Enable Network Policy IE

Enable Network Policy IE in MME

Table 1: Feature History

Feature Name	Release	Description
Support Network Policy IE under mme-service and call control profile	2025.01.0	The feature supports the Network Policy Information Element (IE) in the Attach and Tracking Area Update (TAU) Accept messages. It enhances network security by utilizing operator policies in the vMME. Command introduced: **send-network-policy unsec-redir-not-allowed** : In the MME-service and call-control-profile configuration mode, to enable the network policy configuration, use the **send-network-policy unsec-redir-not-allowed** command to configure unsecured redirection to GERAN not allowed. If the **send- network-policy unsec-redir-not-allowed** command is not enabled, the Network Policy IE is not sent in the Attach/TAU Accept message.

According to 3GPP standards, TS 24.301 Release 15 onwards, Clause 5.5.1.2, the redir-policy bit in the Network policy IE is permitted in the ATTACH Accept and TAU Accept messages.

If operator policies prohibit unsecured redirection to a GERAN cell within the current PLMN, the MME sets the redir-policy bit to indicate "unsecured redirection to GERAN not allowed" in the network policy IE of the Attach Accept and TAU Accept messages as mentioned in the Clause 5.5.3.2.4.

As per TS 24.301, Section 9.9.3.52 on network policy, the network policy value can be defined as either 0 for "unsecured redirection to GERAN allowed" or 1 for "unsecured redirection to GERAN not allowed".

How Network Policy IE in MME Works

The network policy bit is an optional Information Element (IE) in the ATTACH and Tracking Area Update (TAU) accept messages. When enabled, the MME sends this network policy IE with a value of 1, indicating that unsecured redirection to GERAN is not allowed.

The Network Policy IE configuration is applied under the mme-service or call-control-profile settings. If enabled under mme-service, all subscribers are affected. If enabled under a call-control-profile, only subscribers within that profile are impacted. When not configured, the network policy IE is not included in the ATTACH/TAU accept messages

Configurations for Network Policy IE

This section provides these configurations involved in enabling and disabling the Network policy under MME-service and Call Control Profile configuration modes.

Enable Network Policy IE

Use this procedure to enable the Network policy IE in MME.

Procedure

Step 1 Enter the config mode.

Step 2 Enter the **context** *context_name* command to specify a context name.

Example:

```
config
 [ingress]asr5500 (config)context context_name
    [ingress]asr5500 (config-ctx)mme-service service_name
          [ingress]asr5500(config-mme-service) # send-network-policy unsec-redir-not-allowed
         exit
```

Step 3 Enter the **mme-service** *service_name* command to specify the service as MME.

Example:

```
config
  [ingress]asr5500 (config) # context  context_name
```

```
[ingress]asr5500 (config-ctx) mme-service service_name
         [ingress]asr5500(config-mme-service) # send-network-policy unsec-redir-not-allowed
         exit
```

Step 4 Specify the following command:

- enter the **send-network-policy unsec-redir-not-allowed** command to configure Unsecured redirection to GERAN not allowed. If the **send-network-policy unsec-redir-not-allowed** command is enabled, Network policy IE with **unsec-redir-not-allowed** *value 1* is sent in ATTACH and TAU accept messages,

Example:

```
config
  [ingress]asr5500 (config) # context context_name
  [ingress]asr5500 (config-ctx) mme-service service_name
         [ingress]asr5500(config-mme-service) # send-network-policy
unsec-redir-not-allowed
          exit
```

Note
By default, the Network Policy IE is not sent in the ATTACH and TAU Accept messages.

Step 5 Enter the **exit** command to exit the current configuration mode and return to the previous mode.

Example:

```
config
  [ingress]asr5500 (config) context context_name
  [ingress]asr5500 (config-ctx) mme-service service_name
    [ingress]asr5500(config-mme-service) # send-network-policy unsec-redir-not-allowed
    exit
```

Disable Network Policy IE in MME

Use this procedure to disable the Network policy IE in MME.

Procedure

Step 1 Enter the config mode.

Step 2 Enter the **context** *context_name* command to specify a context name.

Example:

```
config
 [ingress]asr5500 context context_name
    [ingress]asr5500 mme-service service_name
        [ingress]asr5500(config-mme-service) # [ no ]unsec-redir-not-allowed
         exit
```

Step 3 Enter the **mme-service** *service_name* command to specify the service as MME.

Example:

```
config
 [ingress]asr5500 context context_name
 [ingress]asr5500 mme-service service_name
        [ingress]asr5500(config-mme-service) # [ no ] send-network-policy unsec-redir-not-allowed
        exit
```

Step 4 Enter the **[no] send-network-policy unsec-redir-not-allowed** command to disable the configuration sending network policy IE in the ATTACH/TAU accept message.

Example:

```
config
 [ingress]asr5500 context context_name
   [ingress]asr5500 mme-service service_name
        [ingress]asr5500(config-mme-service) # [no ] send-network-policy
unsec-redir-not-allowed
        exit
```

Step 5 Enter the **exit** command to exit the current configuration mode and return to the previous mode.

Example:

```
config
 [ingress]asr5500 context context_name
 ingress]asr5500 mme-service service_name
        [ingress]asr5500(config-mme-service) # [ no ]unsec-redir-not-allowed
        exit
```

Enable Network Policy IE under Call Control Profile

Use this procedure to enable the Network policy IE under the call control profile.

Procedure

Step 1 Enter the config mode.

Step 2 Enter the **call-control-profile** *call_control_profile_name* command to specify the name of call control profile.

Example:

```
config
  [ingress]asr5500 call-control-profile call_control_profile_name
          [ingress]asr5500(config-call-control-profile-ccp1) # send-network-policy
unsec-redir-not-allowed
          exit
```

Step 3 Specify the following commands:

- enter the **send-network-policy unsec-redir-not-allowed** command to configure Unsecured redirection to GERAN not allowed. If the **send-network-policy unsec-redir-not-allowed** command is enabled, Network policy IE with **unsec-redir-not-allowed** *value 1* is sent in the ATTACH/TAU accept message.

Example:

```
config
  [ingress]asr5500 call-control-profile call_control_profile_name
         [ingress]asr5500(config-call-control-profile-ccp1) # send-network-policy
 unsec-redir-not-allowed
         exit
```

Note
By default, the Network Policy IE is not sent in the ATTACH and TAU Accept messages.

Step 4 Enter the **exit** command to exit the current configuration mode and return to the previous mode.

Example:

```
config
  [ingress]asr5500 call-control-profile call_control_profile_name
          [ingress]asr5500(config-call-control-profile-ccp1) # send-network-policy
unsec-redir-not-allowed
          exit
```

Disable Network Policy IE

Use this procedure to disable the Network policy IE under the call control profile.

Procedure

Step 1 Enter the config mode.

Step 2 Enter the **call-control-profile** *call_control_profile_name* command to specify the name of the call control profile.

Example:

```
config
  [ingress]asr5500 call-control-profile call_control_profile_name
         [ingress]asr5500(config-call-control-profile-ccp1) # [ no | remove ] send-network-policy
unsec-redir-not-allowed
         exit
```

Step 3 The **[no | remove] send-network-policy unsec-redir-not-allowed** command includes the following.

- enter the **no send-network-policy unsec-redir-not-allowed** command to disable the Network policy IE to be sent in the ATTACH/TAU accept message, or
- enter the **remove send-network-policy unsec-redir-not-allowed** command to remove the configuration for sending network policy IE in the ATTACH/TAU accept message. If this configuration is removed from the call control profile, the action will then be determined by the configuration in the MME service.

Example:

```
config
  [ingress]asr5500 call-control-profile call_control_profile_name
```

```
      [ingress]asr5500(config-call-control-profile-ccp1) # [ no | remove ]
send-network-policy unsec-redir-not-allowed
         exit
```

Step 4 Enter the **exit** command to exit the current configuration mode and return to the previous mode.

Example:

```
config
  [ingress]asr5500 call-control-profile call_control_profile_name
        [ingress]asr5500(config-call-control-profile-ccp1) # [ no | remove ] send-network-policy
unsec-redir-not-allowed
      exit
```

Verifying the Network Policy IE

This section describes how to verify the Network Policy IE is enabled or disabled using the show commands.

show mme-service name

The folowing is an example output to verify the unsecuredredirection to GERAN is enabled or disabled.

```
[ingress]asr5500# show mme-service name <mme service name>
                ..
                Unsecured redirection to GERAN not allowed: Enabled/Disabled
```

show call control control profile full all

The folowing is an example output to verify the unsecuredredirection to GERAN is enabled or disabled.

```
 [ingress]asr5500# show call-control-profile full all
                 ..
               Unsecured redirection to GERAN not allowed: Enabled/Disabled
```