

# Deny Access to Always On VPN Device Tunnels

---

If a managed device is lost or stolen or an endpoint is compromised by malware or ransomware, preventing corporate network access over the Always On VPN device tunnel will be necessary. In this scenario, administrators must perform a series of steps to revoke the endpoint's device certificate, publish a new Certificate Revocation List (CRL), and terminate any currently active device tunnel connections.

## Prerequisites

Not all versions of Windows Server support revocation checks for device certificates. Routing and Remote Access Service (RRAS) must be installed on one of the following versions to support device certificate revocation checks.

- Windows Server 2022
- Windows Server 2019 build 17763.652 and later
- Windows Server 2016 build 14393.3053 and later

Windows Server 2012/R2 is not supported.

In addition, administrators must proactively enable device certificate revocation checking on enterprise VPN servers by setting a registry key. To do this, open an elevated PowerShell window and run the following command.

```
New-ItemProperty -Path  
'HKLM:\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\Ikev2\' -Name  
CertAuthFlags -PropertyType DWORD -Value '4' -Force
```

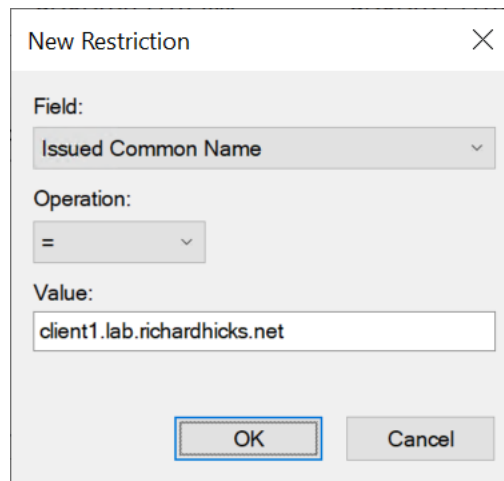
Once complete, restart the RemoteAccess service by running the following command.

```
Restart-Service RemoteAccess -PassThru
```

## Revoke Certificate

Revoking the endpoint's device certificate is the first step to denying Always On VPN device tunnel access. To do this, open the Certification Authority (CA) management console (certsrv.msc) on an issuing CA or a management workstation with the Remote Server Administration Tools (RSAT) installed and perform the following steps.

1. In the navigation tree, expand the CA.
2. Right-click **Issued Certificates** and choose **View > Filter**.
3. Click **Add**.
4. Select **Issued Common Name** from the **Field** drop-down list.
5. Select '=' from the **Operation** drop-down list.
6. Enter the endpoint's fully qualified domain name (FQDN) in the **Value** field.
7. Click **OK**.

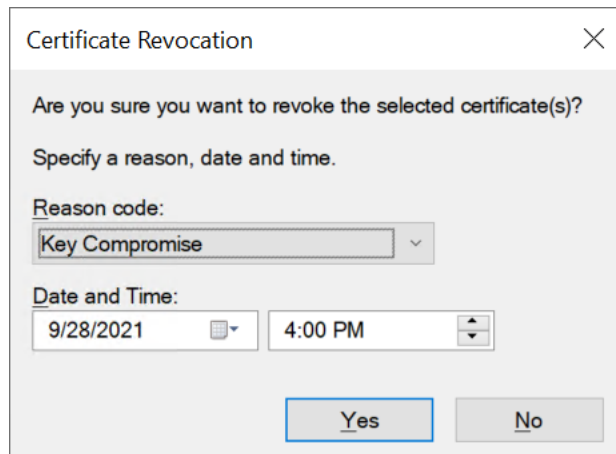


A dialog box titled "New Restriction" with a close button (X) in the top right corner. It contains three sections: "Field:" with a dropdown menu showing "Issued Common Name"; "Operation:" with a dropdown menu showing "="; and "Value:" with a text input field containing "client1.lab.richardhicks.net". At the bottom are "OK" and "Cancel" buttons, with the "OK" button highlighted by a blue border.

8. Click **OK**.

If there is more than one certificate, click twice on the **Request ID** column heading to sort the list, then perform the following steps on the most recently issued certificate.

1. Right-click the certificate and choose **All Tasks > Revoke Certificate**.
2. Select a value from the **Reason code** drop-down list.
3. Click **Yes** to revoke the certificate.



A dialog box titled "Certificate Revocation" with a close button (X) in the top right corner. It contains the following text: "Are you sure you want to revoke the selected certificate(s)?" and "Specify a reason, date and time." Below this are three sections: "Reason code:" with a dropdown menu showing "Key Compromise"; "Date and Time:" with two input fields, the first showing "9/28/2021" and the second showing "4:00 PM"; and "Yes" and "No" buttons at the bottom, with the "Yes" button highlighted by a blue border.

---

*Note: Administrators can select **Certificate Hold** from the **Reason Code** drop-down list if the endpoint is temporarily lost. If found later, the certificate can be unrevoked.*

---

Repeat these steps for all valid certificates issued to the endpoint. If there is more than one issuing CA in the organization, repeat the steps above on each issuing CA to ensure revocation of all certificates issued to the device.

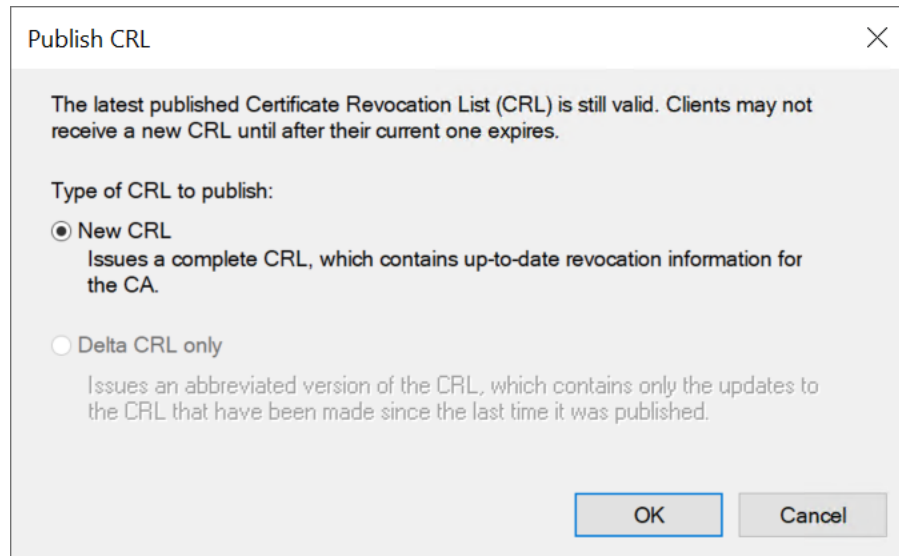
Once complete, perform the following steps to remove the display filter.

1. Right-click **Issued Certificates** and choose **View > Filter**.
2. Click **Remove All**.
3. Click **OK**.

## Issue CRL

After revoking all device certificates for the endpoint, issue a new CRL by performing the following steps.

1. Right-click **Revoked Certificates** and choose **All Tasks > Publish**.
2. Select **New CRL**.
3. Click **OK**.



## Clear CRL Cache

CRLs are cached in memory and on disk by VPN servers performing device certificate authentication. To clear the certificate revocation cache, open an elevated command window and run the following commands. Be sure to run these commands on all enterprise VPN servers.

```
certutil.exe -urlcache * delete
certutil.exe -setreg chain\ChainCacheResyncFiletime @now
```

## Limitations

Revoking a certificate and clearing CRL caches often works unreliably. When using Online Certificate Status Protocol (OCSP) servers, clearing the disk and memory cache on the OCSP server may not be immediately effective. In this case, clearing the CRL caches does not affect cached signed OCSP responses. If the organization uses OCSP, consider adding the endpoint's device certificate to the Untrusted Certificates certificate store on all enterprise VPN servers.

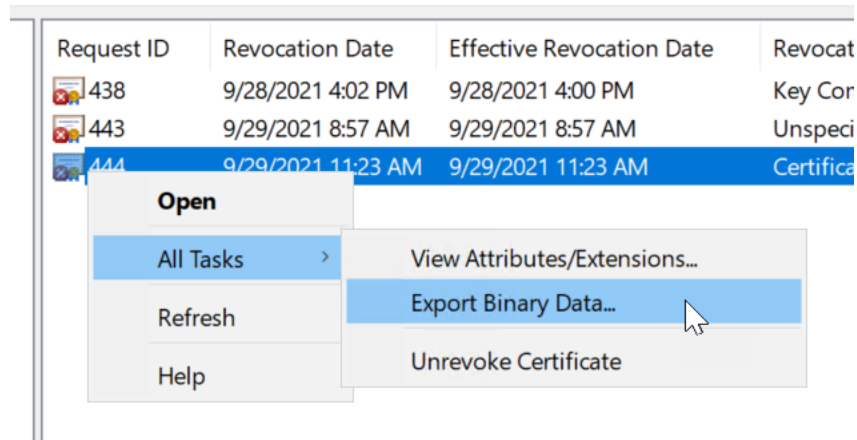
## Untrusted Certificates

To work around the limitations of CRL caching, administrators can place the endpoint's device certificate in the Untrusted Certificates certificate store on all enterprise VPN servers to immediately block Always On VPN device tunnel connections.

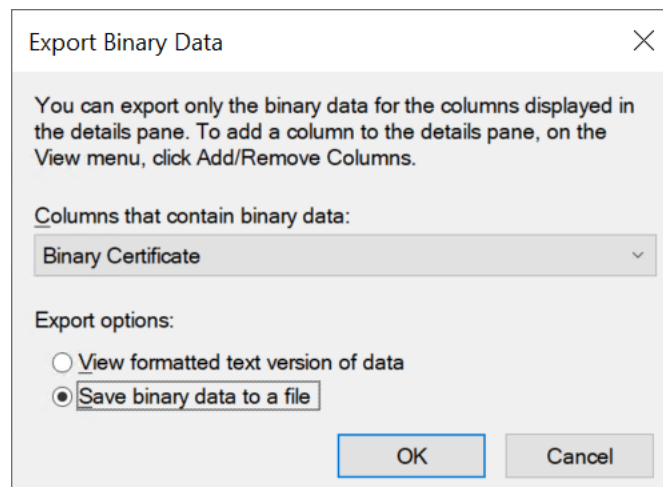
## Export Certificate

Perform the following steps on an issuing CA to export the endpoint's device certificate.

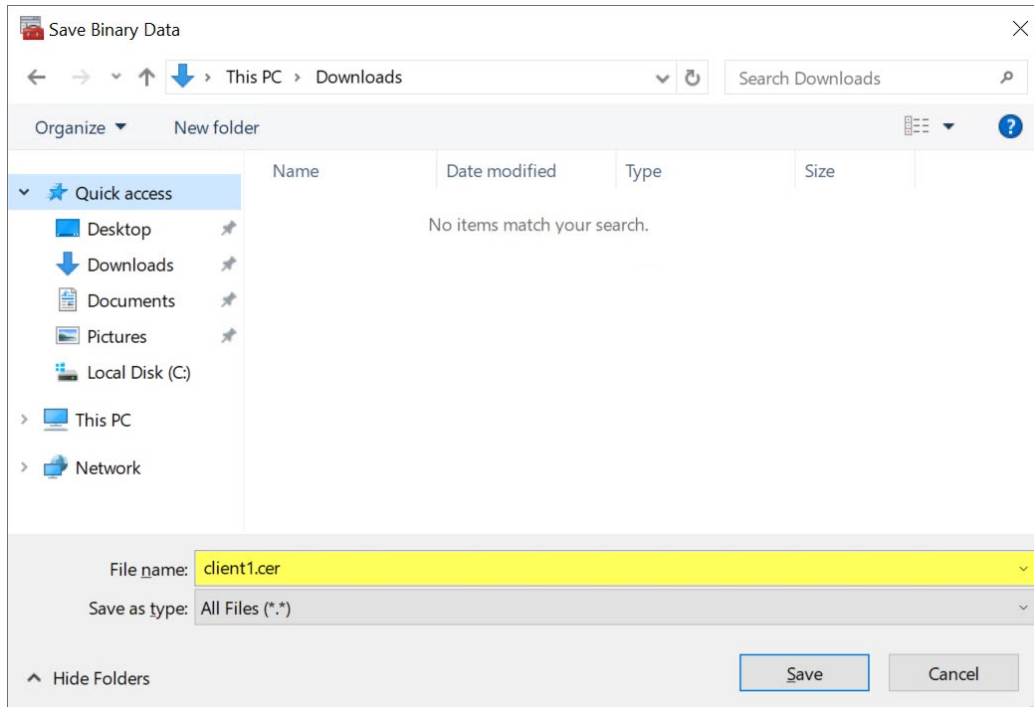
1. Locate the endpoint's device certificate using the guidance outlined previously.
2. Right-click the certificate and choose **All Tasks > Export Binary Data**.



3. Select **Binary Certificate** from the **Columns that contain binary data** drop-down list.
4. Select **Save binary data to a file**.
5. Click **OK**.



6. Enter a name for the certificate in the **File name** field. Include the .cer file extension.



7. Revoke the certificate as outlined previously.

### *Import Certificate*

Perform the following steps on all enterprise VPN servers to import the endpoint's device certificate into the Untrusted Certificates certificate store.

1. Open the Local Computer Certificates management console (certlm.msc).
2. Right-click **Untrusted Certificates** and choose **All Tasks > Import**.
3. Click **Next**.
4. Enter the path to the exported certificate.
5. Click **Next**.
6. Click **Next**.
7. Click **Finish**.

---

*Note: Be sure to repeat this process on all enterprise VPN servers!*

---

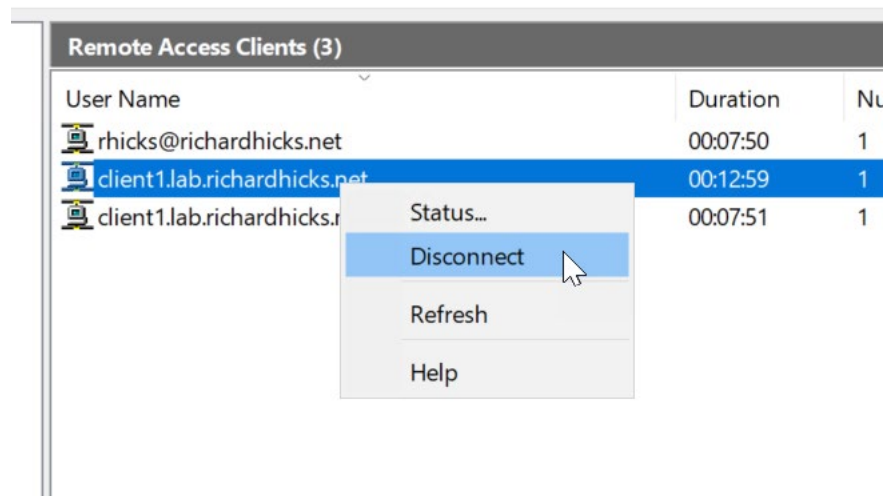
To import the certificate on Windows Server Core servers, open an elevated PowerShell window and run the following command.

```
Import-Certificate -FilePath <path to certificate file> -CertStoreLocation  
Cert:\LocalMachine\Disallowed
```

## Terminate Active Sessions

Administrators will need to terminate any active Always On VPN device tunnel sessions after revoking their device certificate. To do this, open the RRAS management console (rrasmgmt.msc) and perform the following steps.

1. Expand the VPN server and highlight **Remote Access Clients**.
2. Right-click the device connection and choose **Disconnect**.



To terminate active Always On VPN device tunnel sessions on Windows Server Core servers, open an elevated PowerShell window and run the following command.

```
Get-RemoteAccessConnectionStatistics | Where-Object UserName -eq <endpoint fqdn> | Disconnect-VpnUser
```

## More Information

Version: 1.0  
Creation Date: September 29, 2021  
Last Update: September 29, 2021  
Author: Richard Hicks  
Organization: Richard M. Hicks Consulting, Inc.  
Contact: [rich@richardhicks.com](mailto:rich@richardhicks.com)  
Web Site: <https://directaccess.richardhicks.com/>