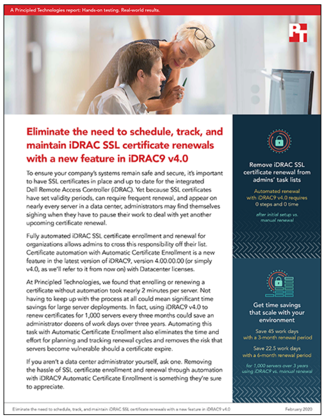


A Principled Technologies report: Hands-on testing. Real-world results.

Eliminate the need to schedule, track, and maintain iDRAC SSL certificate renewals with a new feature in iDRAC9 v4.0

To ensure your company's systems remain safe and secure, it's important to have SSL certificates in place and up to date for the integrated Dell Remote Access Controller (iDRAC). Yet because SSL certificates have set validity periods, can require frequent renewal, and appear on nearly every server in a data center, administrators may find themselves sighing when they have to pause their work to deal with yet another upcoming certificate renewal.

Fully automated iDRAC SSL certificate enrollment and renewal for organizations allows admins to cross this responsibility off their list. Certificate automation with Automatic Certificate Enrollment is a new feature in the latest version of iDRAC9, version 4.00.00.00 (or simply v4.0, as we'll refer to it from now on) with Datacenter licenses.

At Principled Technologies, we found that enrolling or renewing a certificate without automation took nearly 2 minutes per server. Not having to keep up with the process at all could mean significant time savings for large server deployments. In fact, using iDRAC9 v4.0 to renew certificates for 1,000 servers every three months could save an administrator dozens of work days over three years. Automating this task with Automatic Certificate Enrollment also eliminates the time and effort for planning and tracking renewal cycles and removes the risk that servers become vulnerable should a certificate expire.

If you aren't a data center administrator yourself, ask one. Removing the hassle of SSL certificate enrollment and renewal through automation with iDRAC9 Automatic Certificate Enrollment is something they're sure to appreciate.

Remove iDRAC SSL certificate renewal from admins' task lists

Automated renewal with iDRAC9 v4.0 requires 0 steps and 0 time

after initial setup vs. manual renewal

Get time savings that scale with your environment

Save 45 work days with a 3-month renewal period

Save 22.5 work days with a 6-month renewal period

for 1,000 servers over 3 years using iDRAC9 vs. manual renewal

Eliminate the need to schedule, track, and maintain iDRAC SSL certificate renewals with a new feature in iDRAC9 v4.0 February 2020

The science behind the report:

Eliminate the need to schedule, track, and maintain iDRAC SSL certificate renewals with a new feature in iDRAC9 v4.0

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report Eliminate the need to schedule,track, and maintain iDRAC SSL certificate renewals with a new feature in iDRAC9 v4.0.

We concluded our hands-on testing on December 6, 2019. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on November 18, 2019 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

In this study, we compared two ways of keeping track of SSL certificates in Dell iDRAC9 v4.0: manually obtaining and renewing certificates vs. using automation to renew certificates before expiration. The table below shows the time and steps required for our data center expert to obtain a certificate for a single server.

Time to obtain and renew an SSL certificate on a single server

	Time required	Steps required
Manual process		
Obtaining a certificate	1 minute, 48 seconds	11
Renewing a certificate	1 minute, 48 seconds	11
iDRAC9 v4.0 automation		
Setting up the environment	14 minutes, 47 seconds	62
Enabling Automatic Certificate Enrollment	1 minute, 15 seconds	5
Renewing a certificate	0 minutes, 0 seconds	0

Note that setting up the environment for automation is a one-time task that applies to a whole data center, while automation enrollment happens once per server. After these setup tasks, an administrator would never have to lift another finger to renew certificates. By contrast, manually renewing SSL certificates requires an administrator to repeat the process each time.

We used the data above to estimate the time it would take to renew SSL certificates for 1,000 servers over three years. We show the results of these calculations below.

Time required to renew SSL certificates for 1,000 servers over 3 years (extrapolated)

Renewal period	Total number of renewals	Time to manually renew all certificates	Time to complete automatic renewals
3 months	12,000	360 hours	0 hours
6 months	6,000	180 hours	0 hours
12 months	3,000	90 hours	0 hours

To better contextualize the burden of manual renewals, we used the data above to calculate the number of work days an administrator would spend tending to SSL certificates. Our calculations assume the administrator works 8 hours each day with no breaks.

Work days required to manually renew SSL certificates for 1,000 servers over 3 years (extrapolated)

Renewal period	Time to complete renewals manually
3 months	45 work days
6 months	22.5 work days
12 months	11.25 work days

We also calculated the number of steps it would take to renew certificates for 1,000 servers. We present that data below.

Steps required to manually renew SSL certificates for 1,000 servers over 3 years

Renewal time period	Total number of renewals	Total steps for manual renewals	Total steps for automatic renewals
3 months	12,000	132,000	0
6 months	6,000	66,000	0
12 months	3,000	33,000	0

System configuration information

The table below presents detailed information on the system we tested.

Server configuration information	Dell EMC™ PowerEdge™ R640
BIOS name and version	Dell 2.3.10
Non-default BIOS settings	N/A
Operating system name and version/build number	N/A
Date of last OS updates/patches applied	November 22, 2019
Power management policy	Default
Processor	
Number of processors	2
Vendor and model	Intel® Xeon® Silver 4114
Core count (per processor)	10
Core frequency (GHz)	2.20
Stepping	U0
Memory module(s)	
Total memory in system (GB)	64
Number of memory modules	4
Vendor and model	Hynix® HMA82GR7CJR8N-VK
Size (GB)	16
Type	DDR4
Speed (MHz)	2,400
Speed running in the server (MHz)	2,400
Storage controller	
Vendor and model	Dell PERC H740P Mini
Cache size (GB)	2
Firmware version	50.5.1.-2818
Local storage	
Number of drives	2
Drive vendor and model	Dell AL15SEB060NY (KIOXIA)
Drive size (GB)	600
Drive information (speed, interface, type)	10k SAS 12.0 HDD
Network adapter	
Vendor and model	Broadcom® Adv Dual 10GBASE-T Ethernet
Number and type of ports	4 x 10GbE
Firmware version	21.40.25.31

Server configuration information	Dell EMC™ PowerEdge™ R640
Cooling fans	
Vendor and model	Nidec® UltraFlo 4VXP3-X30
Number of cooling fans	8
Power supplies	
Vendor and model	Dell 0PJMDNA01
Number of power supplies	2
Wattage of each (W)	750

How we tested

Managing certificates with iDRAC9

The following methodology provides the steps required to enable and execute automatic certificate enrollment on the latest Dell EMC PowerEdge servers with iDRAC9 version 4.00.00.00. We compare the time it takes to complete the same certificate enrollment process manually.

Both methods require domain services, which we provided using the following Windows Server 2019 virtual machines:

- An Active Directory server with DNS and DHCP
- A routing server using network address translation
- An Enterprise Root Certificate Authority server with the Certificate Authority Web Enrollment feature installed and configured

This methodology does not include the steps required to set up the infrastructure.

An overview of the manual method

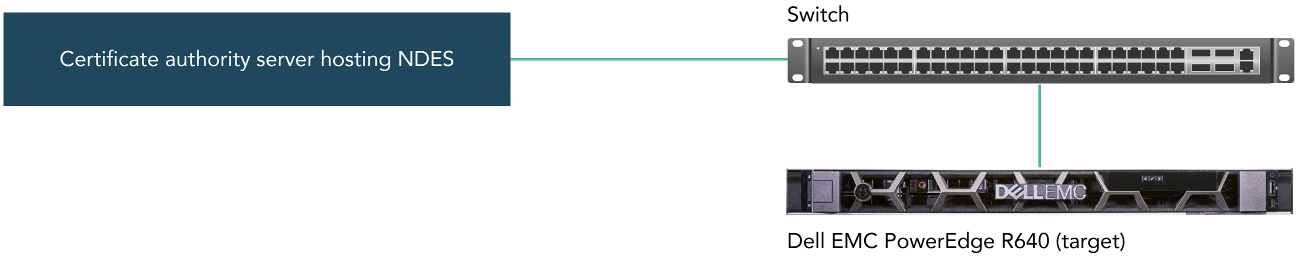
Manually managing certificates with iDRAC9 begins by logging into iDRAC and downloading a certificate request. Next, browse to the web enrollment website hosted by the certificate authority, request the certificate, and download the new certificate. Finally, return to the certificate authority and upload the certificate to the iDRAC system. Each time the certificate expires, you will need to repeat the process.

An overview of the Automatic Certificate Enrollment method

The Automatic Certificate Enrollment method requires additional environmental setup as well as setup on each target server. However, after enrolling the server, renewing a certificate after expiration will no longer require administrative effort.

To enable automated certificate enrollment, configure the Certificate Authority and deploy the Network Device Enrollment Service (NDES). Next, configure the NDES server as we describe below, and navigate to the mscep_admin web page to copy the challenge password. Finally, log into each server and provide the certificate details, the NDES web page, and the challenge password. After enrolling a server in Automatic Certificate Enrollment, iDRAC uses the saved challenge password to complete the initial certificate enrollment with the Certificate Authority. When the certificate is expiring the server will automatically renew the certificate. You will need to re-enroll a server if the challenge password changes.

In addition to the testing described below, we also repeated the same process, replacing the default web server certificate template with a duplicated web server template. We set the duplicate to expire in 5 hours, with a 2-hour renewal period. We then watched the server's logs to verify that iDRAC automatically acquired a new certificate each time the certificate expired.


Certificate authority server hosting NDES
Switch
Dell EMC PowerEdge R640 (target)

Manually renewing a single server's certificate

If you intend to manage certificates manually, you must follow these steps for every system you have.

1. Navigate to the iDRAC console.
2. Under iDRAC settings, click Services.
3. Under Web Server, click SSL Certificate.
4. Click generate CSR.
5. Using a plain-text editor of your choice, open the CSR, and copy the entire text.
6. Navigate to the certsrv on your certificate authority. We used http://ca.ptlabs01.local/certsrv.
7. If the system asks, enter your administrator account credentials.
8. On the Welcome screen, click Request a certificate.
9. Click Advanced certificate request.
10. Paste the CSR text into the Base-64-encoded certificate request form. For Certificate Template, select Web Server. Click Submit.
11. Select Base 64 encoded, and click Download certificate.
12. Return to the iDRAC console, and click Upload Signed Certificate.

Setting up the environment for automatic renewals

Before installing the Network Device Enrollment Service (NDES), we needed to configure a user account and give it the proper permissions. After installation, we set the Web Server template as the default template for publishing upon request, enabled large query strings, and configured NDES for single-password mode.

Adding the NDES service account

1. On the active directory server, open Active Directory Users and Computers.
2. Right-click Users, and click New. Select User.
3. Enter the information for the NDES service account. We used `certadmin`. Click Next.
4. Enter a password, select Password never expires, and click Next.
5. Click Finish.

Setting permissions for the NDES account

1. On the certificate authority server, from the Windows start menu, under administrative tools, launch the Certification Authority Console.
2. Right-click the server name, and click Properties.
3. Click the Security tab, and click Add.
4. Type the name of the NDES service account, and click OK.
5. Click the NDES service account. Check the boxes for Read, Issue and Manage Certificates, Manage CA, and Request Certificates. Click OK.

Setting Read and Enroll permissions on the Certificate Templates

1. In the certsrv window, right-click Certificate Templates, and select Manage.
2. Right-click Web Server template, and click Properties. Make the following changes:
   - Select Security, and click Add.
   - Enter the NDES service account information, and click OK.
   - Change the permissions for the NDES service account so that it has full control. Click OK.
3. Right-click CEP Encryption template, and click Properties. Make the following changes:
   - Select Security, and click Add.
   - Enter the NDES service account information, and click OK.
   - Change the permissions for the NDES service account so that it has full control. Click OK.
4. Right-click Exchange Enrollment Agent template (offline request), and click Properties. Make the following changes:
   - Select Security, and click Add.
   - Enter the NDES service account information, and click OK.
   - Change the permissions for the NDES service account so that it has full control. Click OK.

Setting local system permissions

1. From the start Window, type `lusrmgr.msc` and press Enter to run Local Users and Computers.
2. Under Groups, add the NDES service account and the domain administrator to the following groups:
   - Administrators
   - IIS_IUSRS

Adding a service principal name for the NDES service account

1. Open a PowerShell terminal using elevated privileges.
2. Run the following command:

```
setspn -s http/<computername> <domainname>\<accountname>
```

For example, we ran: `setspn -s http/ca01 ptlabs.local\certadmin`

Installing NDES

1. In Server Manager, click Add Roles and Features.
2. In the Roles and Features Wizard, on the Installation Type screen, click Next.
3. On the Server Selection screen, click Next.
4. In the Roles and Features Wizard, on the Server Roles screen, under ADCS, select Network Device Enrollment Service.
5. On the Features screen, click Next.
6. On the IIS screen, click Next.
7. On the Role Services screen, click Next.
8. On the Confirmation screen, click Install.

Configuring NDES

1. Once the installation is complete, in Server Manager, click the flag. On the destination server, click Configure Certification Authority Web Enrollment.
2. On the ADCS Configuration screen, check the Network Device Enrollment Service checkbox, and click Next.
3. On the Service Account for NDES screen, under Specify service account, click Select.
4. Enter the credentials for the NDES service account, and click OK.
5. Click Next.
6. For RA Information, enter your RA information, and click Next.
7. For Cryptography for NDES, leave the default key length of 2048, and click Next.
8. Click Configure.

After installing, IIS manager will also include mscep and mscep_admin web pages under CertSrv.

Configuring the default template

1. Under the start menu, to open the Registry Editor, type `regedit.exe`
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP.
3. Right-click the General Purpose Template, and select Modify.
4. Replace the value IPSECIntermediateOffline with `WebServer`
5. In the command prompt, run `iisreset`

Configuring IIS to Allow for Large Query Strings

1. Open an elevated command prompt.
2. Run the following command:

```
c:\windows\system32\inetsrv\appcmd.exe set config -section:system.webServer/security/requestFiltering
/requestLimits.maxQueryString:"3072" /commit:apphost
```

Configuring NDES for Single Password mode

1. From the Certificate Authority server, in the Windows Start Menu, type `regedit.exe` to open the Registry Editor.
2. Navigate to HKEY_LOCAL_MACHINE\Microsoft\Cryptography\MSCEP\UseSinglePassword.
3. Double-click UseSinglePassword.
4. Change the Value data to 1. Click OK.
5. Right-click MSCEP, and select Permissions.
6. Click the NDES account.
7. Select Full Control, and click OK.
8. In the Windows Start Menu, to open IIS Manager, type `IIS`
9. Under the server name, select Application Pools.
10. Click SCEP. In the sidebar, click Advanced Settings.
11. Under Process Model, for Load User Profile, select True. Click OK.
12. Right-click SCEP, and click Stop.
13. On a different system, using Remote Desktop and the NDES account, log into the Certificate Authority server.
14. In the Windows Start Menu, to open IIS Manager, type `IIS`
15. Under the server name, select Application Pools.
16. Right-click SCEP, and click Start.

Rebooting the server and copying the challenge password

1. From the start menu, select Reboot.
2. Log into the target server.
3. Browse to your certificate authority server at /certsrv/mscep_admin.
4. When prompted, enter your credentials.
5. Copy the enrollment challenge password.

Enabling Automatic Certificate Enrollment for the target system

To enable Automatic Certificate Enrollment, you must complete the steps below. After enrollment, you will not have to interact with the system to renew a certificate.

1. Navigate to the target IP address.
2. Log into the iDRAC console for the target server.
3. Navigate to iDRAC Settings→Services→Web Server→SSL Certificate, and enter your CSR details.
4. Check Automatic Certificate Enrollment, and enter the mscep location for certserv. We used `http://ca01.labspt.local/certsrv/mscep/`.
5. Paste the challenge password, and click Apply. To verify that the certificate shows as Enrolled, refresh the console.

Dell claims that the Automatic Certificate Enrollment can be scripted using RACADM. This could provide further time savings.

Read the report at http://facts.pt/nck7bzt ▶

This project was commissioned by Dell EMC.

DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:
Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.