



**How to obtain certificates for
VPN connections (Site to Site,
GVC, L2TP)**

**KNOWLEDGE
DATABASE**

How to obtain certificates for VPN connections (Site to Site, GVC, L2TP)

Using digital certificates for authentication instead of preshared keys in VPNs is considered more secure. In SonicWall UTM devices, digital certificates are one way of authenticating two peer devices to establish an IPsec VPN tunnel. The other is IKE using preshared key. The KB article describes the method to configure WAN GroupVPN and Global VPN Clients (GVC) to use digital certificates for authentication before establishing an IPsec VPN tunnel.

Features of IKE Authentication with Certificates in SonicWall WAN GroupVPN and GVC.

- A digital certificate either obtained from a third party CA (like Verisign) or from a private CA (like Microsoft CA or OpenSSL) must be used for this configuration. Self-signed certificates are not supported.
- In the SonicWall, the administrator has the option to create a Certificate Signing Request (CSR) and get it signed by a CA or import a signed certificate in the PKCS#12 format (.pfx or .p12 extension). When importing a signed certificate into the GVC client, it must be in the PKCS#12 format (.pfx or .p12 extension).
- Both peers must trust the issuer of the certificate. In other words, the CA certificate of the user certificate must be imported into the SonicWall as well as the remote GVC client.
- If a certificate has already been imported into the SonicWall signed by a 3rd party CA (for example, Verisign), this can be selected in the WAN GroupVPN. The CA certificate must be imported into the GVC client.
- SonicWall supports digital certificates issued by different CAs to be imported into the SonicWall UTM device and the remote GVC client. SonicWall also supports forcing both peers to use certificates issued by the same CA.

RESOLUTION:

The certificate signing process described here is using a Windows Server 2008 CA. To configure a Microsoft CA to accept a Subject Alternative Name attribute from a certificate request, refer this Microsoft article: [How to configure a CA to accept a SAN attribute from a certificate request](#)

- **Create a Certificate Signing Request (CSR) in the SonicWall**
- **Get the CSR signed from the Windows Server Certificate Enrollment Web Services**
 - **Obtain a certificate to use in WAN GroupVPN configuration**
 - **Download the CA certificate for the signed certificate**
 - **Obtain a certificate for GVC clients.**

Create a Certificate Signing Request (CSR) in the SonicWall

Login to the SonicWall management GUI
 Navigate to the **System | Certificate** page.
 Click on **New Signing Request** to create a similar CSR as under
 Click on **Generate** to save.
 Refresh the page.
 Click on the download button to download the CSR.

Generate Certificate Signing Request

Certificate Alias:

Country:

State:

Locality, City, or County:

Company or Organization:

Department:

Group:

Team:

Common Name:

Subject Distinguished Name:

Subject Alternative Name (Optional):

Domain Name:

Subject Key Type:

Subject Key Size:

Ready

System /

Certificates

Certificates and Certificate Requests

View Style: All certificates Imported certificates and requests Built-in certificates Include expired built-in certificates

#	Certificate	Type	Validated	Expires	Details	Configure
<input type="checkbox"/>	1 WANGroupVPN	Pending request				
<input type="checkbox"/>	2 hal-2010-SERVER2KB-CA	CA certificate		Sep 5 18:44:33 2016 GMT		

WANGroupVPN.p10 - Notepad

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAuIDELMAkGA1UEBhMCU4xCZAJBgNVBAGTAKTBMQwwCgYDVQQH
EwNCTFIxOTALBgNVBAoTBFNOV0wxFzAVBgNVBAMTDnNvbmljbGF1LmV2Y2FsMIGF
MADGCSqGSIb3DQEBAQUAA4GNADCBiQKBggQD00Z0j1s6tcw9B4AggEitw+/Z7AptQ
XoAAkenaoA6qk2Lk3HtMXJF71I/x6MuxNEKk1h/+7vamhr+s7jdpV6+EsQj87ky8
6WaM8aP3Tsox19MeYI3DHqrGnE3csFQlIwrqgP1SPtCnwkL+itSMkMuNLcnTp2BH
2jM4QDqsK8VwbwIDAQABoCwwKgyJKoZIhvcNAQkOMR0wGzAZBgNVHREEjA0gg5z
b25pY2xhyf5sb2NhbDANBgkqhkiG9w0BAQ0FAA0BgQBfZhtCPiBcWYyUEGNxE3W
JvukmCMZdERp76a6iBHNvJzv9ZVw+q9MdeUMSjn1URUj9t78JEN6fxyoDL7uDsNe
8YIxpnz4CbfgaPR76HPyER2pg+ITUAJCGx4xBC5n03r1lzYhN5Jal+lR+84QD6n
5mzZCtDbuLy2lo9Z310J4w=====END CERTIFICATE REQUEST-----

```

Obtain a certificate using the Windows Server Certificate Enrollment Web Services

Obtain a certificate to use in WAN GroupVPN configuration

Open a browser and navigate to the Microsoft Windows Certificate Enrollment page: <http://CertSrv>
When prompted for authentication, enter username and password of Administrator.

Click on **Request a certificate**

Click on **advanced certificate request**.

Copy the contents of CSR in the Saved Request box.

Select Administrator under Certificate Template. Note: **User** or **Web Server** template also could be selected.

Under Attributes, either enter **san:dns=yourdomainname.com** or **san:email=<local-part@domain.com>**. Note: To configure a Microsoft CA to accept a Subject Alternative Name attribute from a certificate request, refer this Microsoft article: [How to configure a CA to accept a SAN attribute from a certificate request](#)

Click on Submit and you will taken to the next page.

On this page click on **Download certificate** or **Download certificate chain** to save the signed certificate to disk.

Microsoft Active Directory Certificate Services - hal-2010-SERVER2k8-CA [Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#) ←
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Microsoft Active Directory Certificate Services - hal-2010-SERVER2k8-CA [Home](#)

Request a Certificate

Select the certificate type:

- [User Certificate](#)

Or, submit an [advanced certificate request](#) ←

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAuUDELMAkGA1UEBhMCU4xCzAJ
EwNCTFExDTALBgNVBAoTBFNOU0wxFzAVBgNVBART
MAOGCSqGSIb3DQEBAQUAA4GNADCBiQRBgQD00ZQj
XoAAkema0A6qk2LkHtMKJF711/x6MuxNEKK1h/+
6VaM9aP3Tsox19MeYI3DHqrGnE3cafQ1IvrqgP1S
-----
```

Certificate Template:

Administrator

Additional Attributes:

Attributes: san:dns=hal-2010.local

Submit >

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAuUDELMAkGA1UEBhMCU4xCzAJ
EwNCTFExDTALBgNVBAoTBFNOU0wxFzAVBgNVBART
MAOGCSqGSIb3DQEBAQUAA4GNADCBiQRBgQD00ZQj
XoAAkema0A6qk2LkHtMKJF711/x6MuxNEKK1h/+
6VaM9aP3Tsox19MeYI3DHqrGnE3cafQ1IvrqgP1S
-----
```

Certificate Template:

Administrator

Additional Attributes:

Attributes: san:email=Admin@hal-2010.local


Submit >

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA

Certificate Issued

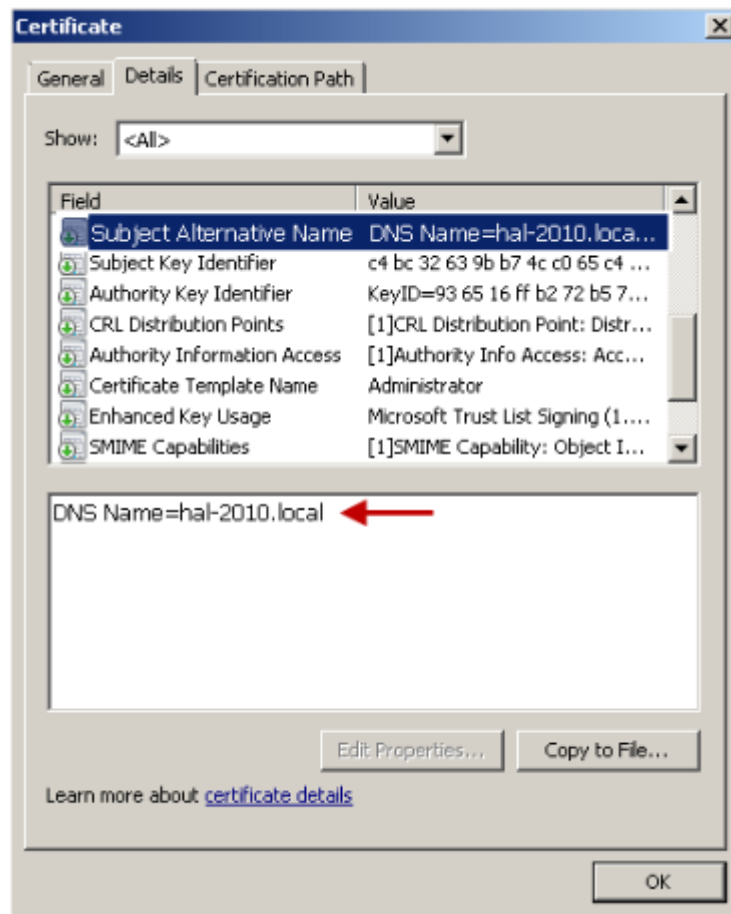
The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#)

[Download certificate chain](#)

Below is an example of a signed certificate's Subject Alternative Name (SAN):



Download the CA certificate for the signed certificate.

Navigate to the Microsoft Windows Certificate Enrollment page: <http://CertSrv>

Click on **Download a CA certificate....**

On the next page, click on **Download CA certificate** and save the certificate to disk.

Microsoft Active Directory Certificate Services – hal-2010-SERVER2K8-CA [Home](#)

Welcome

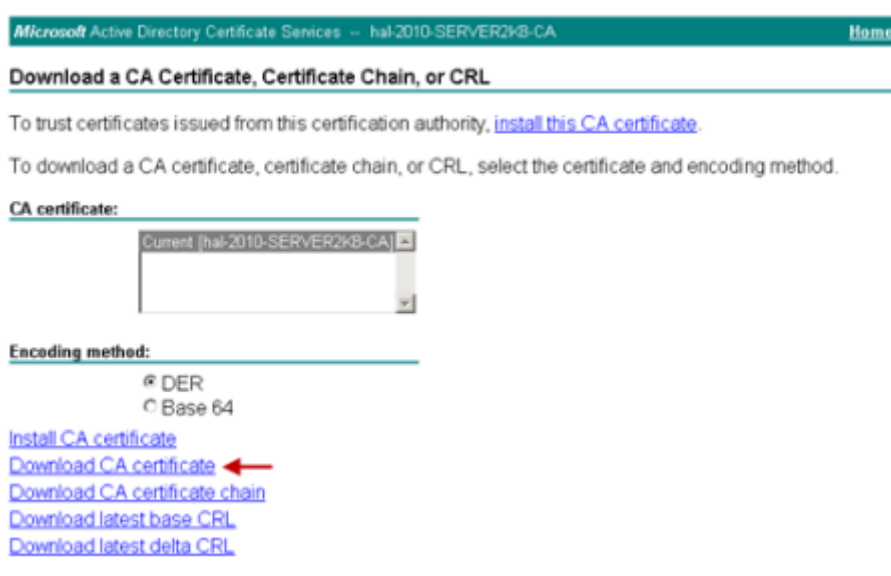
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

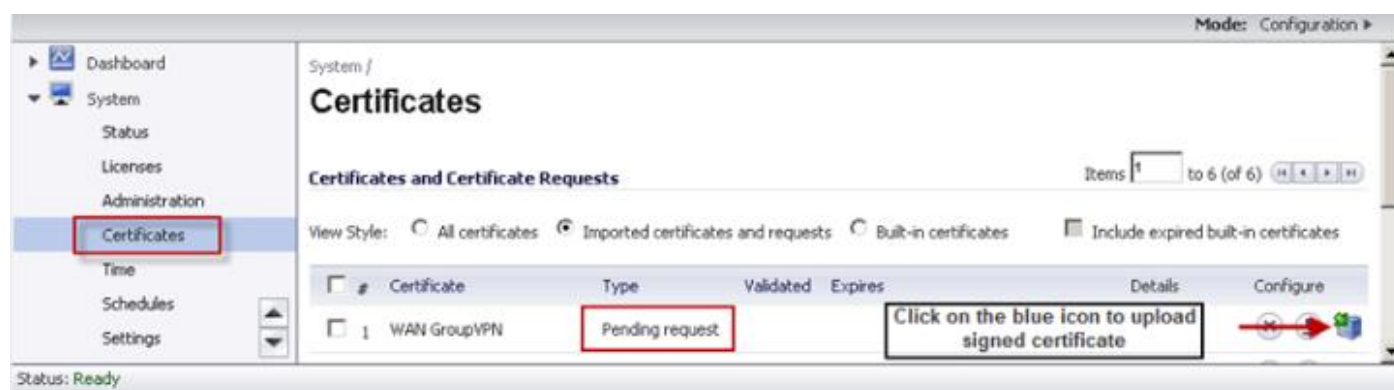
For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#) ←



Upload the signed certificate into the SonicWall via the upload button of the CSR pending request.



To establish trust and complete the validation of the signed certificate, import the CA certificate

System /
Certificates

Certificates and Certificate Requests Items 1 to 1 (of 1)

View Style: All certificates Imported certificates and requests Built-in Include expired built-in certificates

<input type="checkbox"/>	#	Certificate	Type	Validated	Expires	Details	Configure
<input type="checkbox"/>	1	WAN GroupVPN	Local certificate	No	Oct 11 10:25:12 2013 GMT		

Import... New Signing Request... SCEP... Delete Delete All

Status: The configuration has been updated.

Import Certificate

Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file

Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file

Please select a file to import: Choose File certnew (1).cer

Ready

Import Cancel

System /
Certificates

Certificates and Certificate Requests Items 1 to 2 (of 2)

View Style: All certificates Imported certificates and requests Built-in Include expired built-in certificates

<input type="checkbox"/>	#	Certificate	Type	Validated	Expires	Details	Configure
<input type="checkbox"/>	1	WAN GroupVPN	Local certificate	Yes	Oct 11 10:25:12 2013 GMT		
<input type="checkbox"/>	2	hal-2010-SERVER2K8-CA	CA certificate		Sep 5 18:44:33 2016 GMT		

Import... New Signing Request... SCEP... Delete Delete All

Obtain a certificate for GVC clients.

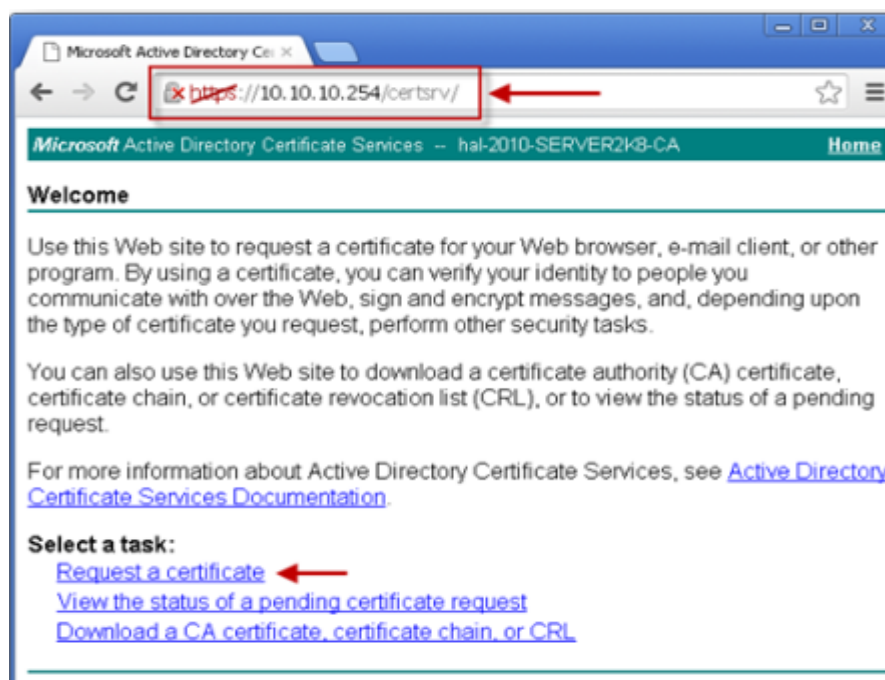
- Navigate to the Microsoft Windows Certificate Enrollment page: *http:///CertSrv*
- When prompted for authentication, enter username and password of a Domain User.
- Click on **Request a certificate**
- Click on **advanced certificate request**.
- Select **Administrator** or **User** under **Certificate Template**.

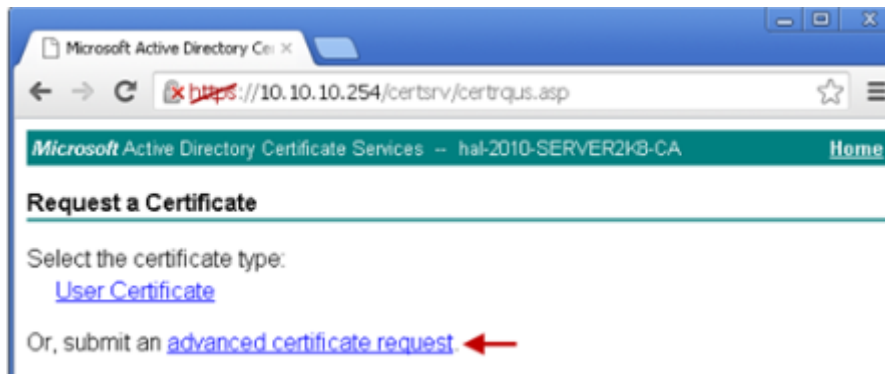
Note:

For Site to Site VPN or GVC, a certificate with **Key Usage**, if present, must have **Digital Signature** and/or **Non-Repudiation** and **Extended Key Usage (EKU)**, if present, with **Client Authentication** seems to work.

If, on the other hand, using L2TP/IPSec VPN, make sure, if **Key Usage** is present, to use **Digital Signature** and/or **Non-Repudiation**. The **Extended Key Usage (EKU)** field SHOULD NOT be used but, if present, may have **Encrypted File System (1.3.6.1.4.1.311.10.3.4)** and/or **IP Security End System (1.3.6.1.5.5.8.2.1)**.

- Under **Attributes**, either enter **san:dns=yourdomainname.com** or **san:email=<local-part@domain.com>**. Note: To configure a Microsoft CA to accept a Subject Alternative Name attribute from a certificate request.
- Click on **Submit** and you will taken to the next page.
- On this page click on **Download certificate** or **Download certificate chain** to save the signed certificate to disk.





Certificate Template:

User

Key Options:

Create new key set Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: Exchange

Key Size: 1024 Min: 384 Max: 10384 (common key sizes: 512 1024 2048 4096 8192 16384)

Automatic key container name User specified key container name

Mark keys as exportable ←

Enable strong private key protection

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm: sha1
Only used to sign request.

Save request

Attributes: san:dns=hal-2010.local ←

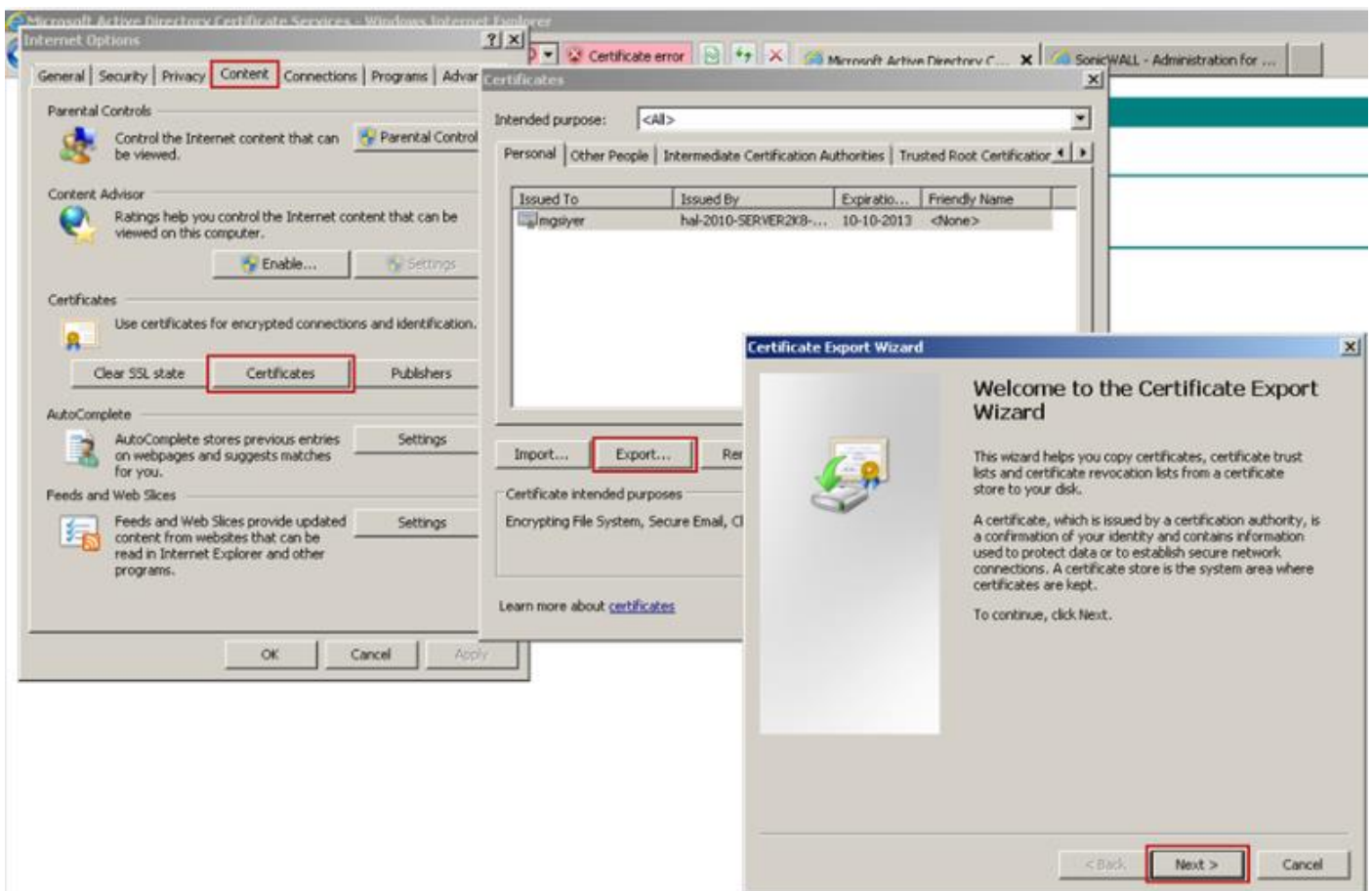
Friendly Name:

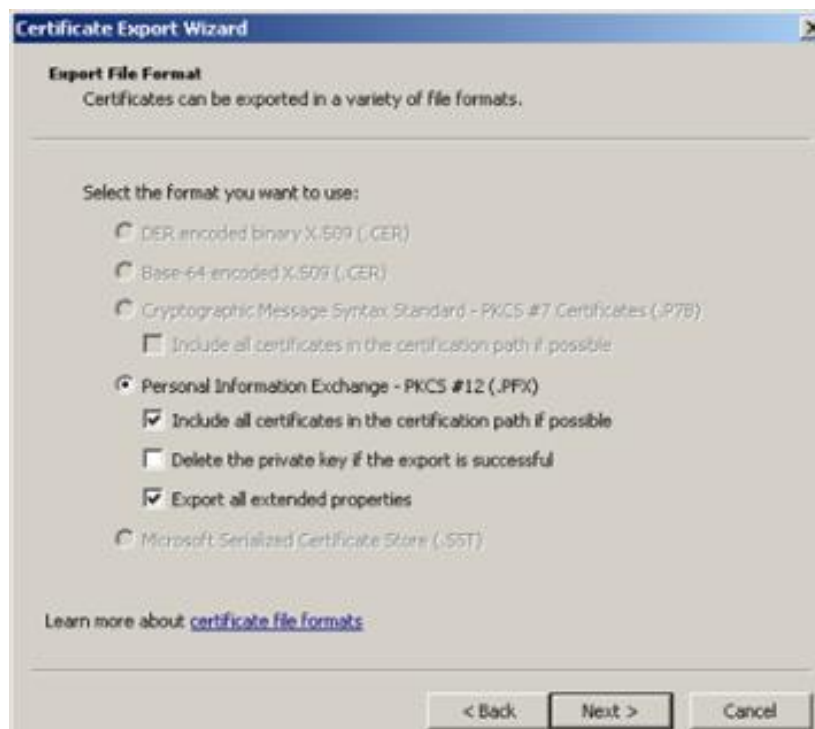


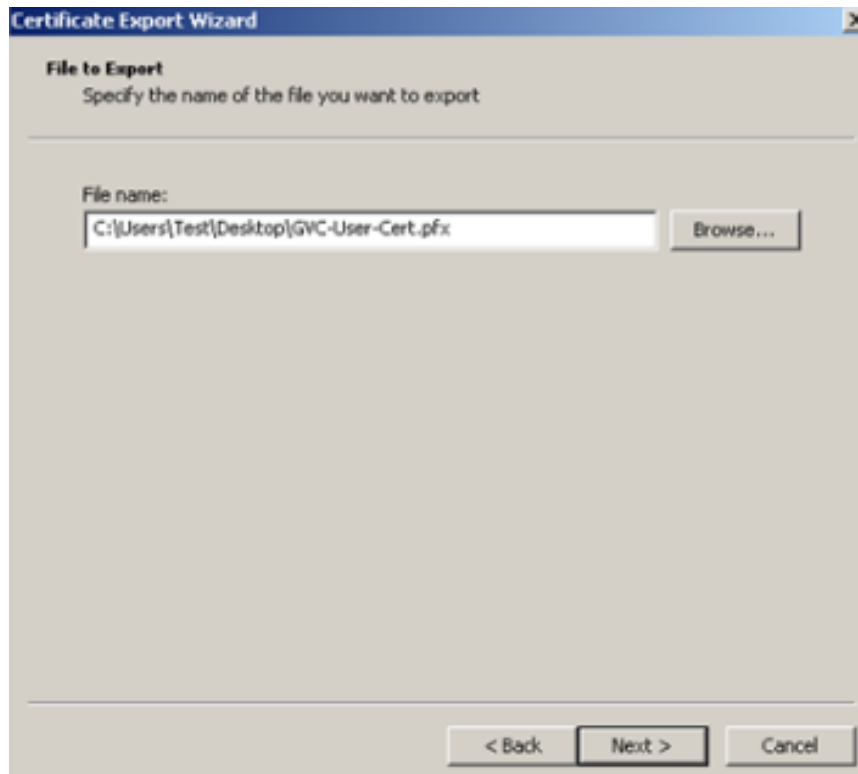
The signed certificate will be installed within the browser.



Export the certificate with its private key from the browser.







Browse Knowledgebase by Category

[Capture Security Center](#)

[Cloud Security](#)

[Email Security](#)

[Endpoint Security](#)

[Firewalls](#)

[Management and Reporting](#)

[MySonicWall](#)

[Secure Mobile Access](#)

[Secure Wireless](#)

How to obtain certificates for VPN connections (Site to Site, GVC, L2TP)

 05/15/2019  1178  17232

DESCRIPTION:

Using digital certificates for authentication instead of preshared keys in VPNs is considered more secure. In SonicWall UTM devices, digital certificates are one way of authenticating two peer devices to establish an IPsec VPN tunnel. The other is IKE using preshared key. The KB article describes the method to configure WAN GroupVPN and Global VPN Clients (GVC) to use digital certificates for authentication before establishing an IPsec VPN tunnel.

Features of IKE Authentication with Certificates in SonicWall WAN GroupVPN and GVC.

- A digital certificate either obtained from a third party CA (like Verisign) or from a private CA (like Microsoft CA or OpenSSL) must be used for this configuration. Self-signed certificates are not supported.
- In the SonicWall, the administrator has the option to create a Certificate Signing Request (CSR) and get it signed by a CA or import a signed certificate in the PKCS#12 format (.pfx or .p12 extension). When importing a signed certificate into the GVC client, it must be in the PKCS#12 format (.pfx or .p12 extension).
- Both peers must trust the issuer of the certificate. In other words, the CA certificate of the user certificate must be imported into the SonicWall as well as the remote GVC client.
- If a certificate has already been imported into the SonicWall signed by a 3rd party CA (for example, Versign), this can be selected in the WAN GroupVPN. The CA certificate must be imported into the GVC client.
- SonicWall supports digital certificates issued by different CAs to be imported into the SonicWall UTM device and the remote GVC client. SonicWall also supports forcing both peers to use certificates issued by the same CA.

RESOLUTION:

The certificate signing process described here is using a Windows Server 2008 CA. To configure a Microsoft CA to accept a Subject Alternative Name attribute from a certificate request, refer this Microsoft article: [How to configure a CA to accept a SAN attribute from a certificate request](#)

- [Create a Certificate Signing Request \(CSR\) in the SonicWall](#)

- [Get the CSR signed from the Windows Server Certificate Enrollment Web Services](#)
 - [Obtain a certificate to use in WAN GroupVPN configuration](#)
 - [Download the CA certificate for the signed certificate](#)
 - [Obtain a certificate for GVC clients.](#)

Create a Certificate Signing Request (CSR) in the SonicWall

Login to the SonicWall management GUI

Navigate to the **System | Certificate** page.

Click on **New Signing Request** to create a similar CSR as under

Click on **Generate** to save.

Refresh the page.

Click on the download button to download the CSR.

Generate Certificate Signing Request

Certificate Alias:

Country:

State:

Locality, City, or County:

Company or Organization:

Department:

Group:

Team:

Common Name:

Subject Distinguished Name:

Subject Alternative Name (Optional):

Domain Name:

Subject Key Type: RSA

Subject Key Size:

Ready

System /

Certificates

Certificates and Certificate Requests

View Style: All certificates Imported certificates and requests Built-in certificates Include expired certificates

<input type="checkbox"/>	#	Certificate	Type	Validated	Expires
<input type="checkbox"/>	1	WANGroupVPN	Pending request		
<input type="checkbox"/>	2	hal-2010-SERVER2K8-CA	CA certificate		Sep 5 18:44:33 2016 GMT


```

-----BEGIN CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAwUDELMAkGA1UEBhMC5U4xCzAJBgNVBAGTAkRBMQwwCgYDVQ0H
EwNCTFIxDTALBgNVBAoTBFNOV0wxFzAVBgNVBAMTDnNvbmljbGFjLmxyY2FsMIGF
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD00ZQj1s6tcw9B4AggEitw+/Z7AptQ
XoAAkenaoA6qk2LkJHtMXJF71I/x6MuxNEKK1h/+7vamhR+s7jdpV6+EsQj87Ky8
6waM8aP3Ts ox19MeYI3DHqrGnE3cs fQlIwrqgP1SPtCnWKL+itSMkMuNLcnTp2BH
2jm4QDqs k8VwbwIDAQABoCwwKgYJKoZIhvcNAQkOMR0wGzAZBgNVHREEEjAQQg5Z
b25pY2xhyi5sb2NhbDANBgkqhkiG9w0BAQQAFAA0BgQBFZNTCPIBCwAyYuEGNXE3W
JvukmCMZdERp76a6iBHNvjzv9Zvw+q9MdeUMSjn1URuj9t78JEN6fxyoDL7uDsNe
8YIXpnz4CbfgaPR76HPyER2pg+ITUAJCGX4XBC5n03r1lzzYhN5Ja1+lR+84QD6n
5mzzCtDbuLy2l09Z310J4w==-----END CERTIFICATE REQUEST-----

```

Obtain a certificate using the Windows Server Certificate Enrollment Web Services

Obtain a certificate to use in WAN GroupVPN configuration

Open a browser and navigate to the Microsoft Windows Certificate Enrollment page: <http://CertSrv>
When prompted for authentication, enter username and password of Administrator.

Click on **Request a certificate**

Click on **advanced certificate request**.

Copy the contents of CSR in the Saved Request box.

Select Administrator under Certificate Template. Note: **User** or **Web Server** template also could be selected.

Under Attributes, either enter **san:dns=yourdomainname.com** or **san:email=<local-part@domain.com>**. Note: To configure a Microsoft CA to accept a Subject Alternative Name attribute from a certificate request, refer this Microsoft article: [How to configure a CA to accept a SAN attribute from a certificate request](#)

Click on Submit and you will taken to the next page.

On this page click on **Download certificate** or **Download certificate chain** to save the signed certificate to disk.

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA

[Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#) ←

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA

[Home](#)

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#). ←

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAwUDELMAkGA1UEBhMCSU4xCzAJ
EwNCTFIxDTALBgNVBAoTBFNOV0wxFzAVBgNVBANT
MAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDOOZQJ
XoAAkenaoA6qk2LkJHtNXJF71I/x6MuxNEKK1h/+
6WaM8aP3Tsox19MeYI3DHqrGnE3csfQ1IwrqgP1S
-----
```

Certificate Template:

Administrator

Additional Attributes:

Attributes: `san:dns=hal-2010.local`

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAwwUDELMAkGA1UEBhMCSU4xCzAJ
EwNCTFIxDTALBgNVBAoTBFN0V0wxFzAVBgNVBAMT
MAOGCSqGSIb3DQEBAQUAA4GNADCB1QKBgQD0OZQj
XoAAkenaoA6qk2LkJHtMXJF71I/x6MuxNEKK1h/+
6WaM8aP3Tsox19MeYI3DHqrGnE3csfQ1IvrqgP1S
-----
```

Certificate Template:

Administrator

Additional Attributes:

Attributes: `san:email=Admin@hal-2010.local`


Submit >

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA Home

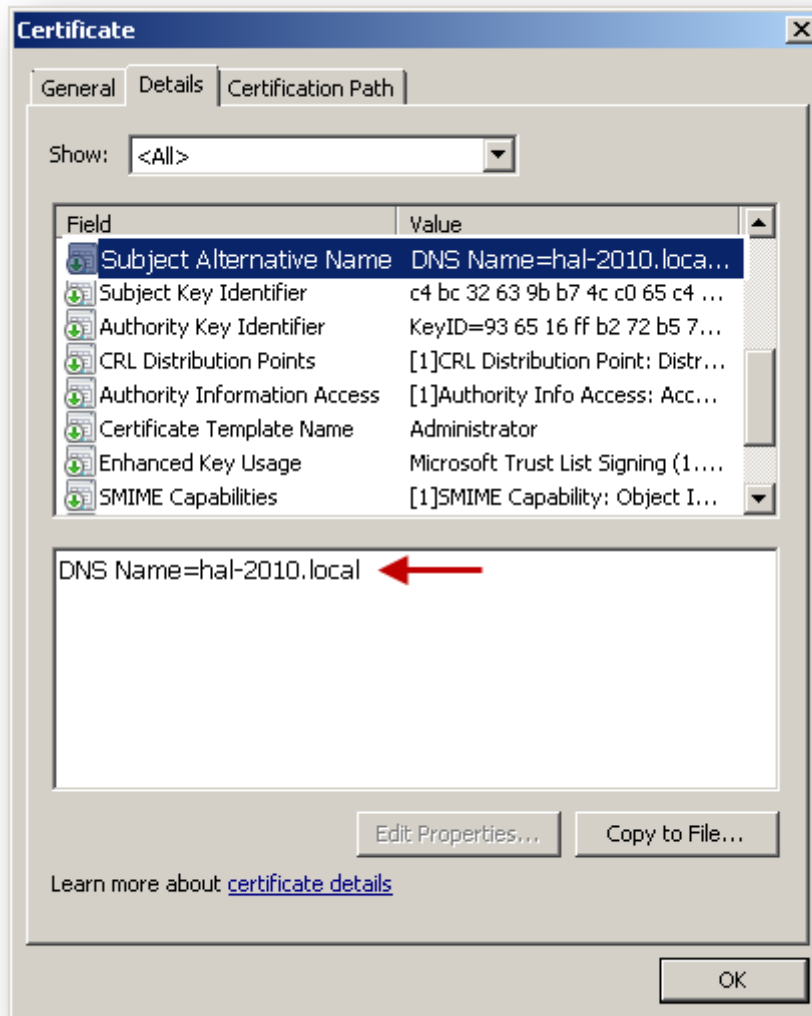
Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)

Below is an example of a signed certificate's Subject Alternative Name (SAN):



Download the CA certificate for the signed certificate.

Navigate to the Microsoft Windows Certificate Enrollment page: <http://CertSrv>

Click on **Download a CA certificate....**

On the next page, click on **Download CA certificate** and save the certificate to disk.

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA [Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#) ←

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA [Home](#)

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [hal-2010-SERVER2K8-CA] ▾

Encoding method:

- DER
 Base 64

[Install CA certificate](#)

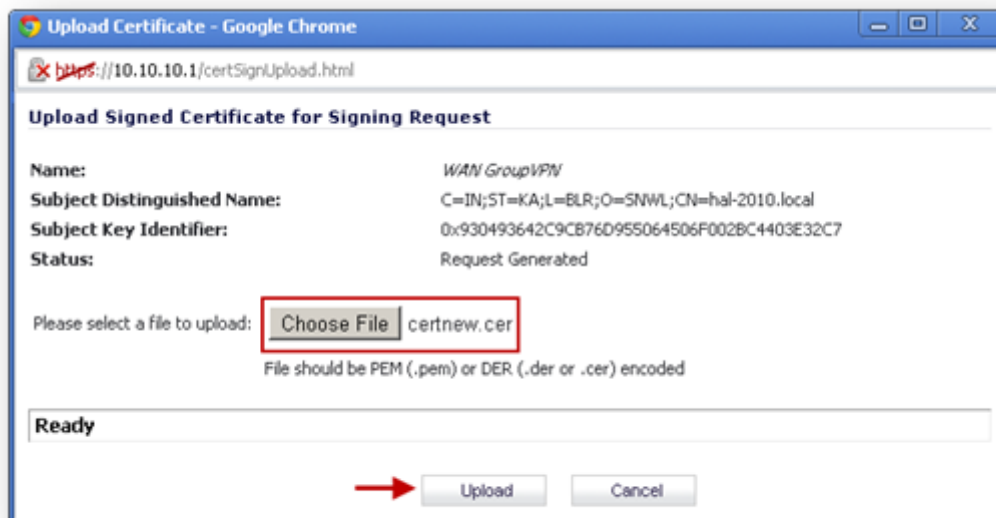
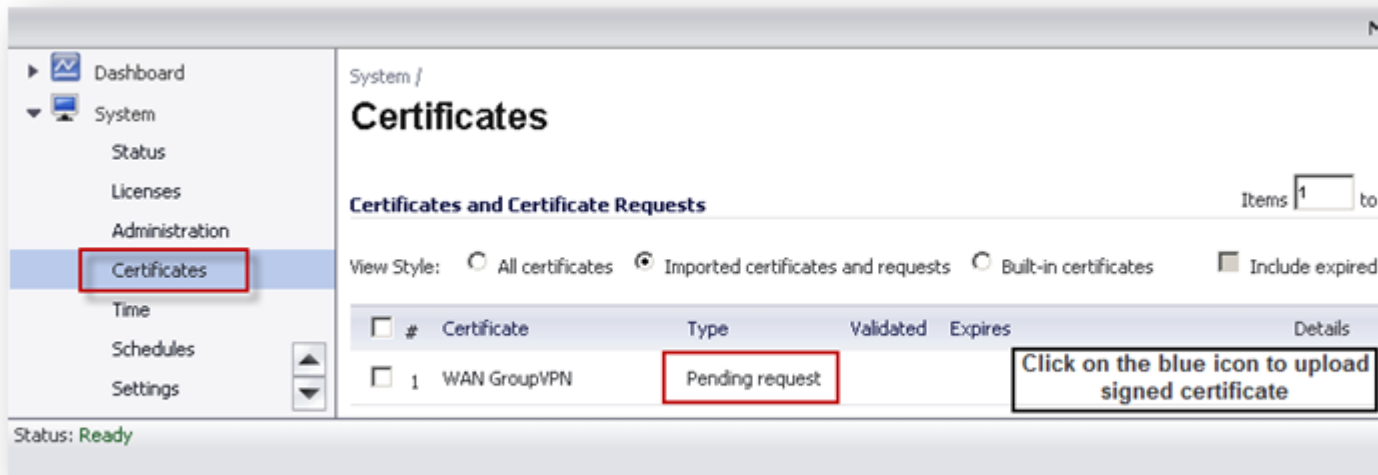
[Download CA certificate](#) ←

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Upload the signed certificate into the SonicWall via the upload button of the CSR pending request.



To establish trust and complete the validation of the signed certificate, import the CA certificate

Mode: Con

System /
Certificates

Certificates and Certificate Requests Items 1 to 1 (of 1)

View Style: All certificates Imported certificates and requests Built-in certificates Include expired built-in certificates

<input type="checkbox"/>	#	Certificate	Type	Validated	Expires	Details
<input type="checkbox"/>	1	WAN GroupVPN	Local certificate	No	Oct 11 10:25:12 2013 GMT	

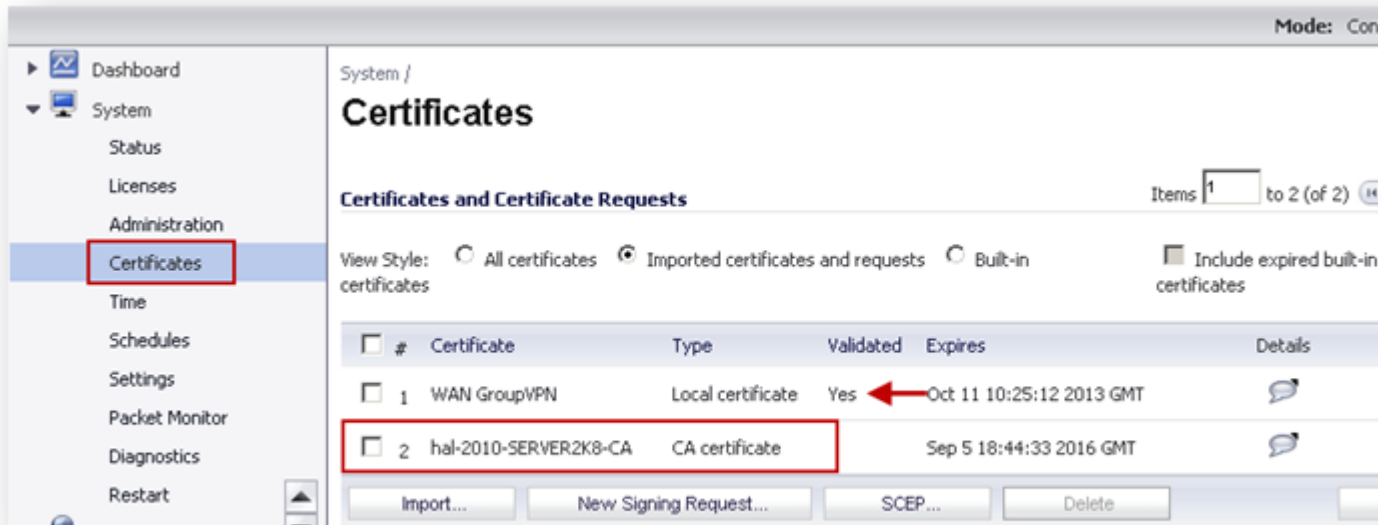
Status: The configuration has been updated.

Import Certificate

Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file
 Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file

Please select a file to import: certnew (1).cer

Ready



Obtain a certificate for GVC clients.

- Navigate to the Microsoft Windows Certificate Enrollment page: <http://CertSrv>
- When prompted for authentication, enter username and password of a Domain User.
- Click on **Request a certificate**
- Click on **advanced certificate request**.
- Select **Administrator** or **User** under **Certificate Template**.

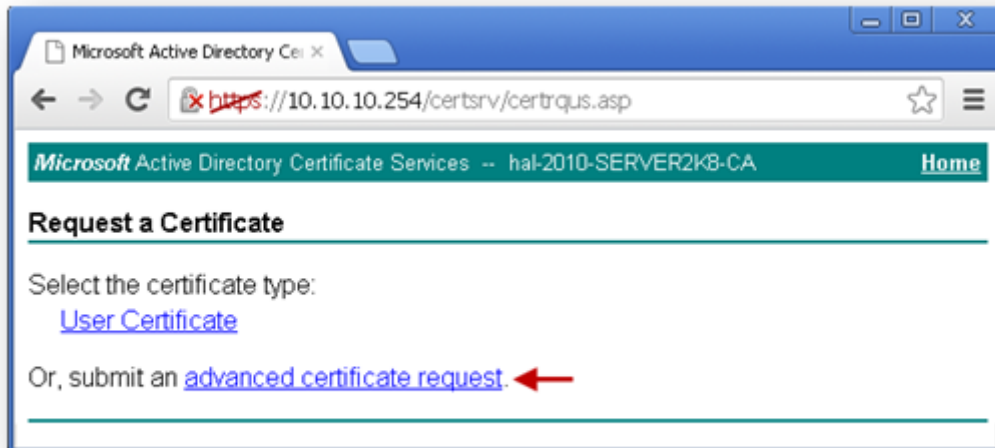
Note:

For Site to Site VPN or GVC, a certificate with **Key Usage**, if present, must have **Digital Signature** and/or **Non-Repudiation** and **Extended Key Usage (EKU)**, if present, with **Client Authentication** seems to work.

If, on the other hand, using L2TP/IPSec VPN, make sure, if **Key Usage** is present, to use **Digital Signature** and/or **Non-Repudiation**. The **Extended Key Usage (EKU)** field SHOULD NOT be used but, if present, may have **Encrypted File System (1.3.6.1.4.1.311.10.3.4)** and/or **IP Security End System (1.3.6.1.5.5.8.2.1)**.

- Under **Attributes**, either enter **san:dns=yourdomainname.com** or **san:email=<local-part@domain.com>**. Note: To configure a Microsoft CA to accept a Subject Alternative Name attribute from a certificate request.
- Click on **Submit** and you will be taken to the next page.
- On this page click on **Download certificate** or **Download certificate chain** to save the signed certificate to disk.





Certificate Template:

User

Key Options:

Create new key set Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: Exchange

Key Size: 1024 Min: 384 Max: 16384 (common key sizes: 512 1024 2048 4096 8192 16384)

Automatic key container name User specified key container name

Mark keys as exportable

Enable strong private key protection

Additional Options:

Request Format: CMC PKCS10

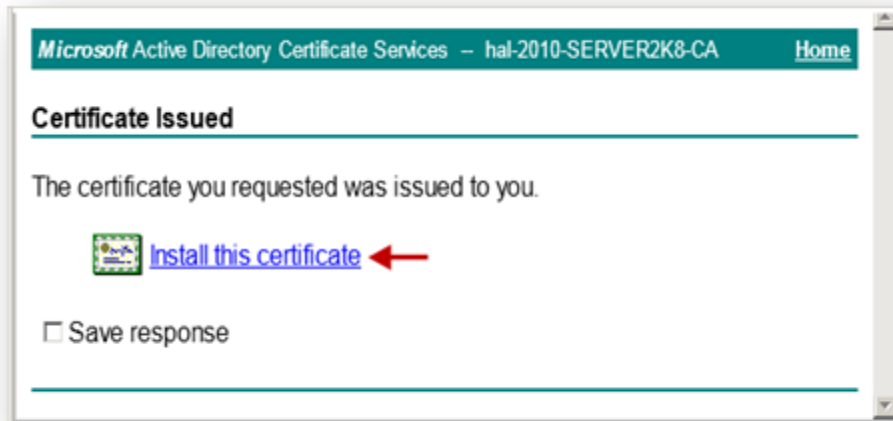
Hash Algorithm: sha1
Only used to sign request.

Save request

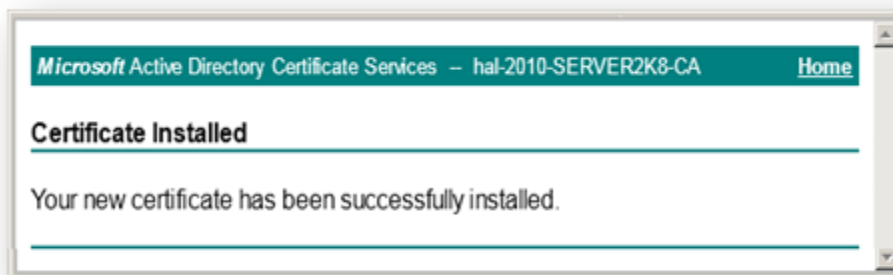
Attributes: san:dns=hal-2010.local

Friendly Name:

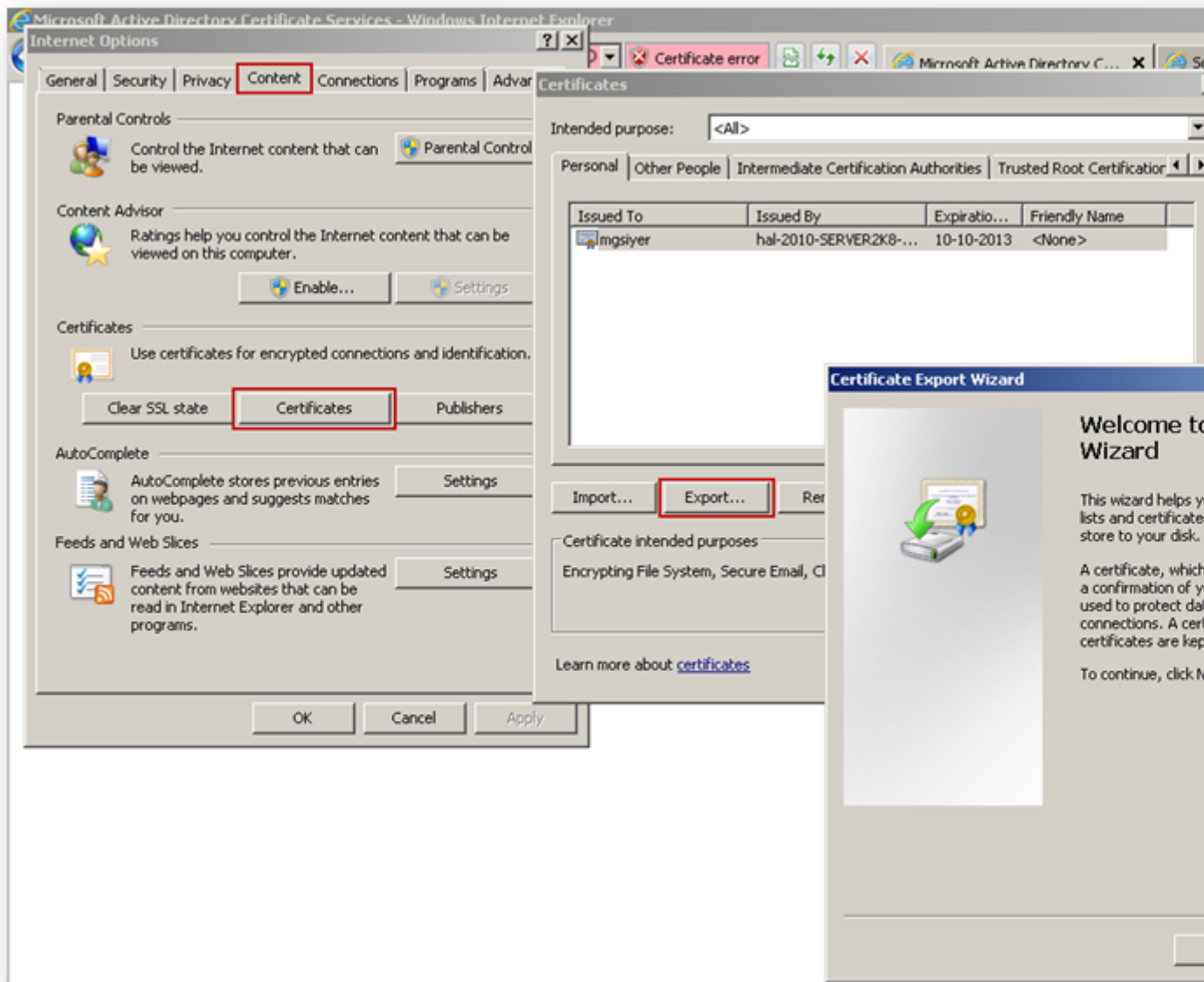
Submit >



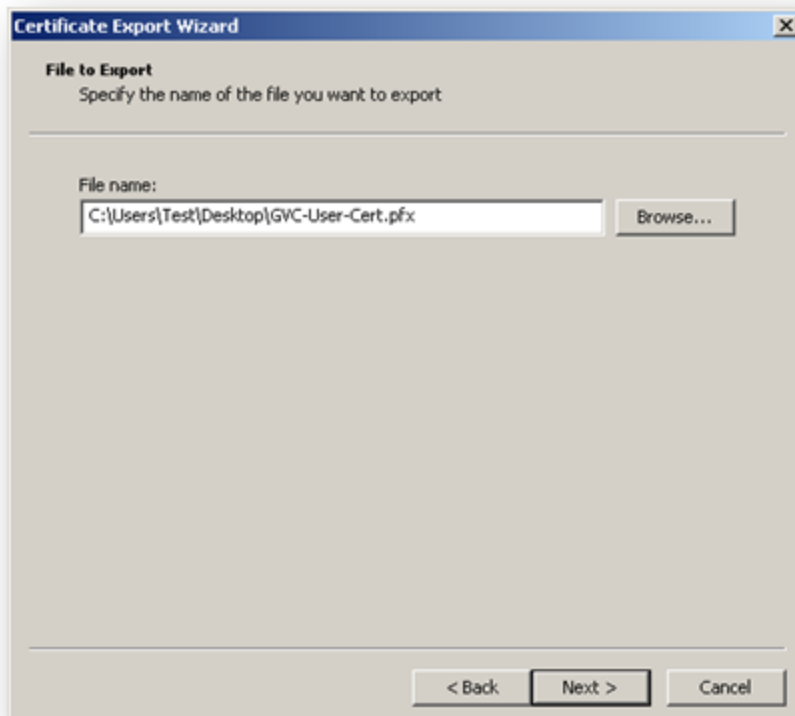
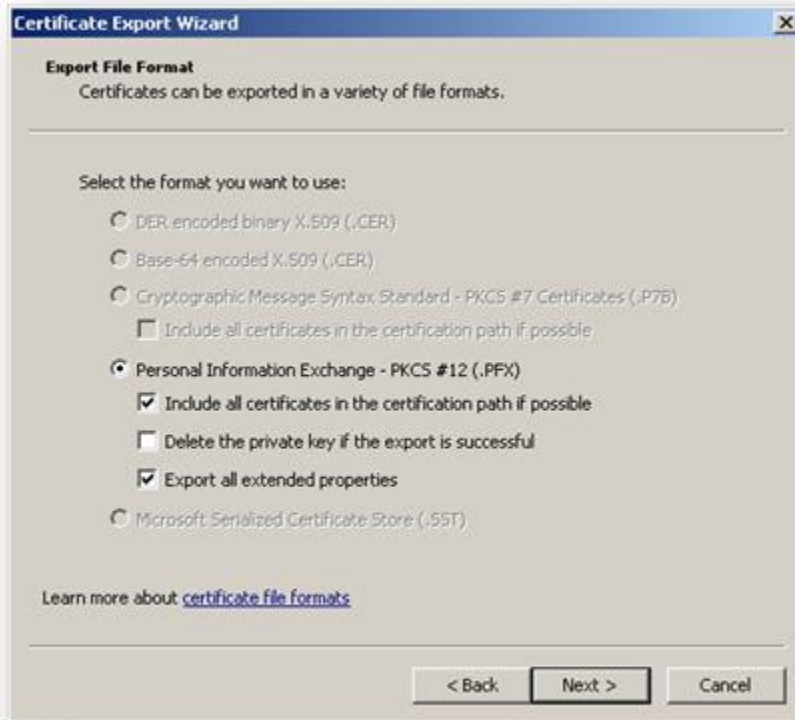
The signed certificate will be installed within the browser.



Export the certificate with its private key from the browser.









RESOLUTION FOR SONICOS 6.5 AND LATER

SonicOS 6.5 was released September 2017. This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 and later firmware.

The certificate signing process described here is using a Windows Server 2008 CA. To configure a Microsoft CA to accept a Subject Alternative Name attribute from a certificate request, refer this Microsoft article: [How to configure a CA to accept a SAN attribute from a certificate request](#)

- **Create a Certificate Signing Request (CSR) in the SonicWall**
- **Get the CSR signed from the Windows Server Certificate Enrollment Web Services**
 - **Obtain a certificate to use in WAN GroupVPN configuration**
 - **Download the CA certificate for the signed certificate**
 - **Obtain a certificate for GVC clients.**

Create a Certificate Signing Request (CSR) in the SonicWall

Login to the SonicWall management GUI
 Navigate to the **Manage | Appliance | Certificates**.

Certificates and Certificate Requests

View Style: All certificates Imported certificates and requests Built-in certificates

#	Certificate
1	www.yourdomain.com
2	SonicWall
3	SonicWallCA

IMPORT NEW SIGNING REQUEST SCEP DELETE

Click on **New Signing Request** to create a similar CSR as under
 Click on **Generate** to save.
 Refresh the page.

Generate Certificate Signing Request

Certificate Alias:

Country

State

Locality, City, or County

Company or Organization

Department

Group

Team

Common Name

Subject Distinguished Name:

Subject Alternative Name (Optional):

Domain Name

Signature algorithm:

Subject Key Type:

Subject Key Size/Curve:

Ready

GENERATE CANCEL

Click on the download button to download the CSR.

Certificates and Certificate Requests

View Style: All certificates Imported certificates and requests Built-in certificates Include expired built-in certificates

	Type	Validated	Expires	Details	Configure
1 www.pouloham.com	Pending request				
2 WANGGroupVPN	Pending request				
3 Secretlab	Local certificate	Yes	Aug 18 18:08:00 2018 GMT		

WANGGroupVPN.p10 - Notepad

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAuUDELMAkGA1UEBhMCSU4xCzAJBgNVBAGTAktBMQwwCgYDVQQH
EwNCTFIxDTALBgNVBAoTBFBNOV0wxFzAVBgNVBAMTDnNvbmljbGF1LmRmY2FsMIGF
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD00ZQj1s6tcw9B4AggEitw+/Z7AptQ
xoAAkenaoA6qk2LkJHTMXJF71I/x6MuxNEKK1h/+7vamhR+s7jdpV6+EsQj87Ky8
6waM8aP3Ts0x19MeYI3DHqrGnE3csfQlIwrqgP1SPtCnWKL+iTSMKMuNLcnTp2BH
2jm4QDqsk8VwbwIDAQABoCwwKgYJKoZIhvcNAQkOMR0wGzAZBgNVHREEEjAqgg5Z
b25pY2xhYi5sb2NhbDANBgkqhkiG9w0BAQQFAA0BgQBfZNTCPIBCwAyYuEGNXE3W
JVukmCMzdERp76a6iBHNvjzV9ZVw+q9MdeUMSjn1URuj9t78JEN6fxyoDL7uDsNe
8YIxpnz4CbfgaPR76HPyER2pg+ITUAJCGx4XBC5n03r1lzZYhN5Jal+lR+84QD6n
5mzzCtDbuLy2lo9Z310J4w==-----END CERTIFICATE REQUEST-----
  
```

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA

[Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#) ←

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).



Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAwUDELHAKGA1UEBhMCSU4xCzAJ
EwNCTFIxDTALBgNVBaoTBFNOV0uxFzAVBgNVBANT
MAOGCSqGSIb3DQEBAQUAA4GNADCB1QKBgQDOO2Qj
XoAAknaoA6qk2LkJHtMXJF71I/x6MuxNEKK1h/+
6WaM8aP3Tsox19MeYI3DHqrGnE3csfQ1IvrqgP1S
  
```

Certificate Template:

Administrator

Additional Attributes:

Attributes: san:dns=hal-2010.local

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAeUDELMAkGA1UEBhMCSU4xCzAJ
EwNCTFIxDTALBgNVBAoTBFNOVOwxFzAVBgNVBAHT
MAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDOOZQj
XoAAkenaoA6qk2LkJHtMXJF71I/x6MuxNEKK1h/+
6VaB8aP3Tsox19MeYI3DHqrGnE3csfQ1IwrqgP1S
```

Certificate Template:

Administrator

Additional Attributes:


Attributes: san:email=Admin@hal-2010.local


Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA [Home](#)

Certificate Issued

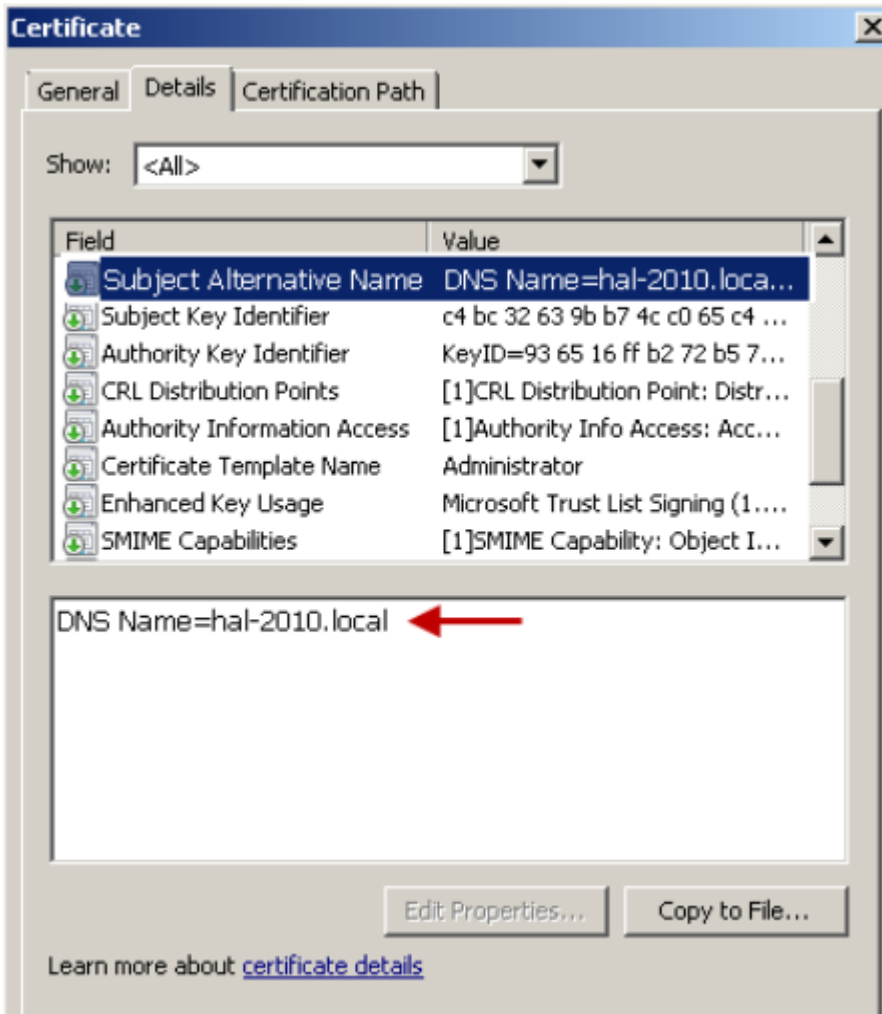
The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#)

 [Download certificate chain](#)

Below is an example of a signed certificate's Subject Alternative Name (SAN):



Download the CA certificate for the signed certificate.

Navigate to the Microsoft Windows Certificate Enrollment page: <http://CertSrv>

Click on **Download a CA certificate....**

On the next page, click on **Download CA certificate** and save the certificate to disk.

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA

[Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#) ←

Microsoft Active Directory Certificate Services -- hal-2010-SERVER2K8-CA [Home](#)

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [hal-2010-SERVER2K8-CA]

Encoding method:

DER
 Base 64

[Install CA certificate](#)
[Download CA certificate](#) ←
[Download CA certificate chain](#)
[Download latest base CRL](#)
[Download latest delta CRL](#)

Upload the signed certificate into the SonicWall via the upload button of the CSR pending request.

Certificates and Certificate Requests

View Style: All certificates Imported certificates and requests Built-in certificates Include expired built-in certificates

#	Certificate	Type	Validated	Expires	Details	Configure
1	www.yourdomain.com	Pending request				
2	WANGroupVPN	Pending request				
3	SonicWall	Local certificate	Yes	Aug 16 18:08:00 2018 GMT		

Upload Certificate - Google Chrome

<https://10.10.10.1/certSignUpload.html>

Upload Signed Certificate for Signing Request

Name: WAN GroupVPN
Subject Distinguished Name: C=IN;ST=KA;L=BLR;O=SNWL;CN=hal-2010.local
Subject Key Identifier: 0x930493642C9CB76D955064506F002BC4403E32C7
Status: Request Generated

Please select a file to upload: certnew.cer

File should be PEM (.pem) or DER (.der or .cer) encoded

Ready

To establish trust and complete the validation of the signed certificate, import the CA certificate

Certificates and Certificate Requests

View Style: All certificates Imported certificates and requests Built-in certificates Include expired built-in certificates

#	Certificate	Type	Validated	Expires
1	www.yourdomain.com	Pending request		
2	WANGroupVPN	Pending request		
3	SonicWall	Local certificate	Yes	Aug 16 18:08:00 2018 GMT
4	SonicWallCA	CA certificate		Aug 16 17:44:00 2017 GMT

Import Certificate - Google Chrome

<https://10.61.130.57/certimport.html>

SONICWALL® Network Security Appliance

Import Certificate

Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file
 Import a CA certificate from a PKCS#7 (.p7c), PEM (.pem) or DER (.der or .cer) encoded file

Certificate Name:

Certificate Management Password:

Please select a file to import: No file chosen

Ready

Import Certificate

Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file
 Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file

Please select a file to import: certnew (1).cer

Ready

Obtain a certificate for GVC clients.

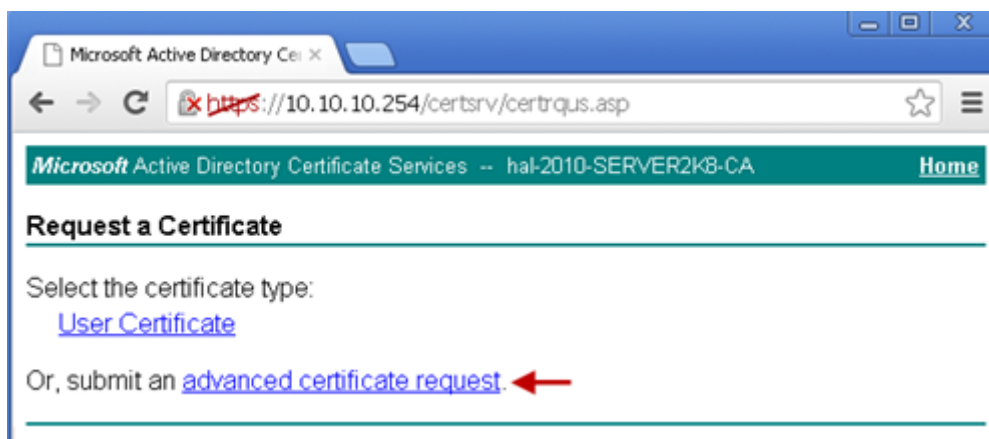
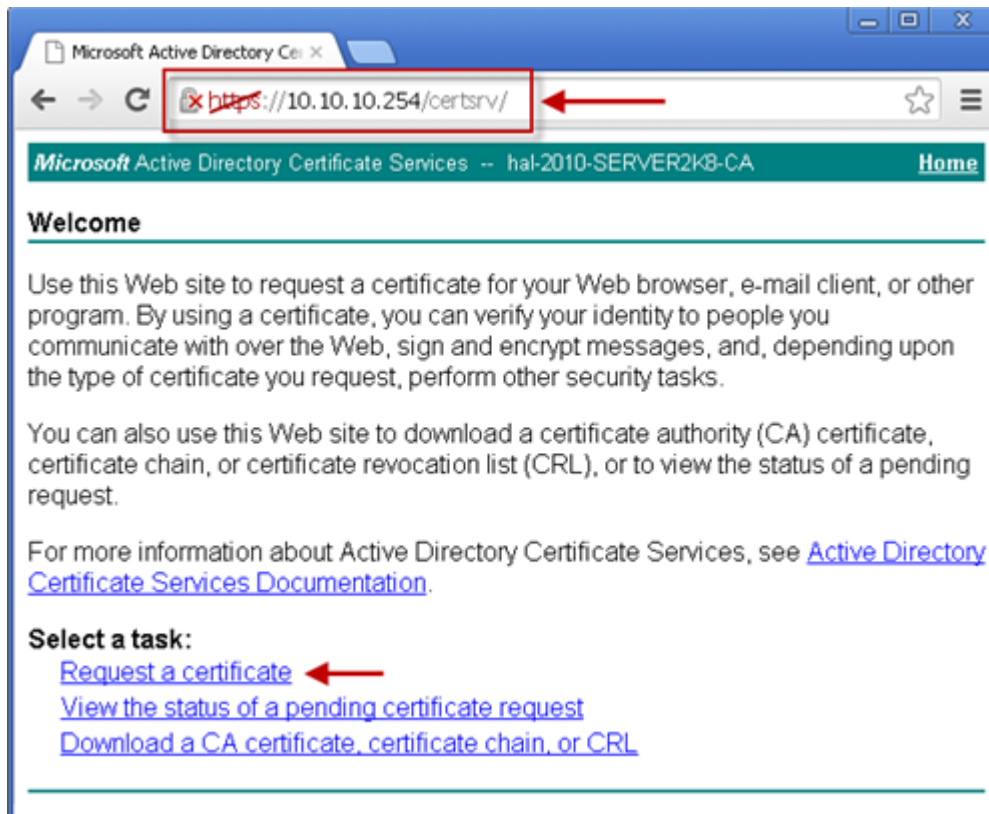
- Navigate to the Microsoft Windows Certificate Enrollment page: <http://CertSrv>
- When prompted for authentication, enter username and password of a Domain User.
- Click on **Request a certificate**
- Click on **advanced certificate request**.
- Select **Administrator** or **User** under **Certificate Template**.

Note:

For Site to Site VPN or GVC, a certificate with **Key Usage**, if present, must have **Digital Signature** and/or **Non-Repudiation** and **Extended Key Usage (EKU)**, if present, with **Client Authentication** seems to work.

If, on the other hand, using L2TP/IPSec VPN, make sure, if **Key Usage** is present, to use **Digital Signature** and/or **Non-Repudiation**. The **Extended Key Usage (EKU)** field SHOULD NOT be used but, if present, may have **Encrypted File System (1.3.6.1.4.1.311.10.3.4)** and/or **IP Security End System (1.3.6.1.5.5.8.2.1)**.

- Under **Attributes**, either enter **san:dns=yourdomainname.com** or **san:email=<local-part@domain.com>**. Note: To configure a Microsoft CA to accept a Subject Alternative Name attribute from a certificate request.
- Click on **Submit** and you will taken to the next page.
- On this page click on **Download certificate** or **Download certificate chain** to save the signed certificate to disk.



Certificate Template:

User

Key Options:

Create new key set Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: Exchange

Key Size: 1024 Min: 384 Max: 16384 (common key sizes: 512 1024 2048 4096 8192 16384)

Automatic key container name User specified key container name

Mark keys as exportable ←

Enable strong private key protection

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm: sha1
Only used to sign request.

Save request

Attributes: san:dns=hal-2010.local ←


Friendly Name:

Submit >

Microsoft Active Directory Certificate Services – hal-2010-SERVER2K8-CA [Home](#)

Certificate Issued

The certificate you requested was issued to you.

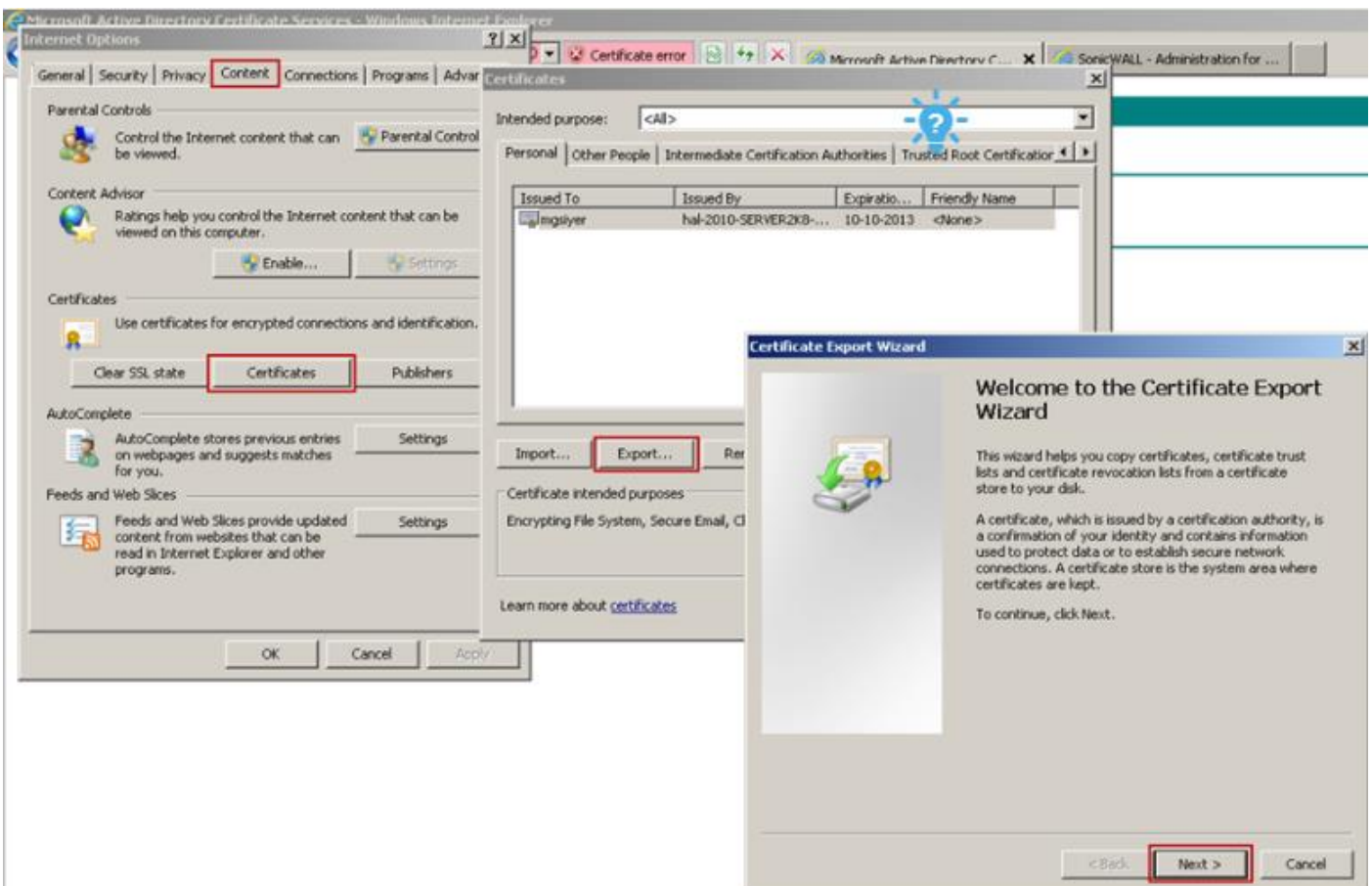
 [Install this certificate](#) ←

Save response

The signed certificate will be installed within the browser.



Export the certificate with its private key from the browser.



Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

Yes, export the private key

No, do not export the private key

Learn more about [exporting private keys](#)

< Back Next > Cancel

Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

DER encoded binary X.509 (.CER)

Base-64 encoded X.509 (.CER)

Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

Include all certificates in the certification path if possible

Personal Information Exchange - PKCS #12 (.PFX)

Include all certificates in the certification path if possible

Delete the private key if the export is successful

Export all extended properties

Microsoft Serialized Certificate Store (.SST)

Learn more about [certificate file formats](#)

< Back Next > Cancel

