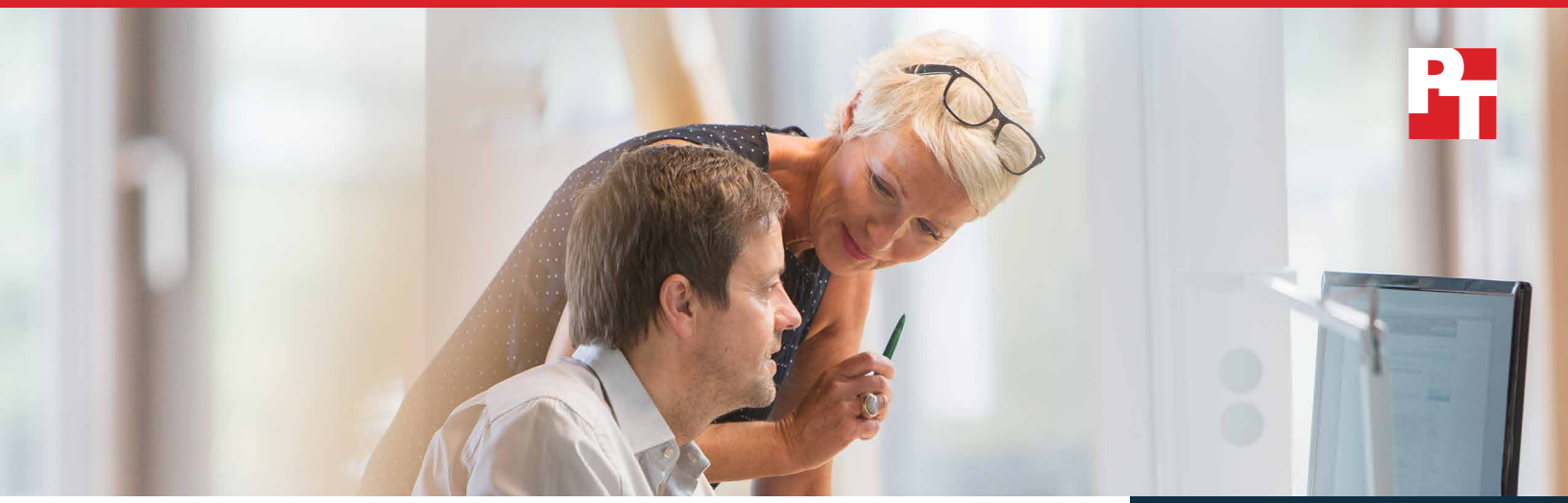


Eliminate the need to schedule, track, and maintain iDRAC SSL certificate renewals with a new feature in iDRAC9 v4.0

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

How iDRAC9 uses automation to make life easier for administrators

Embedded in the latest Dell EMC™ PowerEdge™ servers is iDRAC9. This embedded management controller makes it easier for administrators to deploy and update the PowerEdge servers in their data center through extensive system provisioning automation, and now also offers an option to automate SSL certificate enrollment and renewal for Datacenter license customers. New servers require enrollment with the certificate authority, which iDRAC9 automates with Automatic Certificate Enrollment after an initial one-time setup. In this study, we focus on time savings from certificate renewals.

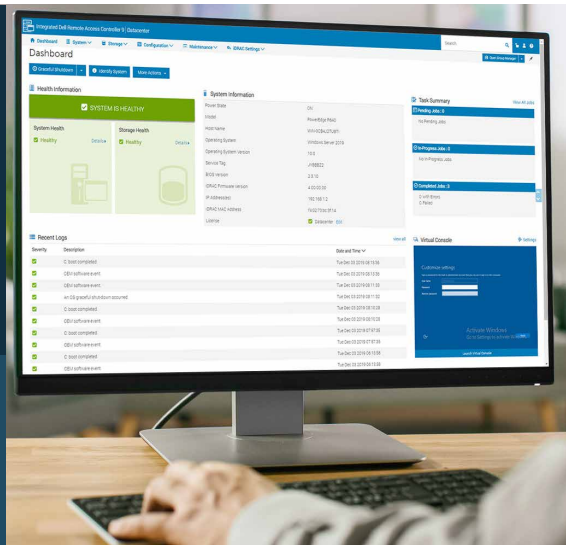
While SSL certificates used to have lengthy validity periods—some as much as five years or more—current industry standards set the limit at 27 months to ensure that security measures are up to date.[1] Many organizations choose to set the validity period to one year, while others with stringent security level agreements may update their SSL certificates twice a year, quarterly, or even more frequently. All these factors affect how beneficial iDRAC SSL certificate renewal automation will be to your specific organization.

Using a Dell EMC PowerEdge R640 server, we tested the iDRAC9 v4.0 SSL certificate renewal automation feature to see how much time and effort Automatic Certificate Enrollment could save compared to doing the same task manually. To learn the step-by-step details of our testing, see the science behind the report.

About Dell EMC PowerEdge servers

Dell Technologies offers a wide-ranging portfolio of servers to meet a variety of business needs. From scalable rack servers to modular infrastructure solutions and more, Dell Technologies embeds iDRAC9 v4.0 in PowerEdge servers to offer management functionality out of the box with no need for additional hardware.

To learn more about Dell EMC PowerEdge servers, visit https://www.delltechnologies.com/en-us/servers/index.htm.



Removing the annoyance of SSL authentication renewal notices

Before iDRAC9 v4.0, keeping track of iDRAC SSL certificates required administrative overhead such as maintaining spreadsheets, setting reminders, or regularly checking the certificate authority. Once a server's certificate was up for renewal, admins would still have to manually upload each one. Depending on the number of servers in your data center, the number of data centers your company has, and the validity period of your iDRAC SSL certificates, this could be a frequent annoyance to say the least.

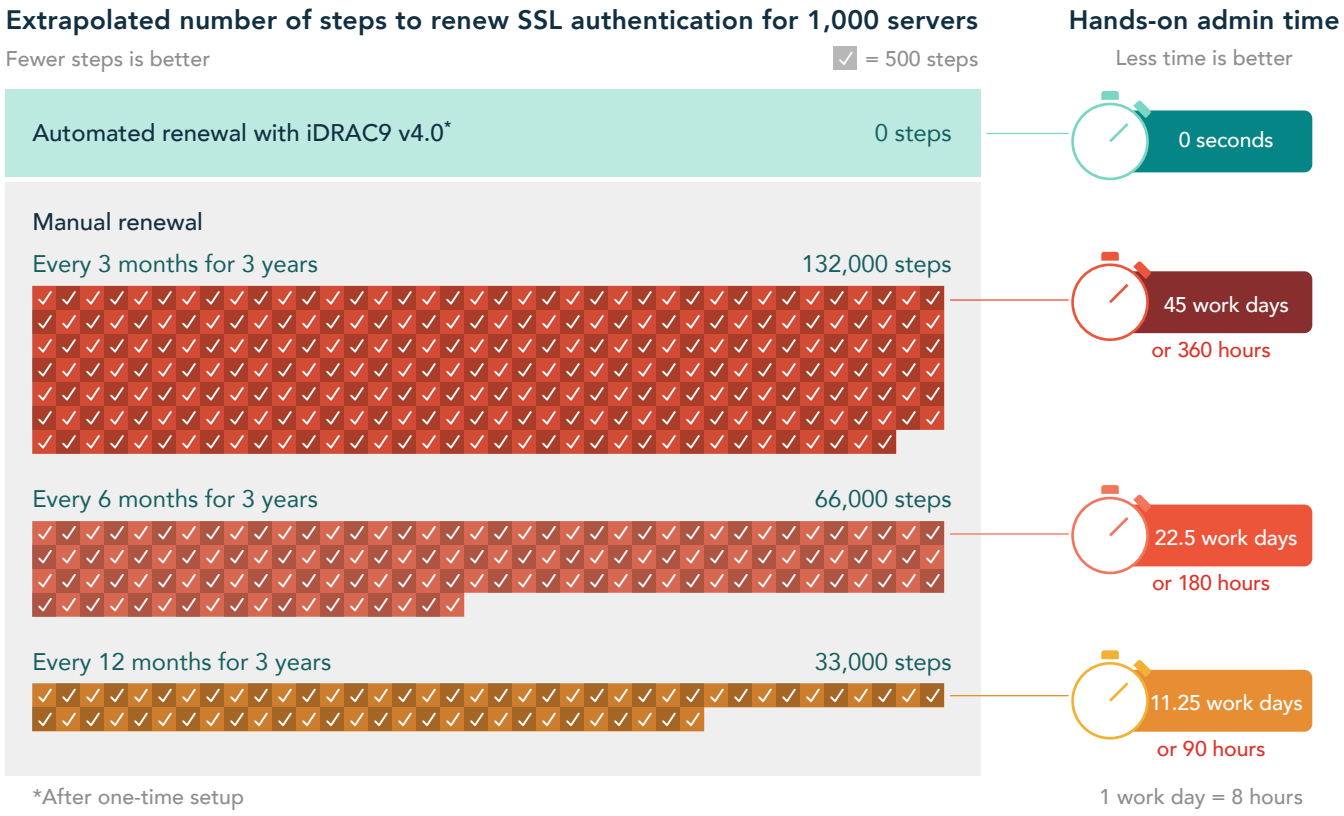
iDRAC9 v4.0 automates the enrollment and renewal process so admins can maintain all of your company's SLA security requirements without wasting time tracking certificates.

Comparing manual and automatic renewals with iDRAC9

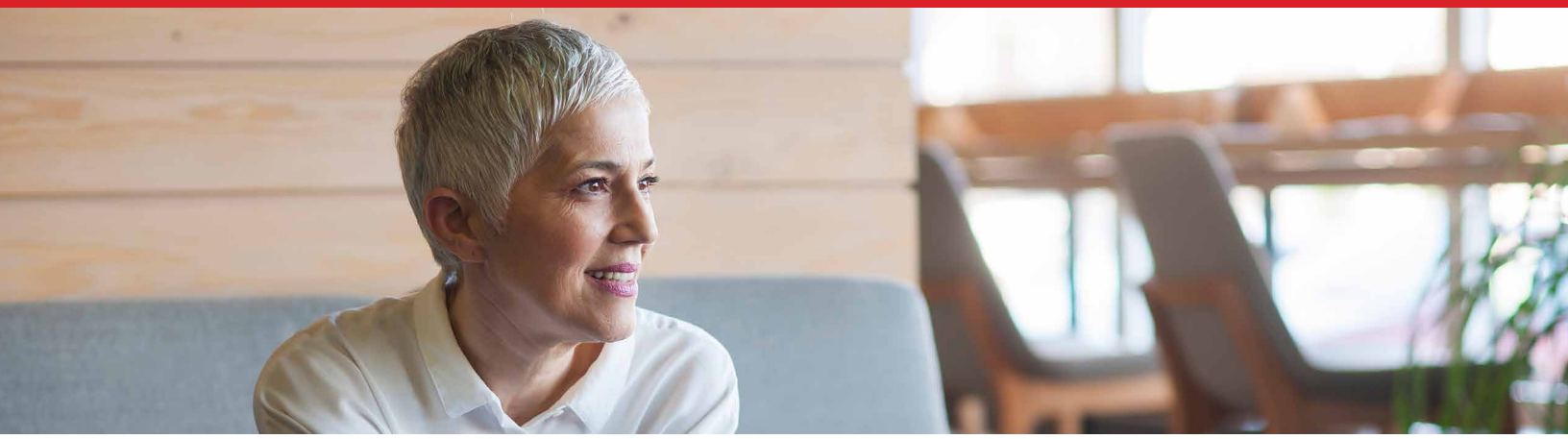
Getting iDRAC9 to automatically renew certificates required a couple of one-time setup processes: Setting up our environment for automatic renewals took 14 minutes and 47 seconds across 62 steps, while enabling Automatic Certificate Enrollment on a single server took 1 minute and 15 seconds across 5 steps. After this initial setup, however, an administrator wouldn't need to do any work at all to keep certificates up to date in iDRAC9, no matter how often your company requires new certificates or how many servers need them.

By contrast, manually obtaining an SSL certificate took 1 minute and 48 seconds over 11 steps for one server. It doesn't stop there, however—administrators would need to repeat these steps for each server, and repeat them again each time certificates require renewal. The ongoing time commitment inherent in manual certificate renewal can present a tedious annoyance to admins with more urgent business initiatives to attend to.

The size of the hassle grows with the size of your server infrastructure and the frequency of your renewals. By extrapolating the data we collected on a single server, we can see just how much time and effort your company can save with more servers:



Say your organization needs to renew SSL certificates for 1,000 servers every three months. Over three years, an admin at your company would spend 45 work days just renewing certificates. By enrolling your servers in automatic renewal, that administrator would save valuable time and avoid wasting effort on the 132,000 steps it would take to manually renew certificates—effort they could instead use for other high-value tasks. (Note that your results will vary based on the number of servers you have.)



The qualitative benefits of SSL certificate renewal automation with iDRAC9

Concrete time and steps savings that free up administrators' workdays are valuable. But what are some of the other benefits of SSL certificate renewal that you can't find in those numbers?

Automating SSL certificate renewal means that you can renew more often.

Why do organizations choose lengthy validity periods for SSL certificates? In many cases, it's because they don't perceive the benefits of more frequent renewals as worth the hassle. But there's something to be said for renewing SSL certificates more often: shorter validity periods mean that your servers benefit from the latest security practices, offering peace of mind for you and your company's IT staff. For organizations that have strict SLAs requiring shorter validity periods, automation with iDRAC9 can help you meet those targets more easily.

Alleviate time and effort spent tracking and planning renewals.

Servers don't all appear in a data center at once, but arrive as business needs expand. This presents a challenge when it comes to tasks like SSL certificate enrollment and renewals: Servers will be up for renewals at different times, and servers with different workloads may have SSL certificates with different validity periods to meet SLAs. The bottom line? Someone has to keep track of all this so certificates don't expire and dissuade customers from making purchases due to security concerns. After you use iDRAC9 to set up a new server in your data center, you'll never have to touch it for SSL certificate renewal again.

Reduce the risk of server vulnerability.

Certificates help prevent malicious actors from making unauthorized changes to your servers and compromising your company's data—that's why it's so important to keep SSL certificates up to date. By relying on a manual process to renew SSL certificates, your company risks a lapse in authentication that can pave the way for a cybersecurity breach.

Allowing iDRAC9 v4.0 to track and automate this procedure reduces the risk of server vulnerabilities, adding another layer of confidence in your company's security.

Conclusion

If your administrators painstakingly monitor and renew iDRAC SSL certificates for the latest Dell EMC PowerEdge servers with Datacenter licenses, there's now an easier way. After a one-time setup process, using iDRAC9 Automatic Certificate Enrollment to automate SSL certificate renewal saved valuable hands-on time that could add up for organizations with large infrastructures and could save hands-on time as you add servers and enroll them with the certificate authority. Based on our tests, we estimate that using iDRAC9 v4.0 to renew certificates for 1,000 servers every three months would save an administrator up to 45 work days over three years. The qualitative benefits of automating SSL certificate renewal are perhaps just as impressive: organizations could renew more often for increased security, remove the time and effort associated with renewal processes, and even reduce server vulnerability resulting from lapsed certificates.

1 Vincent Lynch, "3-Year Certificates to be Eliminated in Industry-Wide Change," accessed December 16, 2019, https://www.digicert.com/blog/3-year-certificates-eliminated-industry-wide-change/.

Read the science behind this report at http://facts.pt/odgevsp ►

Principled Technologies®

Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.
For additional information, review the science behind this report.

This project was commissioned by Dell EMC.