OCS TLS Configuration Guide

Overview

This guide will show you how to configure TLS of your NetBorder Express gateway to work with Microsoft Office Communicator (OCS).

You will find that this guide has several pages but this does not mean it is a highly complex process. Rather, we have included several screen-shots to guide you through the process.

Tools and pre-Requisites

1. Installed version of **NetBorder Express**
2. Installed version of **Microsoft Active Directory Certificate Services (required to sign digital certificate).**

Configuring SIP/TLS/SRTP

When confidentiality is required, the gateway exchanges SIP messages with the Mediation Server using a TLS transport and audio data using a SRTP transport.

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. The protocol TLSv1.2 is described in RFC5246.

The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the audio data carried by a RTP stream. The SRTP protocol is described in RFC3711 .

Here are the steps to follow to configure the gateway and the Mediation Server to use TLS transport.

1. Obtain digital certificate information
2. Configure the gateway to enable SIP/TLS
3. Configure the gateway digital certificate information
4. Configure the gateway to use the right cipher suite
5. Configure the gateway to use the right SSL version
6. Configure the gateway routing rules to make use the SIP/TLS user agent
7. Configure the gateway to enable SRTP
8. Configure the gateway to enable the SIP media forking
9. Configure the Mediation Server Next Hop Connections

Obtain digital certificate information

This section explains how to obtain the digital certificate information to be used by the gateway to identify himself when the gateway communicate with the mediation server and authenticate the mediation server.

Digital certificates are used for:

- Authentication, which verifies the identity of someone or something.
- Privacy, which ensures that information is only available to the intended audience.
- Encryption, which disguises information so that unauthorized readers are unable to decipher it.
- Digital signatures, which provide non-repudiation and message integrity.

To obtain a certificate follow this procedure:

1. Generate a key public/private keys pair and fill the certificate form.
   a) Start and command windows (**cmd.exe**)
   b) Set current folder to **<Netborder Express Install Directory>bin** (example: “c:\Program Files\Netborder\Express\Gateway\bin”).
   c) Run the following command to create the public/private key pair and fill the certificate form.

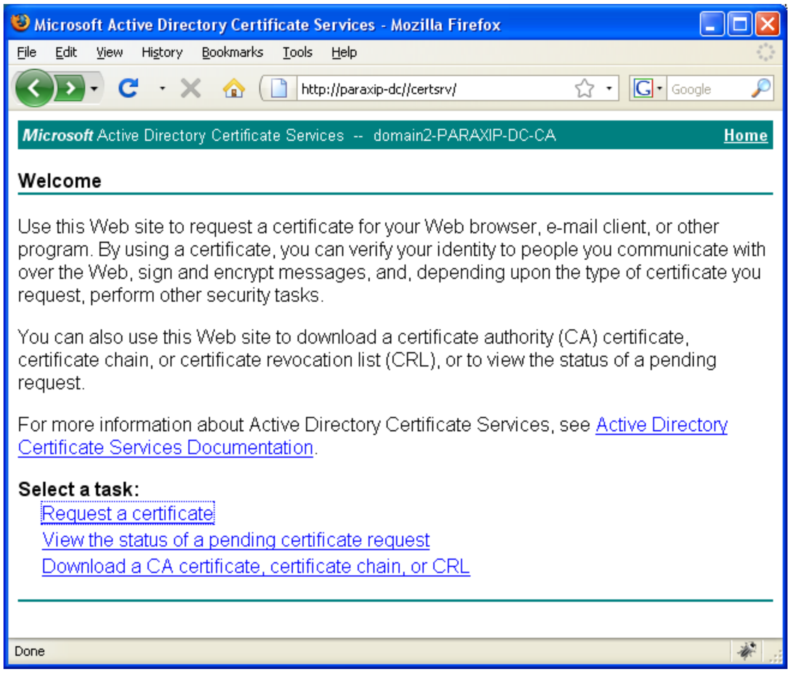
```
netborder-openssl req -newkey rsa:1024 -sha1 -config "../config/certs/openssl.cnf" -keyout
../config/certs/new-private-key.pem -keyform PEM -out ../config/certs/new-certificate-
request.pem -outform PEM
```

   d) Answer to the questions as follow:

```
Enter PEM pass phrase: <enter-a-password-used-to-encrypt-your-private-key>
Verifying - Enter PEM pass phrase: <enter-same-password-as-previous-line>
Country Name (2 letter code) [AU]: <enter-'.'-to-leave-this-field-blank>
State or Province Name (full name) [Some-State]:<enter-'.'-to-leave-this-field-blank>
Locality Name (eg, city) []: <enter-'.'-to-leave-this-field-blank>
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <enter-'.'-to-leave-this-field-
blank>
Organizational Unit Name (eg, section) []: <enter-'.'-to-leave-this-field-blank>
Common Name (eg, YOUR name) []: <enter-FQN-of-the-server-where-the-gateway-will-run>
Email Address []: <enter-'.'-to-leave-this-field-blank>
A challenge password []: <enter-'.'-to-leave-this-field-blank>
An optional company name []: <enter-'.'-to-leave-this-field-blank>
```

2. **Keep the command windows open**, since it will be required later in this procedure.

3. Using your favourite WEB browser, log-on with the Administrator privileges to the Microsoft Active Directory Certificate Services (http://your-domain-controller//certsrv/) and click on the “Request a certificate” hyperlink.


Microsoft Active Directory Certificate Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://paraxip-dc//certsrv/
Google
Done

Microsoft Active Directory Certificate Services -- domain2-PARAXIP-DC-CA **Home**

Welcome

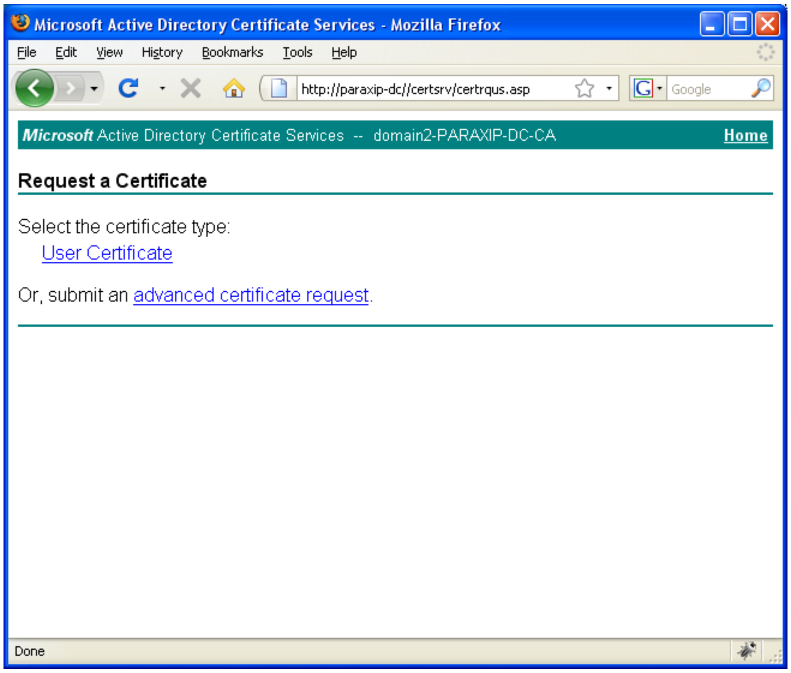
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security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

4. Click on “advanced certificate request”


Microsoft Active Directory Certificate Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://paraxip-dc//certsrv/certrqus.asp
Google
Done

Microsoft Active Directory Certificate Services -- domain2-PARAXIP-DC-CA **Home**

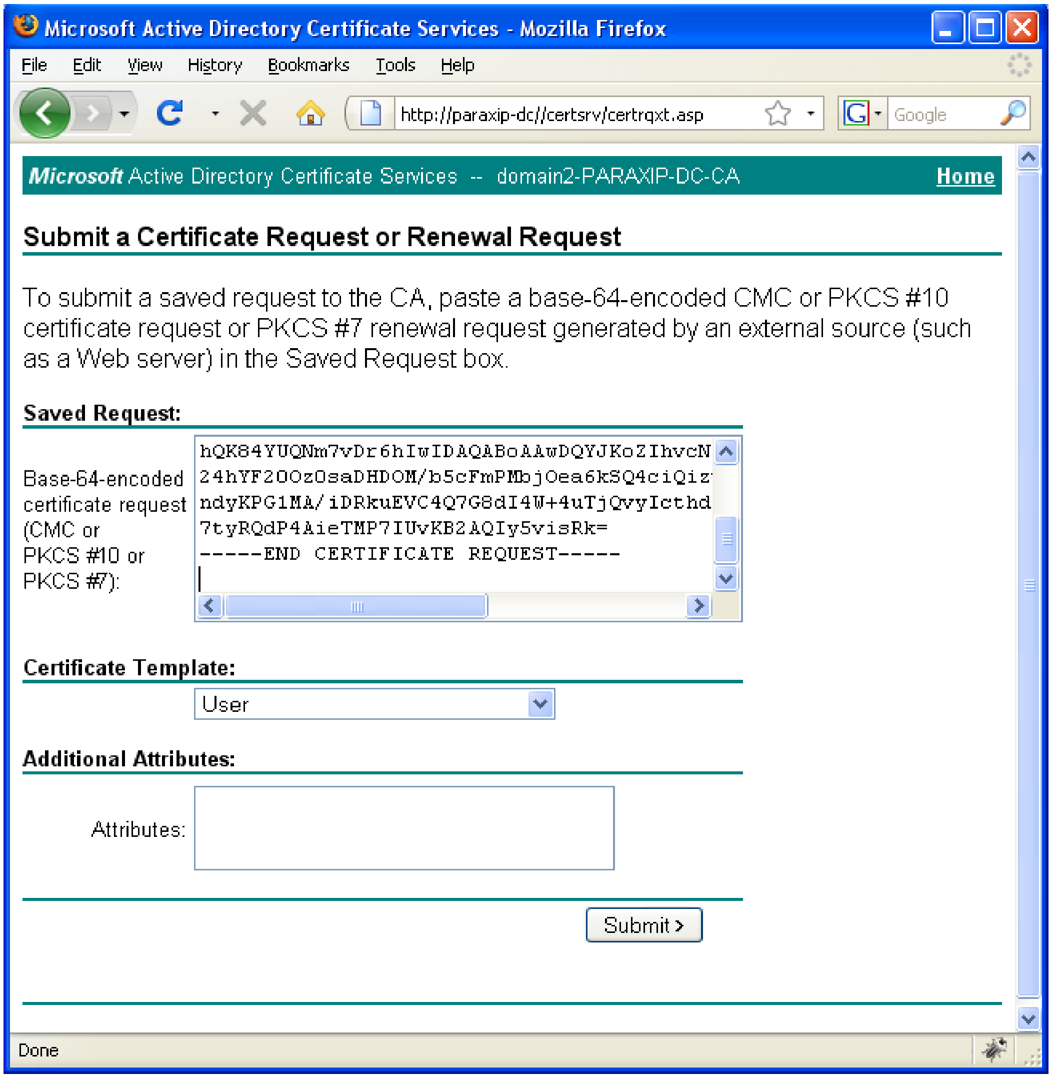
Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

5. With some WEB browsers, Microsoft Active Directory Service will ask if you want to submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file. Select **"base-64-encoded CMC or PKCS #10 file"**.

6. Open the file containing the certificate request generated in step 1 (**<Netborder Express Install Directory>/config/certs/new-certificate-request.pem**) in a text editor such as notepad, copy and paste the whole content of the file in Saved Request text box.


Microsoft Active Directory Certificate Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://paraxip-dc//certsrv/certrqxt.asp
Google
Done

Microsoft Active Directory Certificate Services -- domain2-PARAXIP-DC-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):

```
hQK84YUQNm7vDr6hIwIDAQABoAAwDQYJKoZIhvcN
24hYF2OOzOsaDHDOM/b5cFmPMbjOea6kSQ4ciQiz
ndyKPG1MA/iDRkuEVC4Q7G8dI4W+4uTjQvyIcthd
7tyRQdP4AieTMP7IUvKB2AQIy5visRk=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

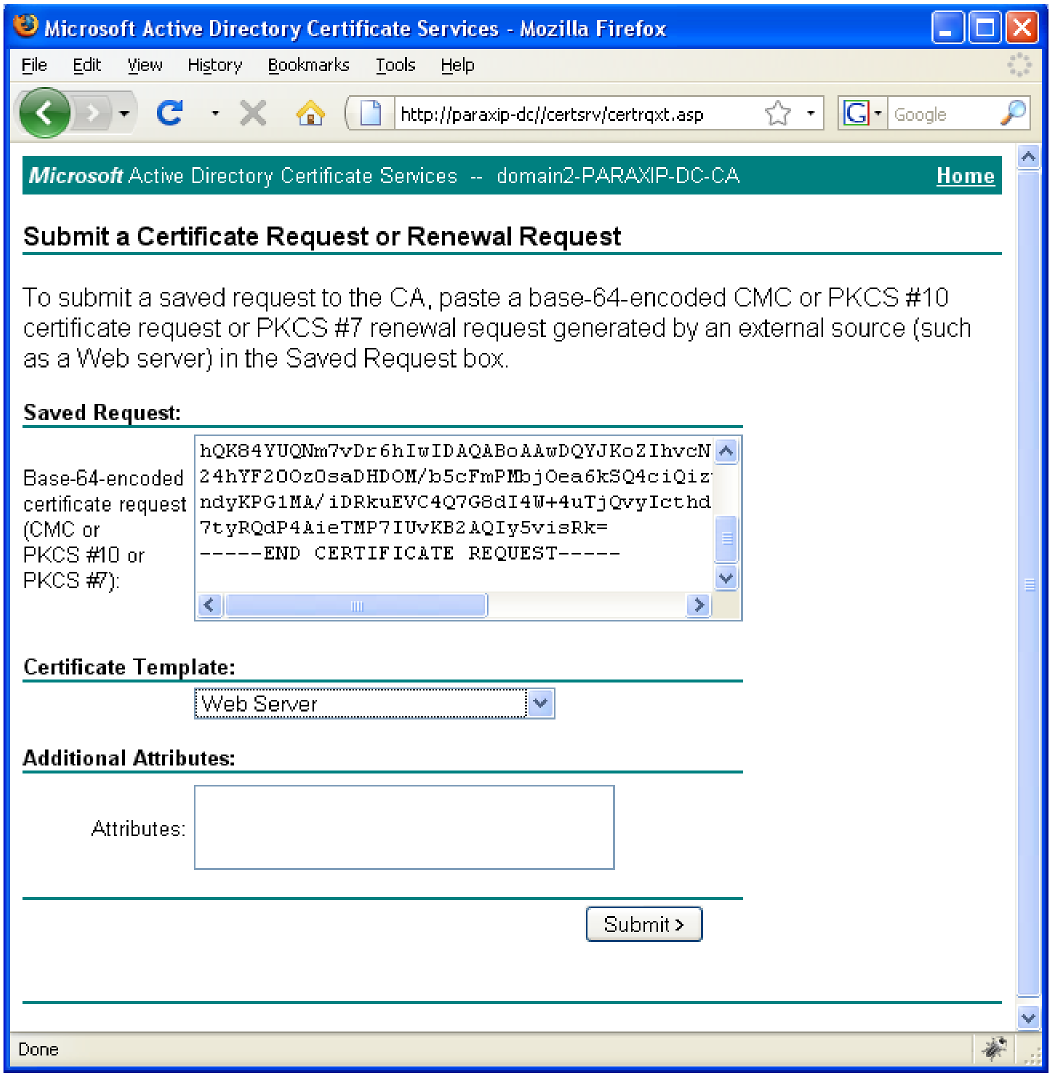
User

Additional Attributes:

Attributes:

Submit >

7. Select the "Web Server" Certificate Template and click on Submit.



Microsoft Active Directory Certificate Services - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://paraxip-dc//certsrv/certrqxt.asp
Google
Done

Microsoft Active Directory Certificate Services -- domain2-PARAXIP-DC-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):

```
hQK84YUQNm7vDr6hIwIDAQABoAAwDQYJKoZIhvcN
24hYF2OOzOsaDHDOM/b5cFmPMbjOea6kSQ4ciQiz
ndyKPG1MA/iDRkuEVC4Q7G8dI4W+4uTjQvyIcthd
7tyRQdP4AieTMP7IUvKB2AQIy5visRk=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

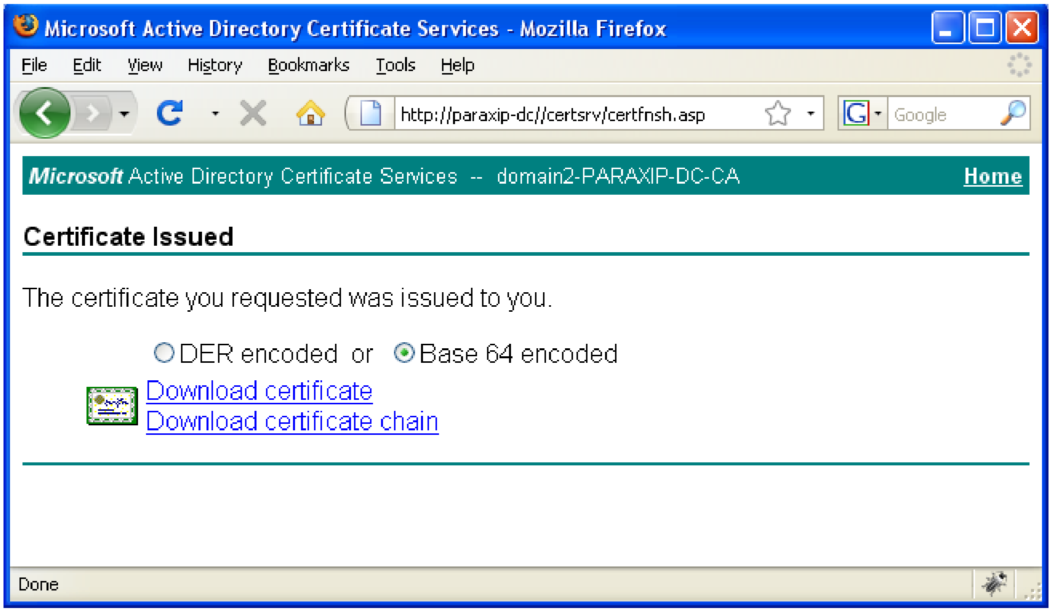
Attributes:

Submit >

8. Select the Base 64 encoded and

   a) Download the certificate and save the file in the folder **<Netborder Express Install Directory>/config/certs**. The default file name is **“certnew.cer”**.

   b) Download the certificate chain and save the file in the folder **<Netborder Express Install Directory>/config/certs**. The default file name is **“certnew.p7b”**.


Microsoft Active Directory Certificate Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://paraxip-dc//certsrv/certfnsh.asp
Google
Done

Microsoft Active Directory Certificate Services -- domain2-PARAXIP-DC-CA **Home**

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

9. In the command windows previously opened, run the following commands to encrypt the private key with the NBE expected password.

```
netborder-protect-key --input-file-pwd <Enter here the pass phrase used to step 1>
../config/certs/new-private-key.pem ../config/certs/new-private-key-protected.pem
```

10. In the same command windows, run the following program to convert the certificate chain to PEM format.

```
netborder-openssl pkcs7 -in ../config/certs/certnew.p7b -out
../config/certs/newTrustedRootCertificatesStore.pem -print_certs -text
```

Configure the gateway to enable SIP/TLS

This section explains how to enable SIP/TLS. By default, the gateway starts a SIP/UDP and a SIP/TCP SIP user agents. To enable SIP/TLS you have to configure the gateway to start SIP/TLS user agent.

To configure the gateway to start the SIP/TLS User Agent that will listen for SIP/TLS requests:

1. Select the **"Netborder Express Gateway>Configuration>Edit global configuration"** from the Windows start menu. This will open the gw.properties file in a text editor.
2. Search for the parameter: **"netborder.sip.userAgent.IPAddress"** and set it to **"INADDR_ANY:5067/tls"**.

> WARNING: For security reasons, it is not recommended to start the gateway with SIP/UDP and SIP/TCP user agents when a SIP/TLS user agent is used.

> NOTE: The gateway does not support to have SIP/TCP and SIP/TLS user agents listening on the same port. Make sure to specify a different port values. For example,
> netborder.sip.userAgent.IPAddress=INADDR_ANY:5066/tcp,INADDR_ANY:5067/tls

3. **Save your modifications**. These modifications will be considered upon next gateway start.

Configure the gateway digital certificate information

The certificate information generated in the section 1 shall be used by the gateway in order to connect successfully with the mediation server.

This section explains how to configure the gateway to use that certificate information.

To configure the gateway certificate information:

1. Select the “Netborder Express Gateway>Configuration>Edit global configuration” from the Windows start menu. This will open the gw.properties file in a text editor.
2. Search for the parameter: **“netborder.sip.tls.serverCertificateFile”** and set it to **“${netborder.Installation.Directory}/config/certs/certnew.cer”**. This parameter sets the file path to the certificate to be used by the gateway during the TLS authentication process. This parameter shall use the certificate that we have generated in the previous section.
3. Search for the parameter: **“netborder.sip.tls.serverCertificatePrivateKeyFile”** and set it to **“${netborder.Installation.Directory}/config/certs/new-private-key-protected.pem”**. This parameter sets the file path to a file containing an encrypted version of the private key used to generate the server certificate. This parameter shall use the private key the that we have generated in the previous section.
4. Search for the parameter: **“netborder.sip.tls.trustedRootCertificatesStore”** and set it to **“${netborder.Installation.Directory}/config/certs/newTrustedRootCertificatesStore.pem”**. This parameter sets the path to a Base64 encoded DER file containing a certificate for each trusted certificate authorities. This parameter shall use the certificate chain downloaded in the previous section.
5. **Save your modifications**. These modifications will be considered upon next gateway start.

Configure the gateway to use the right cipher suite

There are many different algorithms which can be used for encrypting data, and for computing the message authentication code. Some provide the highest levels of security, but require a large amount of computation for encryption and decryption; others are less secure, but provide rapid encryption and decryption. The length of the key used for encryption affects the level of security - the longer the key, the more secure the data.

According to the SIP specification of OCS requirement, the gateway supports the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA (more secure)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (less secure)

By default the gateway will work out of the box with any SIP agents that supports any of these two cipher suite. The gateway always selects the most secure cipher suite during the TLS negotiation procedure.

This section explains how to configure to work with only one cipher suite.

To configure the cipher suite supported by the gateway:

1. Select the **"Netborder Express Gateway>Configuration>Edit global configuration"** from the Windows start menu. This will open the gw.properties file in a text editor.
2. Search for the parameter: **"netborder.sip.tls.cypherSuites"** and set it to your cipher suite flavor. This parameter accept a comma-separated list of cypher suites. Available cypher suites are: TLS_RSA_WITH_AES_128_CBC_SHA (recommended) and TLS_RSA_WITH_3DES_EDE_CBC_SHA (required for backward compatibility).
3. **Save your modifications**. These modifications will be considered upon next gateway start.

Configure the gateway to use the right SSL version

By default the gateway accept only TLSv1 client hello, which is the case of OCS. However, some SIP user agents require SSLv2 Client hello.

To configure the gateway to accept/send SSLv2 Client hello:

1. Select the **“Netborder Express Gateway>Configuration>Edit global configuration”** from the Windows start menu. This will open the gw.properties file in a text editor.
2. Search for the parameter: **“netborder.sip.tls.supportSSLv2ClientHello”** and set it to **“true”**.
3. **Save your modifications**. These modifications will be considered upon next gateway start.

Configure the gateway routing rules to make use the SIP/TLS user agent

This section explains how to configure the gateway to make SIP calls using the TLS transport.

To configure the gateway call the mediation server with SIP/TLS messages:

1. Start the Gateway Manager. **Start menu>Netborder Express Gateway>Gateway Manager.**
2. Select the tab: **Configuration>Routing rules**.
3. Modify existing SIP out routing rules (rules where the outbound_interface is set to “sip”) to:
   a) Send SIP messages to the Mediation Server Gateway listening port (default 5060). Set parameter **"sip.out.requestUri"** to **“sip:%0@<mediation-server-ip-address>:5060”**. Where **<mediation-server-ip-address>** shall be replaced by the IP address of the server where the mediation server is running.

   > Note: The mediation server listens on the same port for SIP/TCP and SIP/TLS (default port 5060).

   b) Use “tls” transport. Set parameter **"sip.out.transport"** to **“tls”**

```
  <rule name="default_sip_out" outbound_interface="sip" qvalue="0.001">
    <condition param="transfer" expr="false"/>
    <condition param="pstn.in.channelName" expr=".*"/>
    <condition param="pstn.in.dnis" expr="(.*)"/>
    <condition param="pstn.in.ani" expr="(.*)"/>
    <condition param="pstn.in.callerName" expr="(.*)"/>
    <out_leg name="" media_type="sendrecv">
      <param name="sip.out.requestUri" expr="sip:%0@mediation-server-ip-address:5060"/>
      <param name="sip.out.from.uri" expr="sip:%1@GW_HOST_IP:GW_SIP_PORT"/>
      <param name="sip.out.from.displayName" expr="%2"/>
      <param name="sip.out.transport" expr="tls"/>
    </out_leg>
  </rule>
```

Configure the gateway to enable SRTP

The gateway provides 3 SRTP modes : “always”, “as-needed” and “never”. The default mode is “as-needed”.

The following table shows how the gateway behaves in each mode when it receives a SDP offer:

Mode	SDP offer with “SRTP Only”	SDP offer with SRTP and RTP	SDP offer with “RTP Only”
always	Use SRTP	Use SRTP	488 (“Unacceptable here” response)
as-needed	Use SRTP	Use SRTP	Use RTP
never	488 (“Unacceptable here” response)	Use RTP	Use RTP

The following table shows how the gateway behaves in each mode when it sends a SDP offer:

Mode	SDP offer
always	Use SRTP only
as-needed	Use SRTP or RTP
never	Use RTP

Also, as for TLS, SRTP has many algorithms for encrypting and authenticating the data of the RTP packets. Some with more security, but needs more computation and some that needs less computation, but are less secure.

The gateway supports two cryptographic suites:

- AES_CM_128_HMAC_SHA1_80 (more secure)
- AES_CM_128_HMAC_SHA1_32 (less secure)

By default the gateway will work out of the box with any SIP agents that supports any of these two crypto suite, prioritizing the first one. OCS will use AES_CM_128_HMAC_SHA1_80.

To change the configuration of the gateway on SRTP support:

1. Select the **“Netborder Express Gateway>Configuration>Edit global configuration”** from the Windows start menu. This will open the gw.properties file in a text editor.
2. Search for the parameter: **“netborder.media.srtp.mode”** and set it to :

   a) “always”: if the gateway only supports SRTP.

   b) “as-needed”: if both SRTP and RTP are supported. SRTP is always preferred.

   c) “never”: if only RTP is supported.
3. Search for the parameter: “**netborder.mdedia.srtp.cryptoSuite**”. This parameter is a comma separated list where the first element has the most priority. Set the parameter to :

   a) “AES_CM_128_HMAC_SHA1_80” if only this crypto suite is supported.

   b) “AES_CM_128_HMAC_SHA1_32” if only this crypto suite is supported.

   c) “AES_CM_128_HMAC_SHA1_80,AES_CM_128_HMAC_SHA1_32” or “AES_CM_128_HMAC_SHA1_32,AES_CM_128_HMAC_SHA1_80” if both crypto suite are supported and the first one has the most priority.
4. **Save your modifications**. These modifications will be considered upon next gateway start.

Configure the gateway to enable the SIP media forking

The SIP media forking is a mean to better manage early media. The SIP media forking is described in RFC3960 .

When the feature is enabled and early media is started for a PSTN to SIP call, the gateway start streaming early media traffic toward the first know RTP source. A RTP is know by the gateway only it received progress SIP message with SDP with the corresponding IP, UDP port and security policies.

WARNING: This feature will not work if the source IP and/or UDP port of the RTP/RTCP packets are different than the values specified in the SDP body of the SIP messages.

Note: When a server has multiple IP interfaces, the RTP/RTCP packets may be send toward the gateway using a different IP address than the one specified in the SDP. The IP interface is selected based the IP routing table. Under Windows you can manager the IP routing table with the command line tool called: route.exe. Consult Windows help to determine how to use this command to create the proper routing entry if needed.

When the feature is disabled, the gateway does not validate the source IP address and UDP port of the RTP/RTCP packets. However, the security policies are applied.

This section explains how to configure the gateway to enable SIP media forking support.

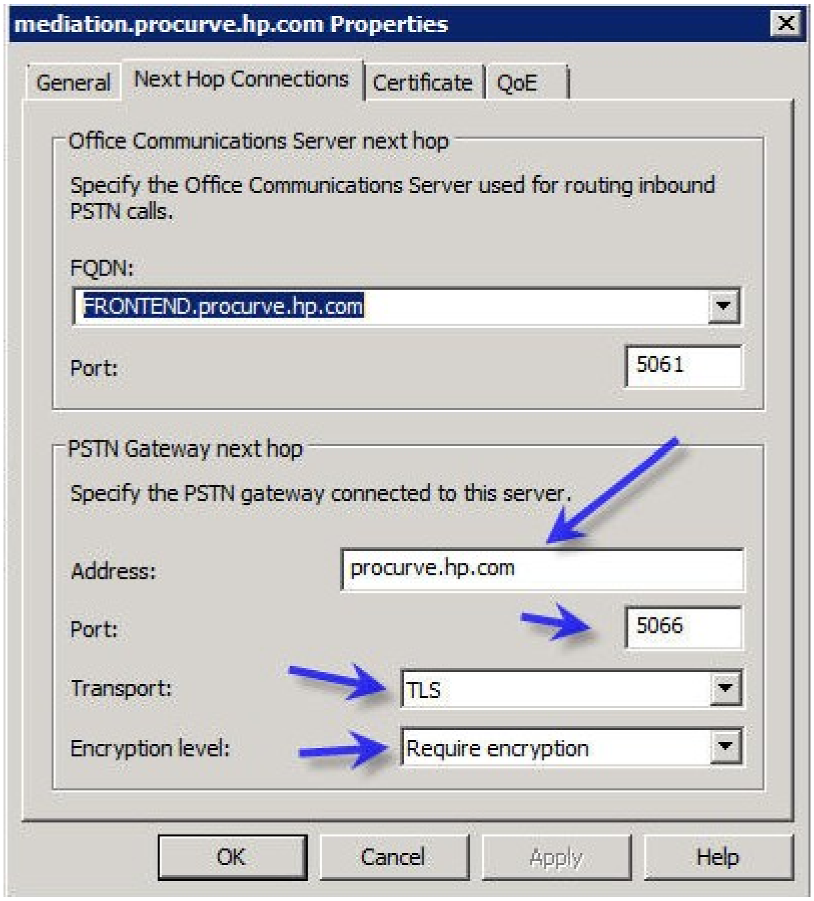
1. Select the **“Netborder Express Gateway>Configuration>Edit global configuration”** from the Windows start menu. This will open the gw.properties file in a text editor.
2. Search for the parameter: **“netborder.media.rtp.lockOnSDP”** and set it to “**true**”.
3. **Save your modifications**. These modifications will be considered upon next gateway start.

Configure the Mediation Server Next Hop Connections

This section explains how to configure the Mediation Server Next Hop Connections.

1. Open the “Microsoft Office Communications Server (2007 R2)”.
2. From the “Microsoft Office Communications Server” Forrest Domain, select your Mediation Server, right click and then click on “Properties”. The figure below should be displayed.
3. Configure the Mediation Server Office Communications Server Next Hop.
4. Configure the PSTN Gateway next hop (the Sangoma Gateway). The Gateway “Address” shall be the gateway FQDN. Be sure to have the exact configuration in the gateway for the Address, Port, Transport and Encryption level (Check the blue arrows).
5. Click OK when done.

Note: the Mediation Server requires a restart when the configuration changes.



Office Communications Server next hop

Specify the Office Communications Server used for routing inbound PSTN calls.

FQDN: FRONTEND.procurve.hp.com

Port: 5061

PSTN Gateway next hop

Specify the PSTN gateway connected to this server.

Address: procurve.hp.com

Port: 5066

Transport: TLS

Encryption level: Require encryption