DELL Technologies

Whitepaper

Using iDRAC9 RSA SecurID 2FA

Abstract

Learn how to improve security by configuring iDRAC9 to enable RSA SecurID two-factor authentication (2FA) for local users, and Active Directory and LDAP users.

December 2020

ID 450

Revisions

Date	Description
September 2020	Initial release

Acknowledgments

Author: Kang Quan

Support: Jason Dale, Doug Roberts, Alaric Silveira, Mark A Evans

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.

Contents

1 Introduction 5

1.1 RSA SecurID 2FA license requirement 5

1.2 Test Environment 5

1.3 Before You Begin 5

2 iDRAC9 Configuration for RSA SecurID 6

2.1 RSA SecurID 2FA Global Configuration 6

2.2 RSA AM Server Certificate (chain) Upload 7

2.3 Test Connection to RSA AM Server 7

2.4 Get RSA SecurID Token App Ready 9

3 RSA SecurID 2FA with Local Users 10

3.1 Enable RSA SecurID 2FA on an iDRAC Local User 10

3.2 Log in to iDRAC from UI with an iDRAC Local User 11

3.3 Log in to iDRAC from SSH with an iDRAC Local User 13

4 RSA SecurID 2FA with Active Directory Users 14

4.1 Enable RSA SecurID 2FA on Active Directory Users 14

4.2 Log in to iDRAC from UI with an AD User 14

4.3 Log in to iDRAC from SSH with an AD User 16

5 RSA SecurID 2FA with Generic LDAP Directory Users 17

5.1 Enable RSA SecurID 2FA on Generic LDAP Directory Users 17

5.2 Log in to iDRAC from UI with an LDAP User Account 17

5.3 Log in to iDRAC from SSH with an LDAP User 19

6 Troubleshooting RSA SecurID Issues 21

6.1 Misconfiguration or iDRAC Configuration Gets Reset 21

6.2 Datacenter License Expires or Gets Downgraded or Deleted 21

6.3 Authentication Failures without being Prompted for RSA Passcode 22

6.4 Authentication failures with Correct RSA Passcode 22

6.5 Authentication Failures with Correct RSA Passcode due to Timeout 22

6.6 RSA Configuration gets lost after importing Server Configuration Profile 22

Appendix A: Configure iDRAC Using RACADM 23

Appendix B: References 25

Executive summary

As enterprise technology continues to advance, security risks are also on the rise. RSA SecurID is a well-known and broadly deployed two-factor authentication (2FA) technology that may be used for authenticating a user on a system. The iDRAC9 with the Datacenter license and firmware version 4.40.00.00 introduces support for RSA SecurID as an additional two-factor authentication method. Another 2FA method that is offered is Easy 2FA, which sends a randomly generated token to user's email box when logging into iDRAC.

This document goes through how to configure iDRAC9 to enable RSA SecurID 2FA on local users, and Active Directory and LDAP users. For information about RSA Authentication Manager server or RSA Cloud Service configuration, see the RSA configuration documentation.

1 Introduction

Enabling iDRAC9 to use RSA SecurID 2FA is relatively easy and straight-forward. This white paper provides detailed instructions on how to enable it for local users and AD/LDAP users. It also covers some common issues that you may run into, and how to quickly troubleshoot them.

In iDRAC9, RSA 2FA enablement requires some global configuration, and per user configuration (only applies to iDRAC local users). This paper shows how to configure RSA SecurID 2FA from iDRAC UI. Administrators can configure it with RACADM commands as well. For more information see the iDRAC RACADM User Guide at dell.com/idracmanuals.

1.1 RSA SecurID 2FA license requirement

iDRAC9 Datacenter license is required to enable this feature.

1.2 Test Environment

The test environment includes the following entities:

- iDRAC9 version 4.40.00.00 or later
- iDRAC9 Datacenter license
- RSA AM server 8.4
- Microsoft Active Directory Server – see the RSA AM documentation for supported versions
- OpenLDAP 2.4.44

1.3 Before You Begin

Before you begin to configure iDRAC9 to enable RSA SecurID, you must have:

- Working knowledge to configure RSA AM server, or you must work with RSA AM server administrator in order to enable RSA SecurID on iDRAC.
- You must have a Microsoft Active Directory server properly configured.
- If you are trying to enable RSA SecurID on all AD users, add the AD server to the RSA AM server as an Identity Source.
- You must have a generic LDAP server (OpenLDAP 2.4.40 or later required by RSA AM 8.4),
- For LDAP users, the Identity Source to the LDAP server must be added in RSA AM server.

2 iDRAC9 Configuration for RSA SecurID

iDRAC9 can only be configured to authenticate with a single RSA AM server at a time. These global settings on RSA AM server apply to all iDRAC local users, AD and LDAP users. We will go through each in details in the following sections:

2.1 RSA SecurID 2FA Global Configuration

To enable RSA SecureID on iDRAC, the following attributes from the RSA AM server are required:

- ➢ RSA Authentication API URL
- ➢ RSA Client-ID
- ➢ RSA Access Key
- ➢ RSA AM server certificate (chain)

RSA Authentication API URL

The URL syntax is: https://<rsa-am-server-hostname>:<port>/mfa/v1_1, and by default the port is 5555.

RSA Client ID

By default, the RSA client ID is the same as the RSA AM server hostname. Find the RSA client ID at RSA AM server's authentication agent configuration page.

RSA Access Key

The Access Key can be retreived on RSA AM by navigating to **Setup** -> **System Settings** -> **RSA SecurID** Authentication API section, which is usually displayed as “l98cv5x195fdi86u43jw0q069byt0x37umlfwxc2gnp4s0xk11ve2lffum4s8302”.

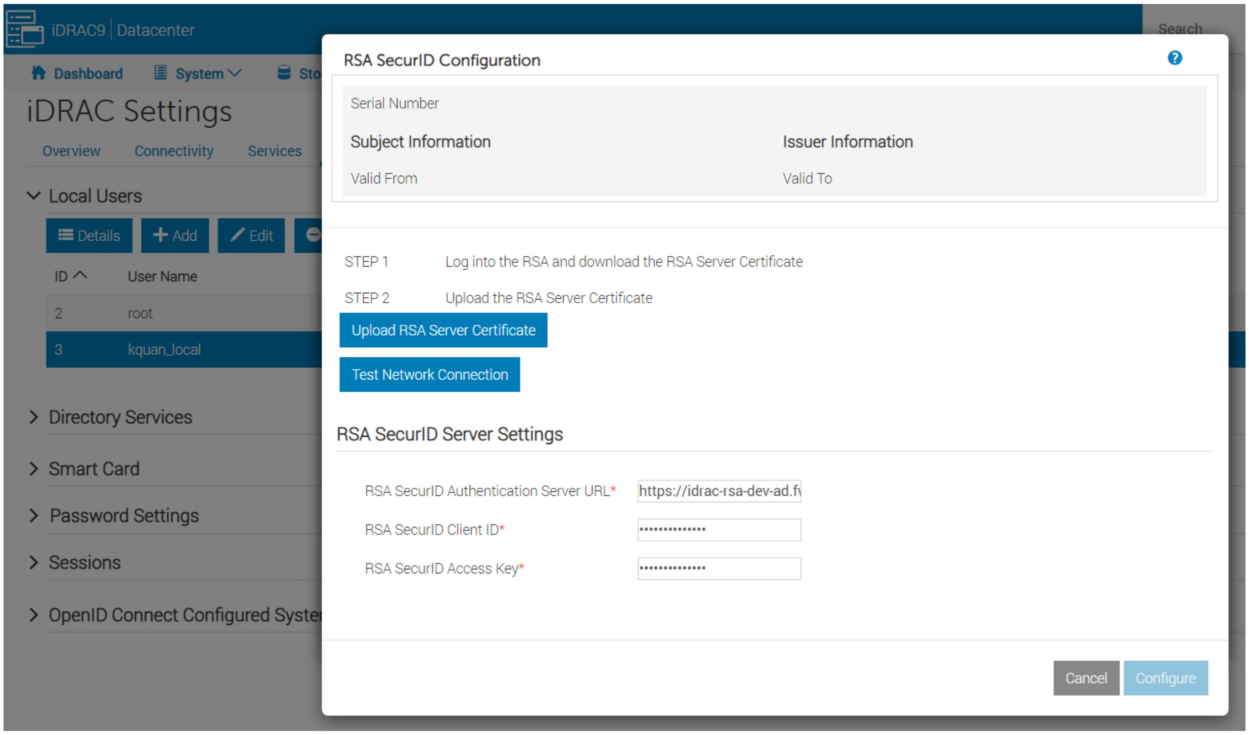
To configure the setting through iDRAC GUI,

1. Go to **iDRAC Settings** -> **Users.**
2. From “Local Users” section, select an existing local user and click **Edit** button.
3. Scroll down to the bottom at the configuration page.
4. In the **RSA SecurID** section, follow the link of **RSA SecurID Configuration** to view or edit these settings.

Another option,

1. Navigate from **iDRAC Settings** -> **Users.**
2. From “Directory Services” section, select **Microsoft Active Service** or **Generic LDAP Directory Service**, and click the **Edit** button.
3. You will find the same link to configure these global settings, and that is covered in a later section of this paper.

The figure below shows what this configuration page looks like.



RSA SecurID Configuration

Serial Number

Subject Information	Issuer Information
Valid From	Valid To

STEP 1 Log into the RSA and download the RSA Server Certificate

STEP 2 Upload the RSA Server Certificate

RSA SecurID Server Settings

RSA SecurID Authentication Server URL*	https://idrac-rsa-dev-ad.f\
RSA SecurID Client ID*	•••••••••••••••
RSA SecurID Access Key*	•••••••••••••••

Figure 1 RSA SecurID Configuration Page

Warning: For RSA AM adminsitrators, iDRAC does NOT support RSA Access ID. RSA Access ID can be used for additional security to ensure the integrity of RSA authentication message exchange. However, make sure this feature is disabled. Note that "disabled" is the default setting of the RSA AM server.

2.2 RSA AM Server Certificate (chain) Upload

RSA AM server certificate or certificate chain must be uploaded into iDRAC so that iDRAC can securely communicate with the configured RSA AM server.

In Figure-1, the RSA SecurID Configuration page allows you to upload the RSA server certificate. Contact your RSA AM server administrator to get the certificate or certificate chain in PEM format. Alternatively, you may also use RACADM to upload the certificate file into iDRAC. Use the subcommand *sslcertupload* with type option set to "RSA CA Certificate." See RACADM Users Guide for further details.

Alternatively, you may run the following command to retrieve the certificate chain. First, remove openssl debug information. Maintain the certificates in a file that can be uploaded later into iDRAC.

```
$ openssl s_client -showcerts -connect <rsa-am-server-hostname>:5555
```

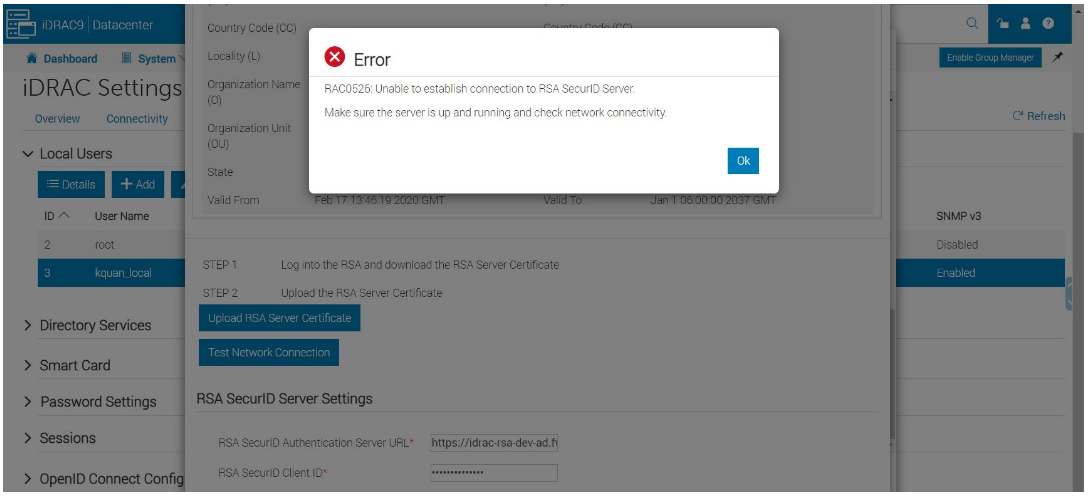
2.3 Test Connection to RSA AM Server

Before you can test connectivity to the RSA AM server:

- Specify all global settings.

- Upload the RSA AM certificate.
- Save the above.
- Ensure that iDRAC can resolve the hostname of the RSA AM server.

Once complete, click “Test Network Connection” to see if iDRAC can communicate with RSA AM server. If the test fails (See Figure 2.), ensure that all the settings are correct, and the firewall policies have been appropriately updated. See Troubleshooting section for more details. For example, if there was a connectivity issue, test connection may fail as below figure demonstrates.


Error

RAC0526: Unable to establish connection to RSA SecurID Server.

Make sure the server is up and running and check network connectivity.

Valid From Feb 17 13:46:19 2020 GMT Valid To Jan 1 06:00:00 2037 GMT

STEP 1 Log into the RSA and download the RSA Server Certificate

STEP 2 Upload the RSA Server Certificate

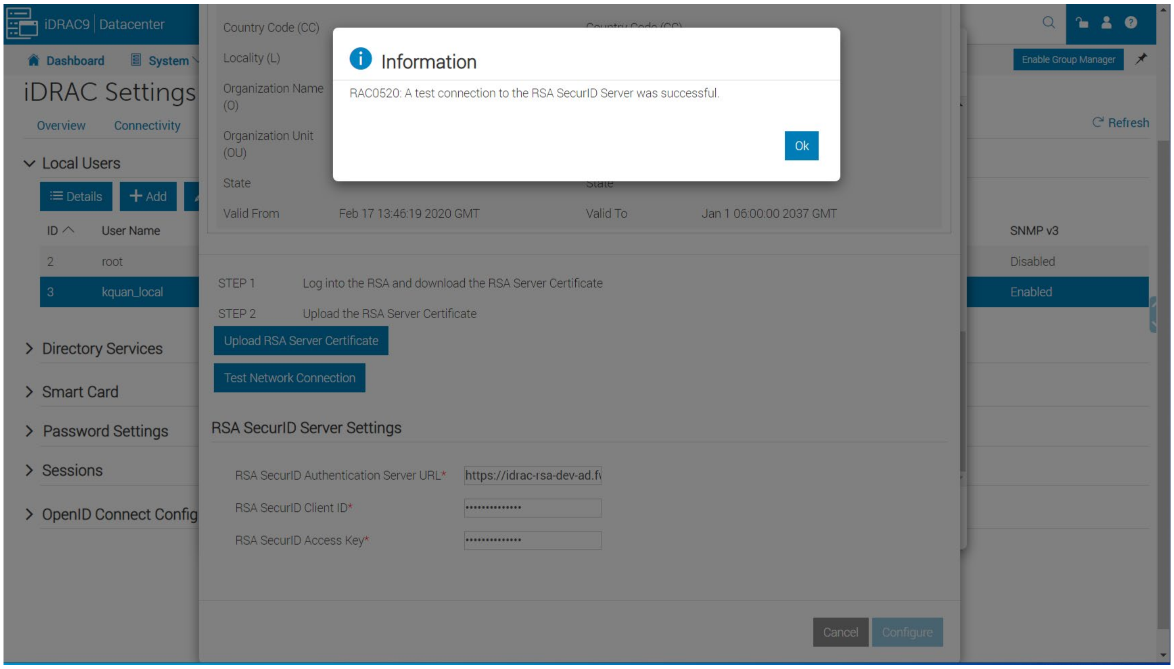
RSA SecurID Server Settings

RSA SecurID Authentication Server URL* https://idrac-rsa-dev-ad.f

RSA SecurID Client ID* ••••••••••••••

Figure 2 Test Connection failed due to connectivity issue

A good configuration shows a successful test connection, as shown below.


Information

RAC0520: A test connection to the RSA SecurID Server was successful.

Valid From Feb 17 13:46:19 2020 GMT Valid To Jan 1 06:00:00 2037 GMT

STEP 1 Log into the RSA and download the RSA Server Certificate

STEP 2 Upload the RSA Server Certificate

RSA SecurID Server Settings

RSA SecurID Authentication Server URL* https://idrac-rsa-dev-ad.f

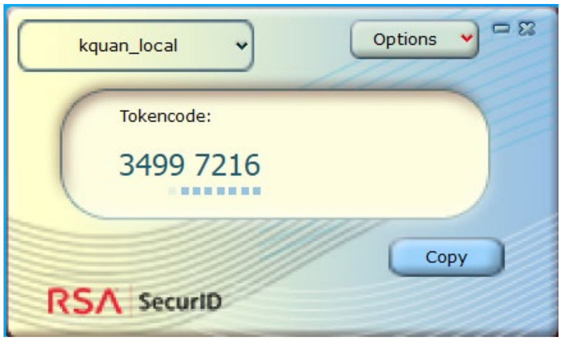
RSA SecurID Client ID* ••••••••••••••

RSA SecurID Access Key* ••••••••••••••

Figure 3 Test Connection succeeds.

2.4 Get RSA SecurID Token App Ready

RSA SecurID Token app is required to be installed on your Windows personal computer or on smart phone. See the RSA SecurID documentations for details. When you try to log in to iDRAC, You will be prompted to enter the passcode, use the RSA SecurID application to retrieve the passcode (Token) as shown in the figure below.



kquan_local

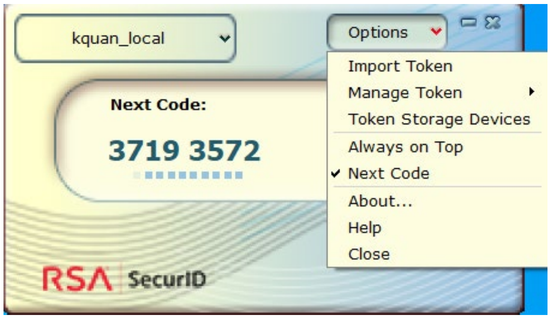
Tokencode:

3499 7216

Figure 4 Get passcode from RSA SecurID App.

If a wrong passcode is entered, the RSA AM server will challenge you to provide the “Next Token.” Sometimes, the next token may be required even after entering the correct passcode. This is to ensure that you own the right token that generated the right passcodes.

You can retrieve the “Next Token” from RSA SecurID Token app by going to Options menu. Check “Next Token,” and the next passcode is available. Time is critical in this step. Otherwise, iDRAC may fail the verification of the next token. If the iDRAC user login session times out, it requires another attempt to log in.



kquan_local

Next Code:

3719 3572

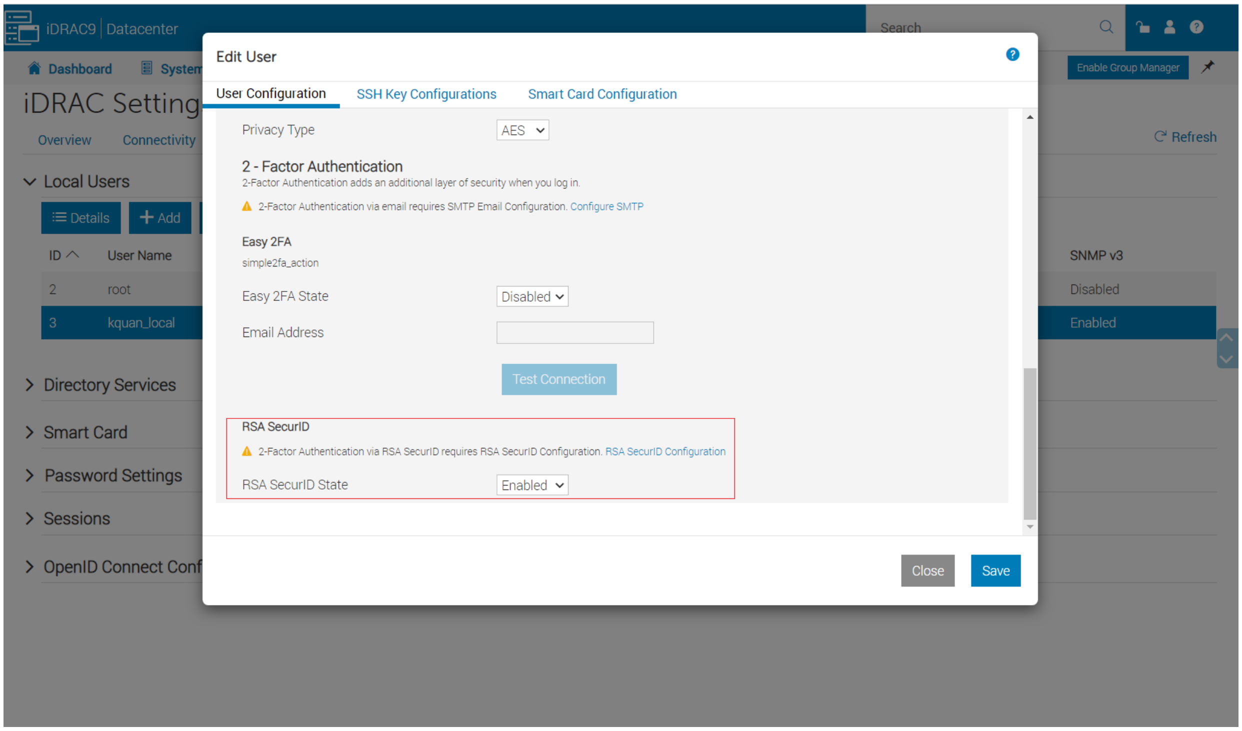
Figure 5 Get Next Token from RSA app.

3 RSA SecurID 2FA with Local Users

3.1 Enable RSA SecurID 2FA on an iDRAC Local User

iDRAC administrator can enable RSA SecurID 2FA on some local users. To do so, follow iDRAC UI navigation menu **iDRAC Settings** -> **Users** -> **Local Users**. Select an existing user and click Edit, the Edit User page will be displayed. At the bottom of the user configuration page, find RSA SecurID section. See image below.

Now you can enable or disable **RSA SecurID**. Click the link **RSA SecurID Configuration** to view or edit RSA SecurID global settings.



Edit User

Privacy Type: AES

2 - Factor Authentication

2-Factor Authentication adds an additional layer of security when you log in.

⚠ 2-Factor Authentication via email requires SMTP Email Configuration. Configure SMTP

Easy 2FA

simple2fa_action

Easy 2FA State: Disabled

Email Address:

RSA SecurID

⚠ 2-Factor Authentication via RSA SecurID requires RSA SecurID Configuration. RSA SecurID Configuration

RSA SecurID State: Enabled

Figure 6 RSA SecurID enablement on a local user

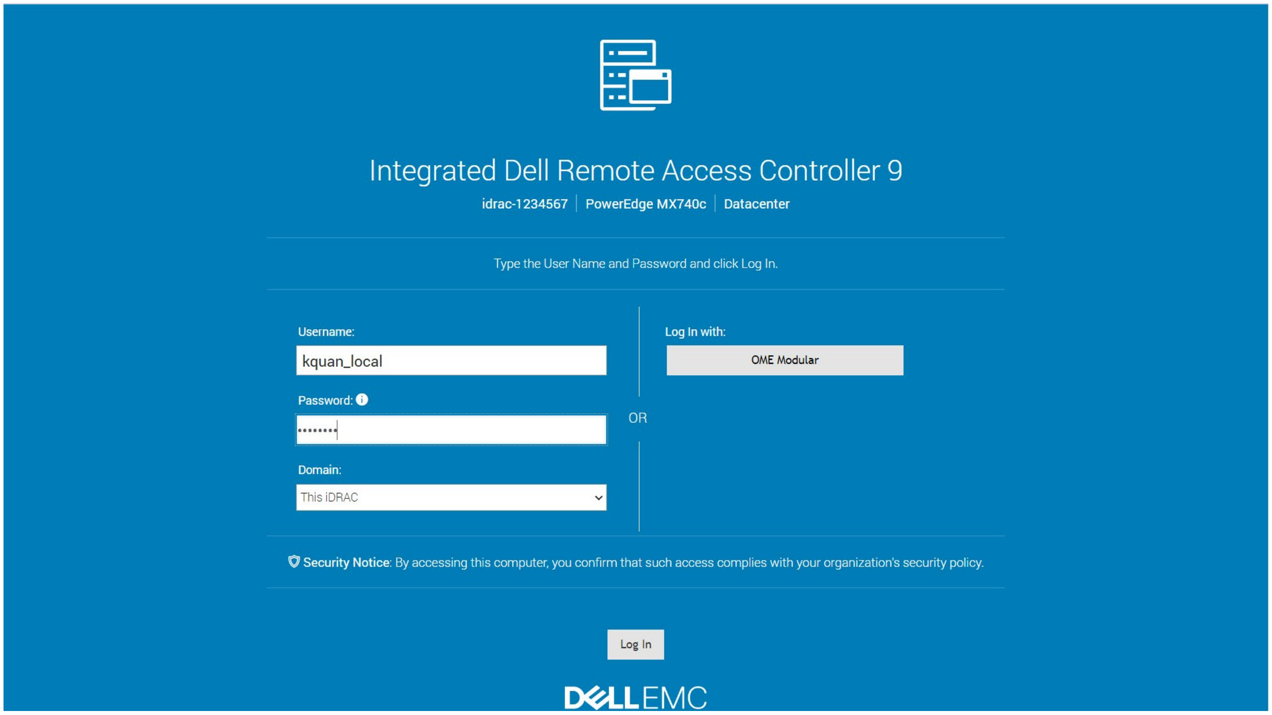
Notes:

1. To make RSA SecurID 2FA work on a local user, the same name user ID must be present or created in RSA AM local user database.
2. iDRAC gives administrators flexibility to turn on either Easy 2FA, or RSA 2FA, or even both for a specified user.

Before logging into iDRAC, ensure that the same user exists in RSA AM internal database and a valid token is assigned to the user. The token is then distributed to the expected recipient. As previously mentioned, iDRAC only supports RSA 2FA on iDRAC GUI login and SSH login.

3.2 Log in to iDRAC from UI with an iDRAC Local User

First log in with user credentials configured in iDRAC.



Integrated Dell Remote Access Controller 9

idrac-1234567 | PowerEdge MX740c | Datacenter

Type the User Name and Password and click Log In.

Username: kquan_local

Password: ••••••••

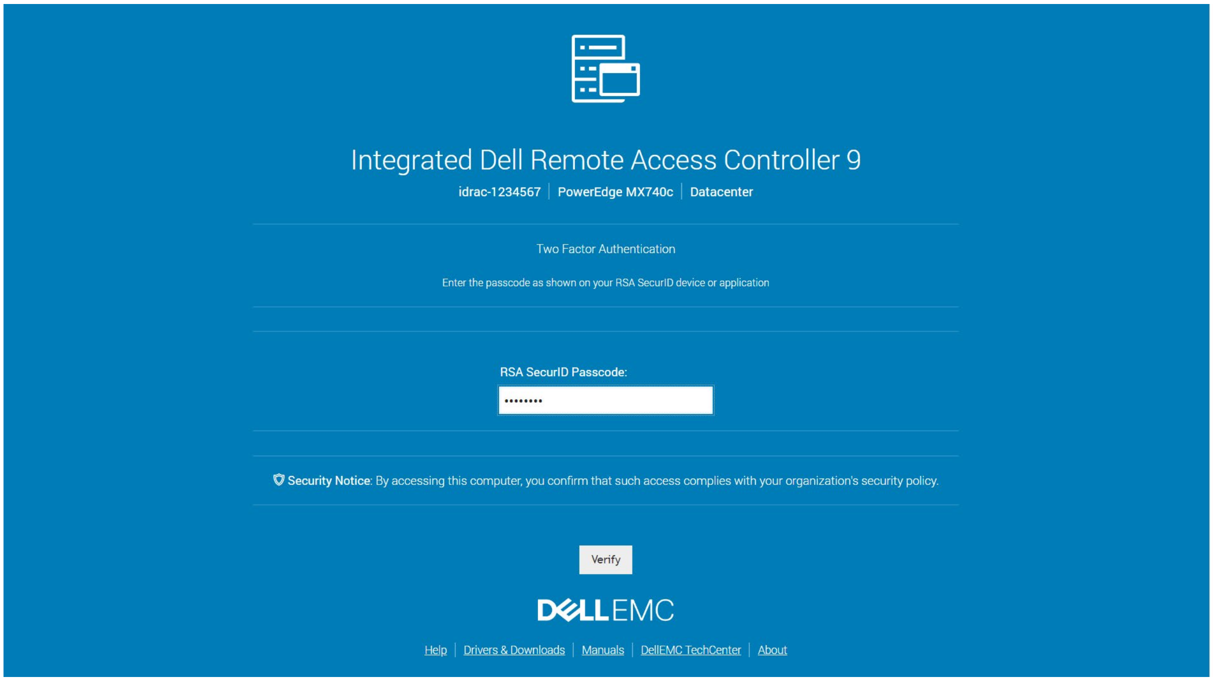
Domain: This iDRAC

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

Figure 7 Logging into iDRAC with RSA 2FA enabled local user

Next, the user is challenged with RSA SecurID. Type in the passcode from RSA SecurID Windows or Mobile application. iDRAC allows a maximum of three attempts to enter the correct passcode. Entering three wrong passcodes in a row, you will be locked out for 60 seconds. After lockout period ends, you must start over from the local user authentication.

If you believe you entered the correct passcode and authentication still fails, then see the Troubleshooting section.



Integrated Dell Remote Access Controller 9

idrac-1234567 | PowerEdge MX740c | Datacenter

Two Factor Authentication

Enter the passcode as shown on your RSA SecurID device or application

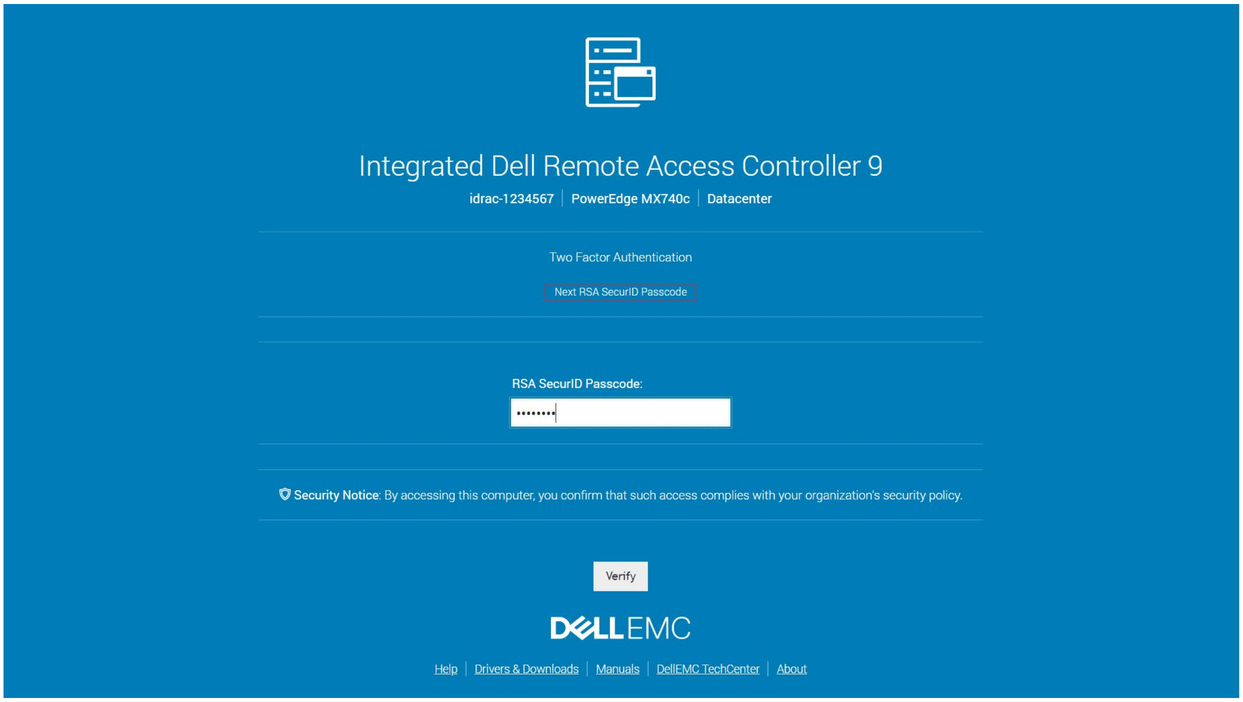
RSA SecurID Passcode: ••••••••

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

Verify
DELL EMC
Help | Drivers & Downloads | Manuals | DellEMC TechCenter | About

Figure 8 iDRAC challenges the user for a passcode.

For added security, you may configure the RSA AM server to ask for a “Next Token” after multiple incorrect passcode attempts. You must get the ‘next code’ from RSA SecurID app as the figure below shows.



Integrated Dell Remote Access Controller 9

idrac-1234567 | PowerEdge MX740c | Datacenter

Two Factor Authentication

Next RSA SecurID Passcode

RSA SecurID Passcode: ••••••••

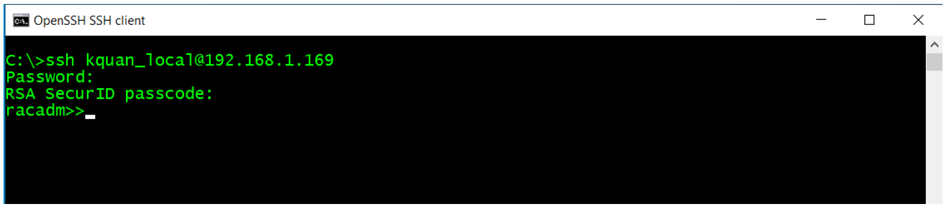
Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

Verify
DELL EMC
Help | Drivers & Downloads | Manuals | DellEMC TechCenter | About

Figure 9 iDRAC challenges the user with next token.

3.3 Log in to iDRAC from SSH with an iDRAC Local User

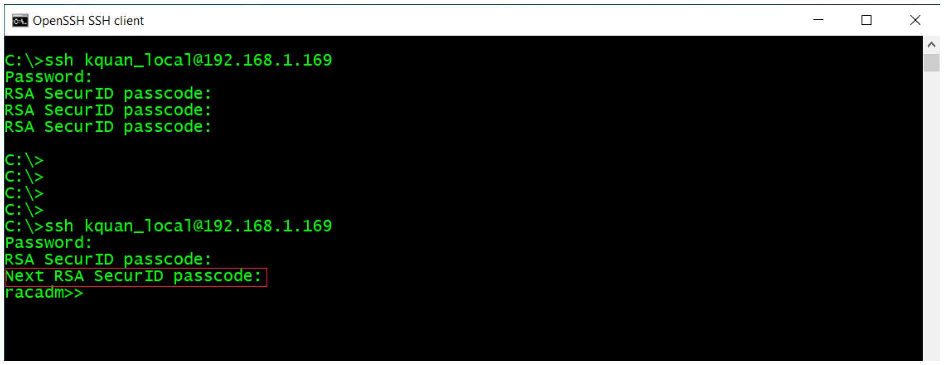
LikeLikethe UI, three attempts are given to enter a correct RSA passcode. Otherwise, you are challenged from the beginning with local user authentication.



```
C:\>ssh kquan_local@192.168.1.169
Password:
RSA SecurID passcode:
racadm>>
```

Figure 10 Logging into iDRAC from SSH with a local user.

If too many wrong passcodes are attempted, “Next token” may be required.



```
C:\>ssh kquan_local@192.168.1.169
Password:
RSA SecurID passcode:
RSA SecurID passcode:
RSA SecurID passcode:

C:\>
C:\>
C:\>
C:\>
C:\>ssh kquan_local@192.168.1.169
Password:
RSA SecurID passcode:
Next RSA SecurID passcode:
racadm>>
```

Figure 11 Local user SSH logging with next passcode required

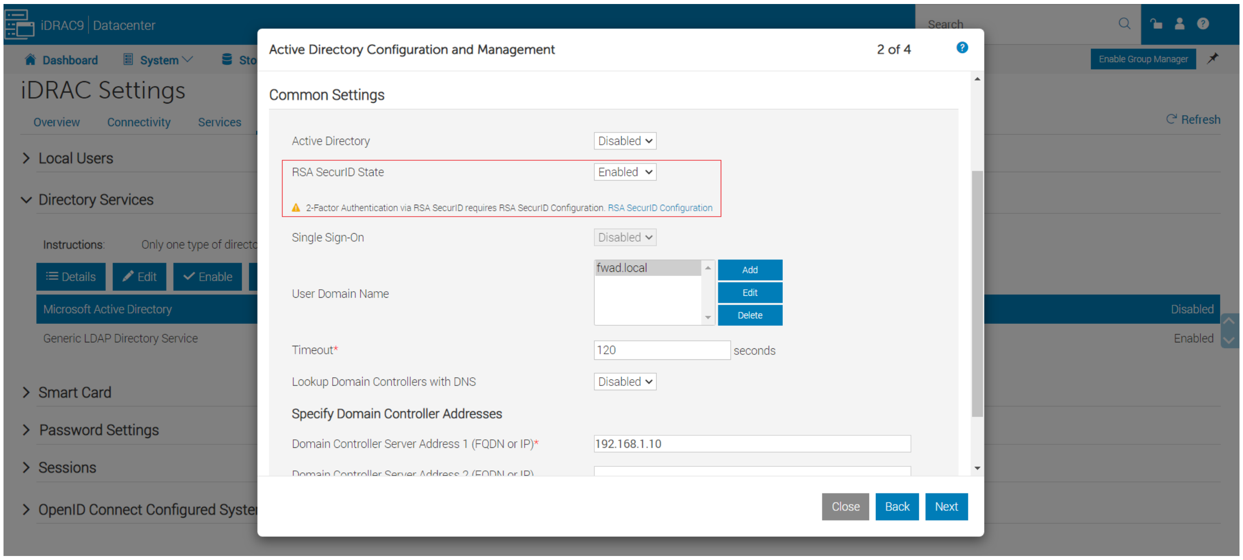
4 RSA SecurID 2FA with Active Directory Users

4.1 Enable RSA SecurID 2FA on Active Directory Users

Note: RSA SecurID 2FA can only be applied to all or none of the Active Directory (AD) users.

To enable or disable RSA SecurID 2FA on AD users, go to iDRAC UI. Then, follow the navigation menu from **iDRAC Settings** -> **Users** -> **Directory Services.** From there, select **Microsoft Active Directory** and click **Edit** button. On the second page of AD configuration, find the RSA SecurID State dropdown box that enables or disables RSA SecurID 2FA on AD users.

Also, there is a link to view or edit RSA SecurID Configuration right below the dropdown box. Configuring iDRAC to authenticate users using Active Directory is not in the scope of this document. For more information see the white paper [Integrate iDRAC with Microsoft's Active Directory]().



Active Directory Configuration and Management 2 of 4

Common Settings

Active Directory: Disabled

RSA SecurID State: Enabled

2-Factor Authentication via RSA SecurID requires RSA SecurID Configuration. RSA SecurID Configuration

Single Sign-On: Disabled

User Domain Name: fwad.local

Timeout*: 120 seconds

Lookup Domain Controllers with DNS: Disabled

Specify Domain Controller Addresses

Domain Controller Server Address 1 (FQDN or IP)*: 192.168.1.10

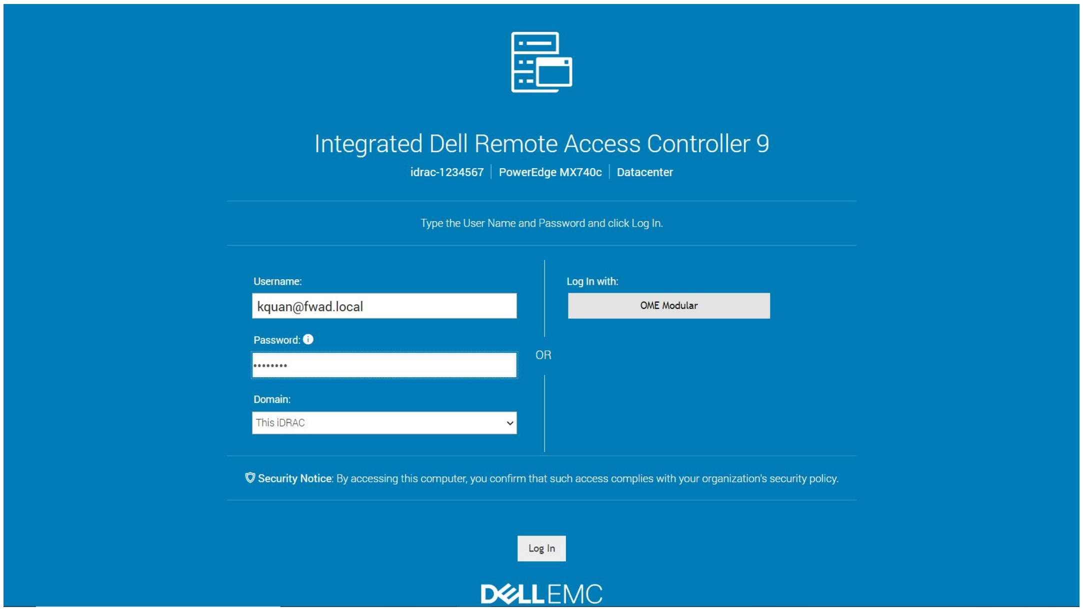
Domain Controller Server Address 2 (FQDN or IP)

Figure 12 RSA SecurID 2FA enablement on AD users

Notes: iDRAC uses UPN name to authenticate with RSA AM. In other words, the RSA AM server the AD username must be mapped to UPN name (userPrincipalName) from default samAccountName. See RSA AM documentation for details - https://community.rsa.com/docs/DOC-46951.

4.2 Log in to iDRAC from UI with an AD User

To log in with AD user, you must use User Principal Name (UPN), and password.



Integrated Dell Remote Access Controller 9

idrac-1234567 | PowerEdge MX740c | Datacenter

Type the User Name and Password and click Log In.

Username: kquan@fwad.local

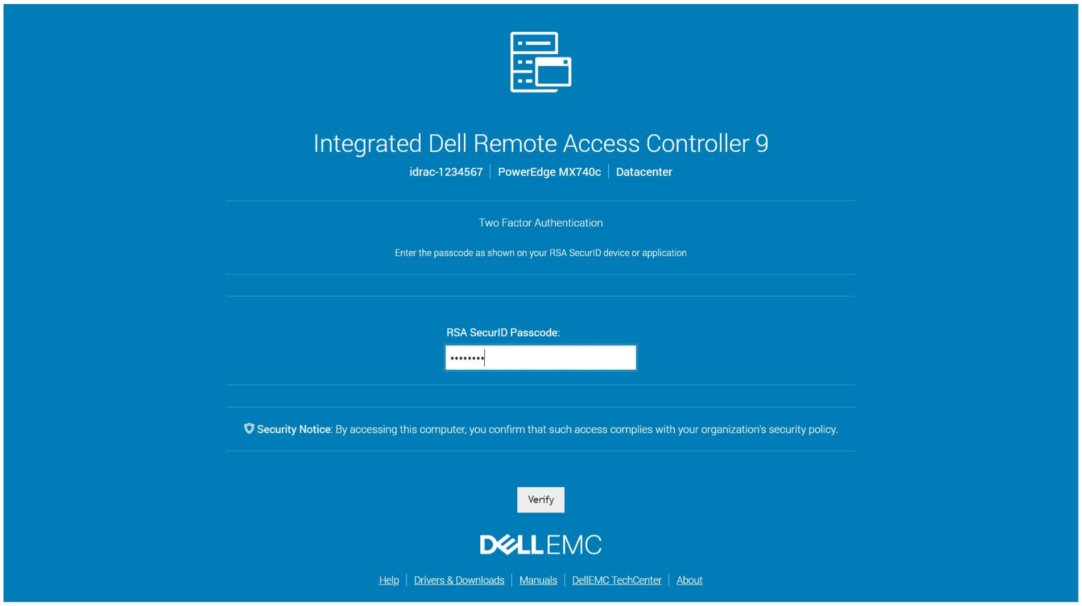
Password: ••••••••

Domain: This iDRAC

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

Figure 13 Logging into iDRAC UI with an AD user

Next, the user is challenged with RSA SecurID, you must get and enter the passcode displayed in the RSA SecurID app for this specific AD user. You have three chances to enter the correct passcode. The same lockout policy applies to AD user as well. For better security, the RSA AM server can be configured to challenge a user with the “next token” after the configurable failed attempts occur. iDRAC will prompt user to enter the next token after a correct passcode is entered and verified by the RSA AM server. The user then must get the “Next Token” from RSA app.



Integrated Dell Remote Access Controller 9

idrac-1234567 | PowerEdge MX740c | Datacenter

Two Factor Authentication

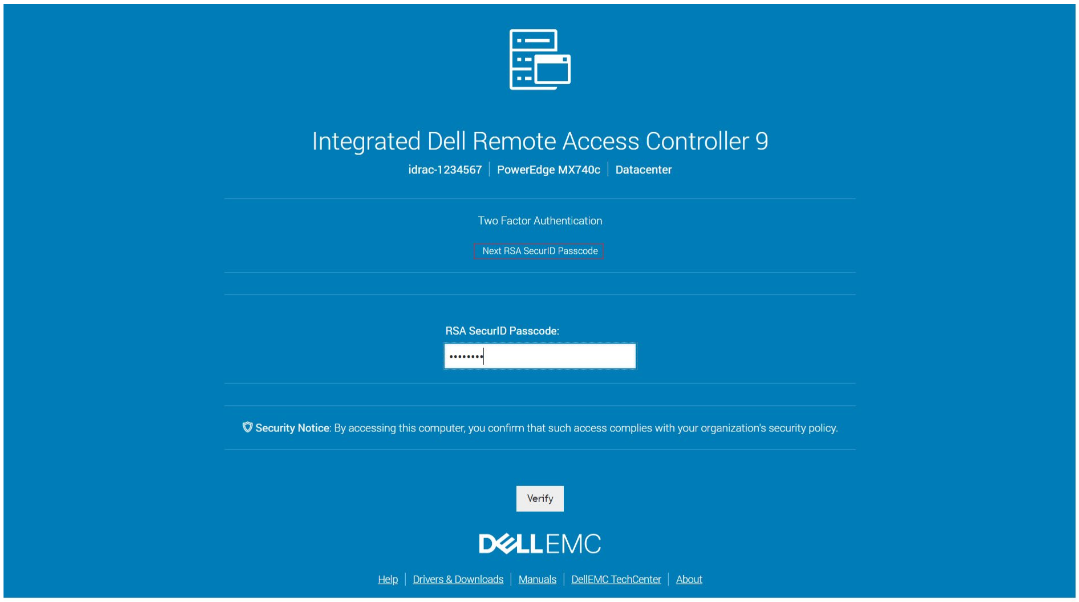
Enter the passcode as shown on your RSA SecurID device or application

RSA SecurID Passcode: ••••••••

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

Verify
DELL EMC
Help | Drivers & Downloads | Manuals | DellEMC TechCenter | About

Figure 14 RSA passcode required for the AD user



Integrated Dell Remote Access Controller 9

idrac-1234567 | PowerEdge MX740c | Datacenter

Two Factor Authentication

Next RSA SecurID Passcode

RSA SecurID Passcode: ••••••••

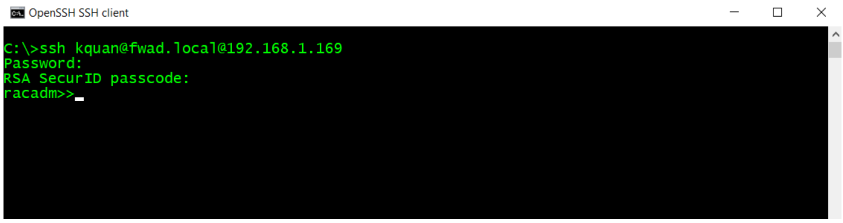
Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

Verify
DELLEMC
Help | Drivers & Downloads | Manuals | DellEMC TechCenter | About

Figure 15 RSA next passcode required for the AD user

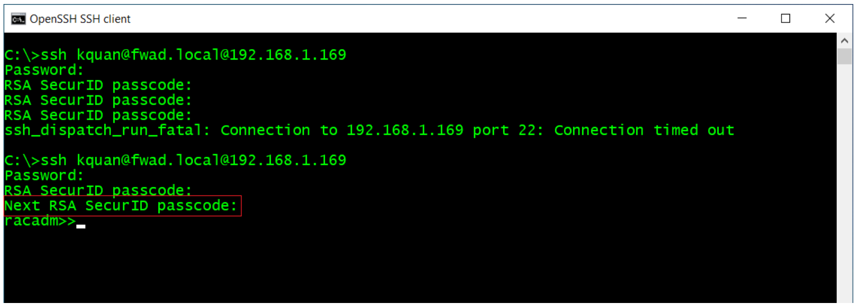
4.3 Log in to iDRAC from SSH with an AD User

To login into SSH, you must use the User Principal Name (UPN) to log in; for example, *kquan@fwad.local*. Also, you have three attempts to enter a correct RSA passcode to be authenticated.



```
C:\>ssh kquan@fwad.local@192.168.1.169
Password:
RSA SecurID passcode:
racadm>>_
```

Figure 16 Logging into iDRAC from SSH with an AD user



```
C:\>ssh kquan@fwad.local@192.168.1.169
Password:
RSA SecurID passcode:
RSA SecurID passcode:
RSA SecurID passcode:
ssh_dispatch_run_fatal: Connection to 192.168.1.169 port 22: Connection timed out

C:\>ssh kquan@fwad.local@192.168.1.169
Password:
RSA SecurID passcode:
Next RSA SecurID passcode:
racadm>>_
```

Figure 17 RSA next passcode required for the AD user

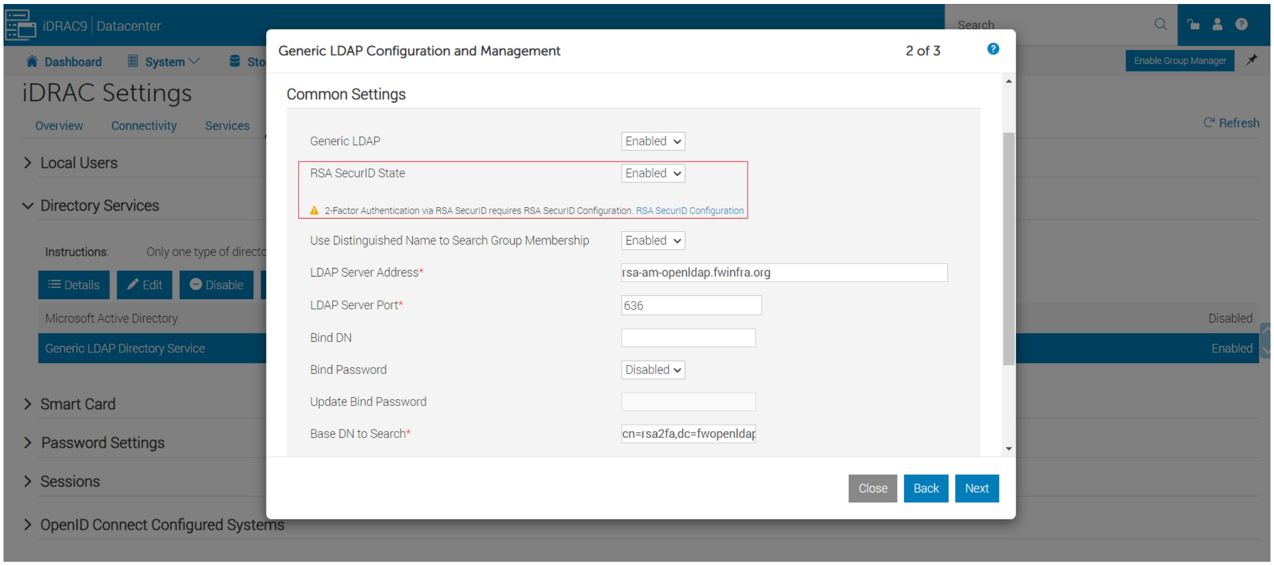
5 RSA SecurID 2FA with Generic LDAP Directory Users

5.1 Enable RSA SecurID 2FA on Generic LDAP Directory Users

Similarly, RSA SecurID 2FA is applied to all or none of LDAP users.

To enable or disable RSA SecurID 2FA on LDAP users, go to iDRAC UI, follow the navigation menu from **iDRAC Settings** -> **Users** -> **Directory Services.** From there, select **Generic LDAP Directory Service** and click **Edit** button. On the second LDAP service configuration page, locate the RSA SecurID State dropdown box to enable or disable RSA SecurID 2FA on LDAP users.

See Figure 4.



Generic LDAP Configuration and Management 2 of 3

Common Settings

Generic LDAP: Enabled

RSA SecurID State: Enabled

2-Factor Authentication via RSA SecurID requires RSA SecurID Configuration. RSA SecurID Configuration

Use Distinguished Name to Search Group Membership: Enabled

LDAP Server Address*: rsa-am-openldap.fwinfra.org

LDAP Server Port*: 636

Bind DN:

Bind Password: Disabled

Update Bind Password:

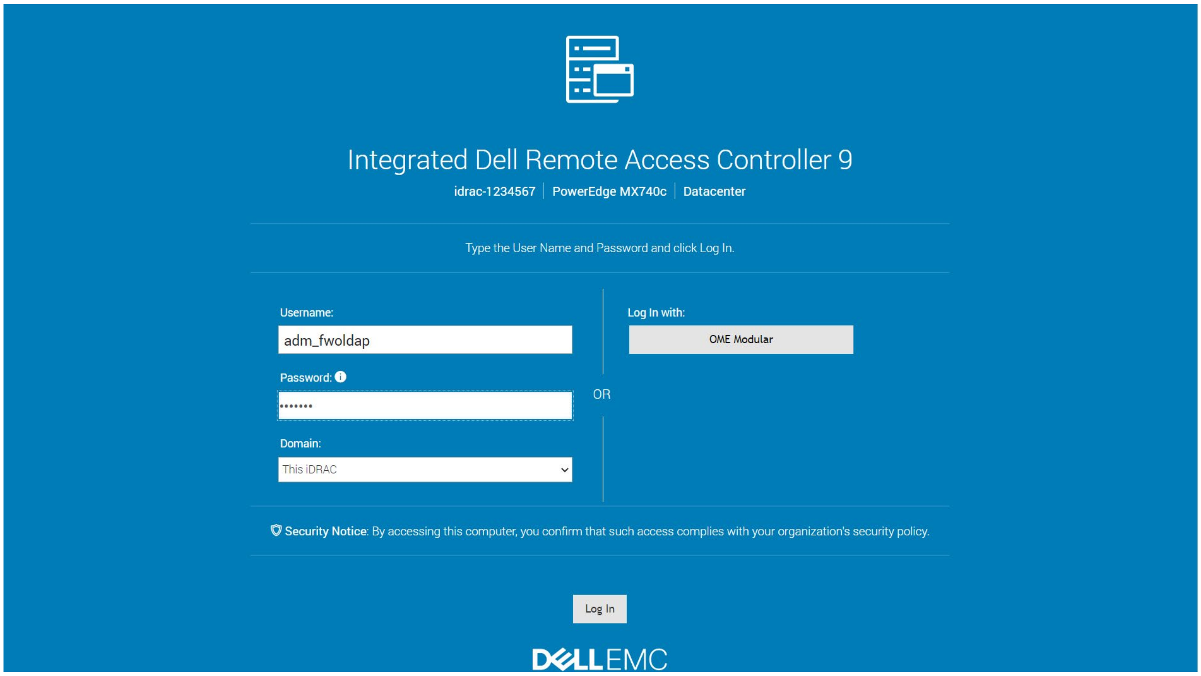
Base DN to Search*: cn=rsa2fa,dc=fwopenldap

Close Back Next

Figure 18 RSA SecurID enablement on generic LDAP directory users

5.2 Log in to iDRAC from UI with an LDAP User Account

Another option is to use an LDAP user **adm_fwoldap** to perform UI login.



Integrated Dell Remote Access Controller 9

idrac-1234567 | PowerEdge MX740c | Datacenter

Type the User Name and Password and click Log In.

Username: adm_fwoldap

Password: •••••••

Domain: This iDRAC

OR

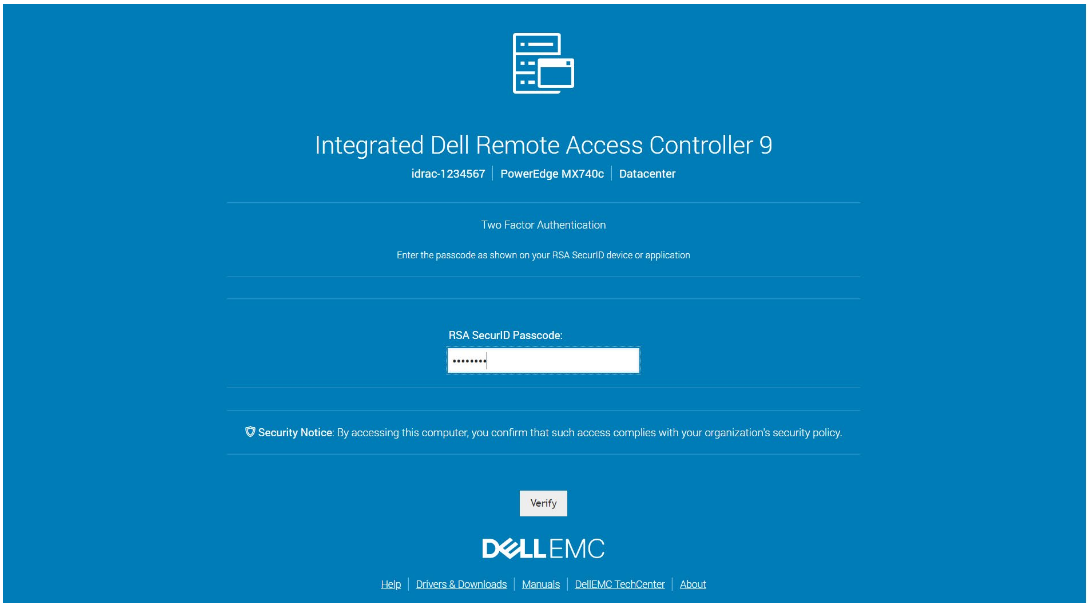
Log In with: OME Modular

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

Log In

Figure 19 Logging in iDRAC from UI with LDAP user

After entering the password, the user is challenged with RSA SecurID, you must enter the passcode displayed in the RSA SecurID app for this specific LDAP user. You have three chances to enter the correct passcode. The same lockout policy applies to LDAP user as well. For better security, an RSA AM server can be configured to challenge a user with the "next token" after the configurable failed attempts occur. iDRAC will prompt user to enter the next token after a correct passcode has been entered and verified by the RSA AM server. The user then must get the "Next Token" from RSA app.



Integrated Dell Remote Access Controller 9

idrac-1234567 | PowerEdge MX740c | Datacenter

Two Factor Authentication

Enter the passcode as shown on your RSA SecurID device or application

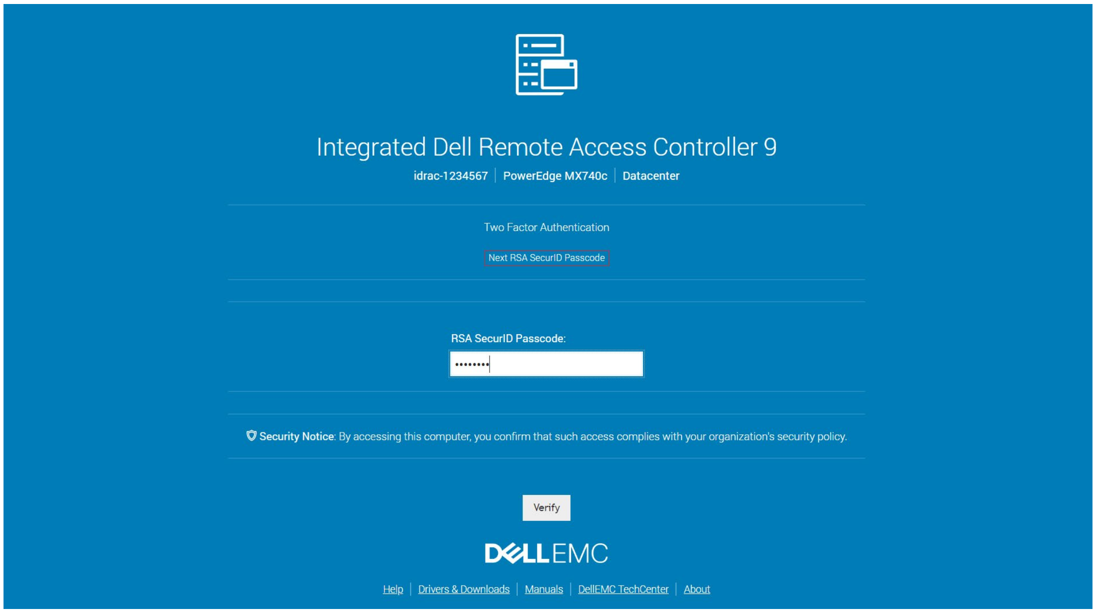
RSA SecurID Passcode: ••••••••

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

Verify

Help | Drivers & Downloads | Manuals | DellEMC TechCenter | About

Figure 20 RSA passcode required for the LDAP user



Integrated Dell Remote Access Controller 9

idrac-1234567 | PowerEdge MX740c | Datacenter

Two Factor Authentication

Next RSA SecurID Passcode

RSA SecurID Passcode: ••••••••

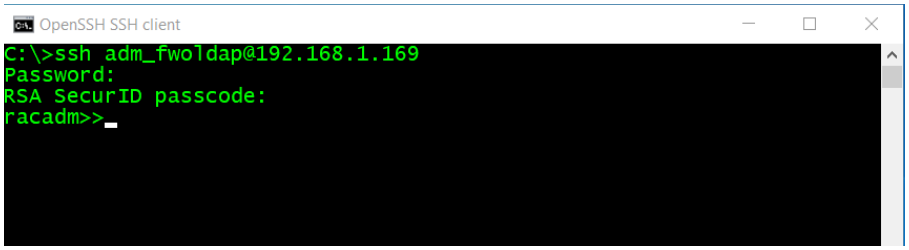
Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

Verify
DELLEMC
Help | Drivers & Downloads | Manuals | DellEMC TechCenter | About

Figure 21 RSA next passcode required for the LDAP user

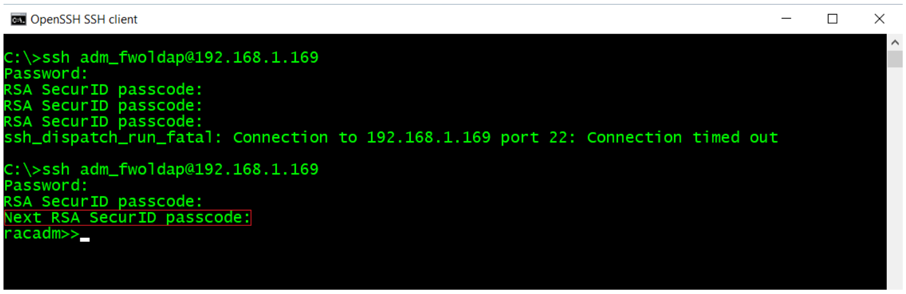
5.3 Log in to iDRAC from SSH with an LDAP User

Similarly, you can log in to iDRAC using an LDAP user “adm_fwoldap” on which RSA SecurID 2FA is enabled.



```
C:\>ssh adm_fwoldap@192.168.1.169
Password:
RSA SecurID passcode:
racadm>>_
```

Figure 22 Logging into iDRAC from SSH with an LDAP user



```
C:\>ssh adm_fwoldap@192.168.1.169
Password:
RSA SecurID passcode:
RSA SecurID passcode:
RSA SecurID passcode:
ssh_dispatch_run_fatal: Connection to 192.168.1.169 port 22: Connection timed out

C:\>ssh adm_fwoldap@192.168.1.169
Password:
RSA SecurID passcode:
Next RSA SecurID passcode:
racadm>>_
```

Figure 23 Next passcode required for the LDAP user

6 Troubleshooting RSA SecurID Issues

When a user with RSA SecurID enabled fails to authenticate, the problem may be in iDRAC or the RSA AM server.

6.1 Misconfiguration or iDRAC Configuration Gets Reset

First, check the Lifecycle Logs in the iDRAC to see if there are Lifecycle Logs to indicate any problems with the RSA 2FA configuration. There can be issues even if all the global settings are set correctly or the RSA AM certificate chain has uploaded.

You can test the connection to RSA AM server configured from UI, see Test Connection to RSA AM Server section to see how you can run the test. iDRAC detects and reports issues below to help you troubleshoot the issue. Test Connection to RSA AM server may return one of the following codes.

RAC0520: A test connection to the RSA SecurID Server was successful.

RAC0521: Unable to connect to the RSA SecurID Server because either invalid RSA SecurID Server settings are entered, or invalid RSA server certificate is uploaded.

RAC0522: Unable to connect to any RSA SecurID Server because either RSA server certificate is not uploaded to iDRAC or something wrong with the uploaded certificate.

RAC0525: Unable to resolve the hostname of RSA SecurID Server. Ensure DNS servers that are configured and work properly.

RAC0526: Unable to make connection to RSA SecurID Server. Ensure that the server configuration is right and the server is up and running, also check if there are any connectivity issues.

RAC0527: Failed to get response from RSA SecurID Server, ensure that the server is working properly and try again.

Next, you must ensure that:

- The users are configured to be RSA 2FA enabled, and the local user is RSA 2FA enabled.
- or AD users are RSA 2FA enabled,
- or LDAP users are configured with RSA 2FA enabled in previous chapter.

You may also check if the iDRAC has been reset to factory default (without preserving user and network settings). If so, you must re-configure RSA 2FA on this iDRAC system depicted in Chapter 2 and enable RSA SecurID 2FA on the desired local users, AD users, or LDAP users.

6.2 Datacenter License Expires or Gets Downgraded or Deleted

If an iDRAC Datacenter License is no longer active, all users who are configured with RSA SecurID cannot log in to the system. Disable RSA SecurID in iDRAC if the system does not have a valid iDRAC Datacenter license.

An administrator can set up a special privileged user without RSA enabled with a strong password. Should a downgrade event happen, you can log in with the privileged user to disable RSA SecurID 2FA on all users.

In extreme case, if no user can log in to system due to the license issue, perform iDRAC "Reset to Defaults" as a last resort.

6.3 Authentication Failures without being Prompted for RSA Passcode

In this scenario, the Lifecycle Controller log may not give you clues as to what might have gone wrong. This behavior is expected since iDRAC does not expose any security information to the potential hackers. Check to see if RSA 2FA global settings are properly configured. To do so, see the Test Connection to RSA AM Server section.

6.4 Authentication failures with Correct RSA Passcode

RSA AM lockout policy could be the source for this failure. Check with RSA AM server administrator to see if the user (either local or AD/LDAP) is locked out. Lockout can be due to the lockout policies defined on the RSA AM server.

Other issues, such as RSA AM lost connection to AD/LDAP server. While not covered in this paper, you may consider this issue while troubleshooting authentication failures when you believe you all correct credentials were provided.

If passcodes are correct and authentication still fails, the passcode that the RSA SecurID app generates may not match the one by the RSA AM. In this case, the user can resynchronize the token with RSA AM by RSA SecurID Self-Service Console. Otherwise, contact the RSA AM administrator for details on how RSA AM is configured. For details, see the RSA documentation Resynchronize a Token.

6.5 Authentication Failures with Correct RSA Passcode due to Timeout

If somehow user types in a correct RSA passcode (either "current" or "next") after the expected time, then iDRAC login session may time out.

The best practice is to input a passcode as soon as possible; especially for the "Next Passcode." Do not wait for RSA SecurID Token app to generate a new code. Instead, ensure that you get and use the next code immediately from the app, as shown in section Get RSA SecurID Token App Ready.

6.6 RSA Configuration gets lost after importing Server Configuration Profile

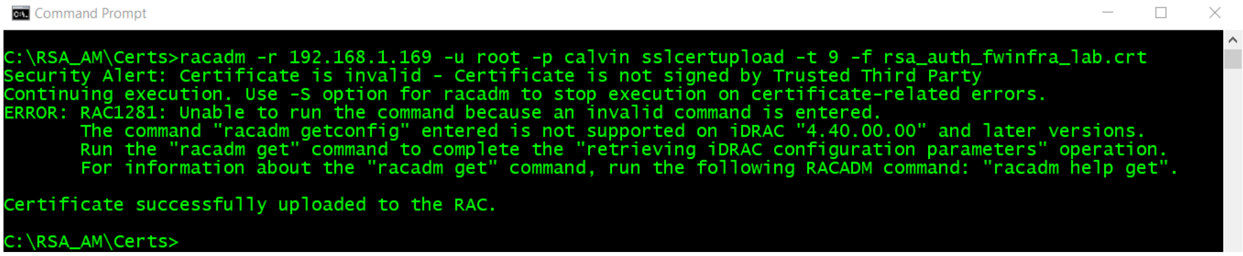
Due to the security reason, currently Server Configuration Profile (SCP) only includes RSA SecurID authentication server URL. In another word, if you save iDRAC configuration via SCP and import it back later, you will basically have to configure RSA SecurID again.

Appendix A: Configure iDRAC Using RACADM

A.1 Upload RSA AM Certificate Chain

Run the following RACADM command to upload RSA AM certificate chain.

Assuming rsa_am.cert contains the certificate of RSA AM server along with its signing certificates in a single file.
C:> racadm -r <idrac-ip-or-hostname> -u <username> -p <password> sslcertupload -t 9 -f rsa_am.cert



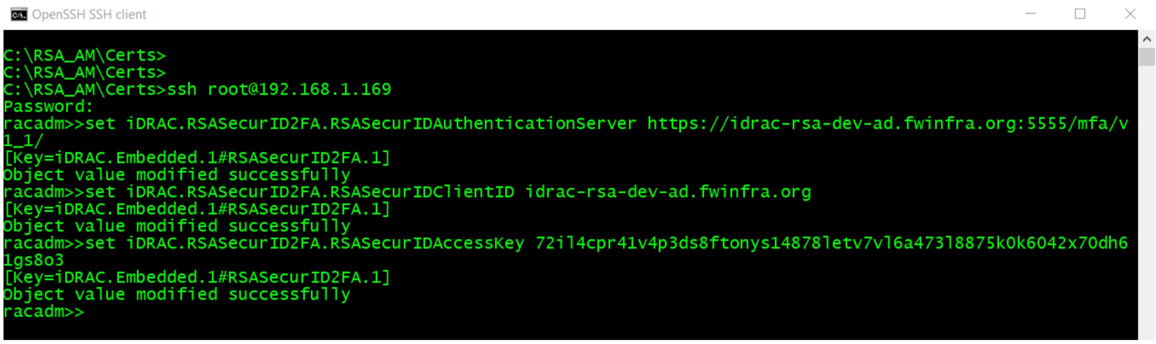
```
C:\RSA_AM\Certs>racadm -r 192.168.1.169 -u root -p calvin sslcertupload -t 9 -f rsa_auth_fwinfra_lab.crt
Security Alert: Certificate is invalid - Certificate is not signed by Trusted Third Party
Continuing execution. Use -S option for racadm to stop execution on certificate-related errors.
ERROR: RAC1281: Unable to run the command because an invalid command is entered.
       The command "racadm getconfig" entered is not supported on iDRAC "4.40.00.00" and later versions.
       Run the "racadm get" command to complete the "retrieving iDRAC configuration parameters" operation.
       For information about the "racadm get" command, run the following RACADM command: "racadm help get".

Certificate successfully uploaded to the RAC.

C:\RSA_AM\Certs>
```

Figure 24 Use RACADM to upload RSA cert chain.

A.2 Configure RSA SecurID Global Settings

Run the following RACADM command to configure RSA SecurID global settings.

racadm>> set iDRAC.RSASecurID2FA.RSASecurIDAuthenticationServer https://<rsa-am-server-hostname>:<port>/mfa/v1_1
racadm>> set iDRAC.RSASecurID2FA.RSASecurIDClientID "idrac-rsa-dev.cec.delllabs.net"
racadm>> set iDRAC.RSASecurID2FA.RSASecurIDAccessKey "n8xh7fud5712v661728ibx2adph5b2zbi25zfp7d609616b607bhd7450cvkbg1x"



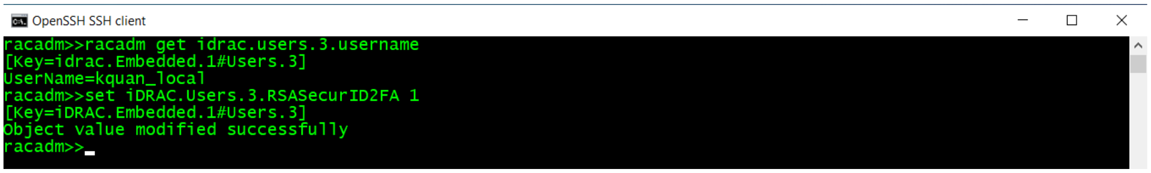
```
C:\RSA_AM\Certs>
C:\RSA_AM\Certs>
C:\RSA_AM\Certs>ssh root@192.168.1.169
Password:
racadm>>set iDRAC.RSASecurID2FA.RSASecurIDAuthenticationServer https://idrac-rsa-dev-ad.fwinfra.org:5555/mfa/v
1_1/
[Key=iDRAC.Embedded.1#RSASecurID2FA.1]
Object value modified successfully
racadm>>set iDRAC.RSASecurID2FA.RSASecurIDClientID idrac-rsa-dev-ad.fwinfra.org
[Key=iDRAC.Embedded.1#RSASecurID2FA.1]
Object value modified successfully
racadm>>set iDRAC.RSASecurID2FA.RSASecurIDAccessKey 72il4cpr41v4p3ds8ftonys14878letv7vl6a47318875k0k6042x70dh6
1gs8o3
[Key=iDRAC.Embedded.1#RSASecurID2FA.1]
Object value modified successfully
racadm>>
```

Figure 25 Use RACADM to configure RSA SecurID 2FA settings.

A.3 Enable RSA SecurID on a Local User

Run the following RACADM command to enable RSA SecurID on a local user.

racadm>> set iDRAC.Users.3.RSASecurID2FA 1



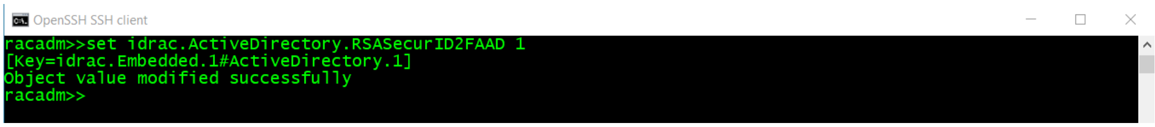
```
racadm>>racadm get idrac.users.3.username
[Key=idrac.Embedded.1#Users.3]
UserName=kquan_local
racadm>>set iDRAC.Users.3.RSASecurID2FA 1
[Key=iDRAC.Embedded.1#Users.3]
Object value modified successfully
racadm>>
```

Figure 26 Use RACADM to enable RSA SecurID 2FA on a local user.

A.4 Enable RSA SecurID on AD Users

Run the following RACADM command to enable RSA SecurID on all AD users.

racadm>> set idrac.ActiveDirectory.RSASecurID2FAAD 1



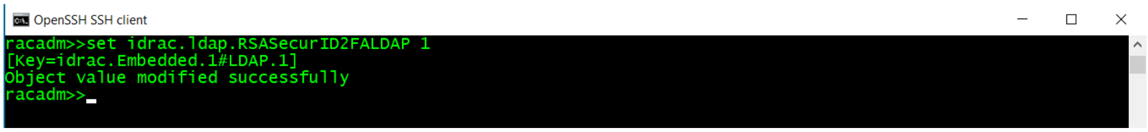
```
racadm>>set idrac.ActiveDirectory.RSASecurID2FAAD 1
[Key=idrac.Embedded.1#ActiveDirectory.1]
Object value modified successfully
racadm>>
```

Figure 27 Use RACADM to enable RSA SecurID 2FA on all AD users.

A.5 Enable RSA SecurID on LDAP Users

Run the following RACADM command to enable RSA SecurID on all LDAP users.

racadm>> set idrac.ldap.RSASecurID2FALDAP 1



```
racadm>>set idrac.ldap.RSASecurID2FALDAP 1
[Key=idrac.Embedded.1#LDAP.1]
Object value modified successfully
racadm>>
```

Figure 28 User RACADM to enable RSA SecurID 2FA on all LDAP users

Appendix B: References

- iDRAC Users Guide and RACADM Users Guide
  www.dell.com/idracmanuals

- RSA Authentication Manager (AM) 8.4 Help
  https://community.rsa.com/docs/DOC-100436

- Integrating iDRAC With Microsoft Active Directory
  https://downloads.dell.com/solutions/general-solution-resources/White%20Papers/Integrate_iDRAC_with_Active_Directory.pdf

- Integrating iDRAC with Generic LDAP Directory (WIP)