

X-Header Insertion and Encryption

- Revision History, on page 1
- Feature Description, on page 1
- How It Works, on page 1
- Configuring X-Header Insertion and Encryption, on page 2
- Monitoring and Troubleshooting the X-Header Insertion and Encryption feature, on page 5

Revision History

Revision Details	Release
Added CLI support to enable spoofing detection in x-header fields using the **delete-existing** keyword option in the **xheader-format** command.	21.28.m0
First introduced.	21.25

Feature Description

The X-Header Insertion and X-Header Encryption features is collectively known as Header Enrichment. This feature enables in appending headers to HTTP or WSP GET and POST request packets, and HTTP Response packets for use by end applications, such as mobile advertisement insertion (MSISDN, IMSI, IP address, user-customizable, and so on).

How It Works

X-Header Insertion

This section provides an overview of the X-Header insertion feature.

Extension header (X-Header) fields are fields that are not defined in RFCs or standards but can be added to protocol headers for specific purposes. The X-Header mechanism allows additional entity-header fields to be defined without changing the protocol, but these fields cannot be assumed to be recognizable by the recipient. The unrecognized header fields must be ignored by the recipient and must be forwarded by transparent proxies.

The X-Header insertion feature enables inserting x-headers in HTTP or WSP GET and POST request packets and HTTP response packets. Operators wanting to insert X-headers in HTTP or WSP request and HTTP response packets, can configure rules for it. The charging-action associated with the rules contain the list of X-headers to be inserted in the packets.

X-Header Encryption

This section provides an overview of the X-Header Encryption feature.

X-Header encryption enhances the X-header insertion feature to increase the number of fields that can be inserted, and also enables encrypting the fields before inserting them.

If X-Header insertion has already happened for an IP flow (because of any X-Header format), and if the current charging-action has the first-request-only flag set, X-Header insertion won't happen for that format. If the first-request-only flag is not set in a charging-action, then for that X-Header format, insertion continues happening in other suitable packets of that IP flow.

Changes to X-Header format configuration will not trigger reencryption for existing calls. The changed configuration will however, be applicable for new calls. The changed configuration will also apply at the next reencryption time to those existing calls for which reencryption timeout is specified. If encryption is enabled for a parameter while data is flowing, since its encrypted value won't be available, insertion of that parameter stops.



Note This feature does not support recovery of flows.

Configuring X-Header Insertion and Encryption

This section describes how to configure the X-Header Insertion and Encryption features, collectively known as Header Enrichment.

X-Header Insertion

Table 1: Procedure

Step	Description
1	Creating/configuring a ruledef to identify the HTTP/WSP packets in which the X-Headers must be inserted.
2	Creating/configuring a rulebase and configuring the charging-action, which inserts the X-Header fields into the HTTP/WSP packets.
3	Creating/configuring the X-Header format.
4	Configuring insertion of the X-Header fields based on the message type in the charging action.

X-Header Encryption

Table 2: Procedure

Step	Description
1	X-Header insertion, encryption, and the encryption certificate are configured in the CLI. **Note** To ensure interoperability with Cisco gateway X-Header encryption, align your key derivation process with the Cisco workflow. Use OpenSSL-compatible EVP_BytesToKey with 14 iterations, consistent hash chaining, and the specified parameters (AES-256-GCM, SHA-384, 32-byte key, 12-byte IV). Inconsistent implementation may result in issues accessing encrypted data.
2	When the call gets connected, and after each regeneration time, the encryption certificate is used to encrypt the strings.
3	When a packet hits a ruledef that has x-header format configured in its charging-action, X-Header insertion into that packet is done using the given X-Header-format.
4	If X-Header-insertion is to be done for fields which are marked as encrypt, the previously encrypted value is populated for that field accordingly.

Configuring X-Header Insertion

This section describes how to configure the X-Header Insertion feature.

To configure the X-Header Insertion feature:

Table 3: Procedure

Step 1	Create or Configure a ruledef to identify the HTTP packets in which the X-headers must be inserted.
Step 2	Create or Configure a rulebase and configure the charging-action, which inserts the X-header fields into the HTTP packets.
Step 3	Create the X-header format as described in *Creating the X-Header Format*.
Step 4	Configure the X-Header format as described in *Configuring the X-Header Format*.

Creating the X-Header Format

To create an x-header format, use the following configuration:

```
configure
  active-charging service ecs_service_name
    xheader-format xheader_format_name
    end
```

Configuring the X-Header Format

To configure an x-header format, use the following configuration:

```
configure
   active-charging service ecs_service_name
      xheader-format xheader_format_name
        insert xheader_field_name string-constant xheader_field_value | variable
{ bearer { 3gpp { apn | charging-characteristics | charging-id | imei |
imsi | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | customer-id |
 ggsn-address | mdn | msisdn-no-cc | radius-string |
radius-calling-station-id | session-id | sn-rulebase |
subscriber-ip-address | username } [ encrypt ] [ delete-existing ] | http
 { host | url } }
        end
```

Configuring X-Header Encryption

This section describes how to configure the X-Header Encryption feature.

Table 4: Procedure

Step 1	Configure X-Header Insertion as described in *Configuring X-Header Insertion*.
Step 2	Create or Configure a rulebase, and configure the encryption certificate to use and the reencryption parameter as described in *Configuring X-Header Encryption*.
Step 3	Configure the encryption certificate to use as described in *Configuring Encryption Certificate*.

Configuring X-Header Encryption

To configure X-Header Encryption, use the following configuration example:

```
configure
   active-charging service ecs_service_name
      rulebase rulebase_name
         xheader-encryption certificate-name certificate_name
         xheader-encryption re-encryption period re-encryption_period
         end
```

NOTES:

- This configuration enables X-Header Encryption for all subscribers using the specified rulebase.
- If the certificate is removed, ECS continues using the copy that it has. The copy is set free once the certificate name is removed from the rulebase.
- Changes to x-header format configuration won't trigger re-encryption for existing calls. The changed configuration will however, be applicable for new calls. The changed configuration will also apply at the next reencryption time to those existing calls for which reencryption timeout is specified. If encryption is enabled for a parameter while data is flowing, since its encrypted value won't be available, insertion of that parameter stops.

Configuring Encryption Certificate

To configure the encryption certificate, use the following configuration:

```
configure
  certificate name certificate_name pem { { data pem_certificate_data private-key
 pem [ encrypted ] data pem_pvt_key } | { url url private-key pem { [
encrypted ] data pem_pvt_key | url url } }
  end
```

Verifying the X-Header Insertion and Encryption Configuration

Enter the following command in the Exec Mode to verify your configuration:

xheader-format *xheader_format_name*

Monitoring and Troubleshooting the X-Header Insertion and Encryption feature

This section provides information on the show commands and/or their outputs available to support this feature.

show active-charging charging-action statistics name

The output of this command displays statistics for X-Header information.

- XHeader Information:
  - XHeader Bytes Injected
  - XHeader Pkts Injected
  - IP Frags consumed by XHeader
  - XHeader Bytes Removed
  - XHeader Pkts Removed

show active-charging rulebase statistics name

The output of this command displays the Header Enrichment statistics.

- HTTP header buffering limit reached