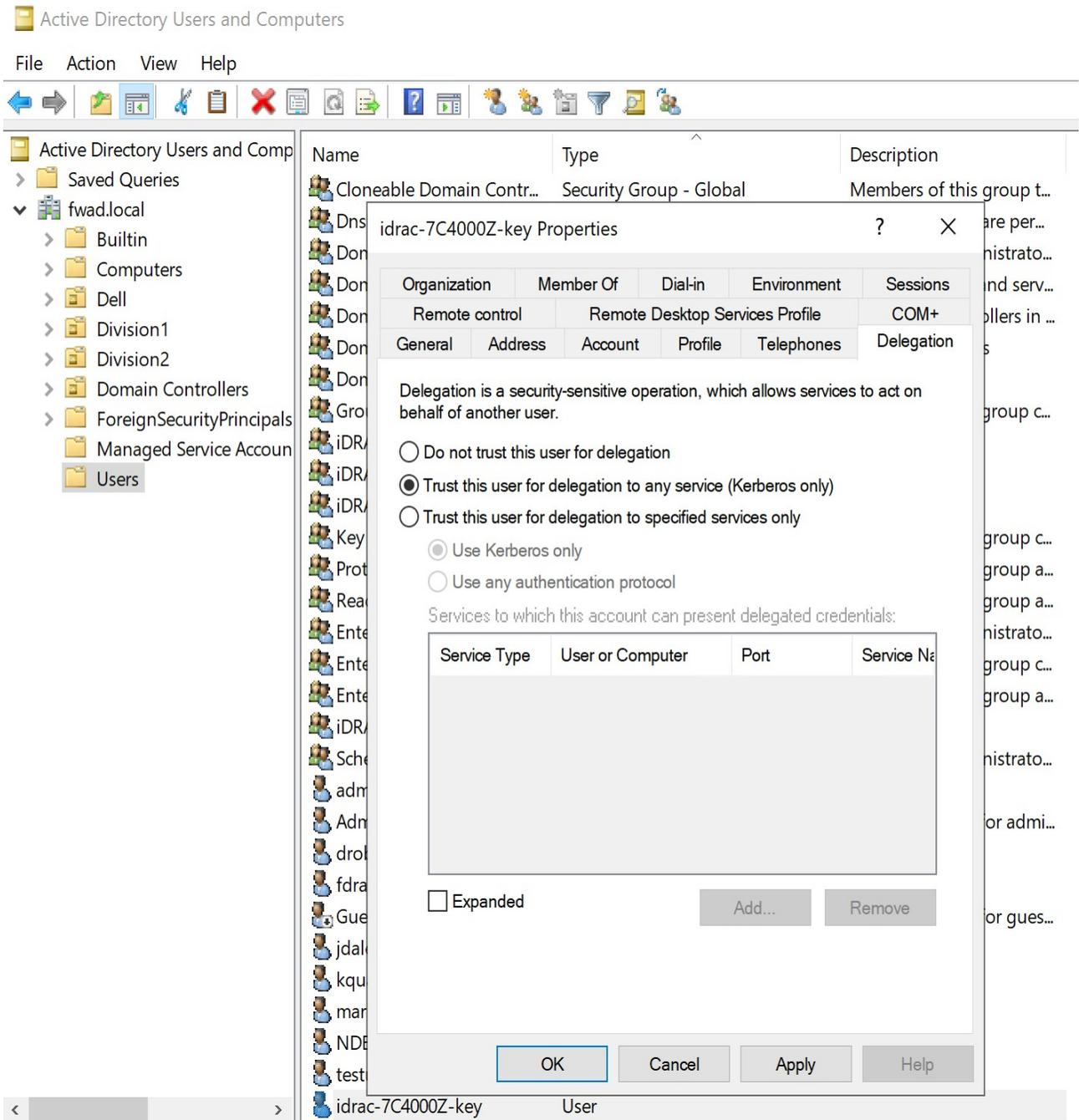


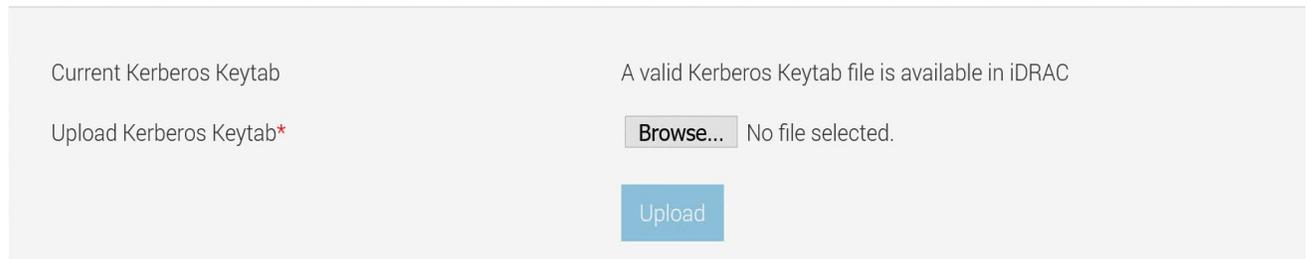
Figure 22: Trust User for Delegation

3.1.2 Upload Kerberos Keytab file in iDRAC

Know the keytab file must be uploaded in to iDRAC. Go to **iDRAC Settings > Users > Directory Services**, click **Edit**.

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

Upload Kerberos Keytab



Current Kerberos Keytab A valid Kerberos Keytab file is available in iDRAC

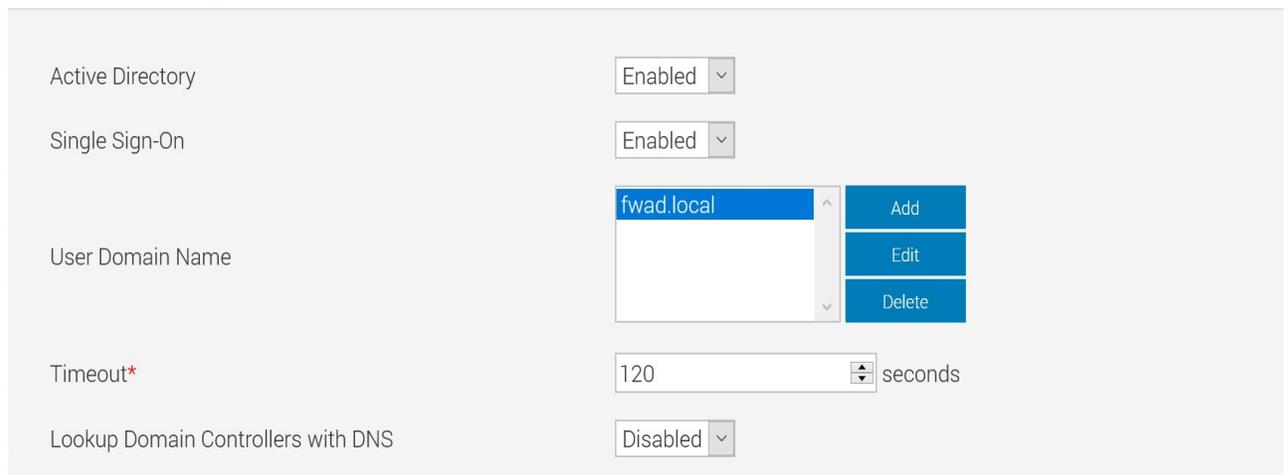
Upload Kerberos Keytab* No file selected.

Figure 23: Upload Kerberos Keytab File.

3.2 Configure iDRAC for Single Sign-On

Now enable Single Sign-On in Common Settings

Common Settings



Active Directory Enabled

Single Sign-On Enabled

User Domain Name fwad.local Add Edit Delete

Timeout* 120 seconds

Lookup Domain Controllers with DNS Disabled

Figure 24: Enable Single Sign-On

3.3 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.

3.3.1 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.

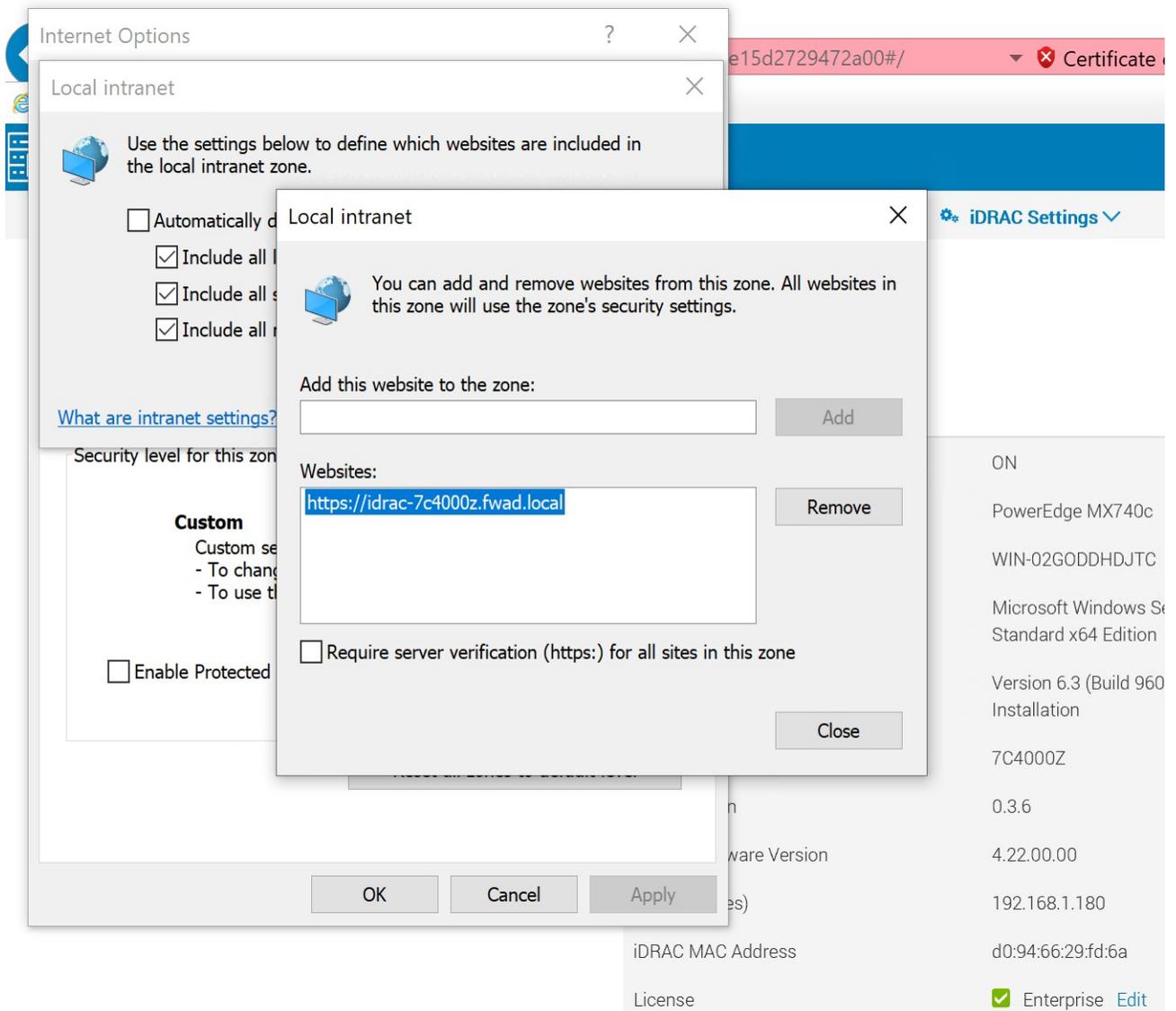


Figure 25: Configure IE for Single Sign-On

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. Now restart the browser.

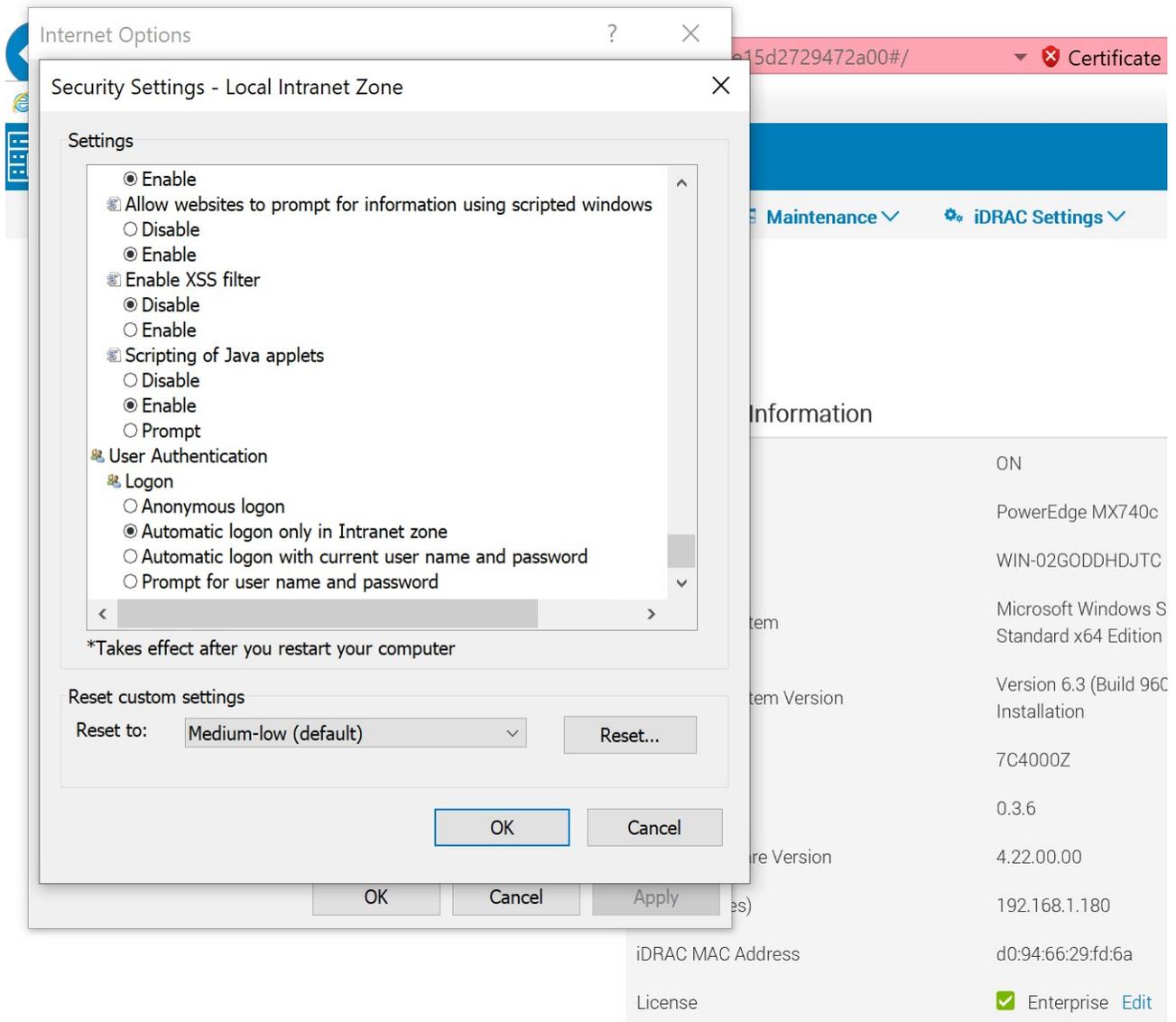


Figure 26: Security Setting – Local Intranet Zone

To test SSO authentication on the client, log in to 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-ddhdjtc.fwad.local**).

If the browser is configured correctly, the browser does not prompt for credentials.

3.3.2 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.

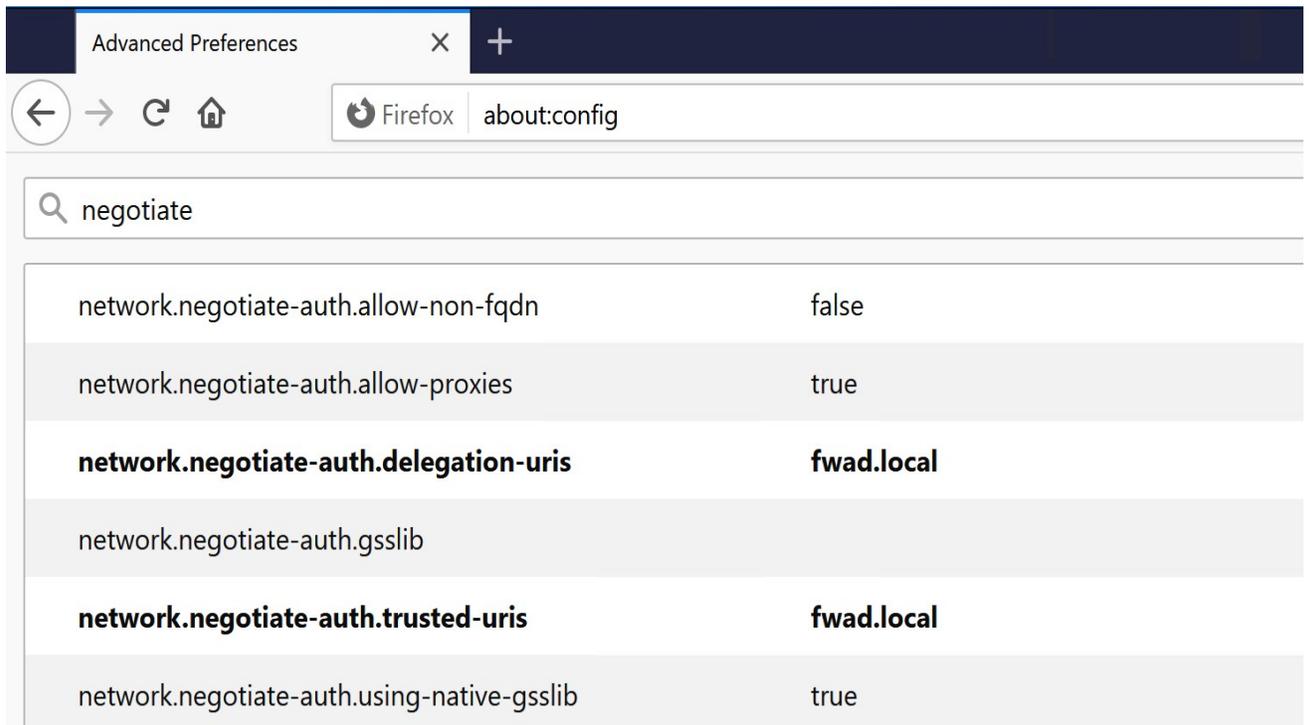


Figure 27: Configure Firefox for Delegation and Trust

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-ddhdjtc.fwad.local**).

If the browser is configured correctly, the browser does not prompt for credentials.

A Configure Active Directory using RACADM

A.1 Configure Digital Certificate

```
racadm>> set iDRAC.ActiveDirectory.CertValidationEnable 1
C:\racadm -r <ip> -u <user> -p <passwd> sslcertupload -t 0x2 -f fwad-rootca.cer
```

A.2 Configure Active Directory Domain Information

```
racadm>> set iDRAC.ActiveDirectory.Enable 1
racadm>> set iDRAC.ActiveDirectory.DomainController1 WIN-4RFKEQCK5CK.fwad.local
racadm>> set iDRAC.ActiveDirectory.GlobalCatalog1 WIN-4RFKEQCK5CK.fwad.local
```

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 Settings

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

racadm>> set iDRAC.ADGroup.1.Name iDRACAdministrator
racadm>> set iDRAC.ADGroup.1.Domain fwad.local
racadm>> set iDRAC.ADGroup.1.Privilege 0x1ff
racadm>> set iDRAC.ADGroup.2.Name iDRACOperator
racadm>> set iDRAC.ADGroup.2.Domain fwad.local
racadm>> set iDRAC.ADGroup.2.Privilege 0x1f3
racadm>> set iDRAC.ADGroup.3.Name iDRACReadonly
racadm>> set iDRAC.ADGroup.3.Domain fwad.local
racadm>> set iDRAC.ADGroup.3.Privilege 0x1
```

A.4 Configure Extended Schema Settings

```
racadm>> set iDRAC.ActiveDirectory.Schema 1
racadm>> set iDRAC.ActiveDirectory.RacName idrac-7c4000z
racadm>> set iDRAC.ActiveDirectory.RacDomain fwad.local
```