Configuring SSL and TLS Decryption in nGeniusONE

The configure SSL Decryption feature supports real-time capture of ASI and ASR traffic flows as well as decoding of Secure Socket Link (SSL) and Transport Layer Security (TLS) packet data from your nGenius InfiniStream appliance. This allows you to analyze the packet data from encrypted packets by providing the decryption key. SSL and TLS are protocols that encrypt certain application data for the transport layer using asymmetric cryptography to exchange keys, symmetric encryption to maintain privacy, and message authentication codes to retain message integrity. Some applications that use SSL include:

- HTTP
- Applications using SSL encryption and RSA keys

NetScout supports two methods of Public/Private key usage for real-time SSL/TLS packet decryption and decoding. The Local option enables storage of Public and Private Keys for this purpose. The Hardware Security Module (HSM) option, on the other hand, provides the means for using a Private Key, which is stored in an HSM device, for this purpose. NetScout provides multiple slots with login credentials for each.

Go to Configuration Step 2: for an overview of NetScout's HSM implementation.

Without decrypting the SSL packet itself, NetScout collects ASI data as well as SSL error codes on the HTTPS protocol only. Upon successful decryption, NetScout collects ASI data on HTTP and HTTPS protocols only.

Scenarios where decryption is supported include:

- Resumed SSL sessions
- SSL chunking/fragmentation
- Certificate fragmentation
- Saving decrypted payloads

Scenarios where decryption is *not* supported include:

- Encrypted SSL handshakes
- Out-of-sequence SSL packets
- Retransmitted packets

Additionally, SSL decryption is successfully performed for conversations only when:

- Handshake packets used to establish the conversation have been mined
- Handshake packets include these messages:
    - ClientHello

    - ServerHello
    - ClientKeyExchange
    - ChangeCipherSpec

Supported SSL and key exchange protocols, and Bulk Ciphers

SSL protocol versions supporting packet analysis and decodes are:

- SSL v3.0
- TLS v1.0
- TLS v1.1
- TLS v1.2

Key exchange protocols define how keys are generated and exchanged. Only RSA-type certificates are supported:

- RSA — used for key exchange and authentication protocols only

Supported bulk ciphers are listed below. These encryption algorithms define how data is encrypted on the wire.

- RC4
- DES
- 3DES
- AES

Configuration Step 1: Setting Privileges and Optional Settings

Perform the following tasks:

1. Optional. Locate and extract a private key (in the form of a certificate) from your Tomcat, Apache or Windows lIS Web server and download it to your server (Local option only). Click **here** for instructions.

   Important: when converting a Local Server to a Global Manager, support for Name-IP Address translations requires you to include the Common Name (CN) - the Fully Qualified Domain Name - of the server in the private key.
2. Authorize SSL privileges for decryption and adding certificates/keys, as described below. Privileges can be assigned to different roles reflecting the nature and importance of the task at hand. For example, for decryption, you may want to assign users a SYSADMIN or NTWKADMIN-level role. For adding certificates/keys, you may want to assign a lower-level privilege such as APPROVR.
    1. Successively click the **Configuration Manager** and **Server Management** icons.
    2. Select the **Users** and **Roles** tabs.

3. Select the appropriate role.
4. In the right-hand pane, match the **Packet Analysis — SSL Admin** privilege with the selected role by clicking the appropriate □checkbox. Repeat the process for the Packet Analysis — SSL/IPSec Decryption privilege. Both checkboxes **must** be selected.

   Important: SSL configuration on the nGeniusONE requires that a user in only the SYSADMIN role can select the Packet Analysis-Admin checkbox. Also, in a distributed environment, a user in the SYSADMIN role can enable SSL functionality only on a Global Manager, not a Local Server.

   Important: When a Local Server is added to a Global Manager where the role for Packet Analysis — Decryption User is defined in SYSADMIN, the Enable Decryption User option will not be present in the Local Server Console and Local trace file decryption cannot be tested even though all configuration settings are pushed down to the Local Server from the Global Manager.
5. Click **Save**.

Configuration Step 2: Enabling HTTPS SSL Decryption and HSM on the InfiniStream

- Enable decryption of HTTPS SSL packets on your nGenius InfiniStream appliance. Be sure to restart your probe after configuring this setting.
- Optional. For Thales/SafeNet HSM users only, configure software on the nGenius InfiniStream appliance (described here)

Configuration Step 3: Enabling SSL Decryption on the nGeniusONE Server

Configure the SSL certificate in the Device Management module using either the *Local* or *HSM* option (described here). The Local option pushes down to and stores the private key (.PEM file) in the PM Server, then InfiniStream, then the Local decryption device. In the case of a Global Manager, the .PEM file is pushed down to and stored in the client device, then Global Manager, then all associated Local Servers, then all InfiniStreams. The HSM (Hardware Security Module) option does not distribute PEM files but does distribute the private key in a similar fashion using the PKCS11 protocol.

1. Successively click **Configuration Manager** and **Global Settings** icons.
2. Click the **SSL Keys** tab.
3. Click either the **Local Decryption** or **Hardware Security Module** (described here) tab in conformance with the type of certificate you have.

Local Decryption

1. Select the **Local** tab and click **Add SSL certificate** ⊕. The Add SSL Certificate dialog box opens.
2. Enter parameters for the following values. Refer to this **Port Parameters table** for supported values.
   - **Server —** an alias for the monitored Web server whose packets will be decrypted such as *VISA Web Server*.
   - **Server IP —** the IP Address of the monitored Web server whose packets will be decrypted.
   - **SSL Port —** the SSL port on the monitored Web server whose packets will be decrypted.
   - **Application Port —** the port which will replace the SSL port after decryption.
   - **Key —** the private key, .PEM file name and path to upload the certificate from (system where the PM Client is running).
3. Click **OK**.
4. If you have more keys to enter, repeat the above steps.
5. If you have Hardware Security Module keys, proceed to the following section.
6. Click **OK** to close the dialog box.

Configuration Step 4: Setting an HTTPS Child for Decryption on the nGeniusONE Server

You must add an HTTPS child application and specify a server IP address in Global Settings to complete decryption configuration on the nGeniusONE server. The HTTPS child should be a URL application.

To configure an HTTPS child:

1. In **Global Settings** 🎚, select the **Applications** tab.
2. Select the **HTTPS** protocol and click **Add Application** ⊕.
3. Enter the appropriate values and click the **URL Application** radio button. Take care that the URL string matches the host name exactly as it appears in the host field.
4. Click **OK**.

Configuration Step 5: SSL/TLS Workflows

Once configured, SSL decryption is available in the following workflows:

- Decode workflows launched by selecting Protocol Decode from the Packet Analysis menu.
- Decode workflows launched from the nEI and nSI.
- Decode workflows launched from the InfiniStream Console software.

You can add an SSL key for an HSM server from the SSL Keys > HSM tabs. The following actions are provided:

- **Add SSL certificate** .
- **Modify selected SSL certificate** .
- **Delete selected SSL certificate** .
- **Show** /**Hide** **the Filter** to display or hide the fields for filtering any of the parameters listed below.
- **Reset the Filter** to adjust it to the default view.
- **Refresh** to refresh data in the table.
- **Note**: right-clicking an entry in the list displays a **Modify** menu item to change settings and **Delete** menu item to remove the entry.

Enter the following parameters and when finished, click **OK**.

Parameter	Description
Server Label	An alias for the monitored Web server whose packets will be decrypted such as VISA Web Server.
Server IP	The IP Address of the monitored Web server whose packets will be decrypted. IPv4 and IPv6 addresses are supported.
SSL Port	The SSL port on the monitored Web server whose packets will be decrypted.
Application Port	The port which will replace the SSL port after decryption.
Key Label	The private key, .PEM file name and path to upload the key from (system where the PM Client is running).
Slot ID	The HSM smart card slot number where the private key is stored.
Password	The unique password used by the HSM to access this key. This value is shadowed (marked by asterisks) as it is entered.
Confirm Password	Re-enter the password typed in the Password field.