**Technical Guide: iDRAC SSL Certificate Management Scripts**

**Introduction**

This document provides a step-by-step guide on how to use two PowerShell scripts for managing SSL certificates on iDRAC interfaces:

1. **CSR Generation Script** – Generates Certificate Signing Requests (CSRs) for iDRAC devices.
2. **Certificate Upload Script** – Uploads SSL certificates to iDRAC devices.

Both scripts follow best practices, including **secure credential handling**, **error logging**, and **color-coded summaries** for clear execution results.

**References**

1. Dell iDrac GitHub: [**https://github.com/dell/iDRAC-Redfish-Scripting/tree/master**](https://github.com/dell/iDRAC-Redfish-Scripting/tree/master)
2. Dell iDrac PowerShell Gallery: <https://www.powershellgallery.com/packages/IdracRedfishSupport/23.0.0.0>
   1. At the time of this writing, 3/25/2025, The latest module has not been uploaded: "**24.0.0."**
   2. Until the 24.0.0 module is available on the PowerShell Gallery, install the module via cmd line from Posh 7. Download the PowerShell module from the below link. Find the currently installed module directory. Copy the iDracRedfishSupport.psd1 and psm1 files into the existing folder, overwrite if prompted. Change the folder name from 23.0.0 to 24.0.0.
   3. <https://github.com/dell/iDRAC-Redfish-Scripting/tree/master/Redfish%20PowerShell/IdracRedfishSupport>

**Prerequisites**

Before running the scripts, ensure the following requirements are met:

* **Windows System** with PowerShell 7 installed.
* **Administrator Privileges** on the system.
* **iDRAC Credentials** with sufficient permissions to generate CSRs and upload SSL certificates. Local or Domain
* **CSV File** containing the target iDRAC devices.
* **OpenSSL or CA Authority** for signing the CSRs.
* **SSL Certificates (.pem format)** for the upload script.
* **Network Connectivity** to target iDRAC devices.

**1. CSR Generation Script**

**Purpose:**

This script generates Certificate Signing Requests (CSRs) for multiple iDRAC devices listed in a CSV file. Because of how the CSR gets verified with the certificate upload, the CSR information must match what is in the iDrac Gui. See the iDrac Gui Location section below

**CSV File Format:**

The CSV file must contain the following columns:

fqdn,ip  
idrac1.example.com,192.168.1.5

idrac2.example.com,192.168.1.6

**Execution Steps:**

1. Open the script in Visual Studio Code "GenerateiDracCSRS.ps1" and verify the Certificate Variables value are correct.
2. A file explorer window will appear. Select the CSV file containing iDRAC targets.
3. The script will:
   1. Verify each iDRAC is reachable.
   2. Ensure DNS resolution matches the provided IP.
   3. Generate a CSR for each device.
4. CSRs will be saved in the same directory as the CSV file.

**iDrac Gui Location:**

1. To find the changes that are made for this script, login to the iDrac and go to iDrac Settings->Services->Web Server->SSL/TLS Certificate Signing Request.

**Output Summary:**

At the end of execution, a summary table will display the results:

===== CSR Generation Summary =====  
idrac1.example.com Success - CSR generated (GREEN)  
idrac2.example.com Failed - Host unreachable (RED)  
==================================

A screen shot of a computer

AI-generated content may be incorrect.

**Post-Execution:**

* Submit the generated CSRs to a Certificate Authority (CA) for signing.
* Download the signed certificates (.pem format) for use in the next script.

**2. SSL Certificate Upload Script**

**Purpose:**

This script uploads SSL certificates to multiple iDRAC devices and restarts their services to apply changes.

**CSV File Format:**

The script uses the same CSV format as the CSR generation script.

**Execution Steps:**

1. Place the **signed SSL certificates (.pem format)** in the same directory as the CSV file.
2. Run the script in PowerShell 7 or preferably in Visual Studio Code:  
   .\UploadiDracCers.ps1
3. Select the CSV file when prompted.
4. The script will:
   * Verify that a corresponding **.pem certificate file** exists for each iDRAC.
   * Check iDRAC reachability and DNS resolution.
   * Upload the certificate and restart iDRAC.

**Output Summary:**

After execution, a color-coded summary displays the upload status:

===== Certificate Upload Summary =====  
idrac1.example.com Success - Certificate uploaded (GREEN)  
idrac2.example.com Failed - PEM file missing (RED)  
=======================================

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

**Troubleshooting**

**Common Errors & Resolutions:**

|  |  |  |
| --- | --- | --- |
| **Error Message** | **Possible Cause** | **Resolution** |
| No valid file selected. Exiting script. | No CSV file was selected. | Rerun the script and select a valid CSV file. |
| ERROR: Host could not be reached. | The iDRAC device is offline or inaccessible. | Check network connectivity and firewall rules. |
| ERROR: DNS mismatch. | The resolved IP does not match the provided IP. | Verify DNS records and ensure correct IP is used. |
| ERROR: PEM file not found. | The certificate file is missing. | Ensure the signed certificate is in the correct folder. |
| ERROR: Upload failed. | iDRAC rejected the certificate. | Check the certificate format and reattempt the upload. |

**Conclusion**

By following this guide, administrators can efficiently **generate, sign, and upload SSL certificates** to iDRAC devices. The scripts provide **secure credential handling, automation, and clear summaries**, making SSL certificate management more streamlined and error-resistant.