

SecureFirst

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, 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: <u>How</u> to configure a CA to accept a SAN attribute from a certificate request

- <u>Create a Certificate Signing Request (CSR) in the SonicWall</u>
 - 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 Requ | est |
|--------------------------------------|---|
| Certificate Alias: | WANGroupVPN |
| Country | INDIA (IN) |
| State | KA |
| Locality, City, or County 💌 | BLR |
| Company or Organization | SNWL |
| Department | |
| Group | |
| Team | |
| Common Name | hal-2010.local |
| Subject Distinguished Name: | C=IN;ST=KA;L=BLR;O=SNWL;CN=soniclab.local |
| Subject Alternative Name (Optional): | |
| Domain Name 💌 | hal-2010.local |
| Subject Key Type: | RSA |
| Subject Key Size: | 1024 bits • |
| Ready | |
| | Generate Cancel |

| Dashboard System Status | System / Certificates | | | | | |
|---------------------------------|---|------------------------------|-------------------------|-------------------------|-----------------|-----------|
| Licenses Administration | Certificates and Certificate Requests | | | | | |
| Certificates | View Style: C All certificates @ Import | ed certificates and requests | C Built-in certificates | Include expired built- | in certificates | |
| Time | 🗖 # Certificate | Туре | Validated | Expires | Details | Configure |
| Settings | 1 WANGroupVPN | Pending request | | | ø - | ې |
| Packet Monitor | 2 hal-2010-SERVER2K8-CA | CA certificate | | Sep 5 18:44:33 2016 GMT | ø | 🛞 🗄 🎒 |

| WANGroupVPN,p10 - Notepad | _ × |
|--|--|
| File Edit Format View Help | |
| BEGIN CERTIFICATE REQUEST MIIBvDCCASUCAQAwUDELMAkGA1UEBhMCSU4xCzAJBgNVBAgTAktBMQwwCgYDV EwNCTFIxDTALBgNVBAoTBFN0V0wxFzAVBgNVBAMTDnNvbm1jbGFiLmxvY2FsM MAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD0020j1s6tcw9B4AggEitw+/Z7A XoAAkenaoA6qk2LkJHtMxJF7II/x6MuxNEKK1h/+7vamhR+s7jdpV6+EsQj87 6WaMBaP3Tsox19MeYI3DHqrGnE3csfQ1IwrqgP1SPtCnWKL+itSMKMUNLcnTp 2 jm4QDqsk8VwbwIDAQABoCwwKgYJKozIhvcNAQkOMR0wGzAZBgNVHREEEjAQg b25pY2xhYi5sb2NhbDANBgkqhkiG9w0BAQQFAA0BgQBfZNtCPIBCwAyYuEGNX JVukmCMZdERp76a6iBHNVjzV9ZVW+q9MdeUMSjn1URuj9t78JEN6fxyoDL7uD 8YIxpnz4CbfqaPR76HPyER2pg+ITUAJCgX4XBC5n03r11zZYhN5Ja1+1r+84Q 5mzzCtDbuLy2109Z310J4w==END CERTIFICATE REQUEST | QQH IGf ptQ 2BH gSz E3W sNe D6n |
| | - |

ITCorporation® Visit our Website: www.itclatam.com



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. <u>Note</u>: **User** or **Web Server** template also could be selected.

Under Attributes, either enter san:dns=yourdomainname.com or san:email=<local-

part@domain.com|. <u>Note</u>: To configure a Microsoft CA to accept a Subject Alternative Name attribute from a certificate request, refer this Microsoft article: <u>How to configure a CA to accept a SAN attribute from a</u> 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.



ITCorporation® Visit our Website: www.itclatam.com Calle 146 #7-64. Bogotá D.C. Colombia +57 1 466 0599 / +57 315 786 8258 sales@itclatam.com / tss@itclatam.com REV 1.01



| Microsoft Active Directory Ce × | Microsoft Active Directory Ce: × |
|---|--|
| ← → C () () (10.10.10.254/certsrv/certrqxt.asp | ← → C ((k buest://10.10.10.254/certsrv/certrqxt.asp 5/2) ≡ |
| Microsoft Active Directory Certificate Services hal-2010-SERVER2K8-CA Home | Microsoft Active Directory Certificate Services - hal-2010-SERVER2K8-CA Home |
| Submit a Certificate Request or Renewal Request | 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. | 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. |
| Base 64-encoded Centificate request (CMC or PKCS #7): HIBVDCCASUCAQAWUDELMAKGAIUEBhMCSU4xCzAJ EWNCTFIxDTALBGNVBACTBFNOVOwYF2AVDgNVBAHT MAGGSQGSIBJDQEBAQUAA4GNADCBIQKBQD002Q) PKCS #7): K K K K K K K K K K K K K | Base-54-encoded certificate request (CMC or PKCS #/O or PKCS #/D o |
| Certificate Template: | Certificate Template: |
| Administrator 🗲 🔄 | Administrator |
| Additional Attributes: | Additional Attributes: |
| Attributes: | Attributes: |
| Submit > | Submit > |
| | |



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





| Certificate | X |
|---|----------------------------------|
| General Details Certification Path | 1 |
| | |
| Show: <ai></ai> | <u> </u> |
| Field | Value 🔺 |
| 5 Subject Alternative Name | DNS Name=hal-2010.loca |
| Subject Key Identifier | c4 bc 32 63 9b b7 4c c0 65 c4 |
| CRL Distribution Points | [1]CRL Distribution Point: Distr |
| authority Information Access | [1]Authority Info Access: Acc |
| Certificate Template Name | Administrator |
| Enhanced Key Usage | Microsoft Trust List Signing (1 |
| Ger Smithic Capabilities | [1]SMIME Capability: Object 1 |
| DNS Name=hal-2010.local ┥ | |
| | |
| | |
| | |
| | |
| | |
| F | it Properties Copy to File |
| Loove every about eastificate details | |
| Learn more about <u>certificate details</u> | |
| | |
| | OK |

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 | |
|---|------|--|
| 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: | | |
| 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.

| Certil | | □ # Certificate | Туре | Validated Expires | | Details | Configure |
|--|---------------------------------------|--------------------------------|-----------------------|-------------------|---------------------|-------------------|---------------------|
| Certi | A A A A A A A A A A A A A A A A A A A | | | | | | |
| - | icates | View Style: C All certificates | Imported certificates | and requests C B | uit-in certificates | Include expired b | uit-in certificates |
| Statu Licen Admir | s ses sistration | Certificates and Certificate R | tequests | | | Items 1 to 6 | (of 6) (H |
| Dashbo System | ard | System / Certificates | | | | | |

| Name: | WAN GroupVPN | |
|---|---|--|
| Subject Distinguished Name: | C=IN;ST=KA;L=BLR;O=SNWL;CN=hal-2010.local | |
| Subject Key Identifier: Status: | 0x930493642C9CB76D955064506F002BC4403E32C7 Request Generated | |
| Please select a file to upload: Choose File (File should be PEM (| certnew.cer .pem) or DER (.der or .cer) encoded | |





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

| | | Mode: Configuration > |
|----------------|--|---------------------------------------|
| 🕨 🖾 Dashboard | System / | |
| 🕶 🐺 System | Certificates | |
| Status | | |
| Licenses | Certificates and Certificate Requests | Items 1 to 1 (of 1) |
| Administration | • | |
| Certificates | View Style: O All certificates Imported certificates and requests O Built-in | Include expired built-in certificates |
| Time | Ceruncases | |
| Schedules | # Certificate Type Validated Expires | Details Configure |
| Settings | 1 WAN GroupVPN Local certificate No Oct 11 10:25:12 2013 GMT | 🝠 🛞 🕭 |
| Packet Monitor | | |
| Diagnostics | Import New Signing Request SCEP Delete | Delete All |
| Restart | | |
| b 🔇 Maturok | | |

 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

| | | Mode: Configuration > | l |
|----------------|--|------------------------------|---|
| 🕨 🖾 Dashboard | System / | - | 4 |
| 🗢 🗮 System | Certificates | | ľ |
| Status | | | ľ |
| Licenses | Certificates and Certificate Requests | Items 1 to 2 (of 2) III I HI | ľ |
| Administration | | _ | ľ |
| Certificates | View Style: C All certificates C Imported certificates and requests C Built-in | Include expired buik-in | ł |
| Time | ceruindues | Cerui caces | ł |
| Schedules | 🗖 # Certificate Type Validated Expires | Details Configure | ł |
| Settings | □ 1 WAN GroupVPN Local certificate Yes ←Oct 11 10:25:12 2013 GMT | 🗩 😒 🕀 | ł |
| Packet Monitor | a bal-2010.SERVER2V2.CA C0 certificate Sep 5 19:44-33 2016 CMT | | ľ |
| Diagnostics | CA CERTINATE SEP 5 10:44:55 2010 GHT | ~ • • • | ų |
| Restart 🔺 | Import New Signing Request SCEP Delete | Delete All | 4 |





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=<localpart@domain.com]. <u>Note</u>: 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.

| Microsoft Active Directory Cel × |
|--|
| ← → C (*)***://10.10.10.254/certsrv/ ← ☆ Ξ |
| 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 <u>Active Directory</u> 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 Cel × | |
|---|-------------|
| ← → C (>)/10.10.10.254/certsrv/certrqus.asp | ☆ = |
| Microsoft Active Directory Certificate Services hal-2010-SERVER2K8-CA | <u>Home</u> |
| Request a Certificate | |
| Select the certificate type: User Certificate | |
| Or, submit an advanced certificate request. | |

| 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 C 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: |
| 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 |

ITCorporation® Visit our Website: www.itclatam.com Calle 146 #7-64. Bogotá D.C. Colombia +57 1 466 0599 / +57 315 786 8258 sales@itclatam.com / tss@itclatam.com REV 1.01



The signed certificate will be installed within the browser.



Export the certificate with its private key from the browser.







| Priva | te keys are password protected. If you want to export the private key with the icate, you must type a password on a later page. |
|-----------|--|
| Doy | ou want to export the private key with the certificate? |
| ſ | Yes, export the private key |
| | No. do not export the private key |
| | |
| Learn mor | e about <u>exporting private keys</u> |

| Certificate Export Wizard | X |
|--|--------|
| Export File Format Certificates can be exported in a variety of file formats. | |
| Select the format you want to use: | |
| C DER encoded binary X.509 (CER) | |
| C Base 64 encoded X.507 (GER) | |
| C Gryptographic Message Syntax Standard - PKCS #7 Certificates (-P78) | |
| 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 | |
| C Mcrosoft Serialized Certificate Store (JSST) | |
| Learn more about certificate file formats | |
| C Morosoft Senalated Certificate Store (557) Learn more about <u>certificate file formats</u> | Cancel |





| le to Export Specify the name of t | he file you want to ex | port | | |
|---------------------------------------|--|--|---------------------------------|-------------------------|
| File name: | | | | |
| L c: (Deers) resc(Desso | op(uvc-oser-cerc.pr | K. | | owse |
| | | < Back | Next > | Cancel |
| icate Export Wizard | | | | |
| <u></u> | Complet Wizard You have suo wizard. You have spe | ing the Co cessfully complet afied the followi | ertificate ted the Certifica | Export ate Export |
| | Export Keys Include all o File Format | ertificates in the | certification pa | Yes th Yes Person |
| | 4 | | | • |
| | | | | |





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)

İ 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

<u>Create a Certificate Signing Request (CSR) in the SonicWall</u>

ITCorporation® Visit our Website: www.itclatam.com



- <u>Get the CSR signed from the Windows Server Certificate Enrollment Web Services</u>
 - Obtain a certificate to use in WAN GroupVPN configuration
 - <u>Download the CA certificate for the signed certificate</u>
 - 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.





| Certificate Alias: | WANGroupVPN | |
|--------------------------------------|---|---|
| Country | INDIA (IN) | - |
| State | KA | |
| Locality, City, or County 💌 | BLR | |
| Company or Organization | SNWL | |
| Department | • | |
| Group | • | |
| Team | • | |
| Common Name | ▼ hal-2010.local | |
| Subject Distinguished Name: | C=IN;ST=KA;L=BLR;O=SNWL;CN=soniclab.local | |
| Subject Alternative Name (Optional): | | |
| Domain Name | hal-2010.local | |
| Subject Key Type: | RSA | |
| Subject Key Size: | 1024 bits 💌 | |
| Ready | | |
| | Generate Cancel | |









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. <u>Note</u>: **User** or **Web Server** template also could be selected.

Under Attributes, either enter san:dns=yourdomainname.com or san:email=<local-

part@**domain.com**|. <u>Note</u>: To configure a Microsoft CA to accept a Subject Alternative Name attribute from a certificate request, refer this Microsoft article: <u>How to configure a CA to accept a SAN attribute</u> 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.



Calle 146 #7-64. Bogotá D.C. Colombia +57 1 466 0599 / +57 315 786 8258 sales@itclatam.com / tss@itclatam.com REV 1.01



<u>Home</u>

<u>Home</u>

| Minnaaft Antina | Disseters | Cadificate Canings | kal 2010 CED//ED2I/9 CA |
|-----------------|-----------|----------------------|-------------------------|
| whereson Active | Directory | Certificate Services | nal-2010-SERVER2NO-UA |

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 <u>Active Directory</u> <u>Certificate Services Documentation</u>.

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

| Microsoft Active Director | v Certificate Services | hal/2010.SERV/ER2k8.CA |
|---------------------------|------------------------|------------------------|
| whereson Active Director | y Certificate Services | TIAI-2010-SERVERZNO-CA |

Request a Certificate

Select the certificate type: User Certificate

Or, submit an advanced certificate request.



| | ſ |
|---|---|
| SONIC WALL ® Knowledge Database | |

| Microsoft Active | Directory Cel × |
|---|---|
| ← → C 🖹 | ://10.10.10.254/certsrv/certrqxt.asp 🖒 🖹 |
| Microsoft Active [| Directory Certificate Services hal-2010-SERVER2k8-CA |
| Submit a Certi | ficate Request or Renewal Request |
| To submit a sav certificate reque (such as a Web | ed request to the CA, paste a base-64-encoded CMC or PKCS #10 est or PKCS #7 renewal request generated by an external source server) in the Saved Request box. |
| Saved Request: | |
| Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7): | BEGIN CERTIFICATE REQUEST MIIBvDCCASUCAQAwUDELMAkGA1UEBhMCSU4xCzAJ EwNCTFIxDTALBgNVBAoTBFNOVOwxFzAVBgNVBAHT MAOGCSqGSIb3DQEBAQUAA4GNADCB1QKBgQD00ZQJ XoAAkenaoA6qk2LkJHtMXJF71I/x6MuxNEKK1h/+ 6WaM8aP3Tsox19MeYI3DHqrGnE3csfQlIwrqgP1S▼ |
| Certificate Templ | ate: |
| | Administrator |
| Additional Attribu | ıtes: |
| Attributes: | san:dns=hal-2010.local |
| | Submit > |
| - | |





| ★ ★ C | Microsoft Active | Directory Ce: × | |
|---|---|---|------------------|
| Microsoft Active Directory Certificate Services - hal-2010-SERVER248-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 To submit a saved request to the Saved Request box. Saved Request: Base-64-encoded ITLIBV0CCASUCAQUEDLANKOATUEBHKSU4XCEAU Eventificate request ITLIBV0CCASUCAQUEDLANKOATUEBHKSU4XCEAU Eventificate request ITLIBV0CCASUCAQUEDLANKOATUEBHKSU4XCEAU Eventificate request ItLIBV0CCASUCAQUEDLANKOATUEBHKSU4XCEAU FKCS #7): ItLIBV0CCASUCAQUEDLANKOATUEBHKSU4XCEAU Eventificate request ItLIBV0CCASUCAQUEDLANCEAUXERSU4XCEAU Additional Attributes: ItLIBV0CCASUCAQUEAUGHANCEAUXERSUF171XCMUERKIAU++ Additional Attributes: ItLIBV0CCASUCAQUEAUGHANCEAUXERSUF171XCMUERKIAU++ Attributes: ItLIBV0CCASUCAQUEAUXERSUF711XCMUERKIAU++ Submit > Submit > Microsoft Active Directory Ce × Submit > Microsoft Active Directory Ce × ItLIBV0CSECS + hal-2010-SERVER2K8-CA Microsoft Active Directory Certificate Services - hal-2010-SERVER2K8-CA Home Certificate Issued The certificate Issued The certificate up ou requested was issued to you. © DER encoded or Base 64 encoded < | ← → C 🖹 | ://10.10.10.254/certsrv/certrqxt.asp | ☆ = |
| 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 Intribuctor Castocolave Distances Received Intribuctor Succolave Distances Veb server) in the Saved Request box. Saved Request: Base-64-encoded Intribuctor Succolave Distances Record Advector Distances Additional Attributes: Intribuctor Intribuctor Intribuctor Additional Attributes: Intribuctor Ce × Intribuctor Intribuctor Intribuctor Intribuctor Intribuctor Intribuctor Intributor Intrintributor < | Microsoft Active [| Directory Certificate Services hal-2010-SERVER2K8-CA | Home |
| 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. Swed Request Base-64-encoded certificate request MILTEXPOCASUCAQUEDELINACAIUEBINCSU4xCEAT EVENCTFIXPTALBGNVBAOTEFINOVOUXFEXVBJRVBATT FWCS #00 or PKCS #00 or PKCS #10 or PKCS #10 or PKCS #00 PKCS #00 or PKCS #00 or PKCS #10 BBg1/2010.10cal FWG/S #70: Submit > Certificate Template: Attributes: Submit > Microsoft Active Directory Ce × EVENCES #00 or PKCS #00.10.254/certsrv/certfinsh.asp Microsoft Active Directory Certificate Services - hal-2010-SERVER2kB-CA Home Certificate Issued The certificate Issued The certificate sysue requested was issued to you. © DER encoded or © Base 64 encoded Download certificate Download certificate chain | Submit a Certi | ficate Request or Renewal Request | |
| Saved Request: Base 64-encoded certificate remptate: Exercise Tip | To submit a sav certificate reque (such as a Web | ed request to the CA, paste a base-64-encoded CMC or Plest or PKCS #7 renewal request generated by an external so server) in the Saved Request box. | (CS #10 ource |
| Base-64-encoded certificate request (CMC or PKCS #7): | Saved Request: | | |
| Certificate Template: Additional Attributes: Attributes: Attributes: Submit > Submit > Microsoft Active Directory Ce: × Microsoft Active Directory Ce: × Microsoft Active Directory Ce: × Microsoft Active Directory Ce: × Microsoft Active Directory Ce: × Microsoft Active Directory Ce: × Microsoft Active Directory Ce: × Microsoft Active Directory Ce: × Microsoft Active Directory Certificate Services hal-2010-SERVER2K8-CA Home Certificate Issued /li> | Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7): | HIIBvDCCASUCAQAwUDELMAkGA1UEBhMCSU4xCzAJ EWNCTFIxDTALBgNUBAOTBFNOVOwxFzAVBgNVBAHT MAOGCSqGSIb3DQEBAQUAAGNADCB1QKBgQDOOZQJ XoAAkenaoA6qk2LkJHtMXJF71I/x6MuxNEKK1h/+ 6WaM8aP3Tsox19MeYI3DHqrGnE3csfQlIwrqgP1S | |
| Administrator Additional Attributes: Attributes: Submit > Submit > Submit > Microsoft Active Directory Ce: × Submit > Submit > Submit > Microsoft Active Directory Ce: × Submit > Subm | Certificate Templ | ate: | |
| Additional Attributes: Attributes: Image: | | Administrator | |
| Attributes: Image: | Additional Attribu | tes: | |
| Submit > Image: Submit > | Attributes: | san:email=&dminghal-2010.local | - 1 |
| Microsoft Active Directory Ce: × ← → C Microsoft Active Directory Certificate Services hal-2010-SERVER2K8-CA Home 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 ○ Dertificate Certificate Download certificate Chain | | Submit > | - 1 |
| Microsoft Active Directory Ce: × ← → C Microsoft Active Directory Certificate Services hal-2010-SERVER2k8-CA Home 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 chain | _ | | |
| ← → C 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 | Microsoft Activ | e Directory Cei × | |
| Microsoft Active Directory Certificate Services hal-2010-SERVER2K8-CA Home Certificate Issued Image: Certificate Services hal-2010-SERVER2K8-CA Home The certificate Issued Image: Certificate Services hal-2010-SERVER2K8-CA Home The certificate Issued Image: Certificate Services hal-2010-SERVER2K8-CA Home Image: Certificate Issued Image: Certificate Services hal-2010-SERVER2K8-CA Home Image: Certificate you requested was issued to you. Image: Certificate Services hal-2010-SERVER2K8-CA Image: Certificate Services hal-2010-SERVER2K8-CA Image: Observe the certificate Services hal-2010-SERVER2K8-CA Image: Certificate Services hal-2010-SERVER2K8-CA Home Image: Observe the certificate Services hal-2010-SERVER2K8-CA Image: Certificate Services hal-2010-SERVER2K8-CA Home Image: Observe the certificate Certificat | ← → C | thes://10.10.10.254/certsrv/certfinsh.asp | £3 ≣ |
| Certificate Issued The certificate you requested was issued to you. © DER encoded or © Base 64 encoded Download certificate Download certificate chain | Microsoft Active | Directory Certificate Services hal-2010-SERVER2K8-CA | Home |
| The certificate you requested was issued to you. © DER encoded or © Base 64 encoded Download certificate Download certificate chain | Certificate Iss | sued | |
| DER encoded or OBase 64 encoded Download certificate Download certificate chain | The certificate | you requested was issued to you | |
| Der encoded or OBase 64 encoded | | | |
| | Do Do | DER encoded or OBase 64 encoded wnload certificate wnload certificate chain | |
| | _ | | |

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





| rtificate General Details Certification Path | 1 | 2 |
|---|----------------------------------|---|
| Show: <all></all> | • | |
| Field | Value 🔺 | 1 |
| Subject Alternative Name | DNS Name=hal-2010.loca | 1 |
| Subject Key Identifier | c4 bc 32 63 9b b7 4c c0 65 c4 | |
| authority Key Identifier | KeyID=93 65 16 ff b2 72 b5 7 | |
| CRL Distribution Points | [1]CRL Distribution Point: Distr | 1 |
| Authority Information Access | [1]Authority Info Access: Acc | |
| Certificate Template Name | Administrator | 1 |
| Enhanced Key Usage | Microsoft Trust List Signing (1 | |
| | | 1 |
| DNS Name=hal-2010.local ◄ | | |
| Ec Learn more about <u>certificate details</u> | lit Properties Copy to File | |
| | ОК | |

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.





<u>ne</u>

| Microsoft Active Director | y Certificate Services | hal-2010-SERVER2K8- | Ha |
|---------------------------|------------------------|---------------------|--|
| ^ * | | | <u><u><u></u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u> |

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 | <u>Home</u> |
|---|-------------|
| 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: | |
| 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.

| 🕨 🔛 Dashboard | 2 | System / | | | | | | |
|-----------------------|---|-------------|--------------------|---|--------------|---------|--------------------------------|--------------------------------|
| 🗢 🚍 System | | Certifi | cates | | | | | |
| Status | | | | | | | | |
| Licenses | | Certificate | s and Certificate | Requests | | | | Items 1 to |
| Administration | | | | | | | | |
| Certificates | 1 | View Style: | C All certificates | Imported certificates | s and reques | sОв | uilt-in certificates | Include expired |
| Time | | □ # C | ertificate | Туре | Validated | Expires | | Details |
| Schedules Settings | - | 🗆 1 V | VAN GroupVPN | Pending request | | | Click on the blue signed co | e icon to upload ertificate |

| Opload Certificate - Google Chron | ne 🗕 🗆 🗙 |
|--|---|
| אייל //10.10.10.1/certSignUpload.ht | m |
| Upload Signed Certificate for S | igning Request |
| Name: | WAN GroupVPM |
| 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: Choos File should | d be PEM (.pem) or DER (.der or .cer) encoded |
| Ready | |
| | Upload Cancel |

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





| | | Mode: Con |
|----------------|---|-----------------------|
| 🕨 🚾 Dashboard | System / | |
| 🕶 💻 System | Certificates | |
| Status | | |
| Licenses | Certificates and Certificate Requests | Items 1 to 1 (of 1) |
| Administration | | |
| Certificates | View Style: ^O All certificates ^O Imported certificates and requests ^O Built-In | Include expired built |
| Time | certificates | - |
| Schedules | 🗐 # Certificate Type Validated Expires | Details |
| Settings | 1 WAN Group VPN Local certificate No Oct 11 10:25:12 2013 GMT | ø |
| Packet Monitor | | |
| Diagnostics | Import | D |
| Restart | | |
| 0 | * | |

| Import Certificate | |
|---|---|
| C Import a local end-user certificate w | vith 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 |
| _ | |







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=<localpart@domain.com|. <u>Note</u>: 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.





| Microsoft Active Directory Cel × |
|---|
| ← → C (*) 10.10.10.254/certsrv/ ← ☆ Ξ |
| 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 <u>Active Directory</u> 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 Cel × | |
|---|-------------|
| ← → C (Lips://10.10.10.254/certsrv/certrqus.asp | ☆ ≡ |
| Microsoft Active Directory Certificate Services hal-2010-SERVER2K8-CA | <u>Home</u> |
| Request a Certificate | |
| Select the certificate type: User Certificate | |
| Or, submit an advanced certificate request. | |
| | |

| Certificate Template: |
|--|
| User |
| Key Options: |
| Create new key set C Use existing key set |
| CSP: Microsoft Enhanced Cryptographic Provider v1.0 |
| Key Usage: @ Exchange |
| Key Size: 1024 Min: 384 (common key sizes: 512 1024 2048 4096 8192 16384) |
| Automatic key container name C 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 |
| san:dns=hal-2010.local |
| Attributes: |
| |
| |
| Submit > |





| Contificate locued | |
|---|--|
| | |
| he certificate you requested was issued to you. | |
| Install this certificate | |
| □ Save response | |
| | |

The signed certificate will be installed within the browser.

| Heroson Active Direct | | INTE |
|-----------------------|----------------------------------|------|
| ertificate Installed | 1 | |
| our new certificate | has been successfully installed. | |
| | | |

Export the certificate with its private key from the browser.





| General Security Privacy Content Connect Parental Controls Control the Internet content that car be viewed. Content Advisor | ons Programs Advar | Certificates Intended purpose: <ai> Personal Other People Intermediate C Issued To Issued By</ai> | Certification Authorities Truste | ed Root Certification |
|--|----------------------------------|--|----------------------------------|--|
| Certificates Use certificates for encrypted connection | content that can be | Total and the second se | RVER2K8 10-10-2013 · | <none></none> |
| Clear SSL state Certificates AutoComplete AutoComplete stores previous entrie on webpages and suggests matches for you. Feeds and Web Slices Feeds and Web Slices provide update content from websites that can be read in Internet Explorer and other programs. | Publishers s Settings d Settings | Import Export Rer Certificate intended purposes Encrypting File System, Secure Email, Cl Learn more about <u>certificates</u> | | Welcome to Wizard This wizard helps lists and certificat store to your disk A certificate, whit a confirmation of used to protect d connections. A ce certificates are ke To continue, click |
| ок | Cancel App | 9 | | |





| You can choose to export the p | rivate key with the certificate. |
|--|--|
| Private keys are password prot certificate, you must type a pas | ected. If you want to export the private key with the ssword on a later page. |
| Do you want to export the priva | ate key with the certificate? |
| Yes, export the private | key . |
| C No, do not export the p | private key |
| arn more about <u>exporting private l</u> | keys |
| | |





| xport File Format Certificates can be exported in a | a variety of file formats. |
|--|---|
| Select the format you want to u | se: |
| C DER encoded binary X-50 | 09 (.CER) |
| C Base-64 encoded X.509 (| (.CER) |
| C Cryptographic Message S | Syntax Standard - PKC5 #7 Certificates (.P78) |
| 📕 Include all certificates | s in the certification path if possible |
| Personal Information Exc | change - PKCS #12 (.PFX) |
| Include all certificates | s in the certification path if possible |
| Delete the private ke | y if the export is successful |
| Export all extended p | properties |
| C Mcrosoft Senaized Certi | ficate Store (.SST) |
| earn more about <u>certificate file form</u> | ats |
| | < Back Next > Cancel |

| File name: | | | |
|-------------------|------------------|--------|--------|
| C:\Users\Test\Des | ktop\GVC-User-Ce | rt.pf× | Browse |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |





| | Completing the Certificate E Wizard You have successfully completed the Certificate | Export |
|---|---|---------|
| 10 m | wizard. | |
| - | File Name | C:\User |
| File Name Export Keys Include all certifi | Export Keys | Yes |
| | Include all certificates in the certification path | Yes |
| | File Format | Person |
| | | |
| | • | • |
| | | |
| | | |
| | | |
| | | |
| | | C |

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: <u>How to configure a CA to accept a SAN attribute from a certificate request</u>

- 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.**





| Updates | Certificates and Certificate Requests |
|--------------------|--|
| Licenses | |
| Firmware & Backups | View Style: |
| WXA Firmware | # Certificate |
| Restart | |
| Connectivity | 1 www.pourdomain.com |
| VPN | 2 Sonicival |
| SSL VPN | 3 SeniciValCA |
| SonicPoints | |
| 3G/4G/Hodem | IMPORT NEW SIGNING REQUEST SCEP DELETE |
| | |
| Policies | |
| Rules | |
| Objects | |
| Sustan Salua | |
| system setup | |
| Appliance | |
| Base Settings | |
| SNPP | |
| Cethcates | |
| System Time | |
| system schedules | |

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. | | WANGroupVPN | | | | |
|--|------|------------------------------------|----------|--|--|--|
| Country • | | INDIA (IN) | • | | | |
| State • | | KA | | | | |
| Locality, City, or County 🔻 | | BLR | | | | |
| Company or Organization 🔻 | | SNWL | | | | |
| Department | ٠ | | | | | |
| Group | ٠ | | | | | |
| Team | ٠ | | | | | |
| Common Name 🔹 | | hal-2010.local | | | | |
| Subject Distinguished Name: Subject Alternative Name (Option: | al): | C=IN;ST=KA;L=BLR;O=SNWL;CN=hal-201 | 10.local | | | |
| Domain Name | ٠ | | | | | |
| Signature algorithm: | | SHA256 T | | | | |
| Subject Key Type: | | RSA 🔻 | | | | |
| Subject Key Size/Curve: | | 1024 bits * | | | | |
| | | | | | | |
| lv . | | | | | | |





Click on the download button to download the CSR.

| Style: 🔍 All certificates 🕷 Seported certificates and requests 🔍 Bult-In certificates | U Defade - | expired built-in | n certificates | | |
|---|-----------------|------------------|--------------------------|----------|-----------|
| Cartoficate | Tops | Validational | Expline | Ortaile. | Configure |
| ene perforation | Pandrog regulat | | | \$2 | |
| I INAG-ANA | Panding regulat | | | 57 | |
| 1 Second | Local cardinate | 144 | Aug 18 38:08:00 2018 GHT | 12 | 0.0 |



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 <u>Active Directory</u> 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 | <u>Home</u> |
|---|-------------|
| Request a Certificate | |
| Select the certificate type: User Certificate | |
| Or, submit an advanced certificate request. | |

| Microsoft Active I | Directory Cel × | | |
|---|---|--|-----------------------------|
| ← → C 🖹 | ://10.10.10.254/certsr | //certrqxt.asp | ☆ = |
| Microsoft Active D | Directory Certificate Services | hal-2010-SERVER2K8-CA | <u>Home</u> |
| Submit a Certi | icate Request or Renew | val Request | |
| To submit a sav certificate reque (such as a Web | ed request to the CA, pas st or PKCS #7 renewal re server) in the Saved Requ | te a base-64-encoded CM equest generated by an exte lest box. | C or PKCS #10 mal source |
| Saved Request: | | | |
| Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7): | BEGIN CERTIFICAT NIIBvDCCASUCAQAvUDELM EwNCTFIxDTALBgNVBAoTB NADGCSqGSIb3DQEBAQUAA XoAAkenaoA6qk2LkJHtMX 6WaM8aP3Tsox19MeYI3DH | E REQUEST AkGA1UEBhMCSU4xCzAJ FNOVOwxFzAVBgNVBAHT 4GNADCB1QKBgQD002Qj JF71I/x6MuxNEKK1h/+ qrGnE3csfQ1IwrqgP15 | |
| Certificate Templ | ate: | | |
| | Administrator 🔶 | • | |
| Additional Attribu | tes: | | |
| Attributes: | san:dns=hal-2010.loca | | |
| | | Submit > | |





| + > C . | ://10.10.10.254/certsrv/certroxt.asp | \$ |
|---|--|-------------------------|
| Microsoft Action 1 | New York Carliers Carless Int 2010 CER EDUC CA | |
| MICROSON ACTIVE L | Arectory Centricate Services hai-2010-SERVER2Rd-CA | nom |
| Submit a Certi | icate Request or Renewal Request | |
| To submit a sav certificate reque (such as a Web | ed request to the CA, paste a base-64-encoded CMC or st or PKCS #7 renewal request generated by an externa server) in the Saved Request box. | r PKCS #10 Il source |
| Saved Request: | | |
| Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7): | BEGIN CERTIFICATE REQUEST MIIBVDCCASUCAQAWUDELMAKGA1UEBhMCSU4xCzAJ EWNCTFIxDTALBgNVBAoTBFNOVOwxFzAVBgNVBAHT MAOGCSqGSIb3DQEBAQUAA4GNADCB1QKBgQD00ZQj XoAAkenaoA6qk2LkJHtMXJF71I/x6MuxNEKK1h/+ 6WaM8aP3Tsox19MeYI3DHqrGnE3csfQlIwrqgP1S | |
| Certificate Templ | ate: | |
| | Administrator | |
| | | |
| Additional Attribu | tes: | |
| Attributes: | san:email=Admin8hal-2010.local | |
| | | |
| | Submit > | |
| | | |
| | | |
| Microsoft Active Direc | tory Cei × | |
| ⇒ C akh# | ://10.10.10.254/certsrv/certfinsh.asp | 52 |
| | | ~ |
| rosoft Active Dire | ctory Certificate Services hal-2010-SERVER2K8-CA | H |
| | | |
| tificate Issued | | |
| certificate vou | requested was issued to you. | |
| | | |
| • DER | encoded or CBase 64 encoded | |
| Downlo | ad certificate | |
| Downlo | ad cortificato chain | |





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

| ertificato General | e Details Certification Path | |
|---|---|---|
| Show: | <all></all> | • |
| Field Sul Sul CR CR CR CR CR CR CR SM SM CR SM SM SM SM SM SM SM SM SM SM | Ibject Alternative Name bject Key Identifier thority Key Identifier L Distribution Points thority Information Access rtificate Template Name hanced Key Usage IME Capabilities | Value DNS Name=hal-2010.loca c4 bc 32 63 9b b7 4c c0 65 c4 KeyID=93 65 16 ff b2 72 b5 7 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc Administrator Microsoft Trust List Signing (1 [1]SMIME Capability: Object I |
| Learn m | Ed | it Properties Copy to File |

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

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-SERVER2H8-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: | |
| Encoding method: © DER © Rece 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.





Dama is to 4 (of 4) minimum

Certificates and Certificate Requests

| = 24 | (e: O Al certificates # Imported certificates and requests O Built-in certificates | ade expired built-in certificates | | | | | |
|------|--|-----------------------------------|-----------|--------------------------|---------|-----|-------|
| | Cestilizate | Type | Validated | Expres | Details | Car | Agure |
| 8 | seus pardonan con | Pending request | | | 97 | | |
| 2 | NAG-set M | Pending request | | | 57 | | |
| 3 | teenal | Local certificate | Tex | Aug 16 18 08 00 2018 GHT | 0 | 8 | 1 |

| Image: WAW Group VPW 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 | 🦻 Upload Certificate - Google Chrome | | | х |
|---|--|---|--|---|
| Upload Signed Certificate for Signing Request Name: WAW Group VPW 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: Choose File Certnew.Cer File should be PEM (.pem) or DER (.der or .cer) encoded Ready Image: Color of the should be PEM (.pem) or DER (.der or .cer) encoded | איז און איז | | | |
| Name: WAW Group VPW 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: Choose File Certnew.cer File should be PEM (.pem) or DER (.der or .cer) encoded Ready Ready | Upload Signed Certificate for Signi | ng Request | | |
| Please select a file to upload: Choose File certnew.cer File should be PEM (.pem) or DER (.der or .cer) encoded Ready | Name: Subject Distinguished Name: Subject Key Identifier: Status: | WAN Group VPN C=IN;ST=KA;L=BLR;O=SNWL;CN=hal-2010.local 0x930493642C9CB76D955064506F002BC4403E32C7 Request Generated | | |
| | Please select a file to upload: Choose File File should be Pl Ready | e certnew.cer EM (.pem) or DER (.der or .cer) encoded | | |

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

| # Certificate | | Tape | Validated | Expires |
|-------------------------------------|--|-------------------|-----------|-------------------------|
| 1 voncytorfaman.com | | Pending request | | |
| 2 WANGrouph/M | 🖝 Import Cestificate - Google Dhome - 🗆 X | Pending request | | |
| 3 Sevential | A Not secure begt//10.61.130.57/certileport.itml | Local certificate | Tes | Aug 18 18:08:00 2018 GP |
| DRITORY NEW SIGNING REQUEST SCEP DO | SONICWALL Network Security Appliance Import Certificate Import a local end-user certificate with private key from a PKCD#12 (p12 or ph) encoded file Import a CA certificate from a PKCD#7 (p7b). PDM (pen) or DDR (der or cer) encoded file Certificate Name: Certificate Name: Certificate Name: Choose File, No file chosen Ready | | | |





| C Import a local end-user certifica | te with private key from a PKCS#12 (.p12 or .pfx) encoded file |
|-------------------------------------|--|
| Import a CA certificate from a P | KCS#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 |

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=<localpart@domain.com]. <u>Note</u>: 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.





| Microsoft Active Directory Cei × |
|---|
| ← → C (> bups://10.10.10.254/certsrv/ ← ☆ Ξ |
| Microsoft Active Directory Certificate Services hal-2010-SERVER2K8-CA |
| 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 <u>Active Directory</u> <u>Certificate Services Documentation</u> . |
| Select a task: Request a certificate <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u> |







| Certificate Template: |
|---|
| User |
| Key Options: |
| Create new key set CSP: Microsoft Enhanced Cryptographic Provider v1.0 ▼ Key Usage: Exchange Key Size: 1024 Min: 384 (common key sizes: 512 1024 2048 4096 8192 16384) Automatic key container name C User specified key container name Mark keys as exportable ▲ Enable strong private key protection |
| Additional Options: |
| Request Format: CMC CPKCS10 |
| Hash Algorithm: sha1 Only used to sign request. |
| □ Save request |
| Attributes: |
| Friendly Name: |
| Submit > |



ITCorporation® Visit our Website: www.itclatam.com



The signed certificate will be installed within the browser.

| Microsoft Active Directory Certificate Services - hal-2010-SERVER2K8-CA | <u>Home</u> | * |
|---|-------------|---|
| Certificate Installed | | |
| Your new certificate has been successfully installed. | | |
| | | Ŧ |

Export the certificate with its private key from the browser.

| Parental Controls Control the Internet content that can Parental Control be viewed. | tended purpose: <pre>C<all> Personal Other People Intermediate Certification Authorities</all></pre> | Trusted Root Certification |
|--|--|--|
| Content Advisor Ratings help you control the Internet content that can be viewed on this computer. Content Advisor Ratings help you control the Internet content that can be viewed on this computer. Set Enable | Issued To Issued By Expiratio | II 3 «None> |
| Use certificates for encrypted connections and identification. Clear SSL state Certificates Publishers AutoComplete AutoComplete stores previous entries Settings | Certificate Export Wi | Welcome to the Certificate Export Wizard |
| for you. ieeds and Web Sikes provide updated content from websites that can be read in Internet Explorer and other programs. | Certificate intended purposes Encrypting File System, Secure Email, Cl | Its's and certificate revocation lists from a certificate store to your diak. A certificate, which is issued by a certification authority, i a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. |
| OK Cancel Acply | earn more about <u>certificates</u> | To continue, click Next. |
| | | |





| Export Private Key You can choose to export the p | private key with the ce | rtificate. | |
|--|--|------------------|-----------------|
| Private keys are password pro certificate, you must type a pa | tected. If you want to issword on a later pag | export the priva | te key with the |
| Do you want to export the priv | vate key with the certif | icate? | |
| Yes, export the private | e key | | |
| C No, do not export the | private key | | |
| Learn more about <u>exporting private</u> | thems | | |
| | | 2 | |

| ertifica | ite Export Wizard | × |
|----------|---|---|
| Espor | rt File Format Certificates can be exported in a variety of file formats. | |
| 5 | ielect the format you want to use: | |
| | C DER encoded binary X.509 (.GER) | |
| | C Base-64 encoded X.509 (JCER) | |
| | Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P78) 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 | |
| | C Mcrosoft Serielzed Certificate Store (:SST) | |
| Learn | more about certificate file formats | |





| le to Export | | |
|---|-----------|--------|
| Specify the name of the file you want t | to export | |
| File name: | | |
| C:\Users\Test\Desktop\GVC-User-Cer | t.pf× | Browse |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| <u>_</u> | You have specified the following settings: | Export |
|----------|---|---------------------------------|
| | File Name Export Keys Include all certificates in the certification path File Format | C:\User Yes Yes Person |
| | <u>د</u> | 2 |



Calle 146 #7-64. Bogotá D.C. Colombia +57 1 466 0599 / +57 315 786 8258 sales@itclatam.com / tss@itclatam.com REV 1.01