Carrier VoIP

Gateway Controller Security and Administration

NN10213-611

Document status: Standard
Document version: 08.02
Document date: 20 October 2006

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

Contents

Gateway Controller Security and Administration

New in this release

The following sections detail what's new in *Gateway Controller Security and Administration* (NN10213-611) for (I)SN09U:

- "Features" (page 5)
- "Other changes" (page 7)

Features

See the following sections for information about feature changes:

- "IPSec PKI Support (on the GWC) - (A00012183)" (page 5)
- "Support for SCTP security on GWC (A00010251)" (page 6)
- "RMGC Security (A00009026)" (page 6)
- "IPSec Integration with AMS (A00007143)" (page 7)

IPSec PKI Support (on the GWC) - (A00012183)

This feature integrates the GWC with the Certificate Manager. The Certificate Manager provides generation, distribution, and monitoring of certificates and keys. The GWC uses X.509 certificates to authenticate remote media gateways and to establish secure associations (SA).

When configuring IPSec on a GWC, you can select either PRESHARED key-based authentication or Digital Signatures (X.509 certificates)-based authentication.

This feature modifies the GWC Manager IPSec GUI to support the Certificate Manager.

This feature introduces or modifies the following sections and procedures:

- "IPSec configuration procedures" (page 8)
- "Download IKE certificates" (page 53) (new)
- "View IKE certificates" (page 55) (new)
- "Delete IKE certificates" (page 57) (new)

- "Configure pre-shared key IKE authentication" (page 59) (new)
- "Configure Digital Signatures IKE authentication" (page 63) (new)
- "Transition IKE authentication method" (page 67) (new)
- "Complete transition of IKE authentication method" (page 71) (new)
- "Modify IKE authentication_change IKE preference list" (page 74) (new)
- "Configure IPSec Preference and Preference List" (page 43)
- "Configure IKE Preference and Preference List" (page 48)
- "Modify IKE pre-shared keys" (page 115)
- "Configure IPSec SECURE or FLEX connection policy with IKE" (page 92)
- "Modify an existing IPSec connection policy" (page 124)
- "Activate or de-activate IPSec with Kerberos using FLEX policy" (page 107)

  Procedure for activating or de-activating IPSec with IKE moved to *Nortel CVoIP IPSec Security Service Implementation Overview* (NN10453-100).

All other IPSec procedures are updated to reflect the modified GUI architecture.

Support for SCTP security on GWC (A00010251)

This feature provides support for the simple control transmission protocol (SCTP) IPSec on the GWC.

This feature adds SCTP references to the following procedures:

- "Configure a BYPASS connection policy" (page 83)
- "Configure a DISCARD connection policy" (page 88)
- "Configure IPSec SECURE or FLEX connection policy with IKE" (page 92)

RMGC Security (A00009026)

This feature enables secure communication between the redirecting media gateway controller (RMGC) and the multimedia terminal adapter (MTA) line gateway for packet cable solutions.

This feature adds RMGC references to the following procedures:

- "Configure IPSec Preference and Preference List" (page 43)
- "Configure Kerberos key management" (page 77)
- "Modify Kerberos service key" (page 118)

IPSec Integration with AMS (A00007143)

This feature integrates the IPSec interactions between the audio controller GWC and the Media Server 2010 gateway as configured on the IEMS.

This feature adds Media Server 2010-specific information to the following procedures:

- "Configure IPSec Preference and Preference List" (page 43)
- "Configure IKE Preference and Preference List" (page 48)

Other changes

Added section "User authentication groups required for GWC IPSec GUI operations" (page 12).

Security and administration strategy overview

User administration for the Gateway Controller (GWC) card is performed using the CS 2000 SAM21 Manager client. GWC node service management is performed using the CS 2000 GWC Manager.

V5.2 line and interface administration is not supported from the CS 2000 GWC Manager. V5.2 line administration is performed using the CS 2000 XA-Core or Compact Call Agent (CCA) MAPCI interface.

Tools and utilities

The CS 2000 SAM21 Manager provides access to platform level services like GWC hardware diagnostics and hardware reset. The CS 2000 GWC Manager provides access to services like connectivity configuration and call processing services.

The CS 2000 SAM21 Manager and the CS 2000 GWC Manager applications use Common Object Request Broker Architecture (CORBA) to communicate with one another. One feature of this architecture is that a lock request at the CS 2000 SAM21 Manager client interface initiates a check with the CS 2000 GWC Manager to determine the call processing activity on the GWC. If the GWC is active or ready to provide service, a warning prompts that a lock can impact service.

ATTENTION

The GWC Manager does not display provisioning data in real time. That is, when two users are changing provisioning data on the same GWC node at the same time, you must refresh your display to see the changes implemented by the other user. Use the Refresh button if available. Otherwise, you may have to select a different GWC node, then re-select again the node which you are updating. To view the provisioning data changes under any tab of the Network Devices or Network Configuration panel, click any other tab in the panel, then return to the tab that you are updating.

For security purposes, the following login session time-outs are provisioned for the GWC Manager GUI:

- user inactivity time-out, which specifies the amount of time a client session can be inactive before the user is required to log in again
- user termination time-out, which specifies the amount of time a user has to log in again before the user is forced to exit the client session

Both time-outs have a default value of 10 minutes, which you can modify using procedure "Modifying login session timeouts on the CS 2000 Management Tools server" in the CS 2000 Management Tools section of the *Nortel ATM/IP Solution-level Administration and Security* (NN10402-600).

Integrated Element Management System

Many FCAPS activities may now be performed using the Integrated Element Management System (IEMS). In addition, access to the CS 2000 GWC Manager and the CS 2000 SAM21 Manager is provided using the IEMS. For more information, see *IEMS Overview* (NN10329-111).

To launch the CS 2000 GWC Manager or the CS 2000 SAM21 Manager, see the following procedures in *IEMS Overview* (NN10329-111):

- "Launching GWC Manager"
- "Launching SAM21 Manager"

Administrative maintenance procedures

The following procedures are available for administering user access to the CS 2000 GWC Manager and to administer the activity status of individual GWC cards.

- "Access a GWC node using the CS 2000 GWC Manager" (page 22)
- "Lock a GWC card" (page 25)
- "Unlock a GWC card" (page 28)
- "Invoke a manual protection switch (warm SWACT)" (page 31)
- "Invoke a cold manual protection switch (cold SWACT)" (page 33)
- "Disable (Busy) GWC card services" (page 35)
- "Enable (RTS) GWC card services" (page 37)

IPSec configuration procedures

Nortel security architecture for VoIP uses Internet Protocol Security (IPSec) to protect the traffic between the GWC and other network devices. This section describes some basic concepts related to the IPSec services provided by the GWC, and the procedures for configuring IPSec on a GWC node.

For more information about IPSec, go to the appropriate Internet Engineering Task Force (IETF) RFC documentation, which can be found at following Web site:

http://www.ietf.org

IPSec overview

The following subsections describe the basic IPSec architecture elements as implemented in the (I)SN09U release.

IPSec services

IPSec offers a set of security services that provide data integrity, authentication, and confidentiality (encryption). These services are provided through the use of traffic security protocols.

Traffic security protocols

IPSec uses two protocols to provide traffic security:

- ESP (encapsulating security payload)
- AH (authentication header)

GWC supports ESP only. ESP protocol provides authentication of the sender, encryption, and data integrity.

Security associations

IPSec services are defined and executed through security associations (SA). An SA is a one-way relationship between the GWC and a gateway. The SA is negotiated and it defines how two network components will use IPSec to communicate securely. To create bi-directional communication between the GWC and a gateway, two IPSec SAs must be created (one in each direction).

SAs specify security parameters, such as, the IPSec protocol (ESP), the authentication and encryption algorithm, the keys, the lifetime of the SA.

Key management protocols

IPSec SAs are negotiated and established by exchanging security keys - using one of the following key management protocols:

- Kerberos - in packet cable solutions only, for SAs between a GWC (including a redirecting media gateway controller [RMGC]) - and a multimedia terminal adapter (MTA) line gateway

ATTENTION

If an application layer gateway (ALG) middlebox is associated with an MTA gateway, IPSec between the GWC, ALG, and MTA gateway is not supported.

- Internet Key Exchange (IKE) - for SAs between a GWC and other network components (except MTAs in packet cable solutions)

  In cable solutions, IKE is used for SAs between a GWC and the cable modem termination system (CMTS) or third-party Trunk Gateway Control Protocol (TGCP) gateways.

IKE creates an authenticated secure communication channel between the GWC and a gateway. This association is called an IKE SA. IKE then uses this secure association to negotiate IPSec SAs.

IKE consists of two phases:

- phase 1, a shared secret is negotiated through a Diffie-Hellman key exchange (IKE SA is created)
- phase 2, IKE SA is used to negotiate IPSec SAs

IKE SA can use main or aggressive mode - GWC supports Main mode only.

There are two authentication methods supported on the GWC:

- Pre-shared key, where authentication is performed by a key that is known to both the GWC and the remote media gateway
- Digital Signatures, where authentication is performed using X.509 certificates and key provided by the Certificate Manager

In cable solutions, Kerberos with public key support (using the PKINIT extension to the Kerberos IETF standard) is used to exchange keys and authenticate an MTA to a GWC. MTA authentication process with the GWC requires a PacketCable key distribution center (KDC) server, which grants authentication tickets to the MTA. These tickets are used to authenticate an MTA to a GWC, and to establish a pair of IPSec SAs on both nodes. The KDC is third-party equipment and must be integrated with the network.

Transport and tunnel mode

ESP supports two modes of operation: tunnel and transport mode. GWC supports transport mode only. In transport mode, IPSec protection applies to higher-layer protocols only (such as, TCP, UDP, or SCTP and only to the payload of the IP packet.

Security connection policies

Connection policies define which security services will be applied to messages exchanged between a GWC and the specific remote gateway (identified by the IP address). Each connection policy associates an IP address (or a range of IP addresses) to one of the following actions:

- BYPASS: IPSec processing is not applied to any packets matching the policy between the GWC and the selected remote gateway. Incoming

IPSec packets are discarded. Outgoing packets are not subject to IPSec processing.

- DISCARD: all packets matching the policy between the GWC and the selected remote gateway are discarded.
- SECURE: before an SA is established, an incoming packet is discarded, and an outgoing packet triggers key negotiation process (using IKE or Kerberos). When an SA is established, IPSec is applied to all incoming and outgoing packets. Incoming packets are authenticated (and if applicable, decrypted); outgoing packets are authenticated (and if applicable, encrypted) before being sent.
- FLEX: this policy is not secure. The FLEX policy must only be used temporarily during the initial activation or de-activation of IPSec, when some gateways associated with the connection policy operate in a secure mode and some do not. The FLEX policy provides the GWC with the flexibility of accepting secure and non-secure messages, so IPSec can be activated on the GWC without a loss of service. When FLEX policy is used to de-activate IPSec, temporary loss of service may occur until security is fully de-activated on the GWC and the gateway.

Each connection policy is identified by a policy ID number. The lower this number is, the greater is the priority of the policy. For any gateway IP address, the GWC applies the corresponding policy with the lowest policy ID number.

GWC support for IPSec

The CS 2000 GWC Manager supports the configuration of the IPSec functionality on a CS 2000. You can configure IPSec for any GWC service profile.

For cable solutions, use the following profiles to configure IPSec:

- for secure communication with MTA line gateways and CMTS:
  - SMALL_LINENA or SMALL_LINEINTL
  - SMALL_LINENA_V2 or SMALL_LINEINTL_V2
  - LINE_TRUNK_AUD_NA or LINE_TRUNK_AUD_INTL
  - AUDCNTL_RMGC or AUDCNTL_RMGCINTL

ATTENTION

If an application layer gateway (ALG) middlebox is associated with an MTA gateway, IPSec between the GWC, ALG, and MTA gateway is not supported.

- for secure communication with third-party TGCP trunk gateways:
  - TRUNKNA and TRUNKINTL

— LINE_TRUNK_AUD_NA and LINE_TRUNK_AUD_INTL

For the complete list of network paths and devices supporting IPSec, as well as an overview of the IPSec implementation in a network, see *Nortel ATM/IP Solution-level Administration and Security* (NN10402-600).

Provision IPSec only if a secure gateway - tested and certified for IPSec configuration - exists in your network.

CAUTION
Possible communication disruption
When configuring IPSec on a GWC node, proceed with caution. Incorrect provisioning values may cause communication disruption between the GWC and the gateway. Contact your network administrator to coordinate the IPSec configuration effort.

User authentication groups required for GWC IPSec GUI operations

All GWC IPSec GUI operations require that your user account belongs to the appropriate authentication group, which specify the operations that you are authorized to perform. The following table maps the GWC IPSec GUI operations and the required authentication groups.

GUI operation	Authentication group
The authentication group mgcrw (read/write) permits all operations; the mgcro (read-only) permits viewing and browsing only.	
Add/Change/Delete IPSec Profile	mgcrw
View IPSec Profile	mgcro
Add/Change/Delete IPSec Preference	mgcrw
View IPSec Preference	mgcro
Add/Change/Delete IPSec Preference List	mgcrw
View IPSec Preference List	mgcro
Add/Change/Delete IKE Preference	mgcrw
View IKE Preference	mgcro
Add/Change/Delete IKE Preference List	mgcrw
View IKE Preference List	mgcro
Add/Change/Delete IKE Authentication	mgcrw
View IKE Authentication	mgcro
Download/Delete IKE Certificate	mgcrw
View/Refresh IKE Certificate	mgcro
Add/Change/Delete Connection Policy	mgcrw

GUI operation	Authentication group
View Connection Policy	mgcro
Add/Change Kerberos	mgcrw
View Kerberos	mgcro

IPSec connection policy configuration procedure on a GWC Manager

ATTENTION

Before starting any configuration procedure, obtain the correct configuration values for each required parameter.

Make sure that you enter each value correctly. Most fields in the configuration tables cannot be modified once an entry is added to a table. Also, if a value in any configuration table used to configure a new connection policy is incorrect, you will not be able to modify this policy. Instead, you will have to re-configure the appropriate table and configure a new policy. The only fields in the Connection Policy table that can be changed are the IPSec preference list and the IPSec policy profile (with limitations).

The following section lists the configuration values that you need to obtain for IPSec with Kerberos.

For recommended configuration values for IPSec with IKE, go to the *Nortel CVoIP IPSec Security Service Implementation Overview* (NN10453-100).

Configuration values for IPSec between GWC and MTA gateways using Kerberos key management (packet cable solutions only)

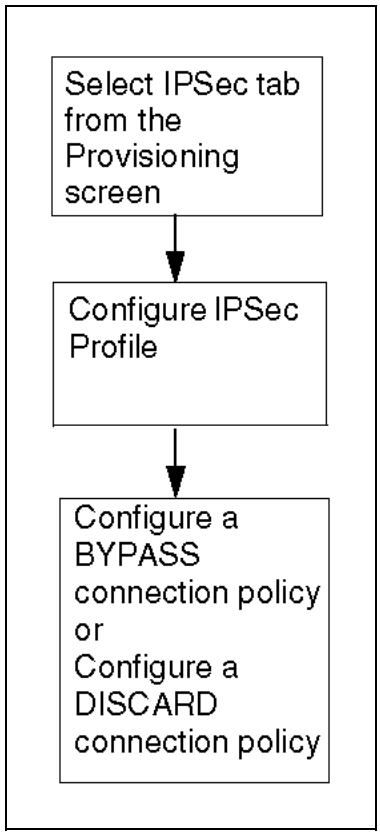
Before configuring IPSec for GWC secure communication with MTA gateways, obtain the following information:

- Kerberos values:
  - REALM (must match the name configured on KDC)
  - principal name (must match the name configured on KDC)
  - Kerberos service key (must match the key configured on KDC)
- IPSec values:
  - authentication algorithm
  - encryption algorithm
  - security associations (SA) lifetime
  - Perfect Forward Secrecy (PFS) group ID (this value must be NONE)

BYPASS or DISCARD connection policy

The following flowchart shows the sequence of tasks that you need to perform to configure an IPSec BYPASS or DISCARD connection policy on a GWC node.

Configure BYPASS or DISCARD connection policy on a GWC node



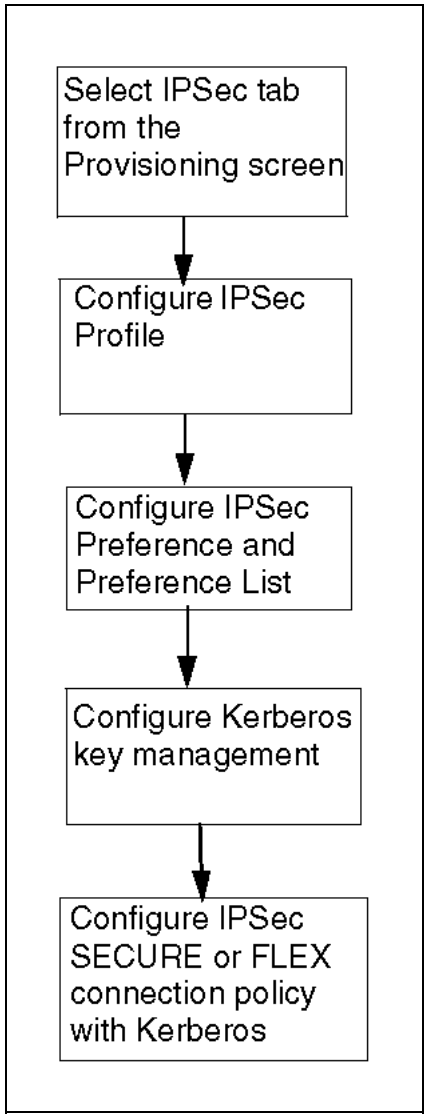
Configure BYPASS or DISCARD connection policy on a GWC node - navigation

- "Configure IPSec Profile" (page 39)
- "Configure a BYPASS connection policy" (page 83)
- "Configure a DISCARD connection policy" (page 88)

SECURE or FLEX connection policy with Kerberos

The following flowchart shows the sequence of tasks that you need to perform on a GWC node to configure an IPSec SECURE or FLEX connection policy with Kerberos.

Configure SECURE or FLEX connection policy with Kerberos



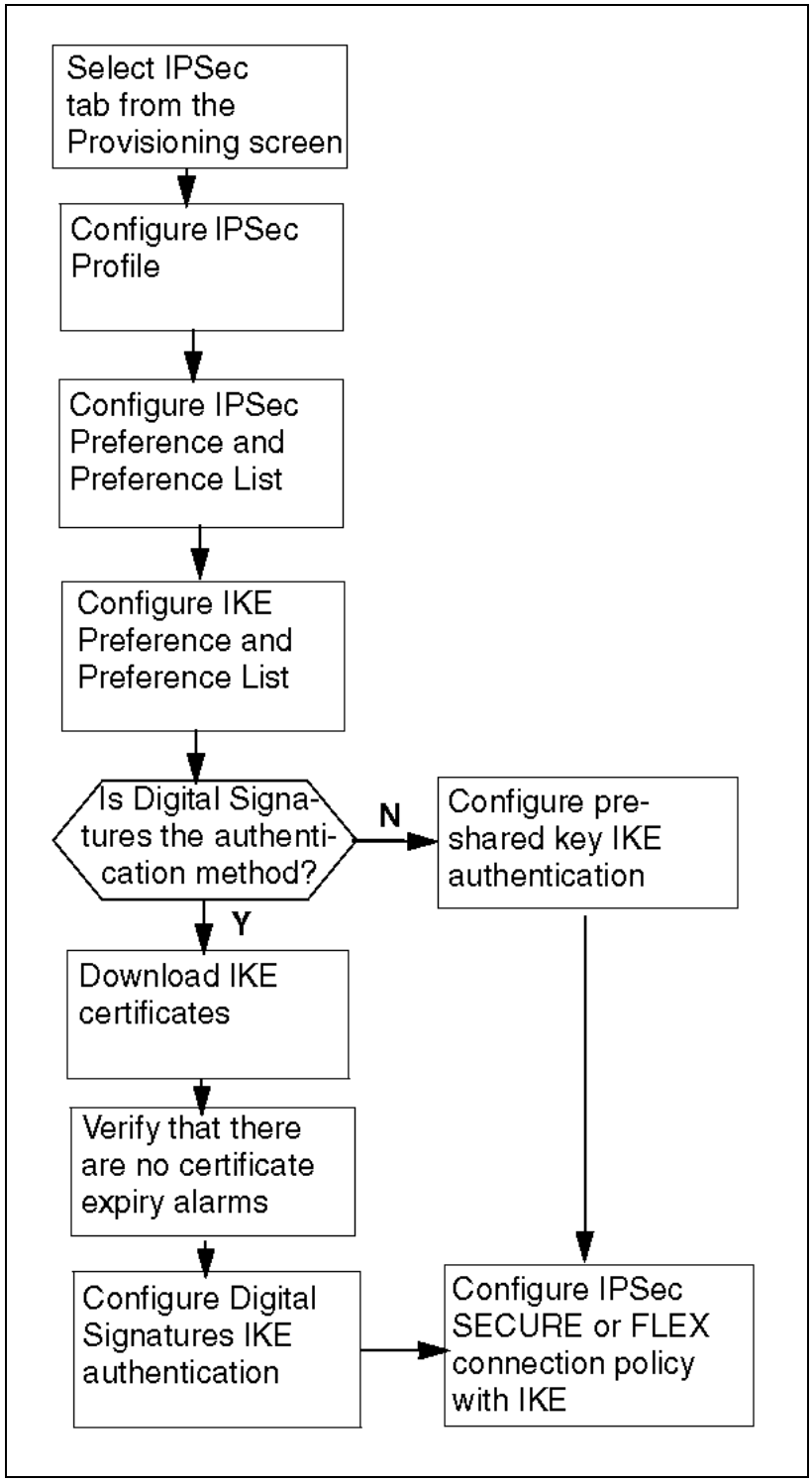
Configure SECURE or FLEX connection policy with Kerberos - navigation

- "Configure IPSec Profile" (page 39)
- "Configure IPSec Preference and Preference List" (page 43)
- "Configure Kerberos key management" (page 77)
- "Configure IPSec SECURE or FLEX connection policy with Kerberos" (page 100)

SECURE or FLEX connection policy with IKE

The following flowchart shows the sequence of tasks that you need to perform on a GWC node to configure an IPSec SECURE or FLEX connection policy with IKE.

Configure SECURE of FLEX connection policy with IKE



Configure SECURE of FLEX connection policy with IKE - navigation

- "Configure IPSec Profile" (page 39)
- "Configure IPSec Preference and Preference List" (page 43)
- "Configure IKE Preference and Preference List" (page 48)
- "Configure pre-shared key IKE authentication" (page 59)
- "Download IKE certificates" (page 53)
- "Configure Digital Signatures IKE authentication" (page 63)
- "Configure IPSec SECURE or FLEX connection policy with IKE" (page 92)

Configuration procedures for IPSec with Kerberos (packet cable solutions only)

The following table lists the configuration procedures that you may need to perform, and the associated tasks.

Procedure	Task
"Configure IPSec Profile" (page 39)	To configure an IPSec profile to be used with a connection policy.
"Configure IPSec Preference and Preference List" (page 43)	To configure IPSec preferences and preference lists to be used with a connection policy.
"Configure Kerberos key management" (page 77)	To configure Kerberos key management for a GWC.
"Configure IPSec SECURE or FLEX connection policy with Kerberos" (page 100)	To configure IPSec between GWC and MTA.
"Disable or enable IPSec between two nodes using BYPASS policy" (page 111)	To disable or enable IPSec processing between GWC and a gateway using BYPASS policy. **CAUTION** When BYPASS policy is used, a loss of communication between the GWC and a remote gateway will occur.

Procedure	Task
"Activate or de-activate IPSec with Kerberos using FLEX policy" (page 107)	Activate or de-activate IPSec processing between GWC and a gateway using FLEX policy. **CAUTION** When FLEX policy is used to activate IPSec, no loss of communication occurs. When FLEX policy is used to de-activate IPSec, temporary loss of service may occur until security is fully de-activated on both nodes.
"Configure a BYPASS connection policy" (page 83)	To add a BYPASS connection policy to a GWC.
"Configure a DISCARD connection policy" (page 88)	To add a DISCARD connection policy to a GWC.
"Modify Kerberos service key" (page 118).	To change the existing Kerberos service key for a selected GWC.
"Disable Kerberos key management" (page 121).	To disable the Kerberos key management for a GWC.
"Modify an existing IPSec connection policy" (page 124)	To change the IPSec preference list or the IPsec profile (with limitations) for an existing connection policy.
"Delete an IPSec connection policy" (page 128).	To delete a connection policy.

Configuration procedures for IPSec with IKE

ATTENTION
For IPSec with IKE, complete the following procedures only if you are directed to them by a higher-level task flow or another procedure.

The following table lists the configuration procedures that you may need to perform, and the associated tasks.

Procedure	Task
"Configure IPSec Profile" (page 39)	To configure an IPSec profile to be used with a connection policy.
"Configure IPSec Preference and Preference List" (page 43)	To configure IPSec preferences and preference lists to be used with a connection policy.
"Configure IKE Preference and Preference List" (page 48)	To configure IKE preferences and preference lists to be used with a connection policy.

Procedure	Task
"Download IKE certificates" (page 53) Applicable only if digital signature is to be used as the IKE authentication method.	To retrieve IKE certificates from the IEMS.
"View IKE certificates" (page 55) Applicable only if digital signature is used as the IKE authentication method.	To view detail information about IKE certificates currently assigned to a GWC.
"Delete IKE certificates" (page 57) Applicable only if digital signature is used as the IKE authentication method.	To delete a set of certificates currently assigned to a GWC.
"Configure pre-shared key IKE authentication" (page 59)	To configure the pre-shared key as the IKE authentication method and to select the IKE preference list to be used with a connection policy.
"Configure Digital Signatures IKE authentication" (page 63)	To configure digital signature as the IKE authentication method and to select the IKE preference list to be used with a connection policy.
"Transition IKE authentication method" (page 67)	To add a second authentication method to an existing IKE authentication table.
"Complete transition of IKE authentication method" (page 71)	To remove one authentication method from an existing IKE authentication table, currently configured with both methods.
"Modify IKE authentication_change IKE preference list" (page 74)	To change the IKE Preference List for an IKE authentication used in a selected connection policy.
"Configure IPSec SECURE or FLEX connection policy with IKE" (page 92)	To configure IPSec between GWC and a remote gateway.
"Disable or enable IPSec between two nodes using BYPASS policy" (page 111)	To disable or enable IPSec processing between GWC and a gateway using BYPASS policy. **CAUTION** When BYPASS policy is used, a loss of communication between the GWC and a remote gateway will occur.
Procedure for activating or de-activating IPSec with IKE using FLEX policy moved to *Nortel CVoIP IPSec Security Service Implementation Overview* (NN10453-100).	Activate or de-activate IPSec processing between GWC and a gateway using FLEX policy.
"Configure a BYPASS connection policy" (page 83)	To add a BYPASS connection policy to a GWC.
"Configure a DISCARD connection policy" (page 88)	To add a DISCARD connection policy to a GWC.

Procedure	Task
"Modify IKE pre-shared keys" (page 115) Applicable only if pre-shared keys are used as the IKE authentication method.	Change IKE pre-shared keys.
"Modify an existing IPSec connection policy" (page 124)	To change the IPSec preference list or the IPsec profile (with limitations) for an existing connection policy.
"Delete an IPSec connection policy" (page 128).	To delete a connection policy.

IPSec fault management

Use the following logs and alarms to monitor and manage faults and other events associated with IPSec:

- SA_PERCENTAGE_USAGE minor alarm
- logs GWC309, GWC320, and GWC400
- logs for the Kerberos application
- GWC320 alarms (various specific problems)
- IPSec and IKE security logs

For more information, see *Gateway Controller Fault Management* (NN10202-911). For the description of log report GWC309, GWC320, and GWC400, see *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

Access a GWC node using the CS 2000 GWC Manager

Purpose of this procedure

This procedure describes how to access the maintenance and provisioning information for a GWC.

When to use this procedure

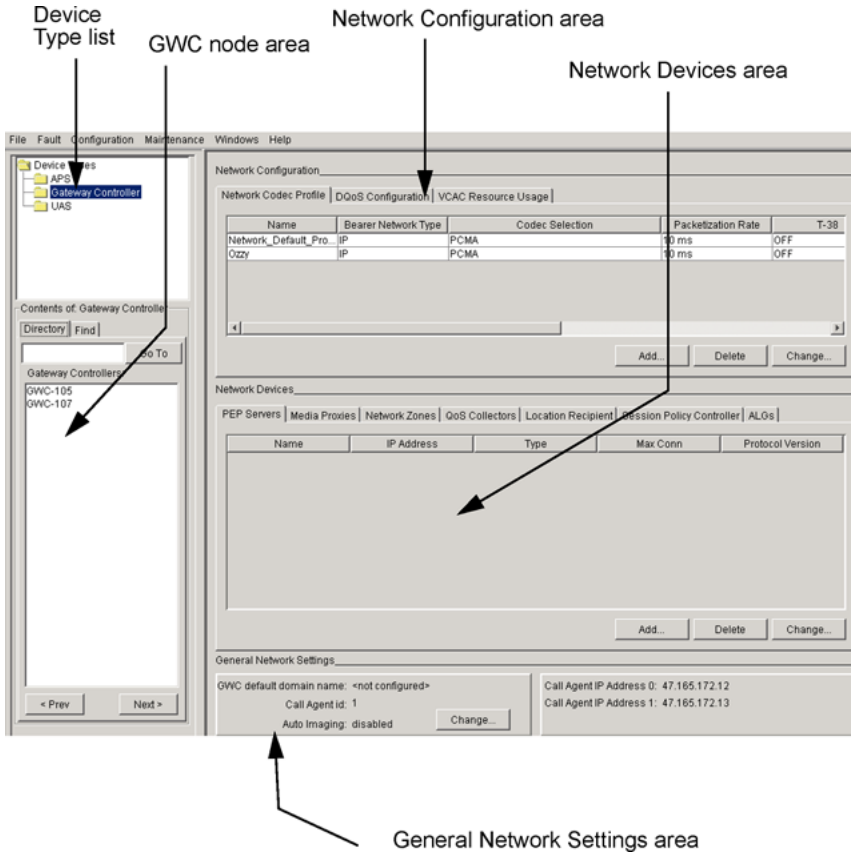
Use this procedure to when you need to access the GWC node to perform maintenance or provisioning tasks.

Prerequisites

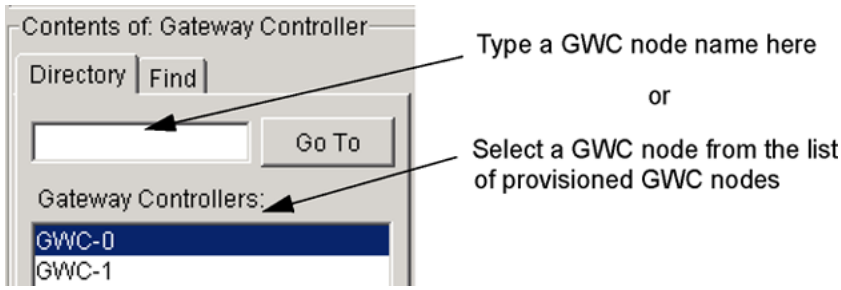
You require access to CS 2000 Management Tools client applications to perform this procedure. For more information, see the CS 2000 Management Tools section in *Nortel ATM/IP Solution-level Administration and Security* (NN10402-600).

Action

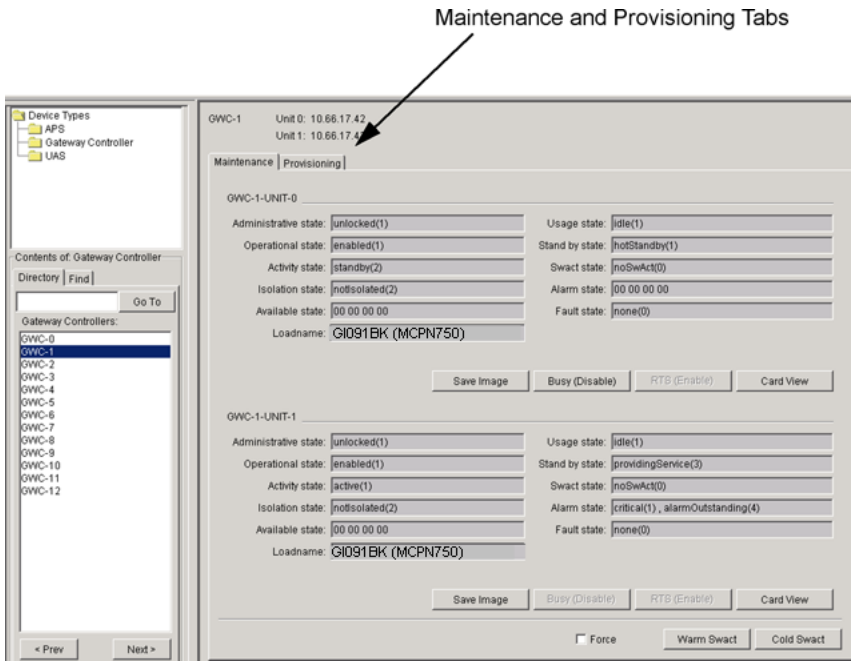
Step	Action
	At the CS 2000 GWC Manager workstation
1	At the CS 2000 Management Tools Selector window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.
2	Review the three primary panes in the main window area that provide access to provisioning and maintenance data and activities. The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.



3 From the Contents of: GatewayController frame, select the GWC node that you wish to view.



4 Click the maintenance and provisioning tabs in the main window area that provide access to provisioning data and maintenance data and activities.



5 The procedure is complete.

—End—

Lock a GWC card

Purpose of this procedure

This procedure locks a single GWC card, stopping the services, applications, and platform software running on the GWC card.

When to use this procedure

Use this procedure:

- when you are removing the card from service
- along with procedure "Unlock a GWC card" (page 28) to reboot a GWC and force a software download
- as part of fault clearing activity to determine if a problem is temporary or persistent
- when you have applied or removed a patch to the GWC software using the Network Patch Manager (NPM) and have created a new GWC software image on the CS 2000 Core Manager.
- when you are removing a GWC node from the CS 2000 GWC Manager database
- when replacing or upgrading hardware

Prerequisites

If the card that you want to lock is currently active, you need to switch call processing to its mate card in the node. This places the card in standby mode. If required, follow procedure "Invoke a manual protection switch (warm SWACT)" (page 31).

When the card is standby, you need to disable (busy) services on the card. Follow procedure "Disable (Busy) GWC card services" (page 35).

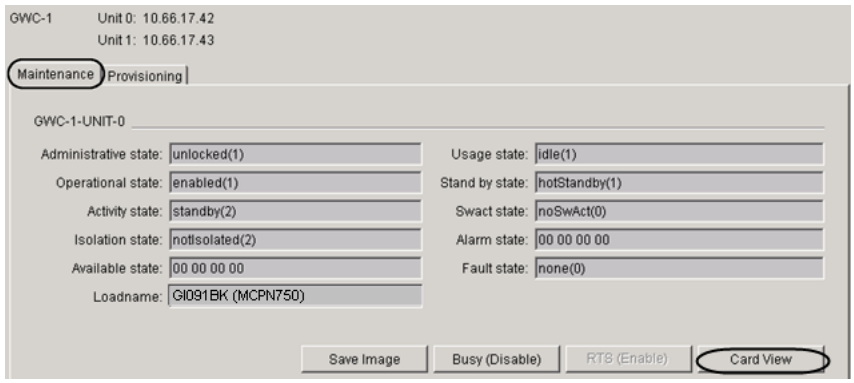
Once services on a standby card have been disabled, you can proceed with locking the card.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.

2 From the Contents of: GatewayController frame, select the GWC node that contains the card you want to lock.

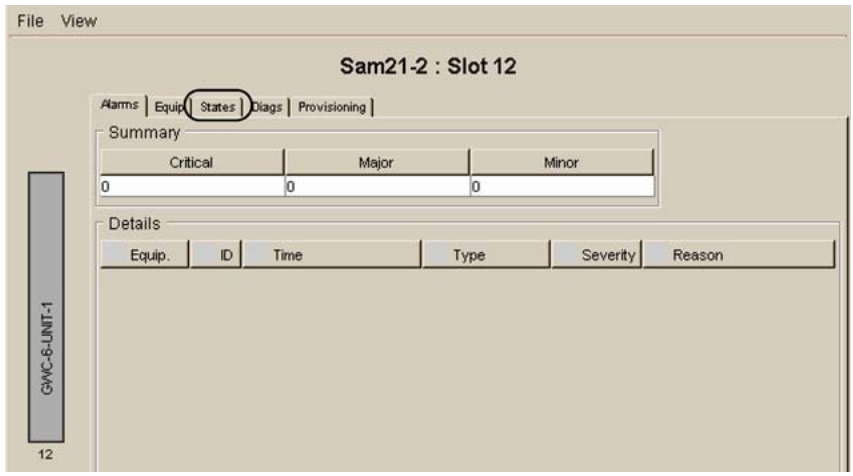
3 Select the **Maintenance** tab to display maintenance information about the node.



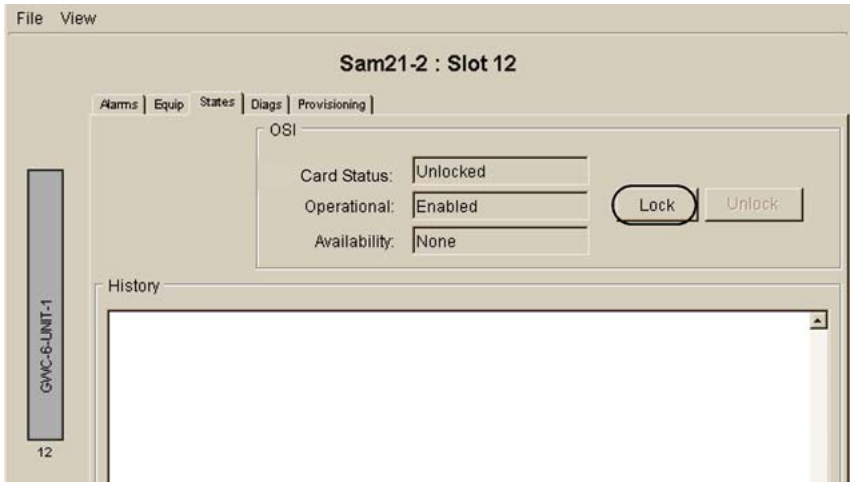
4 Click the **Card View** button for the card you want to lock.

At the CS 2000 SAM21 Manager client

5 In the card view, select the **States** tab.



6 In the States display, click the **Lock** button to lock the card.



7 Observe the system response in the History window.

The card is locked when you see the text "Application locked successfully" in the History display. The lock icon (circled in the following figure) should also be present on the card graphic at the left of the screen:

8 If necessary, return to step 2 and repeat this procedure for the next GWC card in the node.

9 The procedure is complete.

—End—

Unlock a GWC card

Purpose of this procedure

This procedure initiates a reboot of the GWC card causing the card to download its software from the CS 2000 Core Manager and to restart its call processing services and applications software.

When to use this procedure

Use this procedure:

- after replacing a GWC card.
- as part of a fault clearing activity.
- when a new software load is available.
- when you have completed reprovisioning a GWC card or GWC node (a node is made up of unit 0 and unit 1 GWC cards) and you would like the card or node to begin using the new provisioning values.
- when you have applied or removed a patch to the GWC software using the Network Patch Manager (NPM) and have saved a new GWC software image to the CS 2000 Core Manager.

Prerequisites

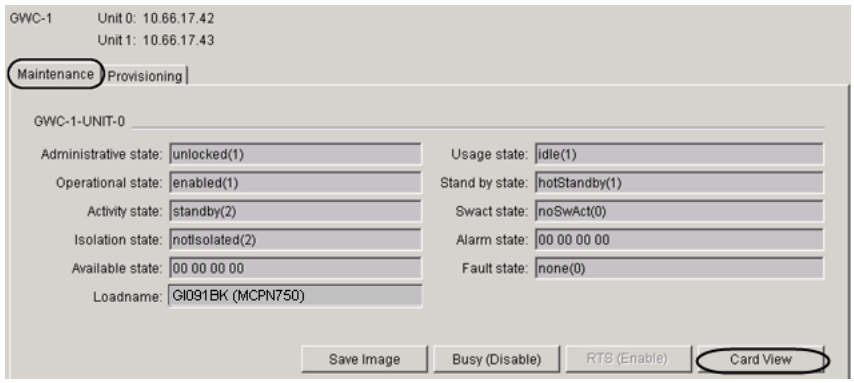
The GWC card must be locked. The procedure "Lock a GWC card" (page 25) provides instruction on how to lock a GWC card.

If the IP addresses for the card that you want to unlock and its mate are not contiguous, you cannot unlock the card. You must correct these addresses using procedure "Manually re-provision GWC cards" in the *Gateway Controller Configuration Management* (NN10205-511) before attempting to unlock the card.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.
2	From the Contents of: GatewayController frame, select the GWC node that contains the card you want to unlock.

3 Select the **Maintenance** tab to display maintenance information about the node.



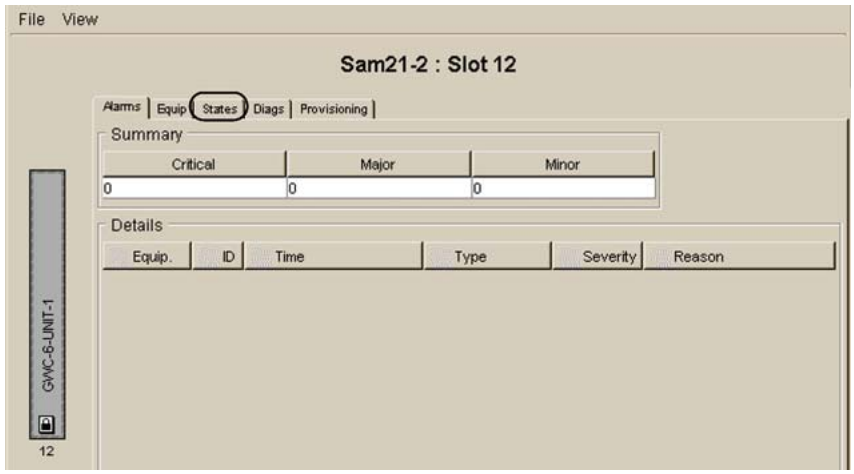
4 Click the **Card View** button for the card you want to unlock. This action opens the CS 2000 SAM21 Manager.

If a card is currently locked, all fields display the value <unknown>.

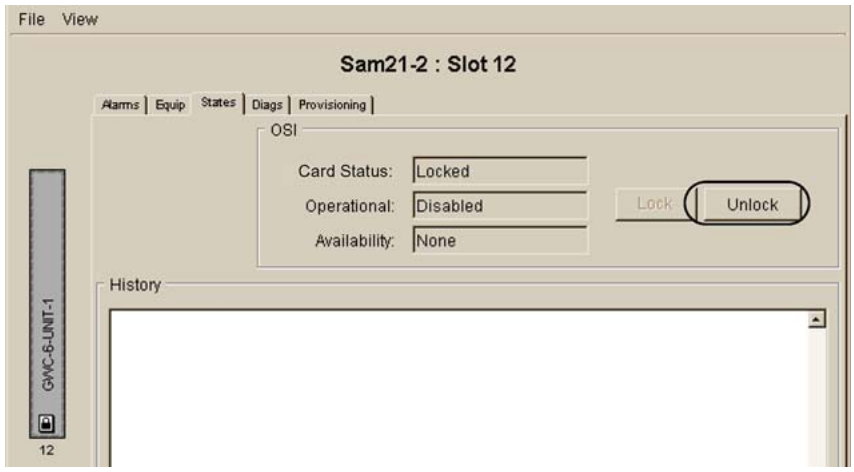
At the CS 2000 SAM21 Manager

5 In the card view, select the **States** tab.

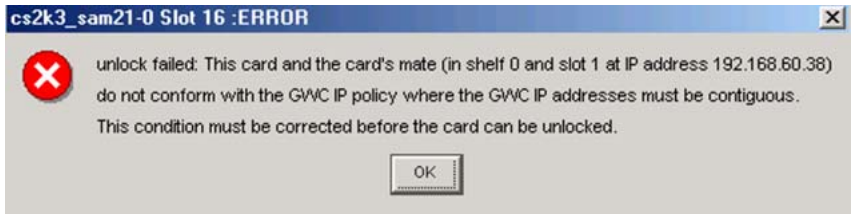
If you want to display the status of all cards in the shelf, select **Shelf View** from the **View** menu.



6 In the States display, click the **Unlock** button to unlock the card.



If the IP addresses for the selected card and its mate are not contiguous, the system displays the following error message:



Follow procedure "Manually re-provision GWC cards" in *Gateway Controller Configuration Management* (NN10205-511) to correct these addresses, then repeat this procedure.

7 Observe the system response in the History window.

The card is unlocked when you see the text "Application unlocked successfully".

8 Return to step 2 and repeat this procedure for the next GWC card until all the GWC cards have been unlocked and brought into service. Remember, each GWC node has two GWC cards.

9 The procedure is complete.

—End—

Invoke a manual protection switch (warm SWACT)

Purpose of this procedure

This procedure describes how to manually switch call processing activity from one GWC card to the mate GWC card within the GWC node.

If you wish to configure the GWC autonomous switch of activity (SWACT), see procedure "Enable or disable GWC autonomous SWACT" in *Gateway Controller Configuration Management* (NN10205-511).

When to use this procedure

Since you cannot busy an active GWC card if a standby GWC card is available, use this procedure before attempting to lock (busy) an active GWC card to reduce the risk of service interruption.

Prerequisites and guidelines

The following guidelines apply to this procedure:

- A warm SWACT converts the active GWC card to standby state. A warm SWACT preserves established calls and IP Security (IPSec) security associations (SA), while calls in setup are lost.
- During a cold or warm SWACT of a DPT GWC, there is no way to inform the far-end DPT GWC about the SWACT. As a result, DPT trunks on the far-end are released by a peer-call SIP INFO audit which runs approximately every 6 minutes.
- During a warm or cold SWACT, calls in setup over SIP-T trunks are lost (as is the case with other trunk types). However, over SIP-T trunks, the far end will continue to receive the setup alert (ringing) until one of the following occurs:
  - The end user answers and terminates the call.
  - A system audit runs and clears the trunks (once every 10 minutes).

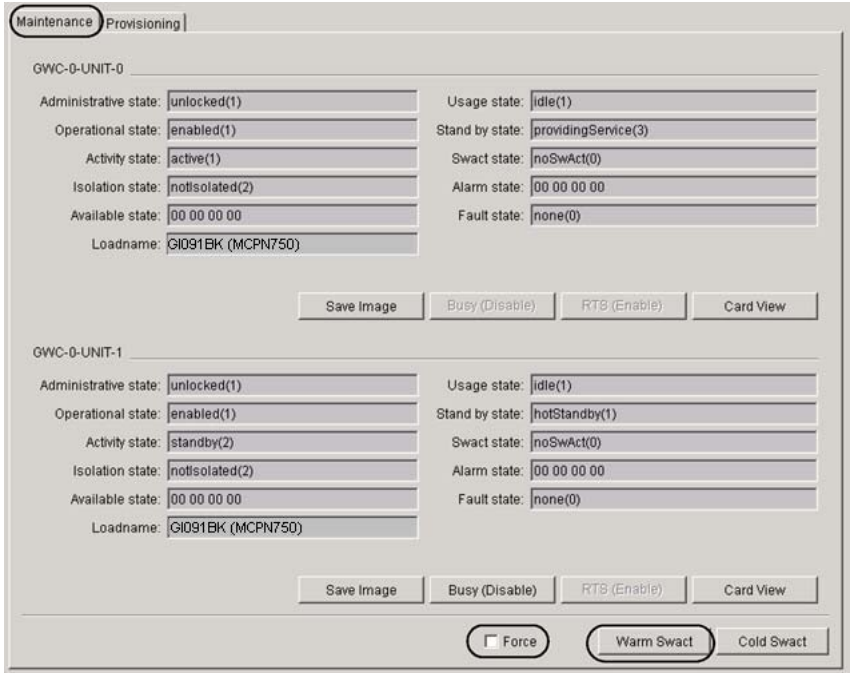
Action

Step	Action
	At the CS 2000 GWC Manager workstation
1	At the CS 2000 Management Tools Selector window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.
2	From the Contents of: Gateway Controller frame, select the GWC node on which you wish to perform the warm SWACT.

3 If necessary, select the Maintenance tab.

If you wish to override any pre-SWACT queries check the **Force** box, located next to the **Warm Swact** button. A pre-SWACT query is an additional set of checks performed before a warm SWACT. It is designed to detect when a warm SWACT is not recommended due to some degradation in the active unit. Only check the **Force** box if you believe that a warm SWACT is needed despite any possibility of degradation.

Click the **Warm Swact** button.



4 At the displayed warning message, click **OK** to confirm that you wish to perform the warm SWACT.

5 Observe the Maintenance Panel. The warm SWACT is successful when the "Stand by state" for the newly active unit is at "providing Service(3)" and the "Stand by state" for the newly standby unit is at "hotStandby(1)" in the Maintenance panel.

6 The procedure is complete.

—End—

Perform a cold manual protection switch of activity (SWACT)

Purpose of this procedure

This procedure provides a service impacting recovery routine. It forces a switch of active GWC cards in a node regardless of call progress on the active card.

When to use this procedure

Use this procedure only when instructed by Nortel support personnel.

Prerequisites

CAUTION
Service disruption
A cold SWACT drops all active calls and all calls in setup.

During a cold or warm SWACT of a DPT GWC, there is no way to inform the far-end DPT GWC about the SWACT. As a result, DPT trunks on the far-end are released by a peer-call SIP INFO audit which runs approximately every 6 minutes.

During a cold or warm SWACT, calls in setup over SIP-T trunks are lost (as is the case with other trunk types). However, over SIP-T trunks, the far end continues to receive the setup alert (ringing) until one of the following occurs:

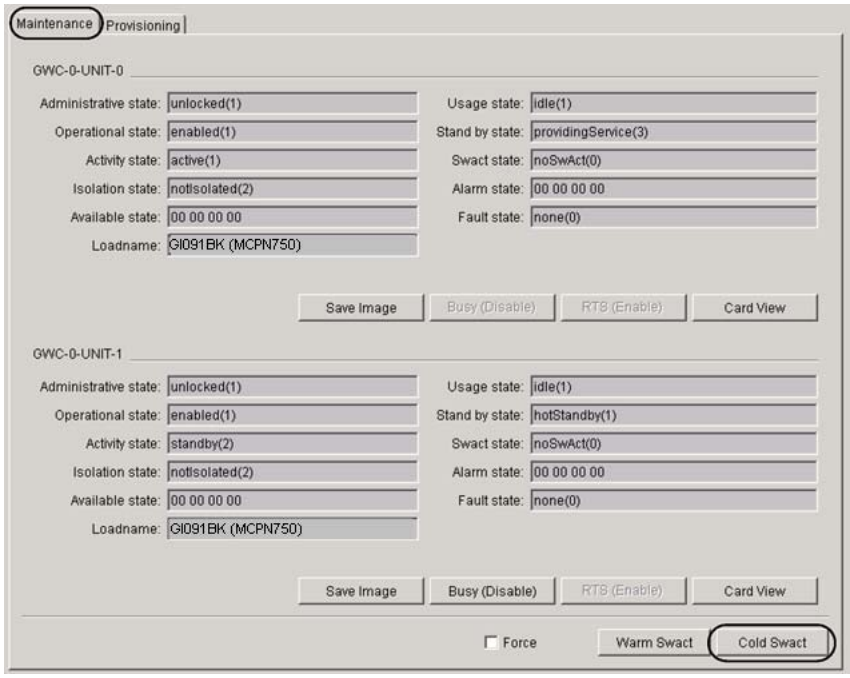
- The end user answers and terminates the call.
- A system audit runs and clears the trunks (once every 10 minutes).

Action

Perform a cold SWACT

Step	Action
	At the CS 2000 GWC Manager workstation
1	At the CS 2000 Management Tools Selector window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.
2	From the Contents of: GatewayController frame, select the GWC node that you wish to cold SWACT.

3 Select the **Maintenance** tab, then select the **Cold Swact** button.



4 At the displayed warning message, click **OK** to confirm that you wish to perform the cold SWACT.

If you wish to abort the operation, click **Cancel**.

5 Observe the Maintenance Panel. The cold SWACT is successful when the "Stand by state" for the newly active unit is at "providing Service(3)" and the "Stand by state" for the newly standby unit is at "hotStandby(1)" in the Maintenance panel.

6 The procedure is complete.

—End—

Disable (Busy) GWC card services

Purpose of this procedure

This procedure disables call processing activity and services on a single, standby GWC card within a GWC node.

If you wish to busy both GWC cards in the node, follow procedure "Busy a GWC node" in *Gateway Controller Configuration Management* (NN10205-511).

When to use this procedure

Use this procedure as part of maintenance or fault clearing activities.

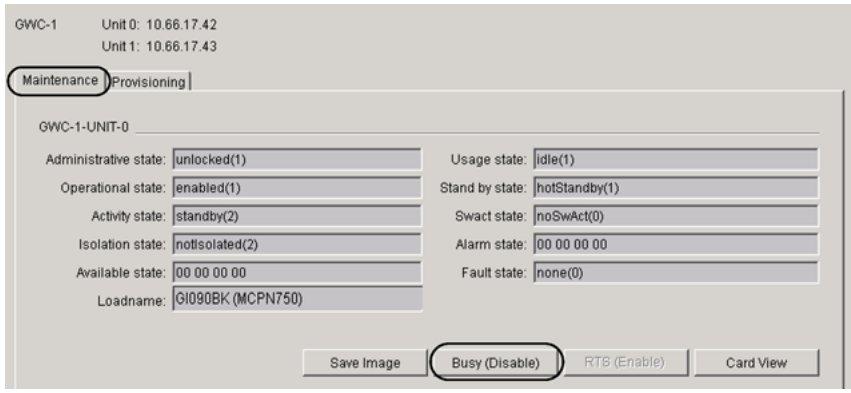
Prerequisites

The following prerequisites apply:

- To busy an active GWC card, you must first busy the standby GWC card or perform a warm SWACT on the node using procedure "Invoke a manual protection switch (warm SWACT)" (page 31).
- To busy a standby GWC card, it must be in the "hotstandby" state.
- To reduce the risk of service interruption, perform procedure "Lock a GWC card" (page 25), after you have performed the steps in this procedure.

Action

Step	Action
	At the CS 2000 GWC Manager workstation
1	At the CS 2000 Management Tools Selector window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.
2	From the Contents of: GatewayController frame, select the GWC node that you wish to busy services on.
3	Select the **Maintenance** tab, then click the **Busy (Disable)** button.



4 The procedure is complete.

—End—

Enable (RTS) GWC card services

Purpose of this procedure

This procedure enables restart of call processing software on the inactive GWC card in a GWC node.

To restart services on both GWC cards in a node, go to procedure "Manually return a GWC node to service" in *Gateway Controller Configuration Management* (NN10205-511).

When to use this procedure

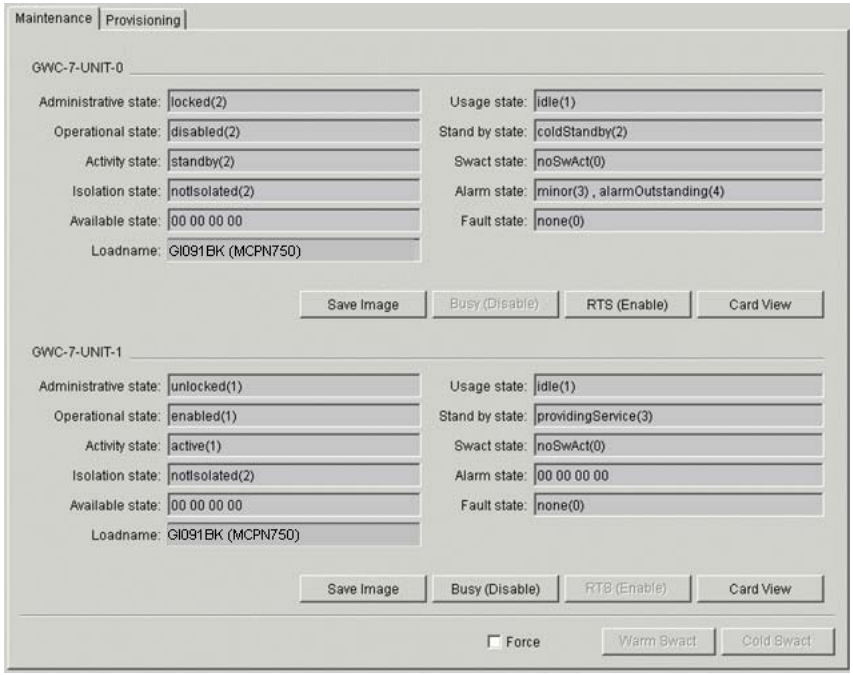
Use this procedure as a part of maintenance or fault clearing activities.

Prerequisites

The services on the GWC card must be in a busied state. Use procedure "Disable (Busy) GWC card services" (page 35) to perform this task.

Action

Step	Action
	At the CS 2000 GWC Manager workstation
1	At the CS 2000 Management Tools Selector window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.
2	From the Contents of: GatewayController frame, select the GWC node that you wish to perform an RTS on.
3	Select the **Maintenance** tab.
4	Determine which GWC card in the node has services busied. If both card's services are busied, see procedure "Manually return a GWC node to service" in *Gateway Controller Configuration Management* (NN10205-511).
5	Click the **RTS (Enable)** button for the standby card.



6 The procedure is complete.

—End—

Configure IPSec Profile on the GWC Manager

Purpose of this procedure

This procedure describes how to configure an IPSec Profile for a connection policy that you want to add to the selected Gateway Controller (GWC) node.

The IPSec Profile table defines the following aspects of a connection policy:

- the type of action (type of connection policy) that the GWC can apply to incoming and outgoing packets
- the key negotiation mechanism that the connection policy will use for IPSec security associations (SA)
- the grace period - the amount of time (in seconds) remaining in the IPSec SA lifetime before the SA is renewed.

When to use this procedure

Use this procedure to define a profile for the connection policy that you want to add to the selected GWC node.

Prerequisites

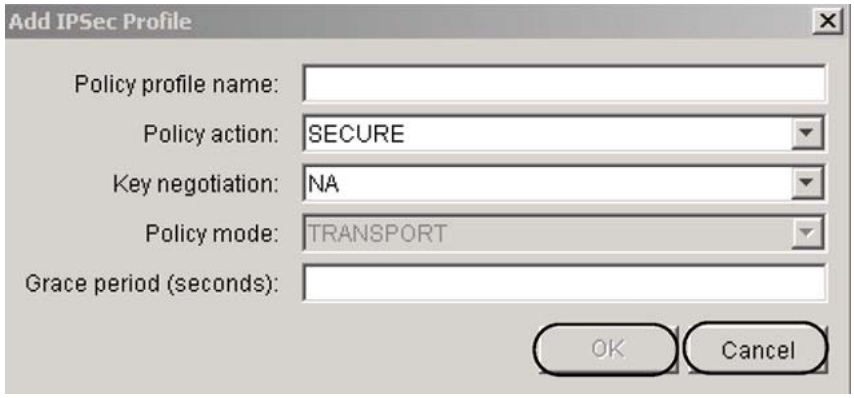
Provision IPSec only if a gateway that supports IPSec exists in your network.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, the **IPSec** tab, and then click the **IPSec Profile** tab.

4	Click the **Add** button in the lower right corner of the IPSec Profile panel to display the Add IPSec Profile dialog box.

You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.



5 Obtain and enter (or select from the drop-down menu) provisioning values for each field described in the following table.

IPSec Profile configuration fields

Field	Value	Description
Policy profile name:	<user defined string of alphanumeric characters>	Enter the name to be assigned to this IPSec profile.
Policy action:		This field defines the type of action (type of connection policy) that the GWC will apply to each packet that matches the policy configuration values. From the drop-down menu, select the appropriate value for the policy that you want to add.
	SECURE	IPSec processing will be applied to each packet that matches the policy.
	BYPASS	IPSec processing will not be applied to packets matching the policy between the GWC and the selected remote gateway. Incoming packets will be discarded. Outgoing packets will not be subject to IPSec processing.
	DISCARD	All packets matching the policy between the GWC and the selected remote gateway, will be discarded.
	FLEX	Use FLEX policy during the transition process, when some gateways associated with this connection policy operate in a secure mode and some do not. The FLEX policy provides the GWC with the flexibility of accepting secure and non-secure messages. FLEX policy supports both IPSec processing and bypassing of IPSec processing.

Field	Value	Description
If you choose the BYPASS or DISCARD policy action, all remaining fields become disabled (with predefined values displayed). Go to step 6 to continue the procedure. If you choose the SECURE or FLEX policy action, configure the remaining fields as follows.		
Key negotiation:	NA IKE KERBEROS	This field indicates the key negotiation mechanism for IPSec security associations (SA). Select KERBEROS only if you are configuring IPSec profile for a policy that will be used between the GWC and multimedia terminal adaptor (MTA) line gateways (cable solutions only). Select IKE if you are configuring IPSec profile for any other policy. If you chose BYPASS or DISCARD policy action, the pre-defined value is NA.
Policy mode:	TRANSPORT (NA)	This field specifies the mode in which IPSec traffic can be sent. This field is pre-defined with the appropriate value for the selected policy action: • TRANSPORT - default mode for SECURE or FLEX policy action • NA - for BYPASS or DISCARD policy action IPSec in tunnel mode is not supported.
Grace period (seconds)	0 to 2419200	Enter a value of 10% to 25% of the configured IPSec lifetime. For example, for an IPSec lifetime of 16 hours, enter a value between 5760 and 14400 (in seconds). This value represents the amount of time remaining in the IPSec SA lifetime before the SA is renewed. For example, an entry of 60 means that 60 seconds before the SA expiration, the selected key management will try to renew the SA. For GWCs with AUDCNTL_RMGC and AUDCNTL_RMGCINTL profiles, the recommended value is 0.

6 When you are finished entering data, click **OK**.

The newly defined policy profile data appears in the IPSec Profile table.

If you need to remove an entry, click the appropriate row, then click the **Delete** button. A Confirm deletion window appears. Click **Yes** to delete the entry.

7 Repeat this procedure as required to add more policy profiles.

8 The procedure is complete.

—End—

Configure IPSec Preference and Preference List on the GWC Manager

Purpose of this procedure

This procedure describes how to configure the IPSec Preference and IPSec Preference List tables.

CAUTION
Possible service disruption
All IPSec Preference provisioning values (except the IPSec preference name) must match the corresponding values configured on the remote gateway. Otherwise, an outage will occur.

The IPSec Preference parameters consist of an encryption and authentication algorithm, and a lifetime. These parameters are used to negotiate and establish pairs of IPSec security associations (SA) between the GWC and another network device.

When to use this procedure

Use this procedure when you wish to define IPSec preferences and preference lists. The IPSec Preference table entries are used to configure the IPSec Preference List table, which is required when configuring a SECURE or FLEX connection policy. These two tables must be configured before you can add a SECURE or FLEX connection policy to the selected GWC node.

You can configure multiple IPSec preferences and multiple preference lists. Each list can contain up to five preferences.

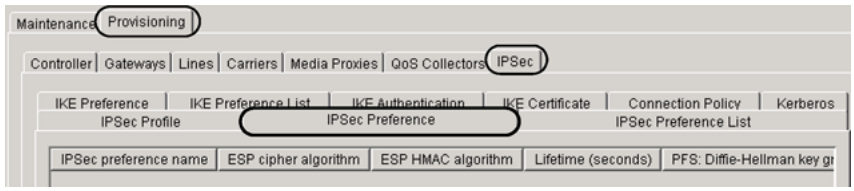
Prerequisites

Provision IPSec only if a gateway that supports IPSec exists in your network.

Action

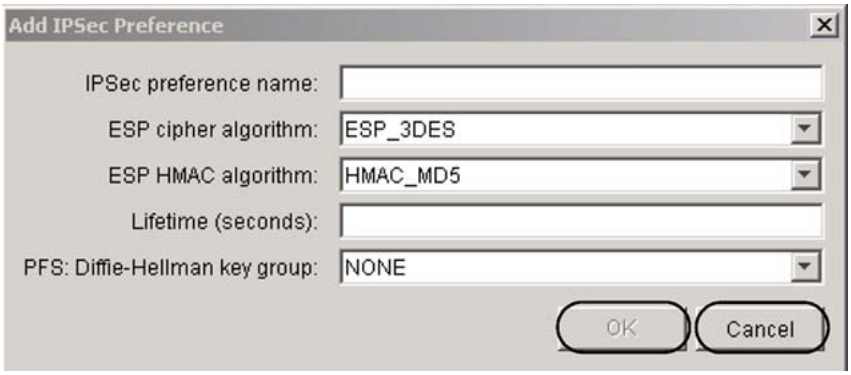
Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.

3 Click the **Provisioning** tab, the **IPSec** tab, then the **IPSec Preference** tab.



4 Click the **Add** button in the lower right corner of the IPSec Preference panel to display the Add IPSec Preference dialog box.

You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.



5 Obtain and enter (or select from the drop-down menu) provisioning values for each field described in the following table.

Once configured, you can only modify the name of the IPSec Preference. You cannot change any other values.

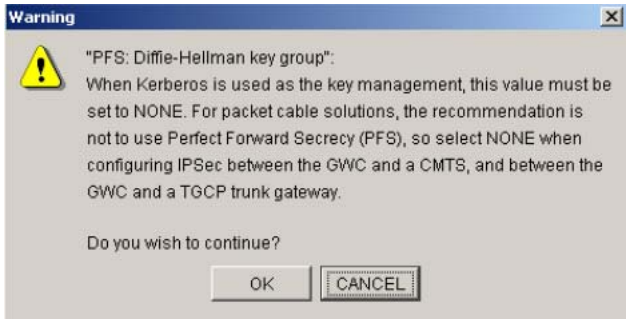
IPSec Preference configuration fields

Field	Values	Description
IPSec preference name:	<user-defined string of alphanumeric characters>	Enter the name to be assigned to this IPSec preference.
ESP cipher algorithm:	ESP_DES ESP_3DES ESP_NULL ESP_AES	This field provides the encryption mechanism that will be applied to the IPSec SA. Select the appropriate encapsulating security payload (ESP) cipher algorithm. Triple DES (3DES) algorithm is more secure than DES. The advanced encryption standard (AES) algorithm is currently not supported. NULL provides no encryption to the data, but does retain data integrity and authentication.

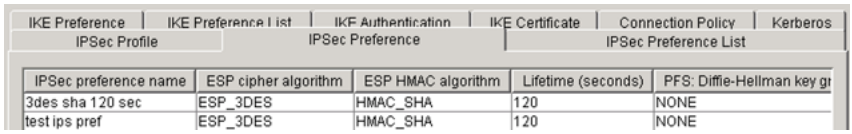
Field	Values	Description
ESP HMAC algorithm:	HMAC_MD5 HMAC_SHA	This field provides the authentication method for this IPSec preference. Select one of the following ESP hashed message authentication code (HMAC) algorithms: • MD5 (message digest 5) • SHA (secure hash algorithm) Both algorithms are one-way functions that take an arbitrary length input and generate fixed-length output called hash value. SHA is considered more secure then MD5.
Lifetime (seconds)	0 to 2419200	Specify (in seconds) the desired lifetime of an IPSec SA established using this preference. **ATTENTION** For AUDCNTL_RMGC and AUDCNTL_RMGCINTL profiles, enter a value between 10 and 20 when configuring a connection policy with Kerberos. The system does not accept any other values.
PFS: Diffie-Hellman key group:	NONE 1 2	When IKE is used as the key management, select 1 or 2 to indicate what Oakley group will be used for a Diffie-Hellman key exchange during phase 2 negotiation (establishing IPSec SAs pair). Select NONE for IPSec • between GWC and Media Server 2010 gateways, which do not support Perfect Forward Secrecy (PFS). • with Kerberos as the key management • between GWC and CMTS or TGCP trunk gateways (in packet cable solutions)

6 When you are finished entering data, click the **OK** button.

The system displays the following warning:



Click **OK** and notice that the newly defined data appears in the IPSec Preference List table.



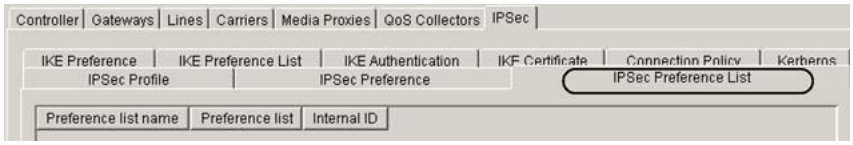
If you need to remove the new entry, click the appropriate row to highlight it, then click the **Delete** button. A Confirm deletion window appears. Click **Yes** to delete the entry.

You cannot delete an IPSec Preference that is used in an existing connection policy.

7 Use the following table to determine your next step.

If you wish to	Do
add more IPSec preferences	repeat steps 4 to 7
configure IPSec Preference List	go to step 8

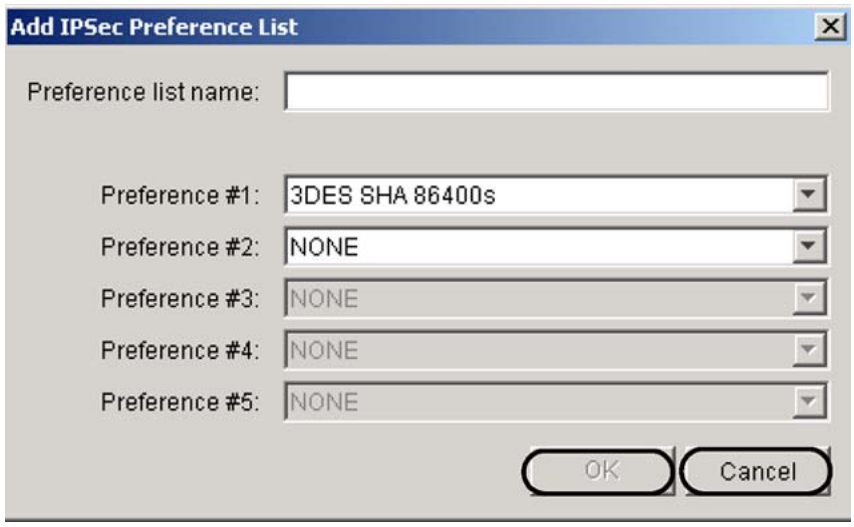
8 Click the **IPSec Preference List** tab.



9 Click the **Add** button in the lower right corner of the IPSec Preference List panel to display the Add IPSec Preference List dialog box.

In the Preference #1: field, the system displays the first preference name from the IPSec Preference table, but you can change this value. The second field is set to NONE, the remaining three fields are disabled. When you select and add the second preference, the third one becomes active, and so on.

You have the option to cancel the procedure at any time (but before you click the **OK** button). To do that, click the **Cancel** button.



10 In the Preference list name: field, enter the name that will be assigned to this IPSec preference list.

Once configured, the only IPSec Preference List field that you can modify is the name.

11 Click the Preference #1: drop-down menu and select the name of one of the previously defined IPSec preferences. This preference constitutes the first item on the list.

If you want to add more items, repeat this step for the remaining fields. Otherwise, go to step 12.

An IPSec preference list can contain up to five preferences. The order of these preferences is very important, since the GWC will try to match first preference #1, then #2, and so on.

12 Click **OK**.

The newly defined data appears in the IPSec Preference List table.

If you need to remove the new entry, click the appropriate row to highlight it, then click the **Delete** button. A Confirm deletion window appears. Click **Yes** to delete the entry.

You cannot delete an IPSec preference list that is used in an existing connection policy.

13 If required, repeat steps 9 to 12 to add more IPSec preference lists.

14 The procedure is complete.

—End—

Configure IKE Preference and Preference List on the GWC Manager

Purpose of this procedure

This procedure describes how to configure the IKE Preference and Preference List tables. IKE is a cryptographic key management mechanism used to negotiate and derive keys for the IPSec security associations (SA).

CAUTION
Possible service disruption
All IKE Preference provisioning values (except the IKE preference name) must match the corresponding values configured on the remote gateway. In particular, the IKE and IPSec lifetime values configured on the GWC must match the IKE and IPSec lifetime values configured at the gateway. Otherwise, an outage will occur.

The IKE Preference parameters are used to negotiate and establish a secure authenticated communication channel between the Gateway Controller (GWC) and another network device. This process is also referred to as phase 1.

Note that only main mode is supported on the GWC (aggressive mode is not supported). Also, there are two IKE authentication methods supported on GWC nodes:

- PRESHARED (pre-shared key)
- Digital Signatures

At the end of phase 1, an IKE SA is created, which is used to negotiate SAs for IPSec.

When to use this procedure

Use this procedure to define IKE preferences and preference lists. The IKE Preference table entries are used to configure the IKE Preference List table, which is required when configuring a SECURE or FLEX connection policy with IKE key negotiation. These two tables must be configured first before you can add a SECURE or FLEX connection policy to the selected GWC node.

You can configure multiple IKE preferences and multiple preference lists. Each list can contain up to 3 preferences.

Prerequisites

None

Action

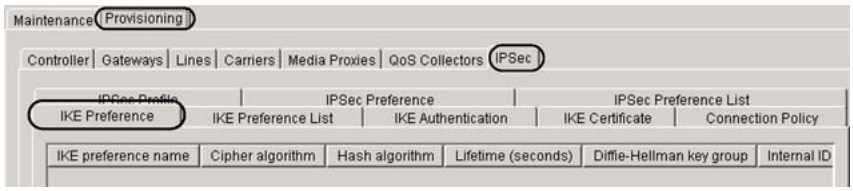
Step	Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

2 From the Contents of: GatewayController frame, select the appropriate GWC node.

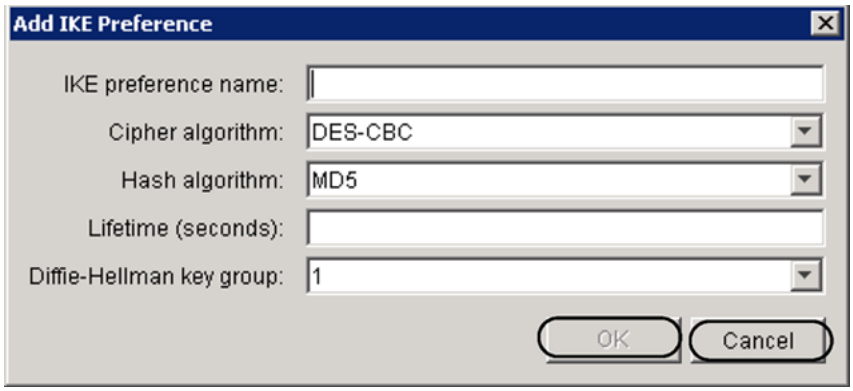
3 Click the **Provisioning** tab, the **IPSec** tab, then the **IKE Preference** tab.



4 Click the **Add** button in the lower right corner of the IKE Preference panel to display the Add IKE Preference dialog box.

Once configured, the only IKE Preference field that you can modify is the name.

You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.



5 Obtain and enter (or select from the drop-down menu) provisioning values for each field described in the following table.

IKE Preference configuration fields

Field	Values	Description
IKE preference name:	<user-defined string of alphanumeric characters>	Enter the name to be assigned to this IKE preference.
Cipher algorithm:	DES-CBC 3DES-CBC AES-CBC	Select the cipher algorithm (in CBC mode) for this IKE preference. Triple data encryption standard (3DES) algorithm is more secure than DES. The advanced encryption standard (AES) algorithm is extremely efficient and very secure but it is not part of the IKE RFC2409, so it is not supported by the remote gateway.
Hash algorithm:	MD5 SHA	This field indicates the cryptographic hash algorithm for this IKE preference. Select one of the following algorithms: • MD5 (message digest 5) • SHA (secure hash algorithm) Both algorithms are one-way functions that take an arbitrary length input and generate fixed-length output called hash value. SHA is considered more secure then MD5.
Lifetime (seconds):	0 to 2419200	Enter the lifetime (in seconds) of an IKE SA established using this preference. The IKE SA can be used to establish several IPSec SAs, so this value is usually larger than the lifetime of an IPSec SA. When the IPSec SA expires, it can be renewed under the protection of the same IKE SA.
Diffie-Hellman key group:	1 2	This field indicates the Oakley group to be used for a Diffie-Hellman (DH) key exchange during phase 1 negotiation (establishing IKE SA). For Media Server 2010 gateways, apply the following guidelines: • DH key group 1 on the GWC corresponds to dH-786-BIT setting on the gateway. • DH key group 2 on the GWC corresponds to dH-1024-BIT setting on the gateway.

6 When you are finished entering data, click **OK** .

The newly defined data appears in the IKE Preference table.

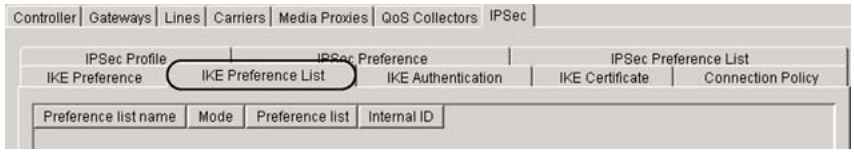
If you need to remove the new entry, click the appropriate row to highlight it, then click the **Delete** button. A Confirm deletion window appears. Click **Yes** to delete the entry.

You cannot delete an IKE Preference that is used in an existing connection policy.

7 Use the following table to determine your next step.

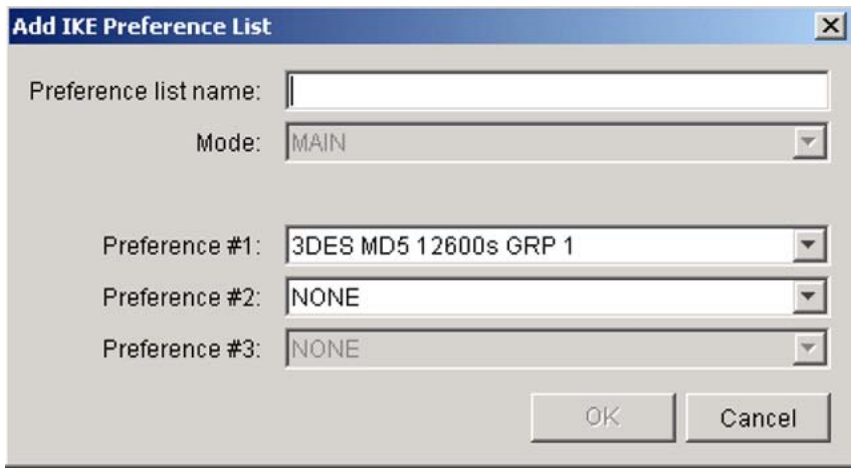
If you wish to	Do
add more IKE preferences	repeat steps 4 to 7
configure IKE Preference List table	go to step 8

8 Click the **IKE Preference List** tab.



9 Click the **Add** button in the lower right corner of the IKE Preference List panel to display the Add IKE Preference List dialog box.

In the Preference #1: field, the system displays the first preference name from the IKE Preference table, but you can change this value. The second field is set to NONE, and the third is disabled. When you select and add the second preference, the third one becomes active.



10 In the Preference list name: field, enter the name that will be assigned to this IKE preference list.

11 Click the Preference #1: drop-down menu and select the name of one of the previously defined IKE preferences. This preference constitutes the first item on the list.

If you want to add more items, repeat this step for the remaining two fields. Otherwise, go to step 12.

An IKE preference list can contain up to three preferences. The order of these preferences is very important, since the GWC will try to match first preference #1, then #2, then #3.

Once configured, the only IKE Preference List field that you can modify is the name.

12 Click **OK**.

The newly defined list data appears in the IKE Preference List table.

If you need to remove the new entry, click the appropriate row, then click the **Delete** button. A Confirm deletion window appears. Click **Yes** to delete the entry.

You cannot delete an IKE preference list that is used in an existing connection policy.

13 If required, repeat steps 9 to 12 to add more IKE preference lists.

14 The procedure is complete. If applicable, return to the higher-level task flow or procedure that directed you to this procedure.

—End—

Download IKE certificates on the GWC Manager

Purpose of this procedure

This procedure describes how to retrieve a set of X.509 digital certificates for a selected Gateway Controller (GWC) node. A GWC uses a Digital Signatures (X.509 Certificates) to authenticate remote media gateways and to establish secure associations (SA).

The GWC Manager retrieves a set of X.509 certificates and the secret private key from the Certificate Manager.

Each set of X.509 certificates contains:

- Root Certificate Authority (CA): the top-level trust anchor
- Intermediate CA: the chain CA signed by the root CA
- Device Certificate: the GWC X.509 certificate issued by the Intermediate CA. This is the Digital Signature that uniquely identifies the GWC.
- Private Key: the hidden private key associated with the device certificate

When to use this procedure

Use this procedure when you wish to configure the selected GWC with the Digital Signatures IKE authentication method.

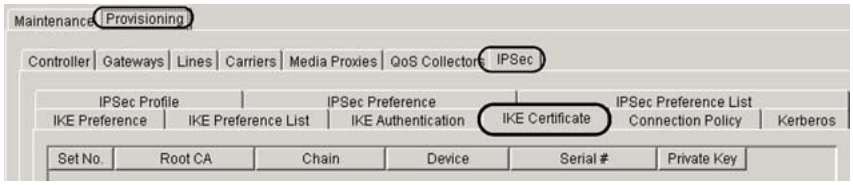
Prerequisites

The GWC and the GWC Manager must be running to an (I)SN09U or up load.

The GWC Manager must be configured to retrieve certificates.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, the **IPSec** tab, then the **IKE Certificate** tab.



4 Click the **Refresh** button in the lower right corner of the IKE Certificate panel to refresh the display.

If there is an existing set of certificates displayed, the **Download** button is disabled. You can only download one set for each GWC node.

If the **Download** button is disabled, go to step 6.

5 Click the **Download** button.

If the retrieve process succeeds, the system retrieves a set of certificates and displays it in the IKE Certificate table.

If the retrieve process fails, the system displays an error message and raises the CMT304 alarm. For the description of the CMT304 log report and the required action, see *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

6 The procedure is complete.

—End—

View IKE certificates on the GWC Manager

Purpose of this procedure

This procedure describes how to access and view detail information about certificates retrieved for a selected Gateway Controller (GWC) node.

For information about how to retrieve certificates for a GWC, see procedure "Download IKE certificates" (page 53).

When to use this procedure

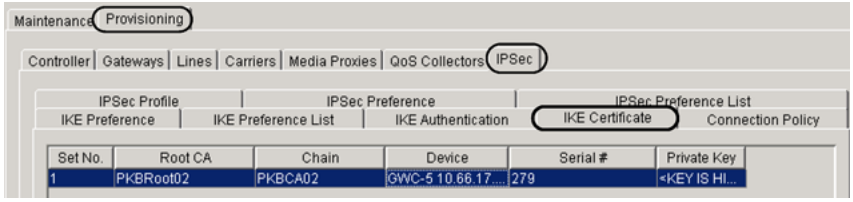
Use this procedure when you wish to view properties of certificates currently assigned to a selected GWC.

Prerequisites

At least one set of certificates must be assigned to a selected GWC.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, the **IPSec** tab, then the **IKE Certificate** tab.
4	Click the displayed certificate set to highlight it.
5	Click the **View** button at the bottom of the screen to display the View IKE Certificates information box.



6 Review and, if required, note properties of the displayed certificates.

The displayed data includes the subject and issuer name, as well as the creation and expiry date for the following certificates:

- Root Certificate Authority (CA): the top-level trust anchor
- Intermediate CA: the chain CA signed by the root CA
- Device Certificate: the GWC X.509 certificate issued by the Intermediate CA. This is the Digital Signature that uniquely identifies the GWC.
- Private Key: the hidden private key associated with the device certificate

  If any of the certificates is expiring within the next 30 days, a GWC320 alarm is raised.

  If any of the certificates is expired, an outage may occur.

7 Click **OK** to close the information box.

8 The procedure is complete.

—End—

Delete IKE certificates on the GWC Manager

Purpose of this procedure

This procedure describes how to delete a set of IKE certificates currently assigned to a selected Gateway Controller (GWC) node.

For information about how to retrieve certificates for a GWC, see procedure "Download IKE certificates" (page 53). For information about how to view certificates currently assigned to a GWC, see procedure "View IKE certificates" (page 55).

When to use this procedure

Use this procedure when you wish to delete a set of certificates currently assigned to a selected GWC.

Prerequisites

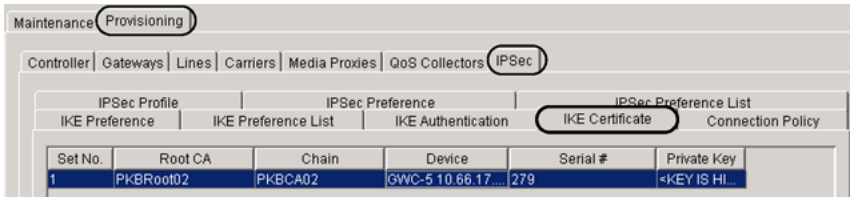
Consider the following rules before starting this procedure:

- If there is only one set of certificates and at least one IKE authentication entry is configured with Digital Signatures authentication method, you cannot delete these certificates.
- After a root certificate change occurs, the system adds a second set of certificates to the GWC, so two sets of certificates are displayed in the IKE Certificates table.

  Once all affected remote gateways have their certificates updated with the new root certificate, you must delete the outdated GWC certificate set. You cannot delete the new set.
- If the selected set of certificates is currently used by a connection policy, you cannot delete these certificates.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, the **IPSec** tab, then the **IKE Certificate** tab.



4 Click the **Refresh** button at the bottom of the screen to update the display.

5 Click the certificate set that you want to delete to highlight it.

If the selected set of certificates is currently used by a connection policy, you cannot delete these certificates.

6 Click the **Delete** button at the bottom of the screen.

7 At the confirmation window, click **Yes** to confirm your request. Click **No** to cancel the command.

8 If the process fails and the system displays the following error message, contact your next level of support. Otherwise, go to the next step.

9 The procedure is complete.

—End—

Configure pre-shared key IKE authentication on the GWC Manager

Purpose of this procedure

This procedure describes how to configure the pre-shared key IKE authentication to be used for secure communication between a Gateway Controller (GWC) and a specified remote media gateway.

IKE is a cryptographic key management mechanism used to negotiate and derive keys for the IPSec security associations (SA).

With the pre-shared key method, the authentication is performed by a key that is known to both the GWC and the media gateway.

When to use this procedure

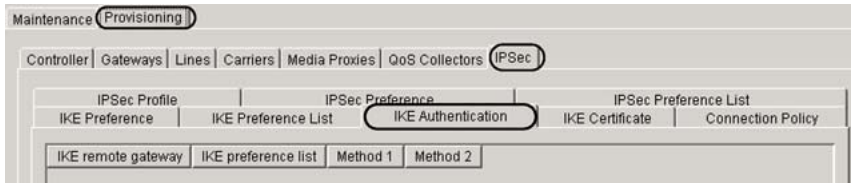
Use this procedure when you need to configure the IKE preference list and the pre-shared key authentication method to be used for secure communication between a Gateway Controller (GWC) and a specified remote media gateway. The IKE Authentication table entries are used when configuring a SECURE or FLEX connection policy with IKE. IKE preference list and IKE authentication method must be configured first, before you can add a SECURE or FLEX connection policy with IKE to the selected GWC node.

Prerequisites

The IKE Preference and IKE Preference List tables must be configured before you start this procedure. If required, complete procedure "Configure IKE Preference and Preference List" (page 48).

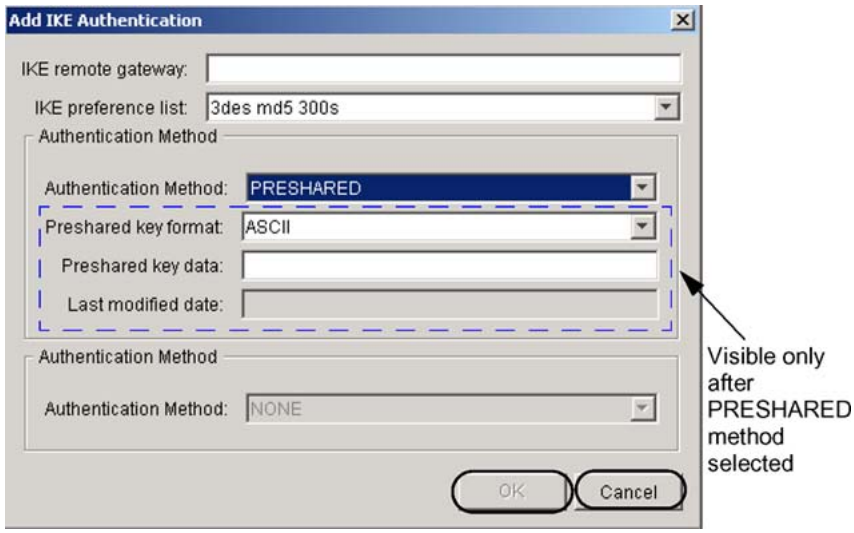
Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, the **IPSec** tab, then the **IKE Authentication** tab.



The most recently added Authentication Method is always listed as Method 1 in the IKE authentication tab. There is no functional significance or special handling of the order of the Authentication Methods.

4 Click the **Add** button in the lower right corner of the IKE Authentication panel to display the Add IKE Authentication dialog box.



You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.

5 Obtain and enter (or select from the drop-down menu) provisioning values for each field described in the following table.

IKE Authentication configuration fields

Field	Values	Description
IKE remote gateway:	<gateway IP address>	Enter the exact IP address of the remote gateway for which you are configuring this authentication method. This IP address must match the remote host address in the connection policy that uses this IKE authentication.

Field	Values	Description
IKE preference list:	<names of the previously defined IKE preference lists>	Click the drop-down menu and select the name of one of the previously defined IKE preference lists. By default, the system displays the first preference list name from the IKE Preference List table. The selected IKE preference list must match the list configured on the remote gateway.
Authentication method:	NONE PRESHARED Digital Signatures	Click the drop-down menu and select PRESHARED as the IKE authentication method to be used for secure communication with the selected remote gateway. The system displays additional configuration fields. The default value is NONE, but NONE is not a valid option when adding an IKE authentication. The second Authentication Method field stays disabled until you complete this procedure. The selected authentication method must match the method configured on the remote gateway.
Preshared key format:	ASCII or HEX	Select ASCII or HEX to indicate the format of the pre-shared key.
Preshared key data:	<user-defined key; 1 to 48 characters>	Enter the 1- to 48-character long pre-shared key that will be used to authenticate the remote gateway. Although the minimum allowed key length is one character, make sure that this key is long and random enough to provide an appropriate level of secrecy and security. The value entered in this field must match the pre-shared key configured on a gateway.
Last modified date:	<date time>	This is a read-only field that displays the date and time when the pre-shared key was last modified. If required, see procedure "Modify IKE pre-shared keys" (page 115) for information about how to modify pre-shared keys.

6 Click the **OK** button.

The newly defined data appears in the IKE Authentication table.

If you need to remove the new entry, click the appropriate row to highlight it, then click the **Delete** button. At the confirmation window, click **Yes** to delete the entry.

You cannot delete an IKE Authentication that is used in an existing connection policy.

7 The procedure is complete.

—End—

Configure Digital Signatures IKE authentication on the GWC Manager

Purpose of this procedure

This procedure describes how to configure the Digital Signatures IKE authentication to be used for secure communication between a Gateway Controller (GWC) and a specified remote media gateway.

IKE is a cryptographic key management mechanism used to negotiate and derive keys for the IPSec security associations (SA).

With this method, Certificate Manager is responsible for management and replacement of X.509 digital certificates and keys used in IPSec and IKE authentication of network elements.

When to use this procedure

Use this procedure when you need to configure the IKE preference list and the Digital Signatures authentication method to be used for secure communication between a Gateway Controller (GWC) and a specified remote media gateway. The IKE Authentication table entries are used when configuring a SECURE or FLEX connection policy with IKE. IKE preference list and IKE authentication method must be configured first, before you can add a SECURE or FLEX connection policy with IKE to the selected GWC node.

Prerequisites

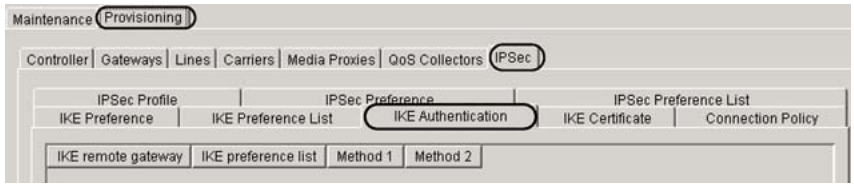
The IKE Preference and IKE Preference List tables must be configured before you start this procedure. If required, complete procedure "Configure IKE Preference and Preference List" (page 48).

You must first retrieve a certificate set for the selected GWC. If required, see procedure "Download IKE certificates" (page 53).

Action

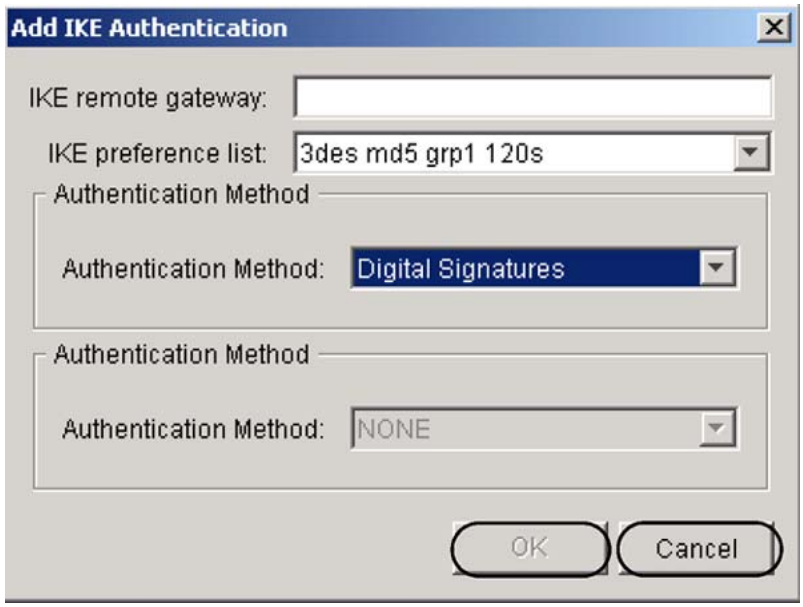
Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.

3 Click the **Provisioning** tab, the **IPSec** tab, then the **IKE Authentication** tab.



The most recently added Authentication Method is always listed as Method 1 in the IKE authentication tab. There is no functional significance or special handling of the order of the Authentication Methods.

4 Click the **Add** button in the lower right corner of the IKE Authentication panel to display the Add IKE Authentication dialog box.



You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.

5 Obtain and enter (or select from the drop-down menu) provisioning values for each field described in the following table.

IKE Authentication configuration fields

Field	Values	Description
IKE remote gateway:	<gateway IP address>	Enter the exact IP address of the remote gateway for which you are configuring this authentication method. This IP address must match the remote host address in the connection policy that uses this IKE authentication.
IKE preference list:	<names of the previously defined IKE preference lists>	Click the drop-down menu and select the name of one of the previously defined IKE preference lists. By default, the system displays the first preference list name from the IKE Preference List table. The selected IKE preference list must match the list configured on the remote gateway.
Authentication method:	NONE PRESHARED Digital Signatures	Click the drop-down menu and select Digital Signatures as the IKE authentication method to be used for secure communication with the selected remote gateway. The default value is NONE, but NONE is not a valid option when adding an IKE authentication. The second Authentication Method field stays disabled until you complete this procedure. The selected authentication method must match the method configured on the remote gateway.

6 Click the **OK** button.

The newly defined data appears in the IKE Authentication table.

If you need to remove the new entry, click the appropriate row to highlight it, then click the **Delete** button. At the confirmation window, click **Yes** to delete the entry.

You cannot delete an IKE Authentication that is used in an existing connection policy.

7 The procedure is complete.

—End—

Transition IKE authentication method on the GWC Manager

Purpose of this procedure

This procedure describes how to add a second authentication method to an existing IKE authentication table, currently configured with one of the following methods:

- PRESHARED (pre-shared key)
- Digital Signatures

You need to add the second authentication method when you are migrating from one authentication method to the other. This procedure must be part of a network-level transition. During the transition process, you can have two authentication methods enabled, so the Gateway Controller (GWC) can be flexible and continue IPSec negotiations with the remote gateway, using the method currently configured on that gateway. Once the authentication method is changed on the remote gateway, you can disable the second method using procedure "Complete transition of IKE authentication method" (page 71).

ATTENTION

Use the following procedure to ensure that authentication methods on both the GWC and the remote gateway match, in order to provide seamless transition between authentication methods and to avoid outage.

When to use this procedure

Use this procedure when you are in the process of changing the IPSec IKE authentication method in your network and you need to reconfigure the IKE authentication method for a selected connection policy.

All changes to the selected IKE authentication table are automatically applied to the connection policy that uses this authentication.

Prerequisites

If you are migrating from pre-shared key to Digital Signatures, IKE certificates set must be first retrieved for the GWC node. If required, see procedure "Download IKE certificates" (page 53).

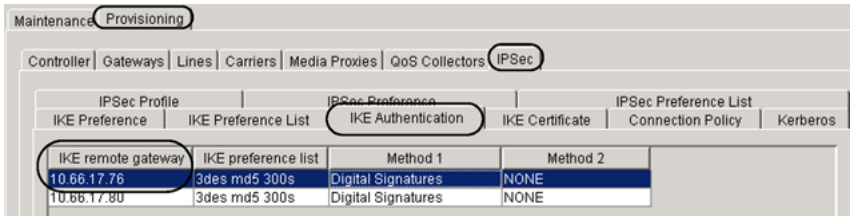
Action

Step	Action
	At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

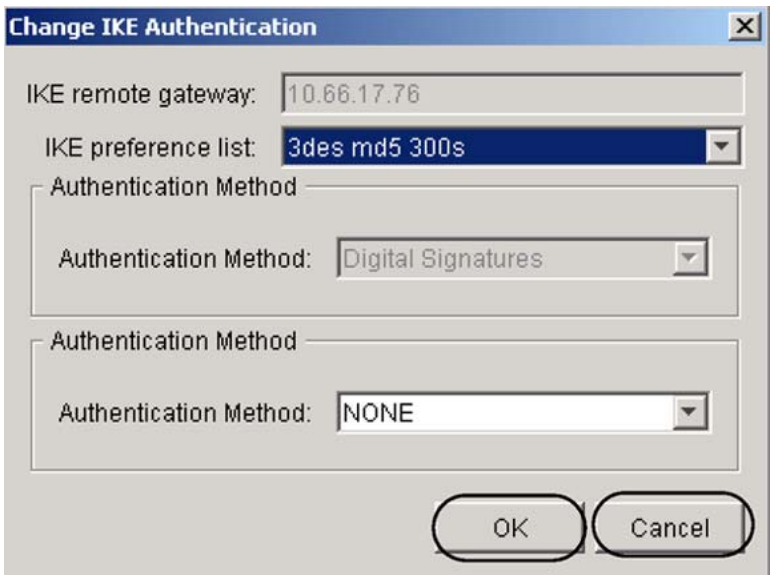
2 From the Contents of: GatewayController frame, select the appropriate GWC node.

3 Click the **Provisioning** tab, the **IPSec** tab, then the **IKE Authentication** tab.



4 Under IKE remote gateway heading, find the IP address of the remote gateway associated with the connection policy, for which you want to add the second authentication method. Click the appropriate row to highlight it.

5 Click the **Change** button in the lower right corner of the IKE Authentication panel to display the Change IKE Authentication dialog box.



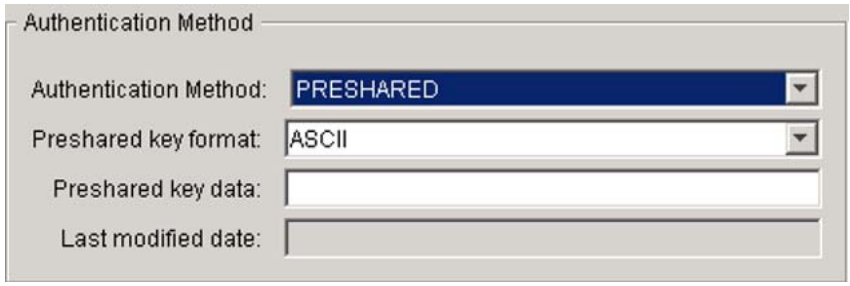
You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.

6 Click the Authentication Method field currently configured with the value NONE and from the drop-down menu, select the second

authentication method. Do not change the existing authentication method. Use the following guidelines:

- You cannot configure two Digital Signatures or two PRESHARED methods. If you try, the system displays an error message.
- If the current method is PRESHARED, select Digital Signatures.
- If the current method is Digital Signatures, select PRESHARED.

  When you select PRESHARED, the system displays the following additional configuration fields.



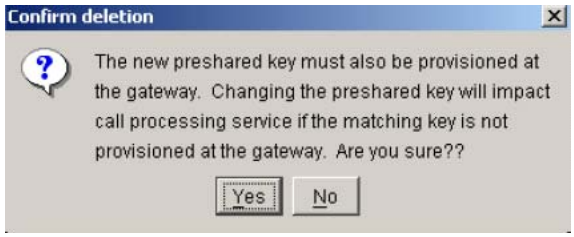
Configure these newly displayed fields, as described in the following table.

Field	Values	Description
Preshared key format:	ASCII or HEX	Select ASCII or HEX to indicate the format of the pre-shared key.
Preshared key data:	<user-defined key; 1 to 48 characters>	Enter the 1- to 48-character long pre-shared key that will be used to authenticate the remote gateway. Although the minimum allowed key length is one character, make sure that this key is long and random enough to provide an appropriate level of secrecy and security. The value entered in this field must match the pre-shared key configured on a gateway. For more information, contact your network administrator.
Last modified date:	<date time>	This is a read-only field that displays the date and time when the pre-shared key was last modified.

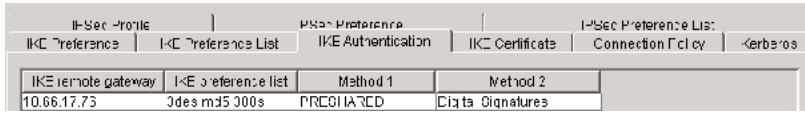
The most recently added authentication method is always listed as Method 1 in the IKE authentication tab. The current authentication method is moved and listed as Method 2 in the IKE authentication tab. There is no functional significance or special handling of the order of Authentication methods.

7 Click the **OK** button.

At the following confirmation message, click **Yes** to continue.



Both authentication methods are displayed in the IKE Authentication table.



8 The procedure is complete.

—End—

Complete transition of IKE authentication method on the GWC Manager

Purpose of this procedure

This procedure describes how to remove one authentication method from an existing IKE authentication table, currently configured with both of the following methods:

- PRESHARED (pre-shared key)
- Digital Signatures

CAUTION
Possible service disruption
The IKE authentication method configured on the GWC and the remote gateway must match. Otherwise, an outage will occur.

You need to remove the second authentication method when you are migrating from one authentication method to the other and the authentication method on the remote gateway has changed. This procedure must be part of a network-level transition. During the transition process, you will have two authentication methods enabled, so the Gateway Controller (GWC) can be flexible and continue IPSec negotiations with the remote gateway, using the method currently configured on that gateway. Once the authentication method is changed on the remote gateway, you can disable the unused method using this procedure.

When to use this procedure

Use this procedure when you are in the process of changing the IPSec IKE authentication method in your network, the new authentication method is already configured on the remote gateway, and now you need to remove the unused authentication method for a selected connection policy on the GWC.

All changes to the selected IKE authentication table are automatically applied to the connection policy that uses this authentication.

Prerequisites

The selected IKE authentication is currently configured with both methods: Digital Signatures and PRESHARED.

Action

Step	Action

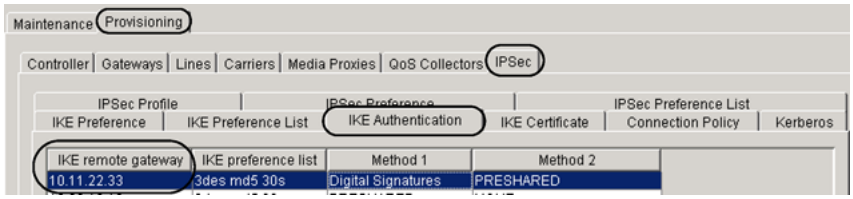
At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

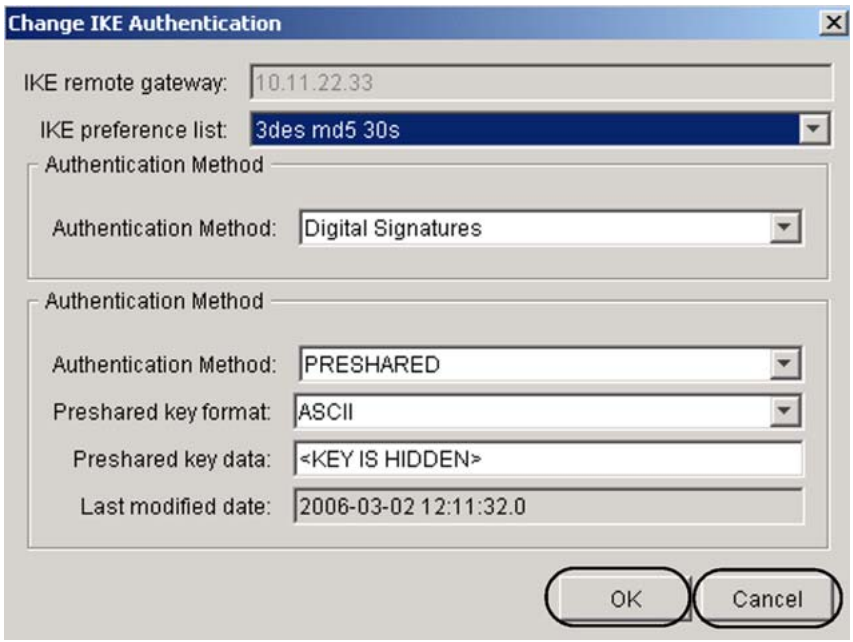
2 From the Contents of: GatewayController frame, select the appropriate GWC node.

3 Click the **Provisioning** tab, the **IPSec** tab, then the **IKE Authentication** tab.

4 Under IKE remote gateway heading, find the IP address of the remote gateway associated with the connection policy, for which you want to modify the IKE authentication. Click the appropriate row to highlight it.



5 Click the **Change** button in the lower right corner of the IKE Authentication panel to display the Change IKE Authentication dialog box.



You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.

6 Click the field with the authentication method that you want to disable and from the drop-down menu, select NONE.

Use the following guidelines:

- If you are migrating from PRESHARED to Digital Signatures, click the Authentication Method field configured with PRESHARED and from the drop-down menu, select NONE. This action will retain only Digital Signatures, confirming successful selection.
- If you are migrating from Digital Signatures to PRESHARED, click the Authentication Method field configured with Digital Signatures and from the drop-down menu, select NONE. This action will retain only PRESHARED, confirming successful selection.
- You cannot change both methods to NONE.

The remaining Authentication Method is always listed as Method 1 in the IKE authentication tab.

7 Click the **OK** button.

8 The procedure is complete.

—End—

Modify IKE authentication: change IKE preference list

Purpose of this procedure

This procedure describes how to change the IKE Preference List for an IKE authentication used in a selected connection policy.

All changes to the selected IKE authentication are automatically applied to the connection policy that uses this authentication.

CAUTION
Possible service disruption
If IPSec is enabled and the selected connection policy is active, do not perform this procedure. Changing IKE Preference List may cause an outage. Complete this procedure only to clear a GWC320 "Phase 1 SA failure" alarm.

When to use this procedure

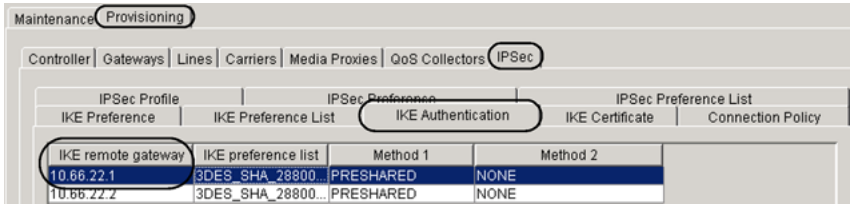
Use this procedure when you are in the process of clearing a GWC320 "Phase 1 SA failure" alarm and you need to change IKE preferences for an affected connection policy.

Prerequisites

Before starting this procedure, you must first add a new list to the IKE Preference List table. If required, see procedure "Configure IKE Preference and Preference List" (page 48).

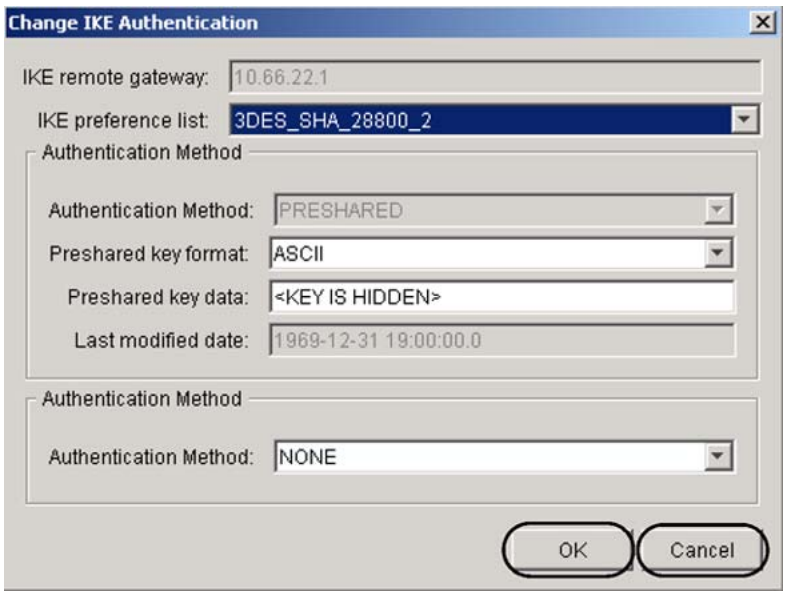
Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, the **IPSec** tab, then the **IKE Authentication** tab.



4 Under IKE remote gateway heading, find the IP address of the remote gateway associated with the connection policy, for which you want to change the IKE preference list. Click the appropriate row to highlight it.

5 Click the **Change** button in the lower right corner of the IKE Authentication panel to display the Change IKE Authentication dialog box.



You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.

6

CAUTION
Possible service disruption
The new preference list must match the list configured on the remote gateway. Otherwise, an outage may occur.

7 Click the IKE preference list: field and from the drop-down menu, select the new list.

8 Click the **OK** button.

9 The procedure is complete.

—End—

Configure Kerberos key management

Purpose of this procedure

This procedure describes how to configure Kerberos key management for one of the following Gateway Controller (GWC) service profiles in packet cable solutions:

- SMALL_LINENA or SMALL_LINENA_V2
- SMALL_LINEINTL or SMALL_LINEINTL_V2
- LINE_TRUNK_AUD_NA or LINE_TRUNK_AUD_INTL
- AUDCNTL_RMGC or AUDCNTL_RMGCINTL

The Kerberos tab is available only when the GWC service profile contains the Kerberos capability.

Kerberos is a network authentication protocol intended for IP networks. It was developed at MIT and has since become a widely available IETF (www.ietf.org) standard in the internet community (RFC 1510).

Kerberos with public key support (using the PKINIT extension to the Kerberos IETF standard) is used in the VoIP solutions as an optimized key management protocol for use with IPSec between the GWC and the multimedia terminal adapter (MTA) line gateways. This security solution is based on the PacketCable Security Specification (see url: www.packetcable.com) and is targeted towards the PacketCable access market.

When to use this procedure

Use this procedure when you wish to configure Kerberos for the selected GWC node.

You need to complete this procedure only if you plan to add a SECURE or FLEX connection policy with Kerberos key negotiation to the selected GWC.

Prerequisites

ATTENTION

If an application layer gateway (ALG) middlebox is associated with an MTA gateway, IPSec between the GWC, ALG, and MTA gateway is not supported.

Provision IPSec with Kerberos only if a secure MTA gateway exists in your network. MTA authentication process with the GWC requires a PacketCable key distribution center (KDC) server, which grants authentication tickets to

the MTA. These tickets are used to authenticate an MTA to a GWC, and to establish a pair of IPSec SAs on both nodes. The KDC is third-party equipment and must be integrated with the network.

CAUTION
Possible communication disruption
The Kerberos parameters configured on the GWC must match the Kerberos parameters defined on the KDC. Otherwise, communication disruption between the GWC and the MTA may occur.

Action

Step	Action

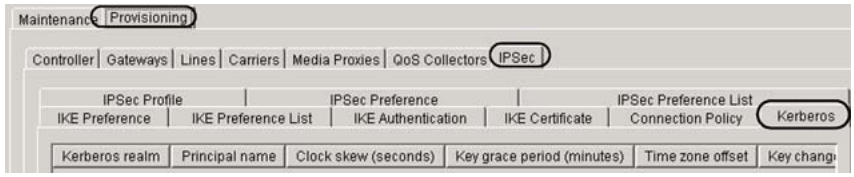
At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

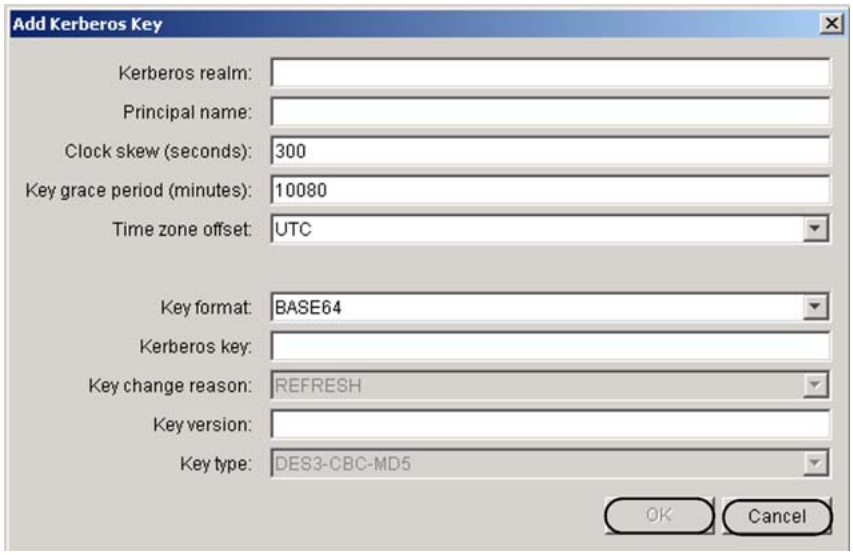
2 From the Contents of: GatewayController frame, select the appropriate GWC node.

3 Click the **Provisioning** tab, the **IPSec** tab, and then the **Kerberos** tab.

The Kerberos tab is visible only when you select a GWC service profile with the Kerberos capability. See the list of GWC service profiles at the beginning of this procedure.



4 Click the **Add** button in the lower right corner of the Kerberos panel to display the Add Kerberos Key dialog box.



If the Kerberos key is already configured for the selected GWC, the **Add** button is not available - you cannot have more then one Kerberos key configured for a GWC. However, you can modify the existing configuration data. For more information see procedure "Modify Kerberos service key" (page 118).

You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.

5 Obtain and enter (or select from the drop-down menu) provisioning values for each field described in the following table.

Kerberos key configuration fields

Field	Values	Description
Kerberos realm:	<user-defined string of all-upper-case alphanumeric characters>	Enter the Kerberos realm to which the GWC belongs, for example, CA.NORTEL.COM. Make sure that this realm is also defined on the KDC Valid realm name must have at least one dot (.). Make sure that you enter this information correctly! If you enter this information incorrectly and you need to modify it later (when this procedure is complete), both GWC units will have to be restarted, and the Kerberos key and key version will have to be changed.

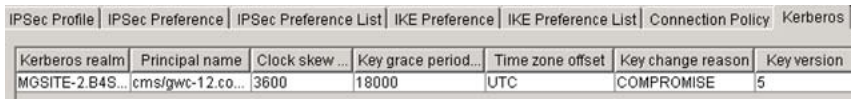
Field	Values	Description
Principal name:	<user-defined string of alphanumeric characters>	Enter a name that uniquely identifies the selected GWC. Use the following format: cms/gwc-<xx>.<clli>.<domain_name> *where:* • xx is the GWC node number • clli is the CM node name • domain_name is the name of the administrative domain to which the GWC belongs The same GWC principal name must be provisioned on the KDC. Make sure that you enter this information correctly! If you enter this information incorrectly and you need to modify it later (when this procedure is complete), both GWC units will have to be restarted, and the Kerberos key and key version will have to be changed.
Clock skew (seconds):	30 to 3600	Enter the maximum allowed time difference (in seconds) between the GWC's local time and any MTA and KDC. The default value is 300 (seconds).
Key grace period (minutes):	30 to 65535	Enter the grace period (in minutes) during which the GWC will accept Kerberos tickets encryptedwith an older key that the GWC has retained and that are still valid (not compromised). All older keys that the GWC has retained could be discarded after they have been retained past this grace period. When a service key is changed because it is compromised, the GWC will still retain all older keys it may have, but will reject any ticket that is encrypted with an older key. After reboot/restart operation, GWC retains only the two most recent service keys. The grace period must be at least as long as the maximum lifetime of a ticket generated by the KDC. The default value is 10080 minutes (7 days).

Field	Values	Description
Time zone offset:	UTC - 12:00 . . . UTC . . . UTC + 12:00	Select the time zone offset that reflects the time zone used throughout the office. It is usually UTC (universal coordinated time).
Key format:	BASE64 HEX	Select the Kerberos key format: BASE64 or HEX.
Kerberos key:	<user-defined>	Enter the Kerberos service key that the GWC will use to decrypt Kerberos tickets sent by the MTA. These tickets (obtained by the MTA from the KDC) are encrypted using the same key. The expected key size is • for BASE64 key format: 32 BASE64 digits The acceptable range of characters is: <a-z, A-Z, 0-9, /+>. • for HEX key format: 48 HEX digits This entry becomes invisible once you complete Kerberos key configuration. The following message will be displayed in this field: <KEY IS HIDDEN>. The key is generated at KDC, then the extracted key must be provisioned (by copying and pasting) at the GWC.
Key change reason:	REFRESH COMPROMISE	A service key can be refreshed as part of a routine key change, and also when the change isrequired because the key was compromised. When this field is set to • REFRESH, the GWC will accept tickets encrypted with an older service key up to a period of time equal to the value specified in field Key grace period. • COMPROMISE, the GWC will reject all tickets encrypted with a service key other than the current version. Older keys are still valid for 30 minutes after the COMPROMISE key change event. When configuring Kerberos key for the first time, this field is disabled and pre-defined with the value of REFRESH. When you change the key later, you can also modify this field.

Field	Values	Description
Key version:	0 to 2147483647	Enter the version number of the service key. It must be the same version number as the one provisioned on the KDC, and used to encrypt GWC tickets.
Key type:	DES3_CBC_MD5	This field specifies the encryption algorithm for which the GWC uses the service key to encrypt and decrypt GWC Kerberos tickets. This field is pre-defined, you cannot change it.

6 When you are finished entering data, click the **OK** button.

The newly defined Kerberos key data appears in the Kerberos table.



7 The procedure is complete.

—End—

Configure a BYPASS connection policy

Purpose of this procedure

This procedure describes how to configure a BYPASS connection policy for a selected Gateway Controller (GWC) node. This policy means that all messages exchanged between the GWC and the specified remote gateway (defined by the IP address, a range of addresses, or a netmask) are not secure. IPSec processing is not applied to any packets matching the policy between the GWC and the selected remote gateway. Incoming IPSec packets are discarded. Outgoing packets are not subject to IPSec processing.

When to use this procedure

Use the non-secure BYPASS policy when no security is required between a GWC and a specified network component. For example, it is used for all captive office local area network (CO-LAN) components that need to communicate with the GWC.

You can also use this policy to temporarily disable security between a GWC and a specified component. If you want to enable it again, delete the appropriate BYPASS policy. For more information see procedure "Disable or enable IPSec between two nodes using BYPASS policy" (page 111).

Prerequisites

CAUTION
Possible communication disruption
Adding a BYPASS policy can cause a communication disruption between the GWC and a gateway that requires IPSec. Proceed with caution.

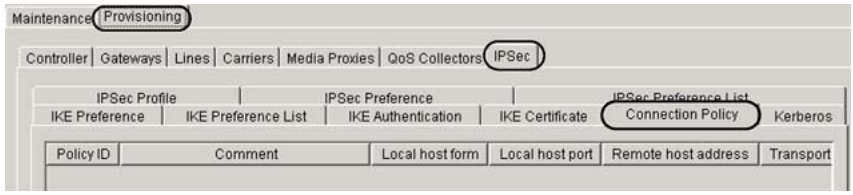
This procedure requires that the IPSec profile with the BYPASS policy action is configured first. If required, complete procedure "Configure IPSec Profile" (page 39).

Action

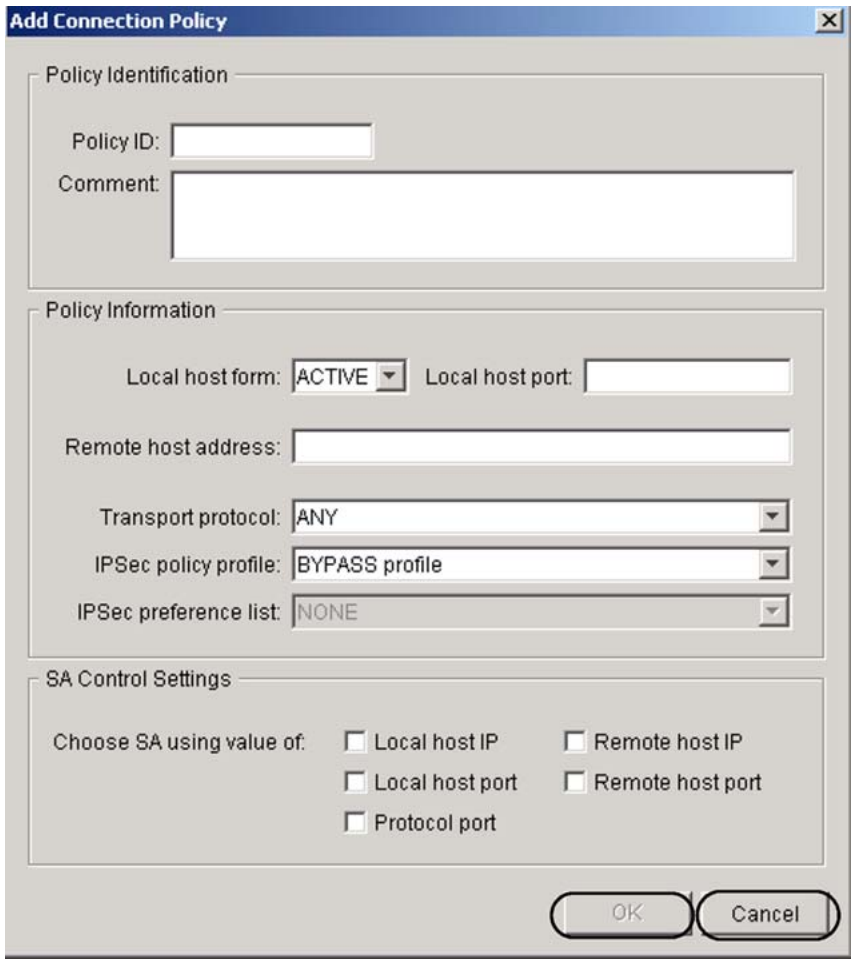
Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

2 From the Contents of: GatewayController frame, select the appropriate GWC node.

3 Click the **Provisioning** tab, the **IPSec** tab, and then the **Connection Policy** tab.



4 Click the **Add** button in the lower right corner of the Connection Policy panel to display the Add Connection Policy dialog box.



You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.

5 Obtain and enter (or select from the drop-down menu) provisioning values for each field described in the following table.

BYPASS connection policy configuration fields

Field	Values	Description
In the Policy Identification panel:		
Policy ID:	1 to 65534	Enter a number that will uniquely identify this policy. The lower the number is, the higher the priority of the policy. For any given IP address, the GWC applies the relevant policy with the lowest Policy ID number. Recommendations: • Do not use policy IDs lower than 100 (so that, if necessary, you can add a higher priority policy - with a lower ID number). • Do not use consecutive numbers between two policy IDs (so that, if necessary, you can add a corrective or modified policy ID between the two policies).
Comment:	<user-defined string of up to 255 characters>	This field is optional. You can use it to add any descriptive additional information regarding this policy.
In the Policy Information panel:		
Local host form:	ACTIVE UNIT	This value indicates whether the active or the unit IP address of the GWC will be used as the local host IP for the connection. Recommended value: ACTIVE (default value), which means that all signaling is done on the active IP address.
Local host port:	0 to 65535	Enter the port number for the local host application. The value of 0 (zero) means any port.
Remote host address:	<gateway IP address or a range of IP addresses>	Enter one of the following values to identify the remote host (gateway): • a unique IP address, with or without a port number (for example, 10.66.17.0 or 10.66.77.0:<port_number>) • a range of IP addresses (for example, 10.66.17.0-10.66.17.7) Make sure that there is no space between the IP addresses and the dash.

Field	Values	Description
		• sub-network address in the form of: ip_address/<bits> (for example, 10.66.17.0/24) The entry in this field means that for every packet received from or sent to the specified IP address, range of addresses, or sub-network, security will not be applied. If you want to use this BYPASS policy to disable security between the GWC and another network device, enter the exact IP address of that device.
Transport protocol:	ANY, ICMP, TCP, or UDP	Select the appropriate transport protocol that matches the protocol configured for the gateway. To configure the SCTP protocol, select ANY. The entry of ANY means any protocol. If you want to use this policy to disable security between the GWC and another network device, you must select ANY.
IPSec policy profile:	<names of the previously defined IPSec policy profiles>	This field identifies the IPSec policy profile for this connection policy. By default, the system displays the first profile from the IPSec Profile table. Click the drop-down menu and select the name of the BYPASS profile that you want to use for this policy. If no IPSec profile is defined, the following message is displayed in this field: *NO PROFILES DEFINED*.
All remaining fields do not apply to a BYPASS policy. Do not attempt to configure them.		

6 Click the **OK** button.

The newly defined policy appears in the Connection Policy table.

If you need to remove the newly added policy, click on it, then click the **Delete** button. A Confirm deletion window appears. Click the **Yes** button to delete the policy.

7 Repeat this procedure, if required, to add more BYPASS policies.

You can configure up to 100 connection policies for a selected GWC.

8 The procedure is complete.

—End—

Configure a DISCARD connection policy

Purpose of this procedure

This procedure describes how to configure a DISCARD connection policy for a selected Gateway Controller (GWC) node. This policy means that all packets matching the policy between the GWC and the selected remote gateway are discarded.

When to use this procedure

It is a good practice to configure a DISCARD policy covering all the IP addresses as the last policy. This policy will prevent a denial_of_service attack from unknown gateways by discarding the message as fast as possible.

Prerequisites

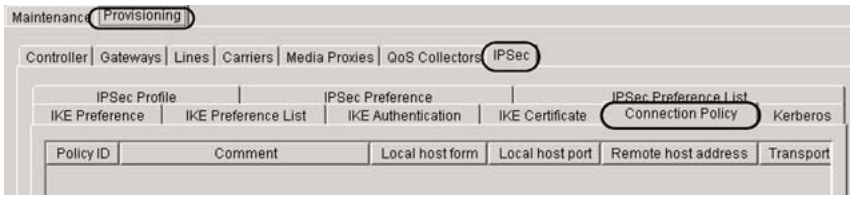
CAUTION
Possible communication disruption
Provisioning a DISCARD policy will cause a communication disruption between the GWC and all the gateways that match this policy.

Provision IPSec only if a secure gateway exists in your network.

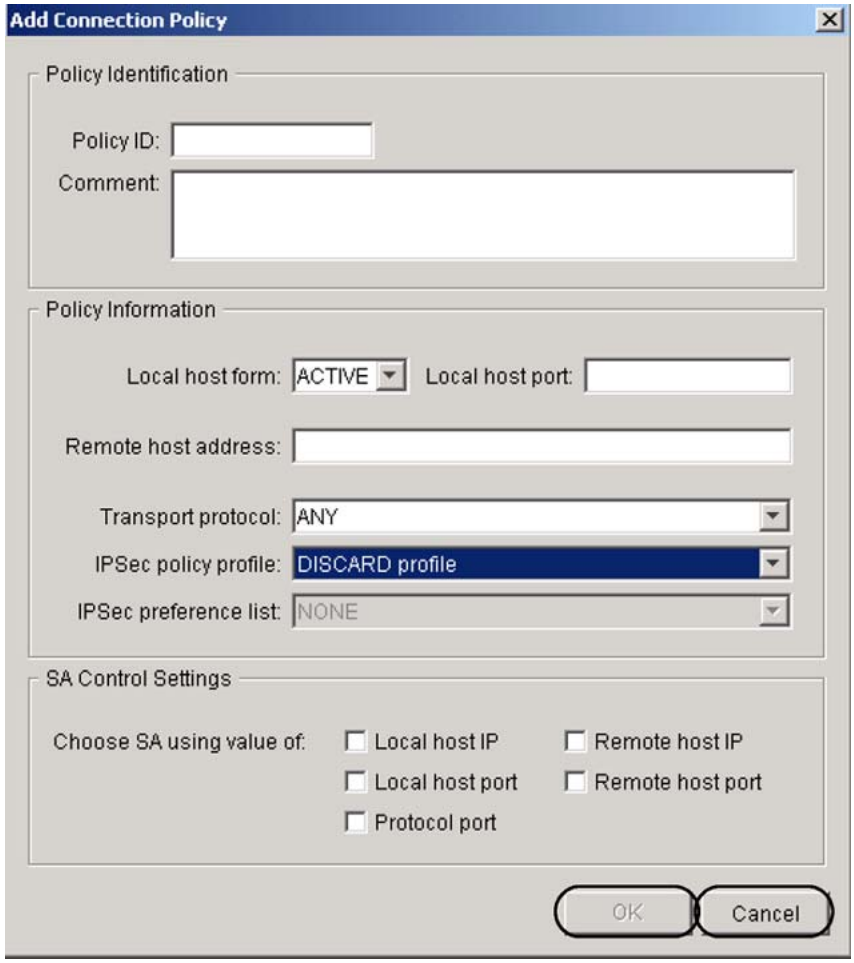
This procedure requires that the IPSec profile with the DISCARD policy action is configured first. If required, complete procedure "Configure IPSec Profile" (page 39).

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the GWC node.
3	Click the **Provisioning** tab, the **IPSec** tab, and then the **Connection Policy** tab.



4 Click the **Add** button in the lower right corner of the Connection Policy panel to display the Add Connection Policy dialog box.



You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.

5 Obtain and enter (or select from the drop-down menu) provisioning values for each field described in the following table.

DISCARD connection policy configuration fields

Field	Values	Description
In the Policy Identification panel:		
Policy ID:	1 to 65534	Enter a number that will uniquely identify this policy. The lower the number is, the higher the priority of this policy. For any given IP address, the GWC applies the relevant policy with the lowest Policy ID number. Recommendations: • Do not use policy IDs lower than 100 (so that, if necessary, you can add a higher priority policy - with a lower ID number). • Do not use consecutive numbers between two policy IDs (so that, if necessary, you can add a corrective or modified policy ID between the two policies).
Comment:	<user-defined string of up to 255 characters>	This field is optional. You can use it to add any descriptive additional information regarding this policy.
In the Policy Information panel:		
Local host form:	ACTIVE UNIT	This value indicates whether the active or the unit IP address of the GWC will be used as the local host IP for the connection. Recommended value: ACTIVE (default value)
Local host port:	0 to 65535	Enter the port number for the local host application. The value of 0 (zero) means any port.
Remote host address:	<gateway IP address or a range of IP addresses>	Enter one of the following values to identify the remote host (gateway): • a unique IP address, with or without a port number (for example, 10.66.17.0 or 10.66.77.0:<port_number>) • a range of IP addresses (for example, 10.66.17.0-10.66.17.7) Make sure that there is no space between the IP addresses and the dash. • sub-network address in the form of ip_address/<bits> (for example, 10.66.17.0/24) The entry in this field means that every packet received from or sent to the specified address (or range of addresses) will be discarded.

Field	Values	Description
Transport protocol:	ANY, ICMP, TCP, or UDP	Select the appropriate transport protocol that matches the protocol configured for the gateway. The value of ANY means any protocol, including SCTP.
IPSec policy profile:	<names of the previously defined IPSec policy profiles>	This field identifies the IPSec policy profile for this connection policy. By default, the system displays the first profile from the IPSec Profile table. Click the drop-down menu and select the name of the DISCARD profile that you want to use for this policy. If no IPSec profile is defined, the following message is displayed in this field: *NO PROFILES DEFINED*.
All remaining fields do not apply to a DISCARD policy. Do not attempt to configure them.		

6 Click the **OK** button.

The newly defined policy appears in the Connection Policy table.

If you need to remove the newly added policy, click on it, then click the **Delete** button. At the displayed confirmation window, click the **Yes** button to delete the policy.

7 Repeat this procedure, if required, to add more DISCARD policies.

You can configure up to 100 connection policies for a selected GWC.

8 The procedure is complete.

—End—

Configure IPSec SECURE or FLEX connection policy with IKE on the GWC Manager

Purpose of this procedure

This procedure describes how to configure IPSec SECURE or FLEX connection policy with the IKE protocol as the key management system.

When to use this procedure

Use this procedure to add one of the following connection policies with IKE as the key management system.

SECURE connection policy

Configure a SECURE-type policy with IKE key management to establish secure communication between a Gateway Controller (GWC) and other network devices, except multimedia terminal adapter (MTA) gateways in a packet network solution.

For MTAs, use the Kerberos/PKINIT protocol as the key management system. For more information, see procedure "Configure IPSec SECURE or FLEX connection policy with Kerberos" in *Gateway Controller Security and Administration* (NN10213-611).

In packet cable solutions, use this procedure to establish IPSec between a GWC and one of the following devices:

- cable modem termination system (CMTS)
- third-party Trunk Gateway Control Protocol (TGCP) trunk gateways

For a complete list of network paths and devices supporting IPSec, as well as an overview of the IPSec implementation in a network, see *Nortel ATM/IP Solution-level Administration and Security* (NN10402-600).

FLEX connection policy

Use the FLEX policy only as a transient policy during the initial activation or de-activation of IPSec, when some gateways associated with the connection policy operate in a secure mode and some do not. The FLEX policy provides the GWC with the flexibility of accepting secure and non-secure messages, so IPSec can be activated on the GWC without a loss of service. When FLEX policy is used to de-activate IPSec, temporary loss of service may occur until security is fully de-activated on the GWC and the gateway.

Once all gateways are configured with IPSec, change the FLEX policy to the appropriate SECURE policy. Follow procedure "Modify an existing IPSec connection policy" (page 124).

ATTENTION

After a connection policy with IKE is provisioned, you will only be able to change the following parameters: IPSec preference list and IPSec policy profile.

If you need to change any other parameters (such as, IKE or IPSec SA lifetimes, encryption algorithms, or authentication algorithms), you must first de-activate security for this link, then re-activate security with the new configuration values.

Prerequisites

Provision IPSec only if a secure gateway exists in your network.

CAUTION

Possible communication disruption

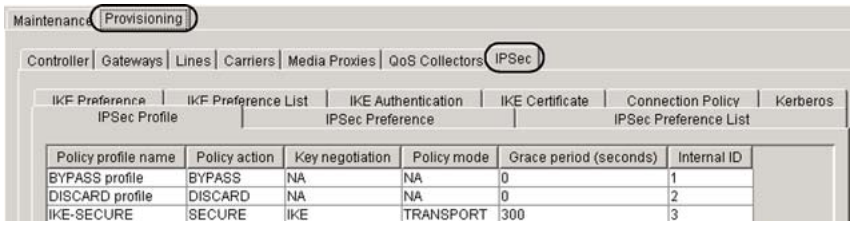
An equivalent IPSec connection policy must be configured at the appropriate gateway. Otherwise, communication disruption between the GWC and the gateway will occur.

This procedure requires that the following tables are configured first:

- IPSec Profile (if required, complete procedure "Configure IPSec Profile" (page 39))
- IKE Preference and IKE Preference List (if required, complete procedure "Configure IKE Preference and Preference List" (page 48))
- IPSec Preference and IPSec Preference List (if required, complete procedure "Configure IPSec Preference and Preference List" (page 43))
- IKE Authentication (if required, complete one of the following procedures: "Configure pre-shared key IKE authentication" (page 59) or "Configure Digital Signatures IKE authentication" (page 63))

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, then the **IPSec** tab. The displayed IPSec panel provides access to IP security configuration data associated with the selected GWC.

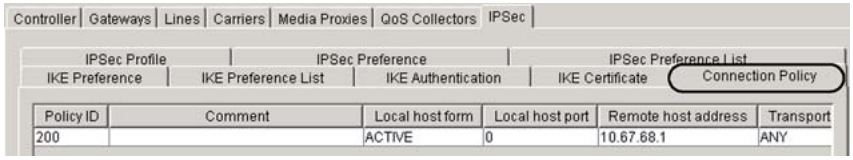


4 Tables displayed under each tab show the currently configured data. You can use the existing data to add a new connection policy. However, if you still need to add data to any of the required tables, complete one of the procedures listed in the following table, then continue with step 5.

If you need to configure	Do
IPSec Profile table	"Configure IPSec Profile" (page 39)
IPSec Preference and IPSec Preference List tables	"Configure IPSec Preference and Preference List" (page 43)
IKE Preference and Preference List tables	"Configure IKE Preference and Preference List" (page 48)
IKE PRESHARED Authentication	"Configure pre-shared key IKE authentication" (page 59)
IKE Digital Signatures Authentication	"Configure Digital Signatures IKE authentication" (page 63)

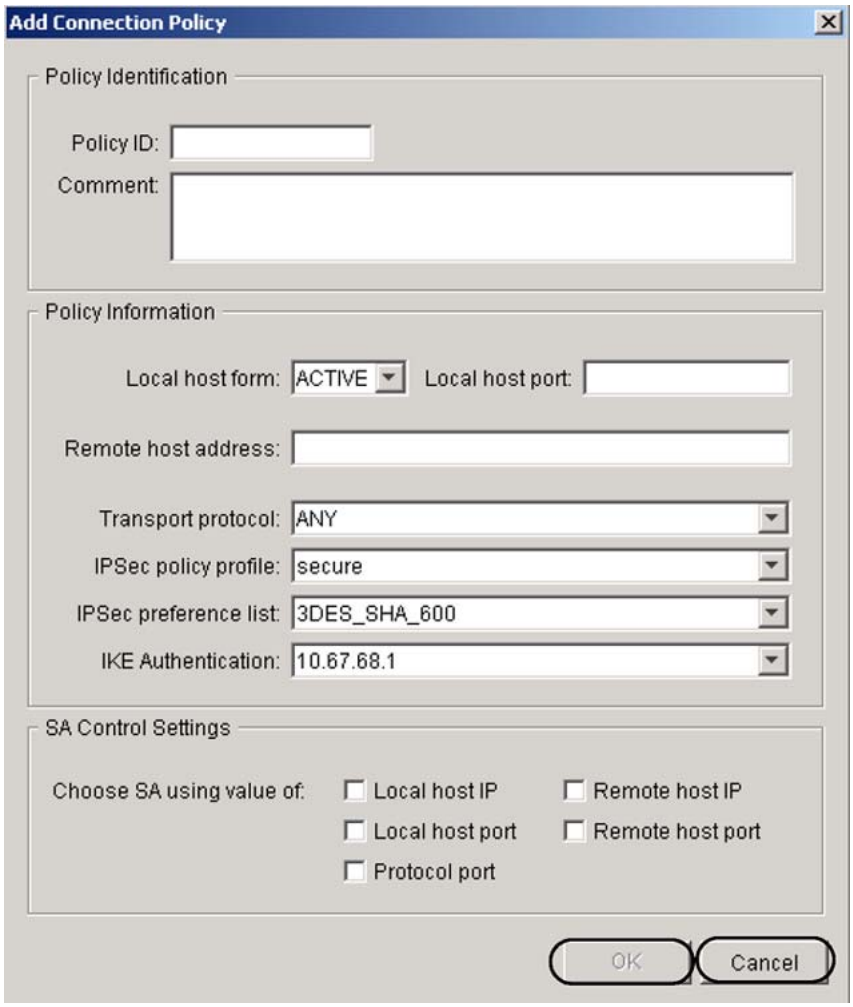
5 Click the **Connection Policy** tab.

The displayed Connection Policy table shows all currently configured policies.



6 Click the **Add** button in the lower right corner of the Connection Policy panel to display the Add Connection Policy dialog box.

You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.



7 Obtain and enter (or select from the drop-down menu) provisioning values for each field described in the following table.

The IPSec provisioning values must match the values provisioned on the remote gateway. Verify these values with your gateway vendor

Some TGCP trunk gateways may not support the following values:

- Local host port: 0
- Remote host address: <IP_of_the_remote_gateway> - without the port number
- Transport protocol: UDP or ANY

Those TGCP trunk gateways require the following provisioning values on the GWC

- Local host port: 2427

- Remote host address: <IP_of_the_remote_gateway>:2427
- Transport protocol: UDP

Connection Policy configuration fields

Field	Values	Description
In the Policy Identification panel:		
Policy ID:	1 to 65534	Enter a number that will uniquely identify this policy. The lower the number is, the higher the priority of this policy. For any given IP address, the GWC applies the relevant policy with the lowest Policy ID number. Recommendations: • Do not use policy IDs lower than 100 (so that, if necessary, you can add a higher priority policy - with a lower ID number). • Do not use consecutive numbers between two policy IDs (so that, if necessary, you can add a corrective or modified policy ID between the two policies).
Comment:	<user-defined string of up to 255 characters>	This field is optional. You can use it to add any descriptive additional information regarding this policy.
In the Policy Information panel:		
Local host form:	ACTIVE UNIT	This value indicates whether the active or the unit IP address of the GWC will be used as the local host IP for the connection. Recommended value: ACTIVE (default value) Active IP address must be used for all call signaling.
Local host port:	0 to 65535	Enter the port number for the local host application. The value of 0 (zero) means any port. See the appropriate gateway documentation to obtain this value.

Field	Values	Description
Remote host address:	<gateway IP address>	Enter a unique IP address to identify the remote host (gateway). Do not use a range of IP addresses or a sub-network address. This entry must match the IKE remote gateway IP address used when configuring the IKE authentication for this remote gateway. You can enter the IP address with or without a port number (for example, 10.66.17.0 or 10.66.77.0:<port_number>) Some gateways are configured to require the port number to be included in the IP address. See the appropriate gateway documentation to determine if the port number is required, and what the number is. The entry in this field means that for every packet received from or sent to the specified IP address, this IPSec connection policy will be applied.
Transport protocol:	ANY, ICMP, TCP, or UDP	Select the appropriate transport protocol that matches the protocol configured for the gateway. Otherwise, the SA negotiation will fail. Nortel recommends the following configuration values: • UDP - for TGCP trunk and MG 9000 gateways • TCP - for CMTS (COPS messages) • ANY (including SCTP) - for all other gateways, including Nortel Media Gateway 3200 • ICMP See the appropriate gateway documentation to determine the value for this field.

Field	Values	Description
IPSec policy profile:	<names of the previously defined IPSec policy profiles>	This field identifies the IPSec policy profile for this connection policy. By default, the system displays the first profile from the IPSec Profile table. Click the drop-down menu and select the name of the SECURE or FLEX profile with IKE key negotiation that you want to use for this policy. If no IPSec profile is defined, the following message is displayed in this field: *NO PROFILES DEFINED*.
IPSec preference list:	<names of the previously defined IPSec preference lists>	This field identifies the IPSec preference list for this connection policy. By default, the system displays the first preference list name from the IPSec Preference List table. Click the drop-down menu and select the name of the IPSec preference list that you want to use for this policy. The lifetime of all preferences in the selected list must be greater than the grace period of the previously selected policy profile. If no IPSec preference list is defined, the following message is displayed in this field: *NO PREFERENCE LISTS DEFINED*.
IKE Authentication:	<list of previously defined IKE authentication entries - identified by the gateway IP address>	This field defines the IKE authentication method and IKE preference list that this connection policy will use. By default, the system displays the first entry from the IKE Authentication table. Each entry is identified by the remote gateway IP address. Click the drop-down menu and select the IP address that matches the IP address entered in the Remote host address: field.
In the SA Control Settings panel: Choose SA using value of:		
Local host IP	<check box>	Leave this box unchecked (default). It means that the system will create an IPSec SA using the value of the local host IP indicated in the policy rather than in the packet.
Local host port	<check box>	Leave this box unchecked (default). It means that the system will create an IPSec SA using the value of the local host port number indicated in the policy rather than in the packet.

Field	Values	Description
Remote host IP	<check box>	Leave this box unchecked (default). It means that the system will create an SA using the value of the remote host IP address indicated in the policy rather than in the packet.
Remote host port	<check box>	Leave this box unchecked (default). It means that the system will create an SA using the value of the remote host port number indicated in the policy rather than in the packet.
Protocol port	<check box>	Leave this box unchecked (default). It means that the system will create an SA using the value of the transport protocol indicated in the policy rather than in the packet.

8 When you are finished entering data, click **OK**.

The newly defined policy data appears in the Connection Policy table.

For the SA Control Settings, if you left the check boxes deselected (blank), a value of FALSE is displayed for each of them in the Connection Policy table. If you selected (checked) any of these boxes, a value of TRUE will be displayed in the Connection Policy table.

9 Repeat this procedure as required to add more SECURE or FLEX connection policies with IKE.

You can configure up to 100 connection policies for a selected GWC.

10 The procedure is complete.

—End—

Configure IPSec SECURE or FLEX connection policy with Kerberos

Purpose of this procedure

This procedure describes how to configure an IPSec SECURE or FLEX connection policy with the Kerberos/PKINIT protocol as the key management system. This procedure applies to packet cable solutions only.

When to use this procedure

Use this procedure to add one of the following connection policies with Kerberos as the key management system.

SECURE connection policy

Configure a SECURE-type policy with Kerberos key management to establish secure communication between the Gateway Controller (GWC), including the redirecting media gateway controller (RMGC), and the multimedia terminal adapter (MTA) line gateways (in packet cable solutions only).

ATTENTION

If an application layer gateway (ALG) middlebox is associated with the MTA gateway, IPSec between the GWC, ALG, and MTA gateway is not supported.

FLEX connection policy

Use the FLEX policy only as a transient policy during the initial activation or de-activation of IPSec, when some gateways associated with the connection policy operate in a secure mode and some do not. The FLEX policy provides the GWC with the flexibility of accepting secure and non-secure messages, so IPSec can be activated on the GWC without a loss of service. When FLEX policy is used to de-activate IPSec, temporary loss of service will occur until security is fully de-activated on the GWC and the gateway. For more information about how to activate or de-active IPSec using FLEX policy, see procedure "Activate or de-activate IPSec with Kerberos using FLEX policy" (page 107).

ATTENTION

Once IPSec is enabled on the remote gateway, change the FLEX policy on the GWC to the appropriate SECURE policy using procedure "Modify an existing IPSec connection policy" (page 124). Otherwise, the gateway IP address can be used to disrupt communication not only between the GWC and this gateway, but also between the GWC and a gateway that is considered secure.

Prerequisites

Provision IPSec only if a secure gateway exists in your network.

CAUTION
Possible communication disruption
An equivalent IPSec connection policy must be configured at the appropriate gateway. Otherwise, communication disruption between the GWC and the gateway will occur.

This procedure requires that the following tables are configured first:

- IPSec Profile (if required, complete procedure "Configure IPSec Profile" (page 39))
- IPSec Preference and IPSec Preference List (if required, complete procedure "Configure IPSec Preference and Preference List" (page 43))
- Kerberos (if required, complete procedure "Configure Kerberos key management" (page 77))

Action

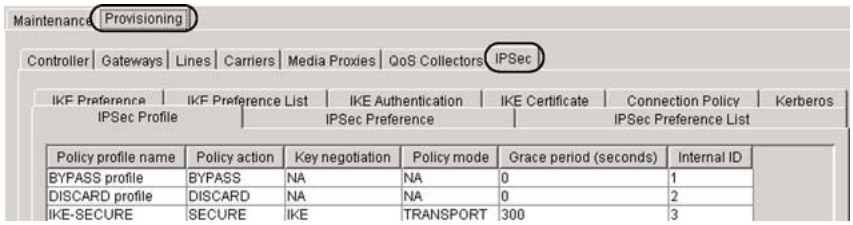
Step	Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

2 From the Contents of: GatewayController frame, select the appropriate GWC node.

3 Click the **Provisioning** tab, then the **IPSec** tab. The displayed IPSec panel provides access to IP security configuration data associated with the selected GWC.



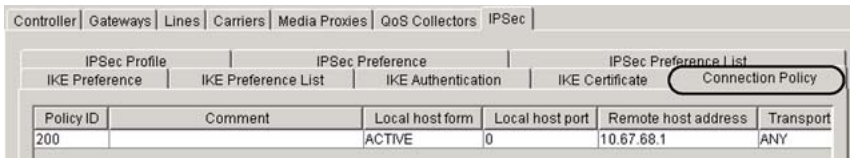
4 Tables displayed under each tab show the currently configured data. You can use the existing data to add a new connection policy. However, if you still need to add data to any of the required tables,

complete one of the procedures listed in the following table, then continue with step 5.

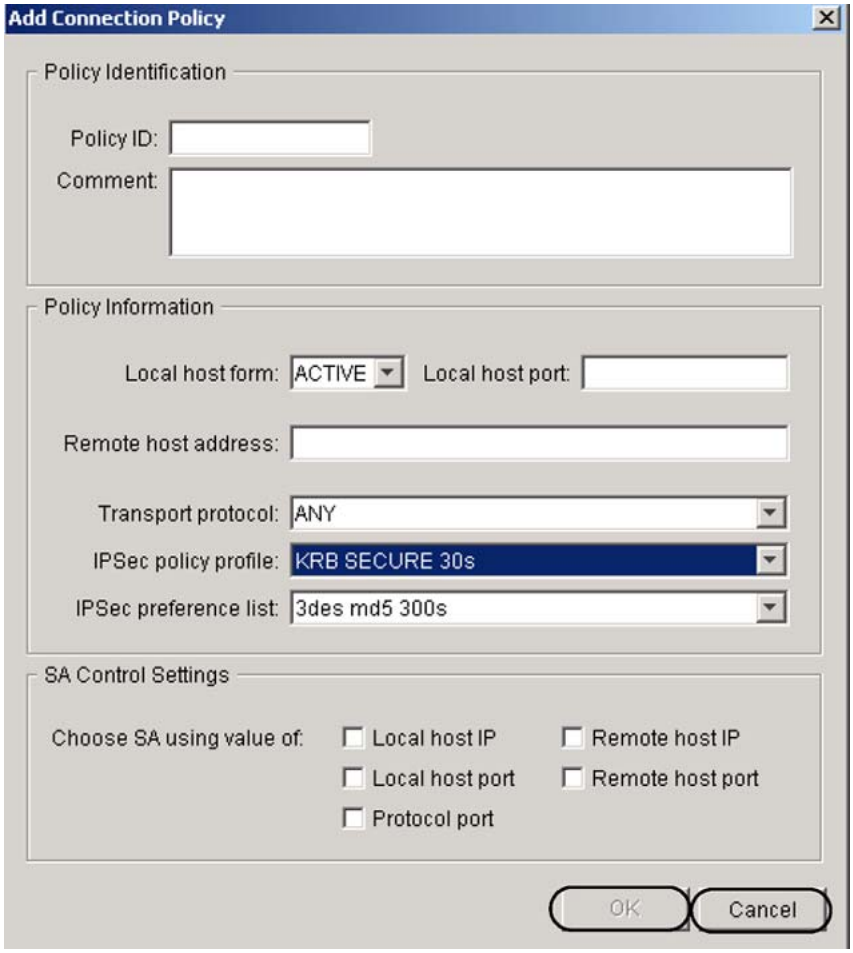
If you need to configure	Do
IPSec Profile table	"Configure IPSec Profile" (page 39)
IPSec Preference and IPSec Preference List tables	"Configure IPSec Preference and Preference List" (page 43)
Kerberos	"Configure Kerberos key management" (page 77)

5 Click the **Connection Policy** tab.

The displayed Connection Policy table shows all currently configured policies.



6 Click the **Add** button in the lower right corner of the Connection Policy panel to display the Add Connection Policy dialog box.



You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.

7 Obtain and enter (or select from the drop-down menu) provisioning values for each field described in the following table.

Connection Policy configuration fields

Field	Values	Description
In the Policy Identification panel:		

Field	Values	Description
Policy ID:	1 to 65534	Enter a number that will uniquely identify this policy. The lower the number is, the higher the priority of this policy. For any given IP address, the GWC applies the relevant policy with the lowest Policy ID number. Recommendations: • Do not use policy IDs lower than 100 (so that, if necessary, you can add a higher priority policy - with a lower ID number). • Do not use consecutive numbers between two policy IDs (so that, if necessary, you can add a corrective or modified policy ID between the two policies).
Comment:	<user-defined string of up to 255 characters>	This field is optional. You can use it to add any descriptive additional information regarding this policy.
In the Policy Information panel:		
Local host form:	ACTIVE UNIT	This value indicates whether the active or the unit IP address of the GWC will be used as the local host IP for the connection. Recommended value: ACTIVE (default value) Active IP address must be used for all call signaling.
Local host port:	0 to 65535	Enter the port number for the local host application. The value of 0 (zero) means any port. See the appropriate gateway documentation to obtain this value.
Remote host address:	<gateway IP address or a range of IP addresses>	Enter one of the following values to identify the remote host (gateway): • a unique IP address, with or without a port number (for example, 10.66.17.0 or 10.66.77.0:<port_number>) Some gateways are configured to require the port number to be included in the IP address. See the appropriate gateway documentation to determine if the port number is required, and what the number is. • a range of IP addresses (for example, 10.66.17.0-10.66.17.7) Make sure that there is no space between the IP addresses and the dash. • sub-network address in the form of ip_address/<bits> (for example, 10.66.17.0/24)

Field	Values	Description
		The entry in this field means that for every packet received from or sent to the specified IP address, range of addresses, or sub-network, this IPSec connection policy will be applied. If you specify a range of addresses, make sure that you select the Remote host IP check box in the SA Control Settings panel. Otherwise, only one IPSec security association (SA) will be created for the entire IP address range, which is not supported.
Transport protocol:	ANY, ICMP, TCP, or UDP	Select the appropriate transport protocol that matches the protocol configured for the gateway. Otherwise, the SA negotiation will fail. The recommended configuration for packet cable MTA line gateways is UDP. See the appropriate gateway documentation to determine the value for this field.
IPSec policy profile:	<names of the previously defined IPSec policy profiles>	This field identifies the IPSec policy profile for this connection policy. By default, the system displays the first profile from the IPSec Profile table. Click the drop-down menu and select the name of the SECURE or FLEX profile with Kerberos key negotiation that you want to use for this policy. If no IPSec profile is defined, the following message is displayed in this field: *NO PROFILES DEFINED*.
IPSec preferenc e list:	<names of the previously defined IPSec preference lists>	This field identifies the IPSec preference list for this connection policy. By default, the system displays the first preference list name from the IPSec Preference List table. Click the drop-down menu and select the name of the IPSec preference list that you want to use for this policy. The lifetime of all preferences in the selected list must be greater than the grace period of the previously selected policy profile. If no IPSec preference list is defined, the following message is displayed in this field: *NO PREFERENCE LISTS DEFINED*.
In the SA Control Settings panel: Choose SA using value of:		
Local host IP	<check box>	Leave this box unchecked (default). It means that the system will create an IPSec SA using the value of the local host IP indicated in the policy rather than in the packet.

Field	Values	Description
Local host port	<check box>	Leave this box unchecked (default). It means that the system will create an IPSec SA using the value of the local host port number indicated in the policy rather than in the packet.
Remote host IP	<check box>	**ATTENTION** If in field Remote host address: you have specified • a range of addresses, you must click this box to activate this flag. Otherwise, only one IPSec SA will be created for the entire IP address range. • an exact address, leave this box unchecked (default). It means that the system will create an SA using the value of the remote host IP address indicated in the policy rather than in the packet.
Remote host port	<check box>	Leave this box unchecked (default). It means that the system will create an SA using the value of the remote host port number indicated in the policy rather than in the packet.
Protocol port	<check box>	Leave this box unchecked (default). It means that the system will create an SA using the value of the transport protocol indicated in the policy rather than in the packet.

8 When you are finished entering data, click the **OK** button.

The newly defined policy data appears in the Connection Policy table.

For the SA Control Settings, if you left the check boxes deselected (blank), a value of FALSE will be displayed for each of them in the Connection Policy table. If you selected (checked) any of these boxes, a value of TRUE will be displayed in the Connection Policy table.

9 Repeat this procedure as required to add more SECURE or FLEX connection policies.

You can configure up to 100 connection policies for a selected GWC.

10 The procedure is complete.

—End—

Activate or de-activate IPSec with Kerberos using FLEX policy

Purpose of this procedure

This procedure describes how to activate or de-activate IPSec between the Gateway Controller (GWC) and a multimedia terminal adapter (MTA) line gateway in packet cable solutions - using FLEX connection policy.

When to use this procedure

Use this procedure when you wish to activate or de-activate IPSec with Kerberos using a FLEX policy.

FLEX policy is not a secure policy. You must only use it during the transition process, when some gateways associated with the connection policy operate in a secure mode and some do not. FLEX policy provides the GWC with the flexibility of accepting secure and non-secure messages, so IPSec can be activated on the GWC without a loss of service. When FLEX policy is used to de-activate IPSec, temporary loss of service may occur until security is fully de-activated on both nodes.

CAUTION
Possible communication disruption
Once IPSec is enabled on the remote gateway, upgrade the FLEX policy on the GWC to the appropriate SECURE policy. Otherwise, the gateway IP address can be used to disrupt communication not only between the GWC and this gateway, but also between the GWC and a gateway that is considered secure (if this gateway is using Kerberos as its key management protocol).

Use one of the following sub-procedures to complete the selected task:

- "Activate IPSec with Kerberos using FLEX policy" (page 108)
- "De-activate IPSec with Kerberos using FLEX policy" (page 108)

Prerequisites

This procedure requires some configuration activities to be performed on a remote gateway. Make sure that you have access to the appropriate remote gateway documentation. If required, contact your network administrator for assistance.

Action

Activate IPSec with Kerberos using FLEX policy

Complete the following steps to activate the IPSec processing between the GWC and an MTA gateway with IPSec currently disabled (no SECURE policy is configured for that gateway).

Step	Action
	At the CS 2000 GWC Manager client
1	Add a FLEX policy covering the IP address of the MTA gateway for which you want to activate IPSec. Follow procedure "Configure IPSec SECURE or FLEX connection policy with Kerberos" (page 100). If an application layer gateway (ALG) middlebox is associated with an MTA gateway, IPSec between the GWC, ALG, and MTA gateway is not supported. At this point, because IPSec on the remote gateway is still disabled, the GWC continues to exchange messages with that gateway without applying any IPSec services to these messages.
2	Enable IPSec on the remote MTA gateway. See the appropriate gateway documentation to complete this step. If required, contact your network administrator for assistance. As soon as IPSec is enabled, the remote gateway initiate the key management process to establish IPSec security associations (SA). When the SAs are established, GWC applies IPSec services to all packets sent to the remote gateway.
3	Change the FLEX policy to the appropriate (same remote IP address) SECURE policy as soon as possible. Follow procedure "Modify an existing IPSec connection policy" (page 124). If you need to add an appropriate IPSec profile with the Policy action: SECURE, follow procedure "Configure IPSec Profile" (page 39).
4	The procedure is complete.
	—End—

De-activate IPSec with Kerberos using FLEX policy

Complete the following steps to de-activate the IPSec processing between the GWC and an MTA gateway with IPSec currently enabled (a SECURE active policy is configured for that gateway).

When FLEX policy is used to de-activate IPSec, temporary loss of service may occur until security is fully de-activated on both nodes.

Step	Action

At the CS 2000 GWC Manager client

1 Change the SECURE policy to a FLEX policy covering the IP address of the remote MTA gateway for which you want to de-activate IPSec. Follow procedure "Modify an existing IPSec connection policy" (page 124).

If you need to add an appropriate IPSec profile with the Policy action: FLEX, follow procedure "Configure IPSec Profile" (page 39).

The GWC and the gateway continue to communicate securely.

2 Disable IPSec on the remote gateway. See the appropriate gateway documentation to complete this step. If required, contact your network administrator for assistance.

As soon as IPSec is disabled on the gateway, the remote gateway terminates its SA. GWC stops applying IPSec services to all packets sent to and received from the remote gateway. Depending on the characteristics of a gateway, the two nodes either continue to communicate, or the communication stops until security is fully de-activated on both nodes.

3 Add a BYPASS policy for the remote gateway, for which the IPSec was disabled in step 2. If required, follow procedure "Configure a BYPASS connection policy" (page 83).

4 Delete the FLEX policy identified in step 1 by completing the following sub-steps.

CAUTION
Possible communication disruption
Deleting a FLEX policy will also delete any active IPSec security associations (SA). If any of the gateways associated with this FLEX policy have IPSec enabled and SAs active, deleting this policy will result in temporary loss of communication between the GWC and the gateways - until IPSec is disabled at the affected gateways.

a. In the Connection Policy table, click the FLEX policy that you want to delete (identified by the gateway IP address in the Remote host address column).

b. Click the **Delete** button. At the displayed confirmation window, click the **Yes** button to delete the policy.

5 The procedure is complete.

—End—

Disable or enable IPSec between two nodes using BYPASS policy

Purpose of this procedure

This procedure describes how to disable or enable the IPSec processing between a Gateway Controller (GWC) and the specified gateway - using a BYPASS connection policy.

When to use this procedure

Use this procedure when you wish to disable security (that is, the existing active SECURE policy) between a GWC node and the specified gateway, using a BYPASS policy.

You can also use this procedure to re-establish a SECURE policy that was previously disabled with a BYPASS policy.

CAUTION
Communication disruption
When you use a BYPASS policy to disable or enable IPSec, a loss of communication between the GWC and a remote gateway will occur. To restore communication, enable or disable IPSec on the remote gateway to match the GWC policy configuration.

Use one of the following sub-procedures to complete the selected task:

- "Disable IPSec using BYPASS policy" (page 111)
- "Enable IPSec by removing a BYPASS policy" (page 114)

Prerequisites

This procedure assumes that a SECURE connection policy (with IKE or Kerberos key management) exists between the GWC and the gateway.

Make sure that an appropriate IPSec profile with Policy action: BYPASS is configured for the selected GWC node. If required, add a new profile (with Policy action: BYPASS) using procedure "Configure IPSec Profile" (page 39).

Action

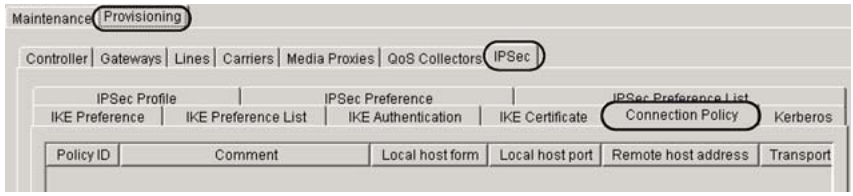
Disable IPSec using BYPASS policy

Step	Action
	At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

2 From the Contents of: GatewayController frame, select the appropriate GWC node.

3 Click the **Provisioning** tab, the **IPSec** tab, then the **Connection Policy** tab to display connection policies currently configured for this GWC node.



4 In the Remote host address column, look for the IP address of the gateway, for which you want to disable security. Identify the policy (with this IP address) that you want to disable. Click on it to highlight it.

From the highlighted row, record the following values:

- Policy ID
- Remote host address

5 Use the following table to determine your next step.

If the highlighted policy uses	Do
Kerberos as the key management system	step 6
IKE as the key management system	step 7

6 Change the profile for the highlighted policy from SECURE to FLEX. If required, follow procedure "Modify an existing IPSec connection policy" (page 124).

7 Click the **Add** button in the lower right corner of the Connection Policy panel to display the Add Connection Policy dialog box.

You have the option to cancel the procedure at any time (but before you click **OK**). To do that, click the **Cancel** button.

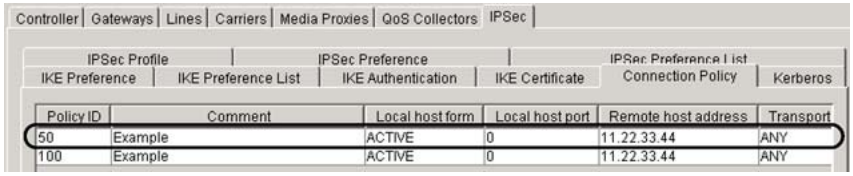
8 Enter (or select from the drop-down menu) provisioning values for each field described in the following table.

BYPASS connection policy configuration fields

Field	Description
In the Policy Identification panel:	
Policy ID:	Enter a number that is lower than the Policy ID number recorded in step 4.
Comment:	This field is optional. You can use it to add any descriptive additional information regarding this policy.
In the Policy Information panel:	
Local host form:	Select ACTIVE (default value).
Local host port:	Enter 0 (zero).
Remote host address:	Enter the exact IP address of the gateway, as recorded in step 4.
Transport protocol:	Select ANY.
IPSec policy profile:	Select the name of the BYPASS profile that you want to use for this policy.
All remaining fields do not apply to a BYPASS policy. Do not attempt to configure them.	

9 Click the **OK** button.

10 The newly defined policy appears in the Connection Policy table in front of the SECURE or FLEX policy that you wanted to disable. This means that for all messages exchanged between this GWC and the specified gateway, no IPSec processing will be applied.



11 The procedure is complete.

—End—

Enable IPSec by removing a BYPASS policy

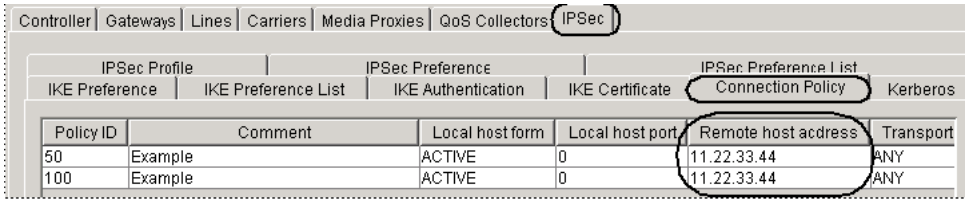
Step	Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

2 From the Contents of: GatewayController frame, select the appropriate GWC node.

3 Click the **Provisioning** tab, then **IPSec** tab, then the **Connection Policy** tab to display connection policies currently configured for this GWC node.



4 In the Remote host address column, look for the IP address of the gateway, for which you want to re-establish security. Identify the BYPASS policy (with the same remote host address) listed in front of the SECURE policy that you want to enable. Click the BYPASS policy to highlight it.

5 Click the **Delete** button. At the displayed confirmation window, click the **Yes** button to delete the policy.

6 The procedure is complete.

—End—

Modify IKE pre-shared keys on the GWC Manager

Purpose of this procedure

This procedure describes how to change IKE pre-shared keys for an existing IKE authentication.

Any connection policy configured with the IKE authentication that you are modifying, will be automatically updated with the new pre-shared keys.

When to use this procedure

Use this procedure when you wish to modify the IKE pre-shared keys for an existing IKE authentication.

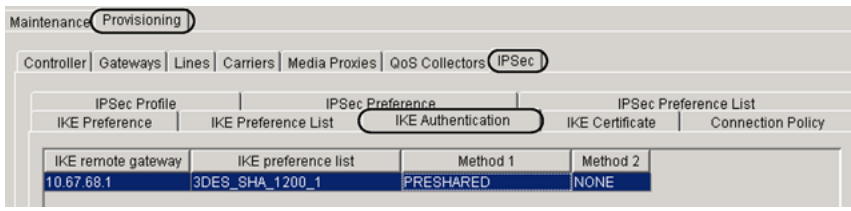
Prerequisites

This procedure assumes that an IKE authentication entry, with PRESHARED authentication method, exists in the IKE Authentication table.

CAUTION
Possible communication disruption
The pre-shared key configured for a GWC must match the key configured on a remote gateway. Otherwise, communication disruption between the GWC and the gateway may occur.

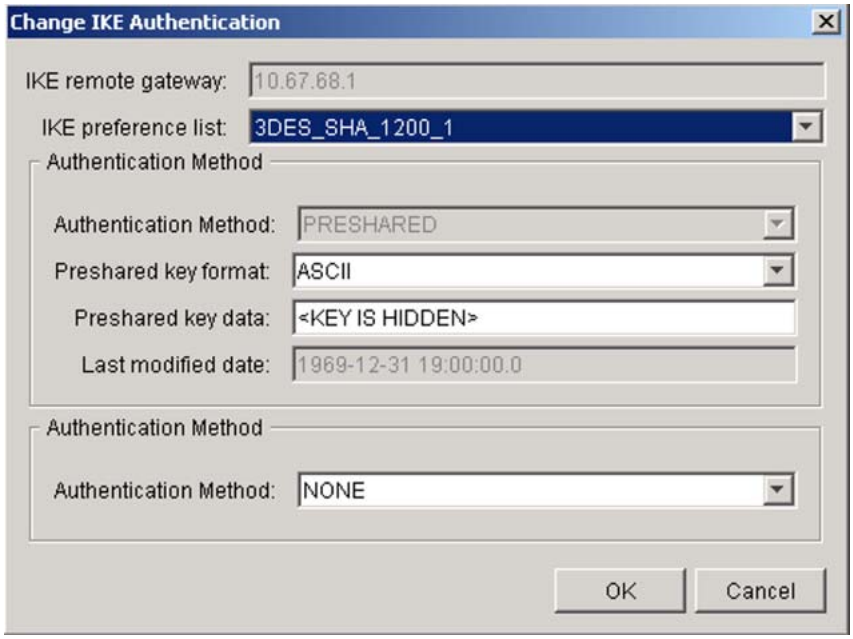
Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, the **IPSec** tab, then the **IKE Authentication** tab to display IKE authentication entries currently configured for the selected GWC node.



4 Click the IKE authentication table entry that you want to modify to highlight it

5 Click the **Change** button to display the Change IKE Authentication dialog box.



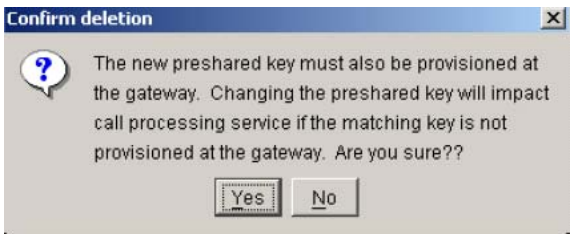
6 If you wish to change the pre-shared key format, click the Preshared key format: drop-down menu and select the new format (ASCII or HEX). Otherwise, continue with the next step.

7 In the Preshared key data: field, enter the new preshared key (1- to 48-character long). Although the minimum allowed key length is one character, make sure that this key is long and random enough to provide an appropriate level of secrecy and security.

The value entered in this field must match the preshared key configured on a gateway. For more information, contact your network administrator.

8 Click the **OK** button.

At the following confirmation message, click **Yes** to continue.



9 The procedure is complete.

—End—

Modify Kerberos service key

Purpose of this procedure

This procedure describes how to modify Kerberos service key for one of the following Gateway Controller (GWC) profiles in packet cable solutions:

- SMALL_LINENA or SMALL_LINENA_V2
- SMALL_LINEINTL or SMALL_LINEINTL_V2
- LINE_TRUNK_AUD_NA or LINE_TRUNK_AUD_INTL
- AUDCNTL_RMGC or AUDCNTL_RMGCINTL

When to use this procedure

Use this procedure when you wish to modify Kerberos service key settings for the selected GWC node. To change the service key, you need to modify the following parameters:

- Kerberos key
- key change reason
- key version

ATTENTION

For packet cable solutions, the following specifications apply:

- When a new key is provisioned on the GWC, the previous key is kept for a duration at least equal to the Key grace period parameter defined in the Kerberos panel.
- Only two Kerberos service keys are kept in the database: the new key (version n) and the previous key (version n-1).
- If a service key is changed more than twice during the key grace period, then you must manually delete the Kerberos ticket on all the MTAs that are still using a Kerberos ticket encrypted with a key version older than n-1.

Prerequisites

CAUTION

Possible communication disruption

The Kerberos key and the key version configured on the GWC must match the key and the key version defined on the KDC. Otherwise, communication disruption between the GWC and MTAs may occur.

Action

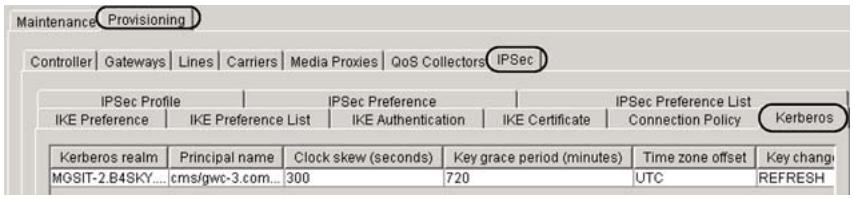
Step	Action

At the CS 2000 GWC Manager client

1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.

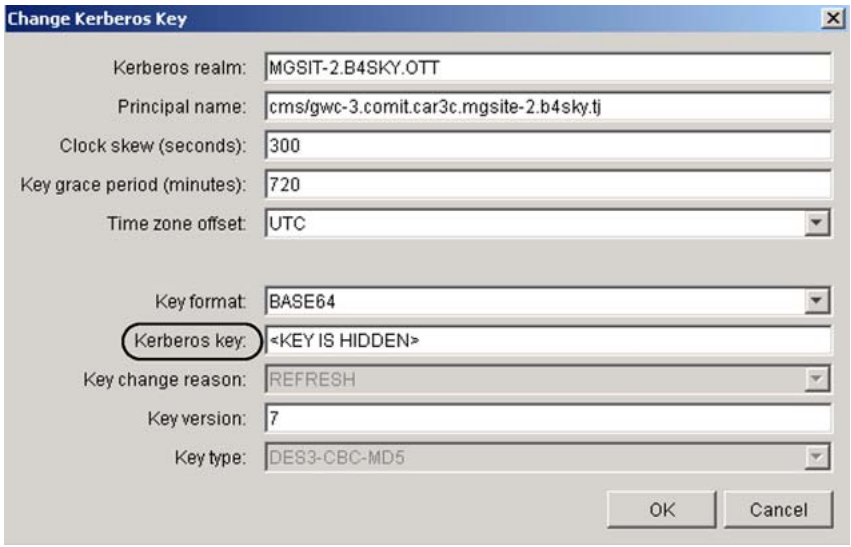
2 From the Contents of: GatewayController frame, select the appropriate GWC node.

3 Click the **Provisioning** tab, the **IPSec** tab, then the **Kerberos** tab to display the existing single entry in this table.



4 Click this entry to highlight it.

5 Click the **Change** button to display the Change Kerberos Key dialog box.



6 In the Kerberos key: field, delete the <KEY IS HIDDEN> value, then paste the new Kerberos key value generated at KDC.

The key is generated at KDC, then the extracted key must be provisioned (by copying and pasting) at the GWC.

Make sure that you enter the valid number of characters. Otherwise, the system displays an error message.

The expected key size is:

- for BASE64 key format: 32 BASE64 digits

  The acceptable range of characters is: <a-z, A-Z, 0-9, /+>.

- for HEX key format: 48 HEX digits

7 If you need to change the reason, click the Key change reason: field and from the drop-down menu, select one of the following values:

- REFRESH - corresponds to a routine key change. The GWC will continue to accept the AP_REQ messages, for which the ticket is encrypted using the old Kerberos service key for a period of time equal to at least the Key grace period parameter value defined in the Kerberos panel.
- COMPROMISE - the change is required because the previous key was compromised. The GWC will refuse the AP_REQ messages, for which the ticket is encrypted using the old Kerberos service key; a Kerberos error message will be sent to inform the MTA to derive a new Kerberos ticket from the KDC.

8 If you change the key, you must also change the key version. Otherwise, the system displays an error message.

In the Key version: field, delete the current value, then enter the new key version.

9 When you are finished entering data, click the **OK** button.

10 The procedure is complete.

—End—

Disable Kerberos key management

Purpose of this procedure

This procedure describes how to disable Kerberos key management for one of the following Gateway Controller (GWC) profiles in packet cable solutions:

- SMALL_LINENA or SMALL_LINENA_V2
- SMALL_LINEINTL or SMALL_LINEINTL_V2
- LINE_TRUNK_AUD_NA or LINE_TRUNK_AUD_INTL
- AUDCNTL_RMGC or AUDCNTL_RMGCINTL

When to use this procedure

Use this procedure when you wish to disable Kerberos key management for the selected GWC node.

You need to complete this procedure only if you plan to disable all SECURE and FLEX connection policies between the selected GWC and the multimedia terminal adapter (MTA) line gateways.

Prerequisites

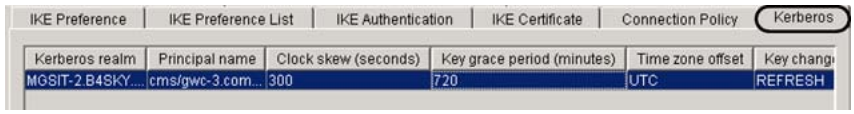
CAUTION
Communication disruption
Once you disable Kerberos key management for the selected GWC, all secure (configured with IPSec) MTA gateways will lose communication with this GWC.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, then on the **IPSec** tab, then click the **Connection Policy** tab to display connection policies currently configured for this GWC node.

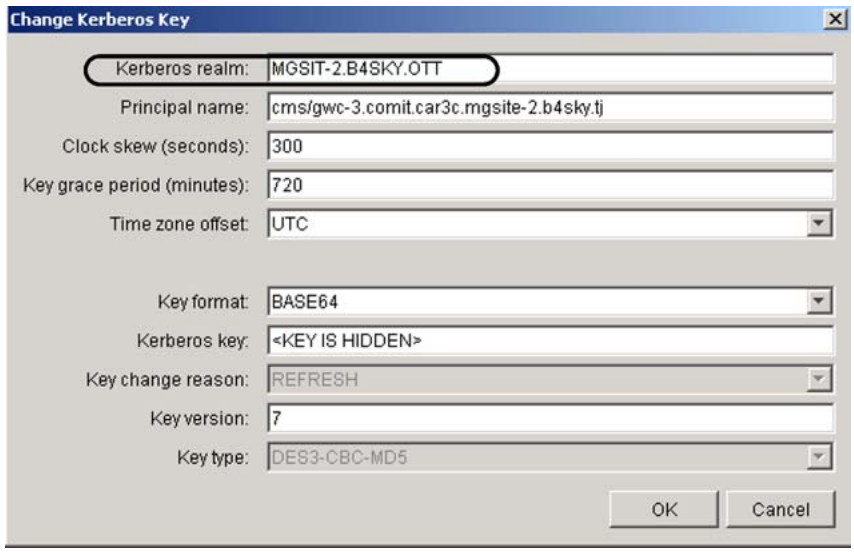
4 Identify all FLEX and SECURE connection policies with the Kerberos key management. Add a BYPASS policy in front (with a lower Policy ID number) of each of these policies. See procedure "Disable or enable IPSec between two nodes using BYPASS policy" (page 111).

5 Click the **Kerberos** tab to display the existing single entry in this table.



6 Click this entry to highlight it.

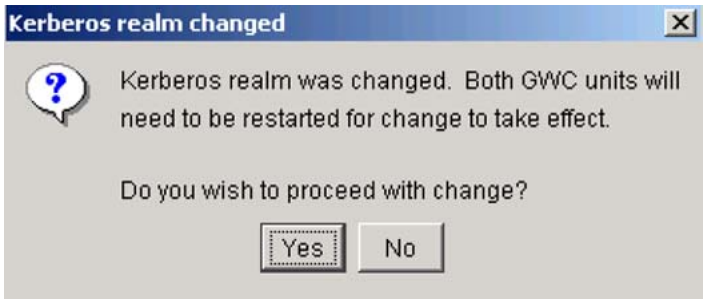
7 Click the **Change** button to display the Change Kerberos Key dialog box.



8 In the Kerberos realm: field, delete the existing entry and type: NULL.REALM.

9 Click **OK**.

The system displays the following message:



10 Click **Yes** to confirm.

11 Restart the GWC node using the following steps:

a. Busy the inactive unit. Follow procedure "Disable (Busy) GWC card services" (page 35) in this NTP.

b. Return the inactive unit to service. Follow procedure "Enable (RTS) GWC card services" (page 37) in this NTP.

c. Switch the activity from one GWC card to the mate GWC card. Follow procedure "Invoke a manual protection switch (warm SWACT)" (page 31) in this NTP.

The active unit becomes inactive, and the inactive unit becomes active.

d. Repeat steps a and b for the newly inactive (previously active) GWC unit.

12 The procedure is complete.

The entry in the Kerberos table cannot be deleted. It remains displayed, even though the Kerberos functionality has been disabled.

—End—

Modify an existing IPSec connection policy on the GWC Manager

Purpose of this procedure

CAUTION
Possible communication disruption
IPsec preference lists configured on the GWC and the remote gateway must match. Otherwise, communication disruption between the GWC and the gateway will occur.

This procedure describes how you can change the following characteristics of an existing connection policy, without configuring a new policy:

- IPSec preference list
- IPSec policy profile, which changes the type of action that an existing connection policy applies to incoming and outgoing packets. However, this method is only allowed for the following changes:

From a policy with action	To a policy with action
BYPASS	FLEX
BYPASS	SECURE
FLEX	SECURE
SECURE	FLEX
FLEX	FLEX
SECURE	SECURE

If you attempt to make any other change, the system displays an error message listing the allowed changes.

You cannot change from a policy with key negotiation of IKE to a policy with Kerberos, or from a policy with Kerberos to a policy with IKE. If you attempt to make such change, the system displays an appropriate error message.

Each connection policy is identified by a policy ID number. The lower this number is, the greater is the priority of the policy. For any gateway IP address, the GWC applies the corresponding policy with the lowest policy ID number.

When to use this procedure

Use this procedure when you want to change one or both of the following elements for an existing connection policy, but you do not want to configure a new policy:

- type of action that an existing connection policy applies to messages exchanged between the Gateway Controller (GWC) and a gateway (see the preceding table for the list of allowed changes)
- list of IPSec preferences, which include the following parameters: encryption and authentication algorithm, lifetime

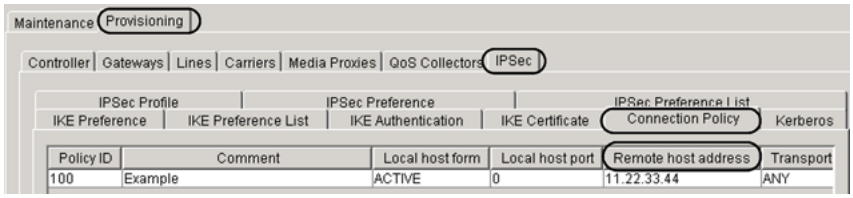
Prerequisites

This procedure requires that the following tables are configured first:

- IPSec profile with the appropriate policy action that you want to use for the selected policy. If required, complete procedure "Configure IPSec Profile" (page 39).
- IPSec preference list that you want to use for the selected policy. If required, complete procedure "Configure IPSec Preference and Preference List" (page 43).

Action

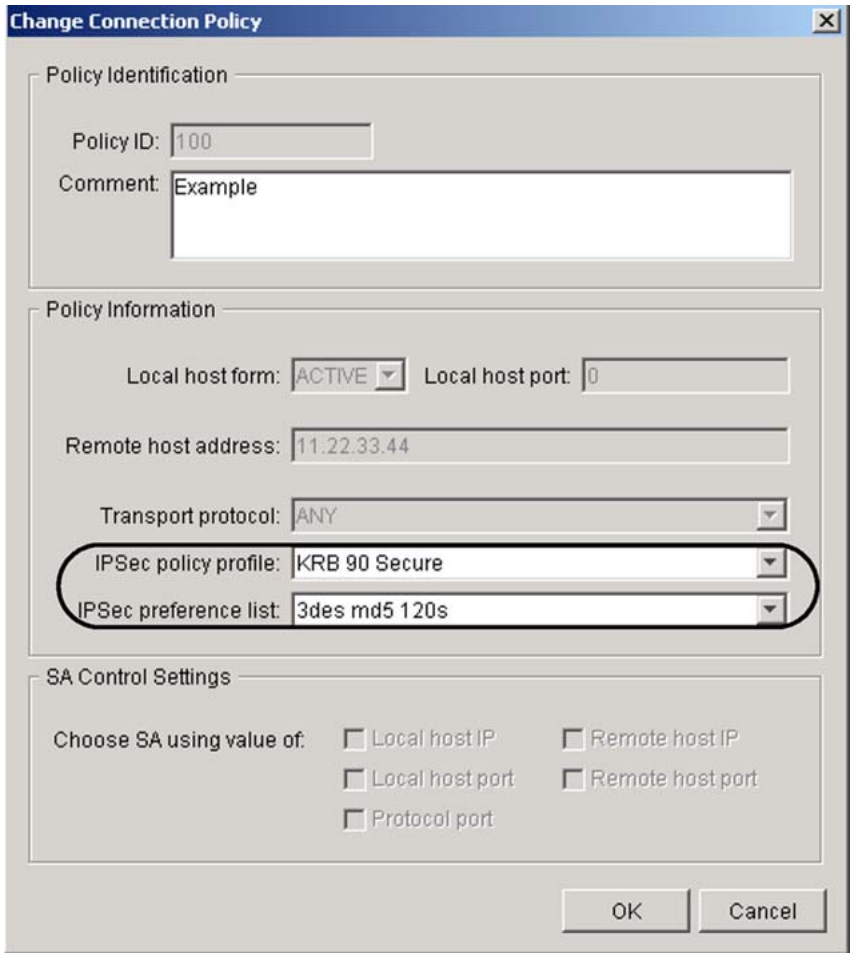
Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, then on the **IPSec** tab, then click the **Connection Policy** tab to display connection policies currently configured for the selected GWC node.



4	In the Remote host address (gateway IP address) column, identify the policy that you want to modify. Click that entry to highlight the policy.

5 Click the **Change** button in the lower right corner of the Connection Policy panel to display the Change Connection Policy dialog box.

Note: You have the option to cancel the procedure at any time (but before you click). To do that, click the **Cancel** button.



6 If you wish to change the policy action, click the IPSec policy profile: drop-down menu and select the name of the appropriate profile (containing the action that you want to use for this policy).

Only certain changes are acceptable. See the table at the beginning of this procedure for the list of allowed changes.

7 If you wish to change the IPSec preference list, click the IPSec preference list: drop-down menu and select the name of the new list that you want to use for this policy.

8 Click the **OK** button.

9 The procedure is complete.

—End—

Delete an IPSec connection policy on the GWC Manager

Purpose of this procedure

This procedure describes how to delete an existing IPSec connection policy from the Gateway Controller (GWC).

Each connection policy is identified by a policy ID number. The lower this number is, the greater is the priority of the policy. For any gateway IP address, the GWC applies the corresponding policy with the lowest policy ID number.

When to use this procedure

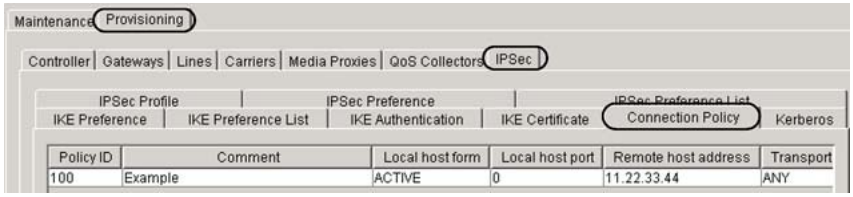
Use this procedure when you need to delete an IPSec connection policy currently configured on a GWC.

Prerequisites

An IPSec connection policy must be configured on a GWC.

Action

Step	Action
	At the CS 2000 GWC Manager client
1	At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.
2	From the Contents of: GatewayController frame, select the appropriate GWC node.
3	Click the **Provisioning** tab, the **IPSec** tab, then the **Connection** Policy tab to display connection policies currently configured for the selected GWC node.



Use the following table to determine your next step.

If you wish to delete a	Do
SECURE policy	go to step 4
FLEX policy	go to step 5
BYPASS or DISCARD policy	go to step 6

4 You cannot delete a SECURE policy. If you attempt to delete a SECURE policy, the system displays the following error message:

To delete a SECURE policy, complete the following sub-steps:

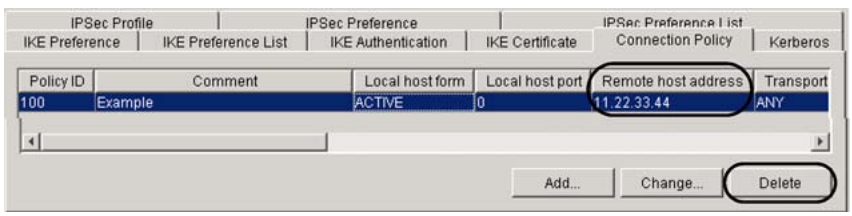
a. Downgrade the policy from SECURE to FLEX using procedure "Modify an existing IPSec connection policy" (page 124).

b. Continue with step step 5.

CAUTION
Possible communication disruption
Deleting a FLEX policy will also delete any active IPSec security associations (SA). If any of the gateways associated with this FLEX policy have IPSec enabled and SAs active, do not delete this policy. Otherwise, temporary loss of communication between the GWC and the gateways will occur until IPSec is disabled at the affected gateways.

5 If you wish to continue, go to step step 6.

6 In the Remote host address (gateway IP address) column, identify the policy that you want to delete. Click that row to highlight the policy.



7 Click the **Delete** button in the lower right corner of the Connection Policy panel.

8 At the displayed confirmation window, click the **Yes** button to delete the selected policy.

9 The procedure is complete.

—End—

Carrier VoIP

Gateway Controller Security and Administration

Publication: NN10213-611
Document status: Standard
Document version: 08.02
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback .

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.