Gateway Controller Security and Administration

What's new in SN08

The following changes have been made to this NTP for the SN08 release:

- A00007300 - Enable by Default IPSec on All GWC Profiles
- A00007927 - SAM21 EM Enhancements from Bell Canada VO

Security and administration strategy overview

User administration is not controlled by the Gateway Controller (GWC). GWC card administration is performed using the CS 2000 SAM21 Manager client. GWC node service management is made available through the CS 2000 GWC Manager.

Note: 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 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.

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 now provided using the IEMS. For more information, refer to the *Integrated EMS Basics* NTP, NN10329-111.

To launch the CS 2000 GWC Manager or the CS 2000 SAM21 Manager, refer to the following procedures in the *Integrated EMS Basics*, 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 on page 13
- Lock a GWC card on page 17
- Unlock a GWC card on page 23
- Invoke a manual protection switch (warm swact) on page 29
- Invoke a cold manual protection switch (cold swact) on page 33
- Disable (Busy) GWC card services on page 37
- Enable (RTS) GWC card services on page 39

IPSec configuration procedures

Nortel Networks security architecture for VoIP uses Internet Protocol Security (IPSec) to protect the traffic between the Gateway Controller (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.

Note: For more detailed IPSec information, refer to the appropriate Internet Engineering Task Force (IETF) RFC documentation, which can be found at http://www.ietf.org.

Overview of IPSec

The following subsections describe the basic IPSec architecture elements as implemented in the SN08 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 describes 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. For more information on how to configure these parameters, refer to procedure Configure IPSec Preference and Preference List on page 53.

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 and a multimedia terminal adapter (MTA) line gateway

  Note: 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)

  Note: 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. Also, only pre-shared key authentication is supported on the GWC (digital signature authentication or public key encryption authentication are not supported). For information on how to configure IKE parameters, refer to procedure Configure IKE Preference and Preference List on page 45.

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. For information on how to configure Kerberos parameters, refer to procedure Configure Kerberos key management on page 59.

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 or UDP) 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: no IPSec services are applied to packets exchanged between the GWC and the specified gateway. For more information, refer to procedure Configure a BYPASS connection policy on page 67.
- DISCARD: all packets sent by the GWC to the specified gateway, or received by the GWC from that device, are discarded. For more information, refer to procedure Configure a DISCARD connection policy on page 73.
- 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 decrypted; outgoing packets are authenticated and 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. For more information on how to activate or de-active IPSec using FLEX policy, refer to procedure Activate or de-activate IPSec using FLEX policy on page 99.

  Note: For more information on configuring SECURE or FLEX policy, refer to the following procedures: Configure IPSec SECURE or FLEX connection policy with IKE on page 79 and Configure IPSec SECURE or FLEX connection policy with Kerberos on page 89.

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. Starting in SN08, you can configure IPSec for any GWC service profile. However, IPSec is not supported between an audio controller GWC and the Media Server 2010 gateway.

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

- SMALL_LINENA and SMALL_LINEINTL - for secure communication with MTA line gateways and CMTS

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

- TRUNKNA and TRUNKINTL - for secure communication with third-party 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, refer to the *ATM/IP Solution-level Security and Administration* NTP, 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.

Overall IPSec configuration procedure on a GWC

ATTENTION

Before starting the configuration procedure, obtain the correct configuration values for each parameter listed below.

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 field in the Connection Policy table that can be changed (with limitations) is the IPSec policy profile. For more information, refer to procedure Change the policy action for an existing IPSec connection policy on page 121

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)

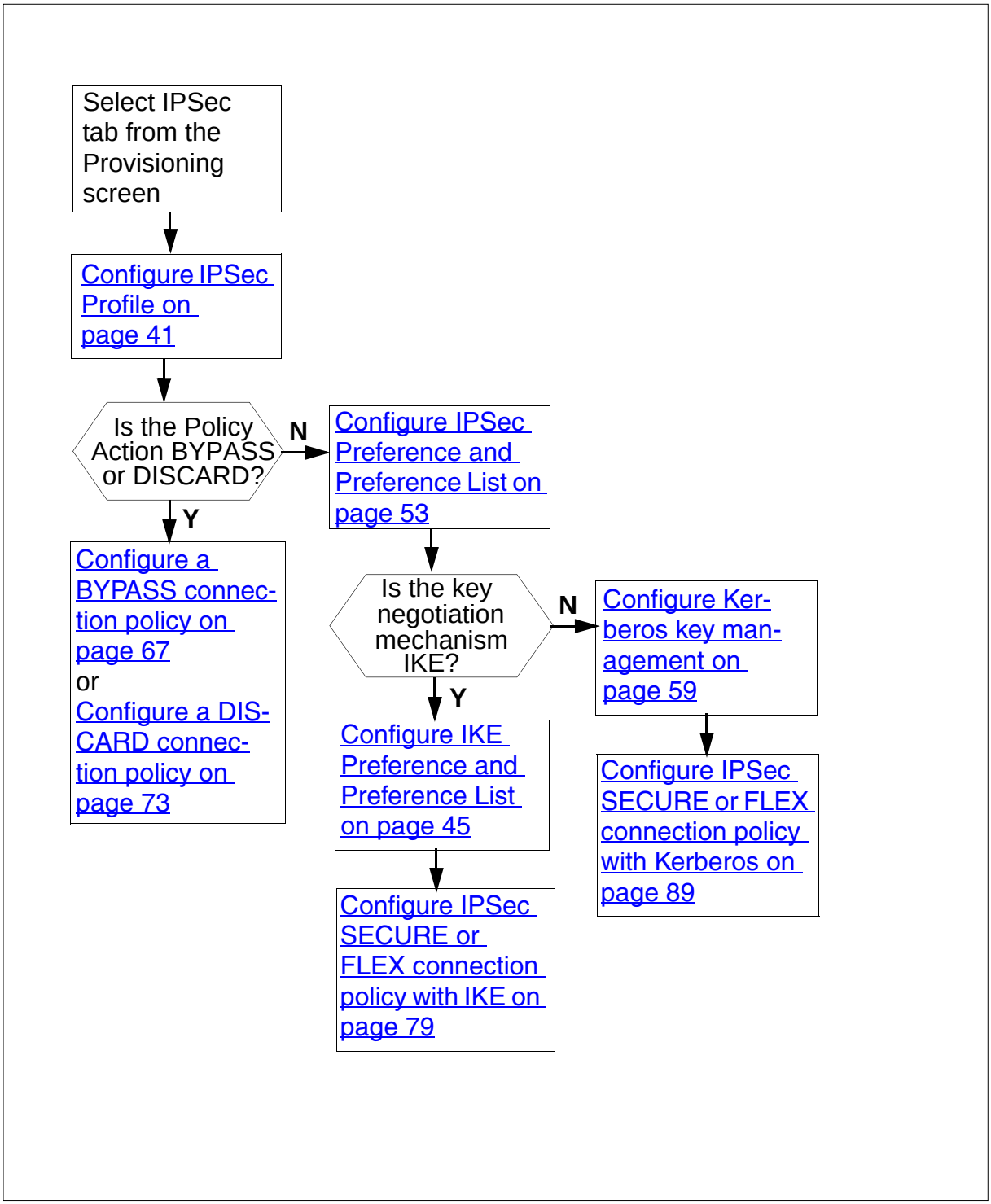
Configuration values for IPSec between GWC and a gateway using IKE key management

Before configuring IPSec for GWC secure communication with a gateway (other than an MTA in packet cable solutions), obtain the following information:

- IKE values:
  - authentication algorithm (must match the value configured on the remote gateway)
  - encryption algorithm (must match the value configured on the remote gateway)
  - Diffie-Hellman group ID
  - IKE SA lifetime (must match the value configured on the remote gateway)
  - pre-shared key
- IPSec values:
  - authentication algorithm (must match the value configured on the remote gateway)
  - encryption algorithm (must match the value configured on the remote gateway)
  - security associations (SA) lifetime (must match the value configured on the remote gateway)
  - Perfect Forward Secrecy (PFS) group ID (in SN08, this value must be NONE)

The following flowchart provides the summary of the procedure for configuring IPSec connection policies on a GWC node.

Summary of configuring IPSec connection policy on a GWC node



Detailed configuration tasks for IPSec between GWC and MTA line gateways (packet cable solutions only)

The following table lists the detail configuration tasks that you may need to perform, and the appropriate actions.

Task	Action
Configure IPSec for a GWC connection with MTA.	Complete procedure Configure IPSec SECURE or FLEX connection policy with Kerberos on page 89.
Disable or enable IPSec processing between GWC and a gateway using BYPASS policy. ***Note:*** When BYPASS policy is used, a loss of communication between the GWC and a remote gateway will occur.	Complete procedure Disable or enable IPSec between two nodes using BYPASS policy on page 103.
Activate or de-activate IPSec processing between GWC and a gateway using FLEX policy. ***Note:*** 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.	Complete procedure Activate or de-activate IPSec using FLEX policy on page 99.
Change Kerberos service key.	Complete procedure Modify Kerberos service key on page 113.
Disable the Kerberos key management	Complete procedure Disable Kerberos key management on page 117.
Delete a connection policy	Complete procedure Delete an IPSec connection policy on page 127.

Detailed configuration tasks for IPSec between GWC and a gateway

The following table lists the detail configuration tasks that you may need to perform, and the appropriate actions.

Task	Action
Configure IPSec for the GWC connection with a gateway.	Complete procedure Configure IPSec SECURE or FLEX connection policy with IKE on page 79.
Disable or enable IPSec processing between GWC and a gateway using BYPASS policy. ***Note:*** When BYPASS policy is used, a loss of communication between the GWC and a remote gateway will occur.	Complete procedure Disable or enable IPSec between two nodes using BYPASS policy on page 103.
Activate or de-activate IPSec processing between GWC and a gateway using FLEX policy. ***Note:*** 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.	Complete procedure Activate or de-activate IPSec using FLEX policy on page 99.
Change IKE pre-shared key.	Complete procedure Modify IKE pre-shared keys on page 109.
Delete a connection policy	Complete procedure Delete an IPSec connection policy on page 127.

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 and GWC400
- logs for the Kerberos application
- logs for the IKE management system

For more information, refer to the *Gateway Controller Fault Management* NTP, NN10202-911.

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 select the GWC to maintain or provision.

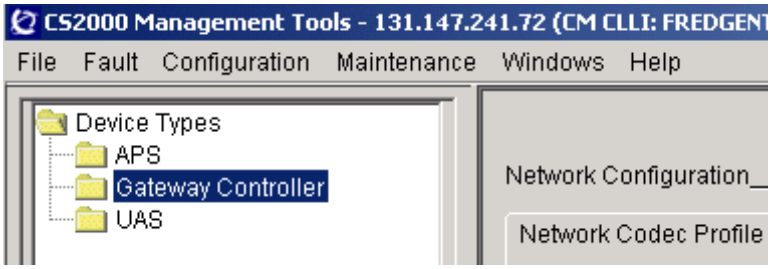
Prerequisites

You require access to CS 2000 Management Tools client applications to perform this procedure. For details, refer to the CS 2000 Management Tools section in the *ATM/IP Solution-level Security and Administration* NTP, NN10402-600.

Action

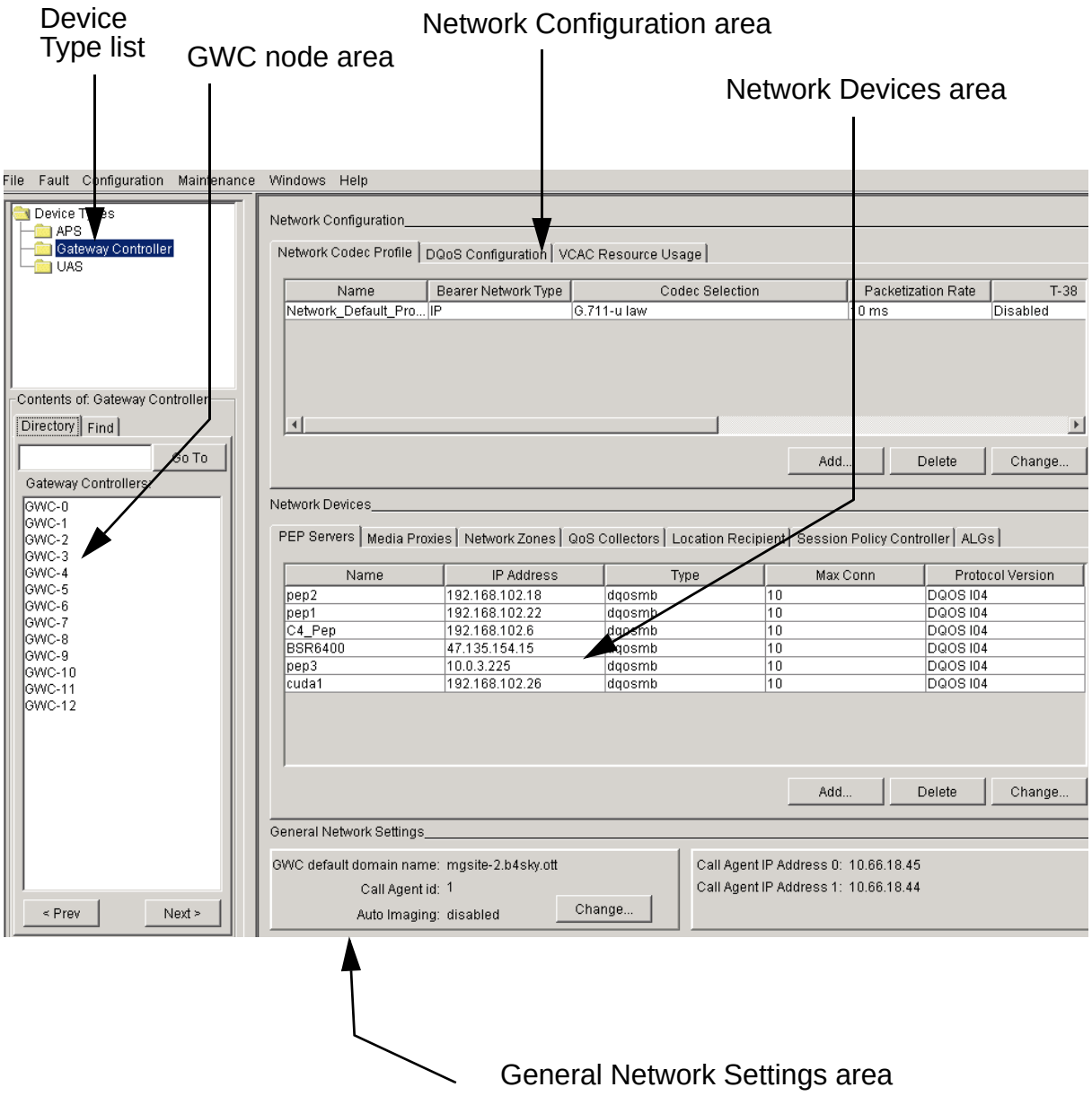
At the CS 2000 GWC Manager workstation

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.

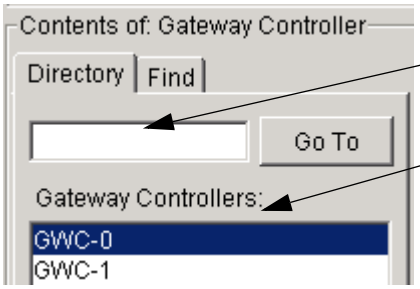


2 Review the three primary panes in the main window area that provide access to provisioning data and maintenance data and activities.

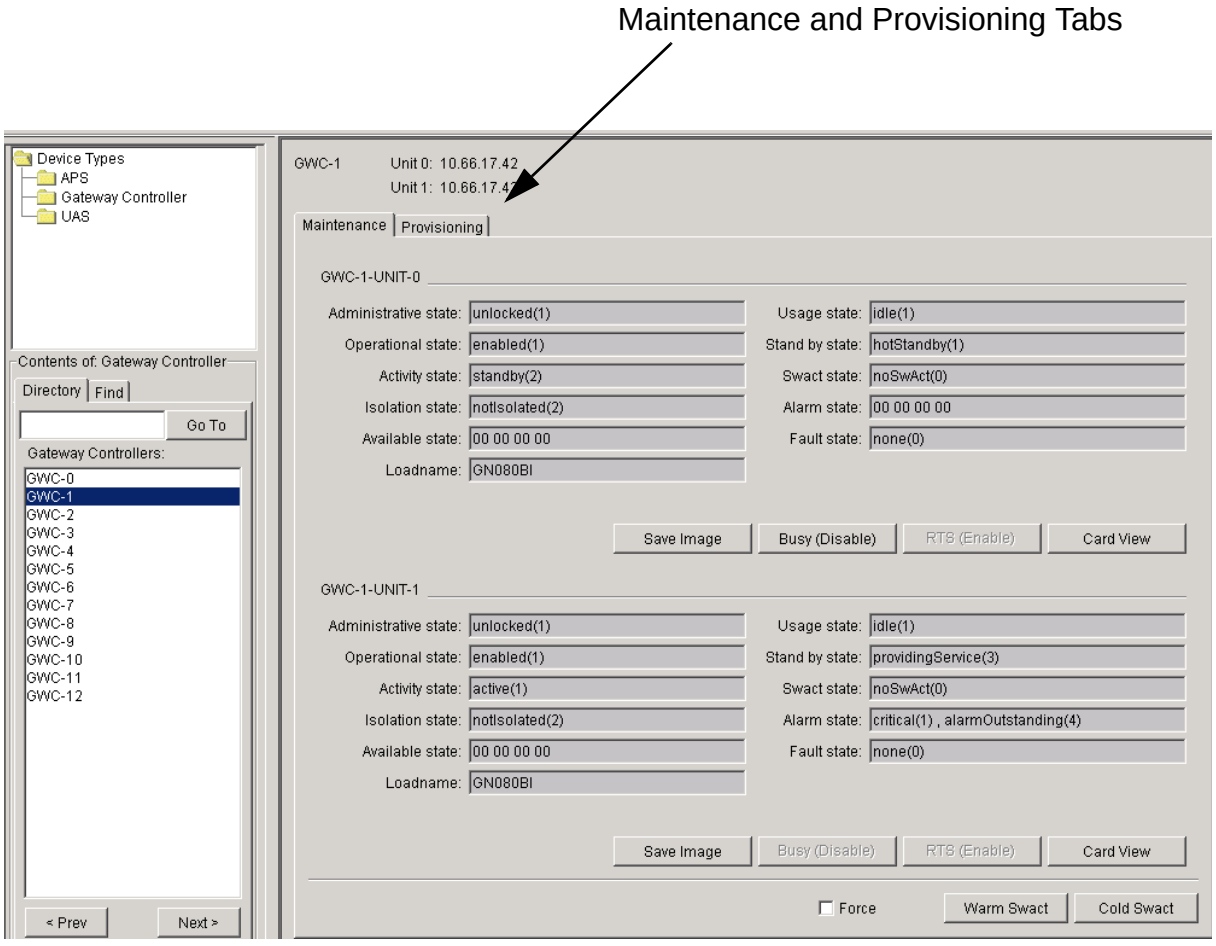
Note: The **VCAC Resource Usage** tab is not displayed when the Network VCAC status is ON.



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 This procedure is complete.

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 on page 23 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

Prerequisites

If the card 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. Refer to procedure Invoke a manual protection switch (warm swact) on page 29.

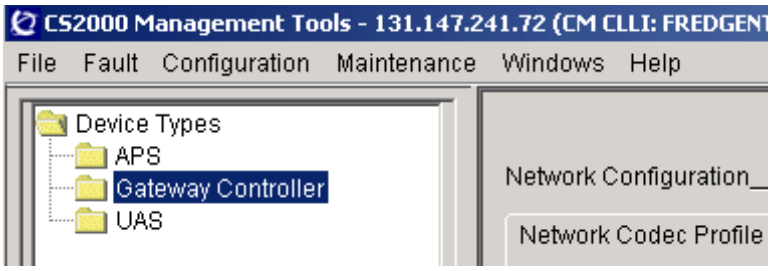
When the card is standby, you need to disable (busy) services on the card. Refer to the procedure Disable (Busy) GWC card services on page 37.

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

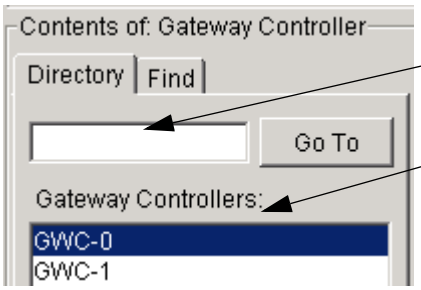
Action

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.

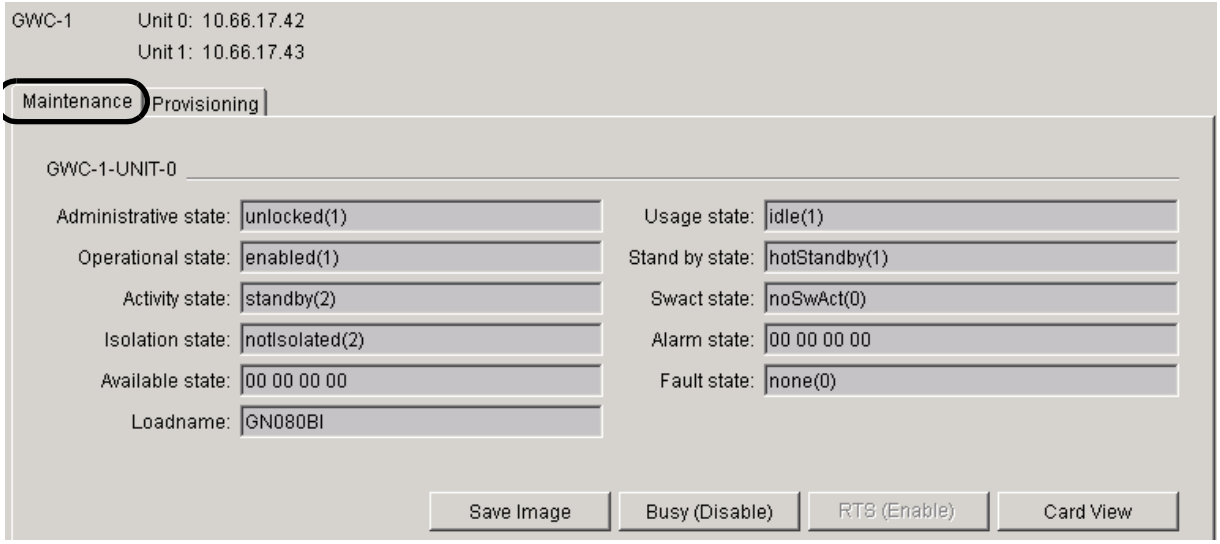


Type a GWC node name here,

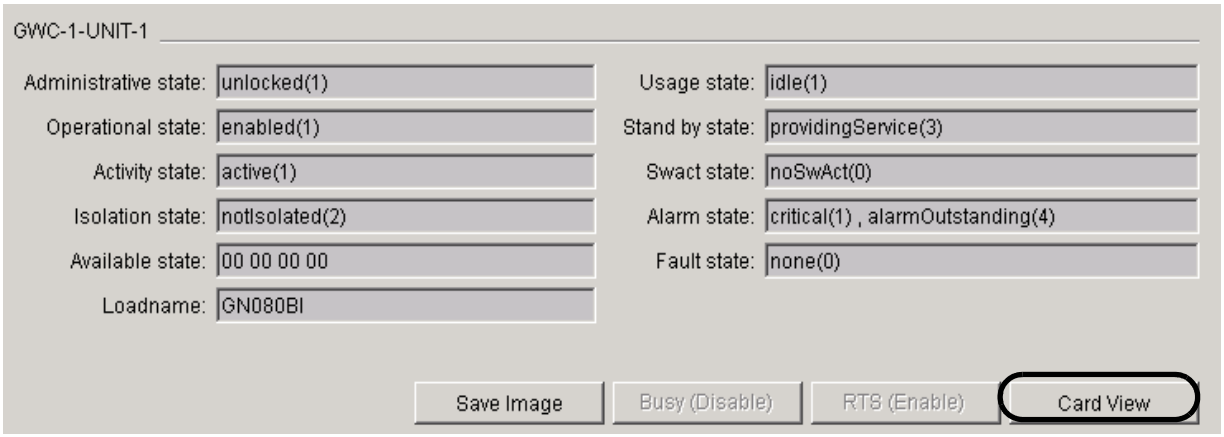
or

Select a GWC node from the list of provisioned GWC nodes.

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

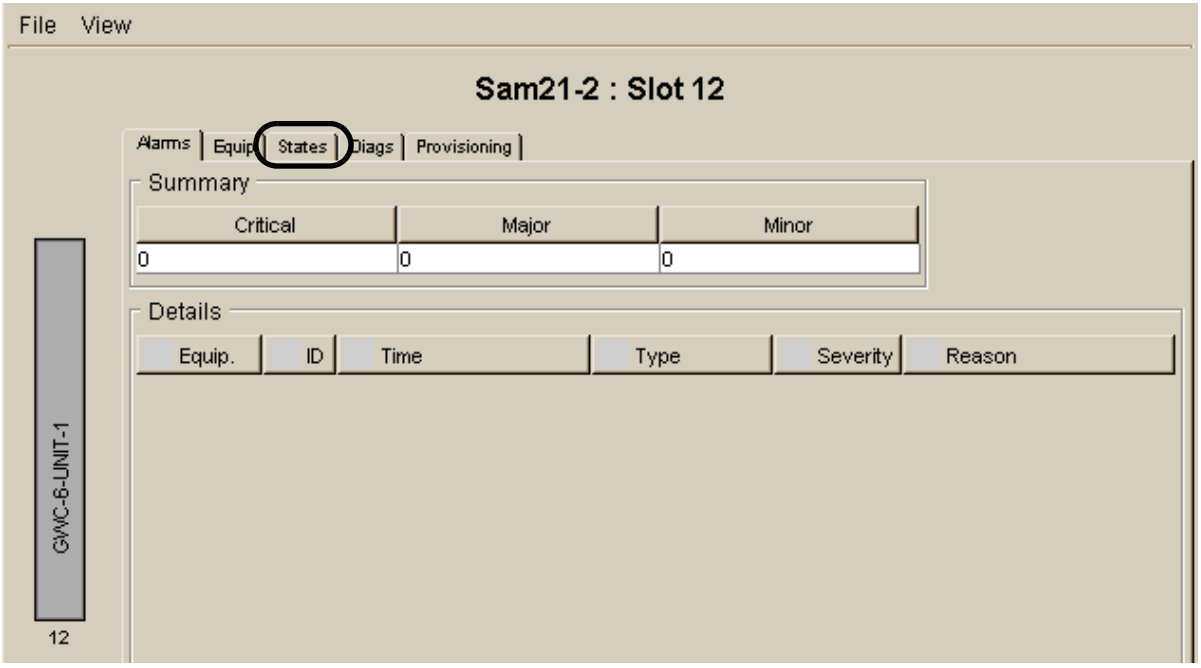


4 Click the **Card View** button for the card you want to lock.

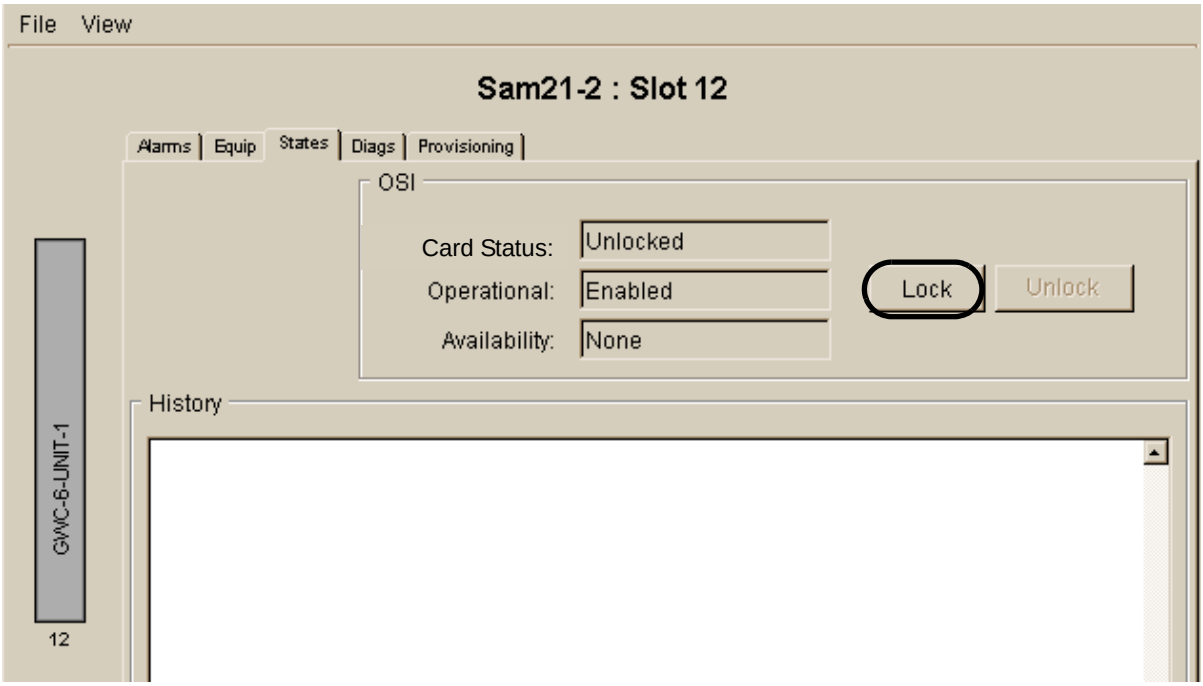


At the CS 2000 SAM21 Manager client

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

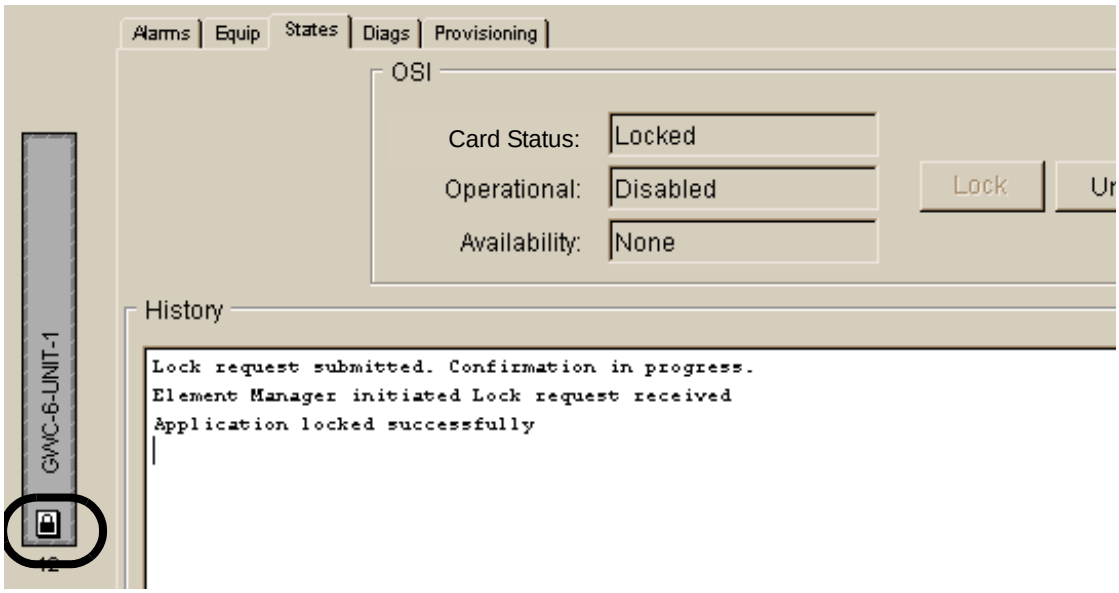


6 In the States display, click the **Lock** button to lock the card.



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 screen shot below) 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.

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.

Note: For more information about upgrading or patching GWC software, refer to the *Upgrading the Gateway Controller* NTP, NN10196-461.

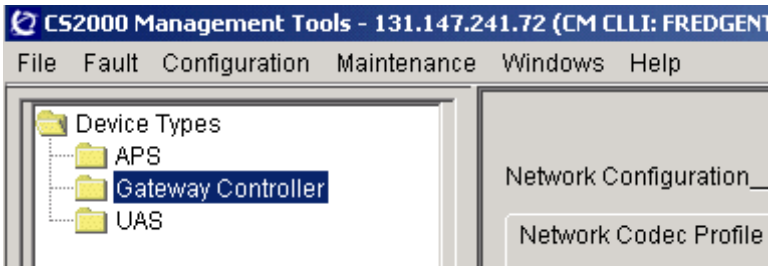
Prerequisites

The GWC card must be locked. The procedure Lock a GWC card on page 17 in this NTP provides instruction on how to lock a GWC card.

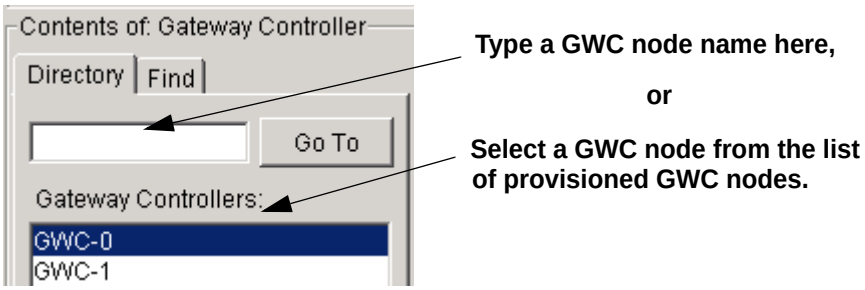
Action

At the CS 2000 GWC Manager client

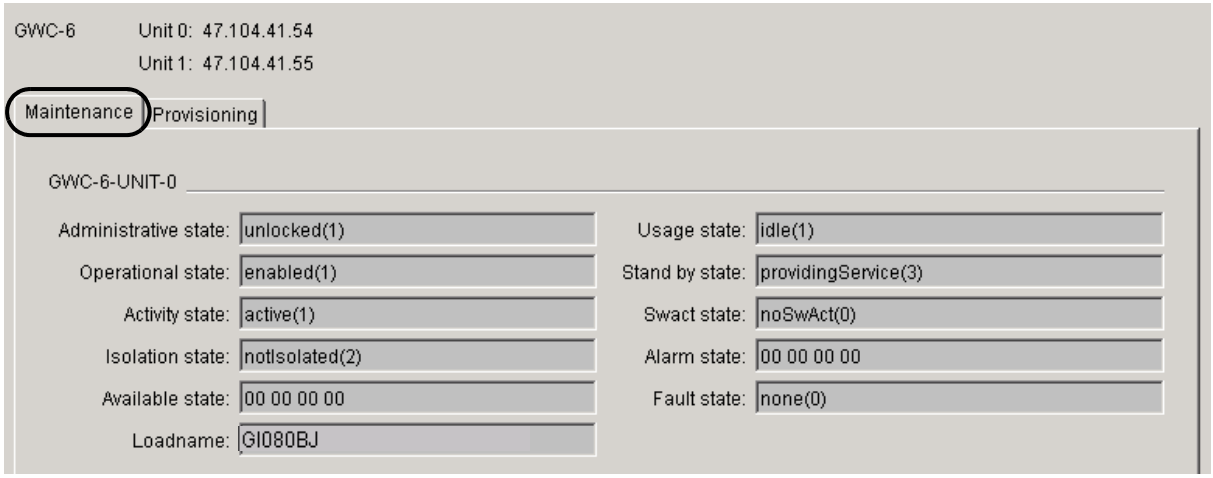
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



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

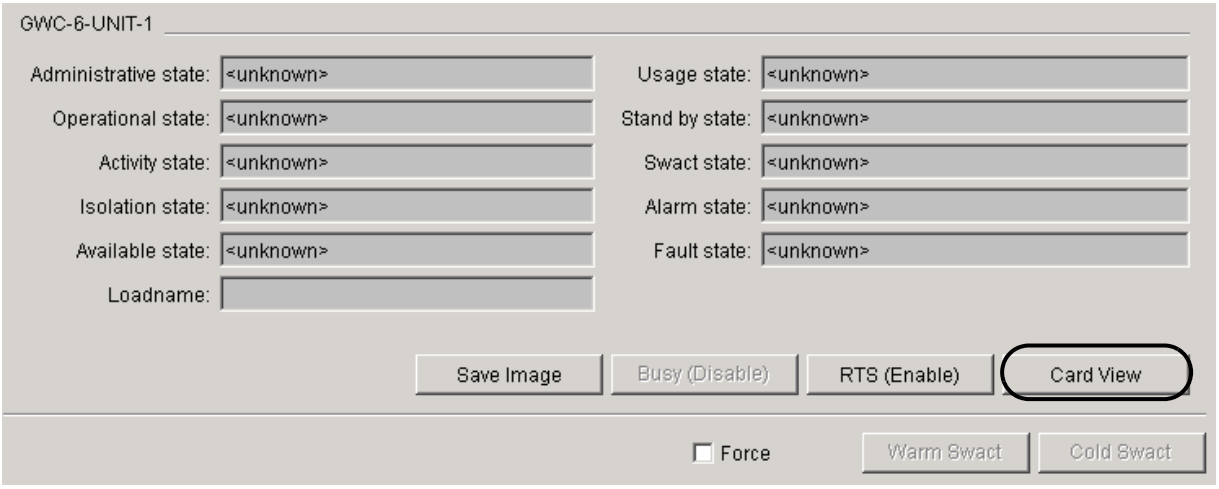


3 Select the **Maintenance** tab to display maintenance information about the node.



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

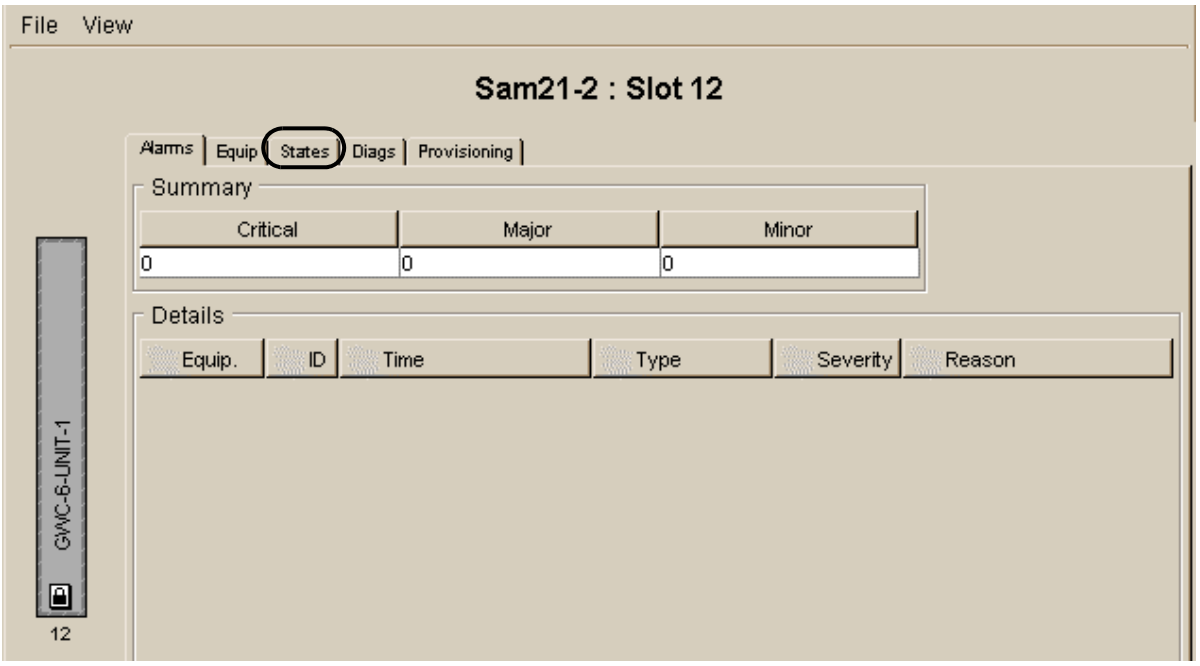
Note: If a card is currently locked, all fields display the value <unknown>.



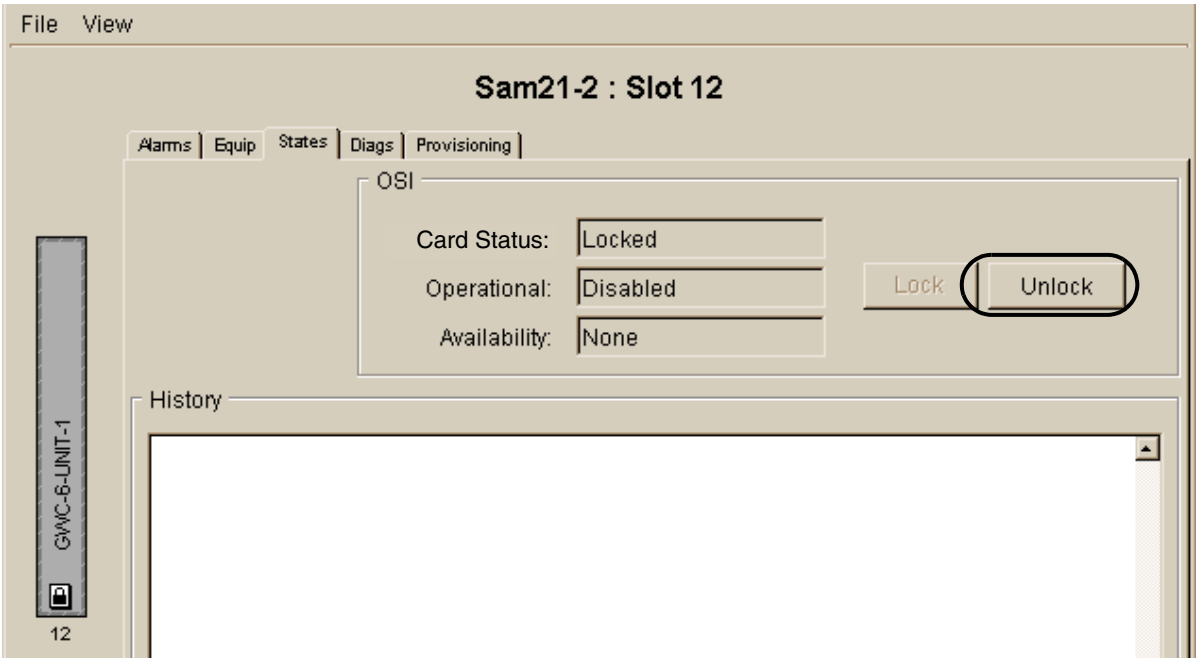
At the CS 2000 SAM21 Manager

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

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

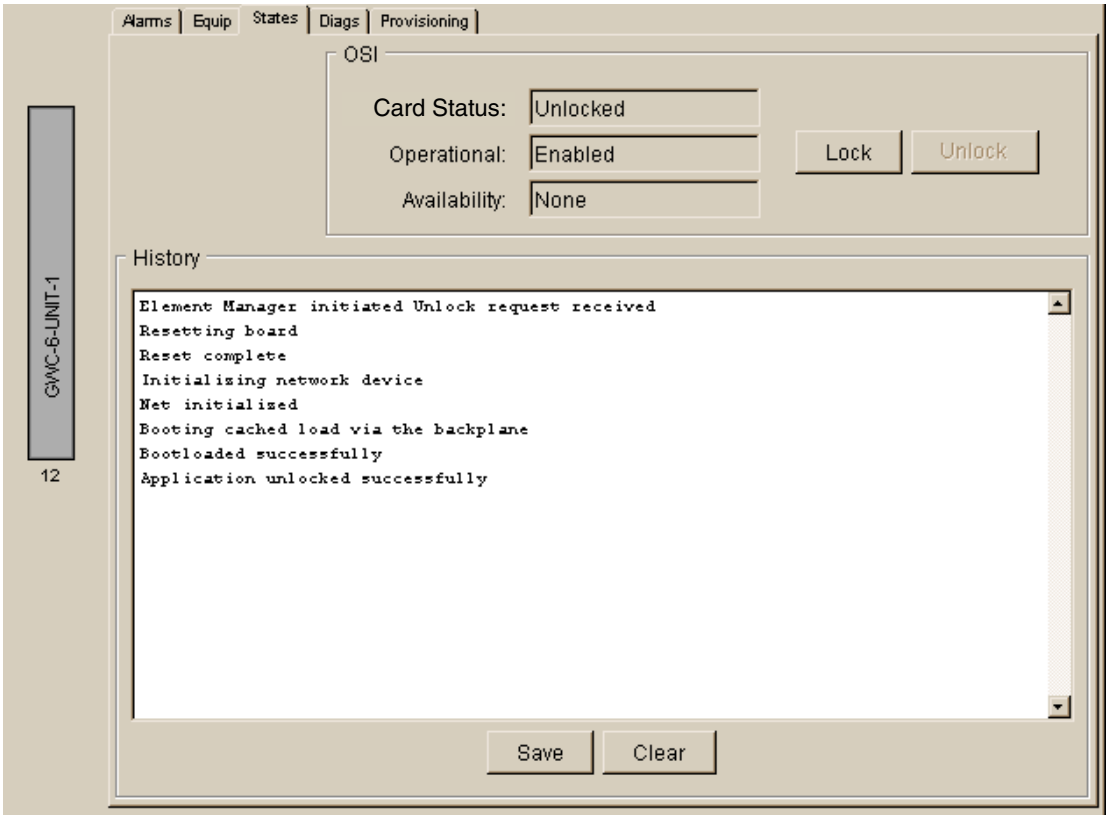


6 In the States display, click the **Unlock** button to unlock the card.



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.

Invoke a manual protection switch (warm swact)

Purpose of this procedure

This procedure switches call processing activity from one GWC card to the mate GWC card within the GWC node.

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

A warm swact will convert 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.

Note 1: 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.

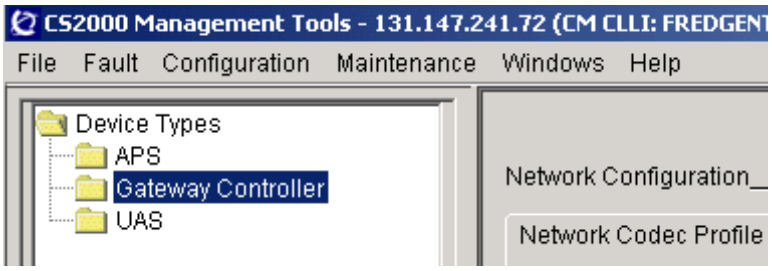
Note 2: During a warm or cold swact, calls in setup over SIP-T trunks are lost (as is the case with other trunk types). However, over SIP-T trunks, the far end will continue to receive the setup alert (ringing) until one of the following occurs:

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

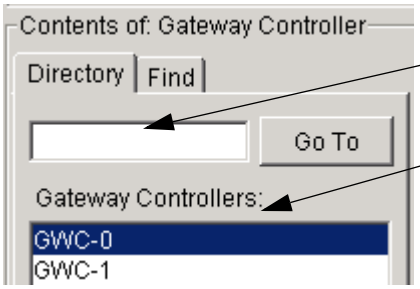
Action

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 the warm Swact on.

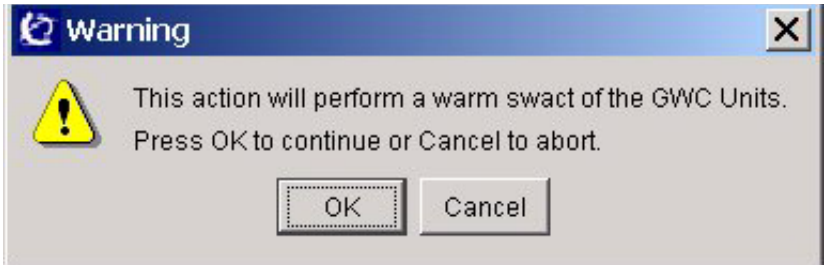


3 If necessary, select the Maintenance tab.

Click the **Warm Swact** button.

Note: 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.

4 Confirm that you wish to perform the warm swact by clicking the **OK** button.



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 This procedure is complete.

Invoke a cold manual protection switch (cold swact)

Purpose of this procedure

This procedure provides a service impacting recovery routine. If 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 Networks support personnel.

Prerequisites

CAUTION

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.

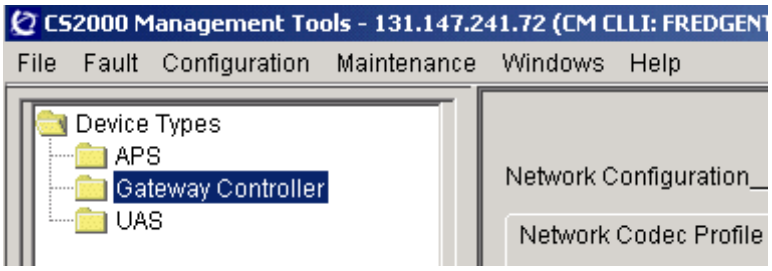
During a cold or warm swact, calls in setup over SIP-T trunks are lost (as is the case with other trunk types). However, over SIP-T trunks, the far end will continue to receive the setup alert (ringing) until one of the following occurs:

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

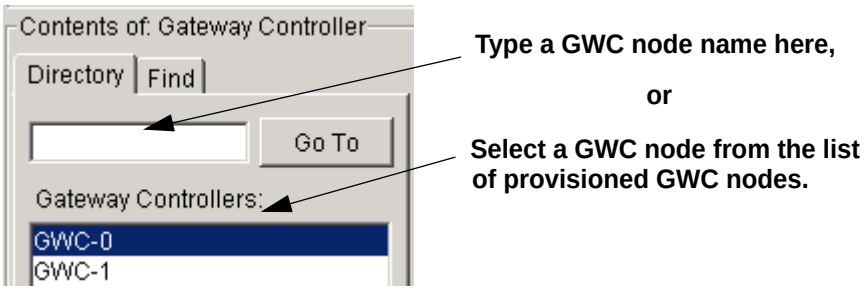
Action

At the CS 2000 GWC Manager workstation

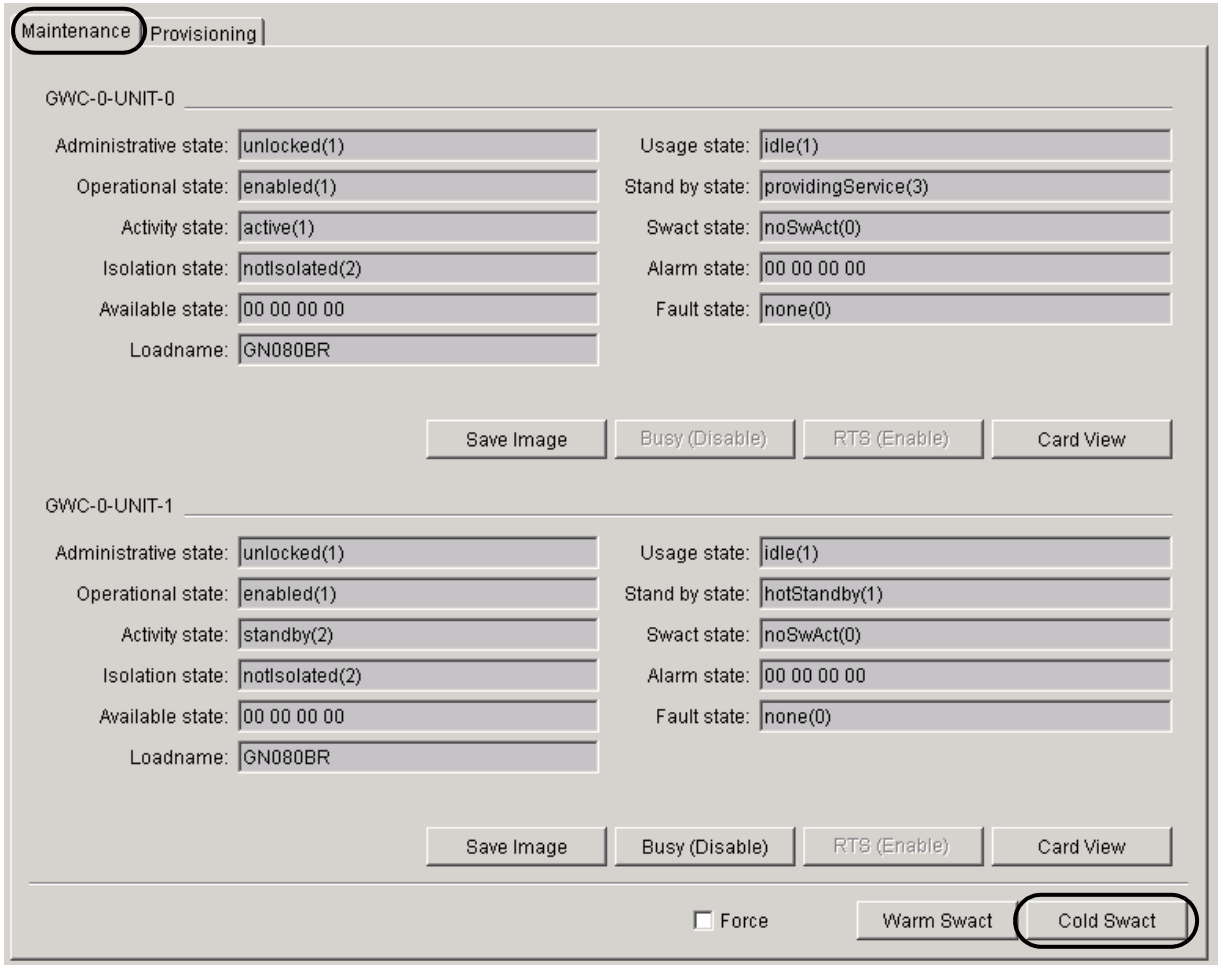
1 At the CS 2000 Management Tools Selector window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



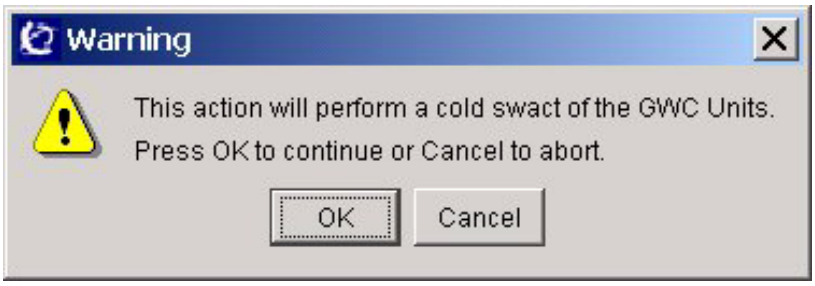
2 From the Contents of: GatewayController frame, select the GWC node that you wish to cold swact.



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



4 Confirm that you wish to perform the cold swact by click the **OK** button.



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 This procedure is complete.

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.

Note: If you wish to busy both GWC cards in the node, refer to procedure “Busy a GWC node” in the *Gateway Controller Configuration Management* NTP, NN10205-511.

When to use this procedure

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

Prerequisites

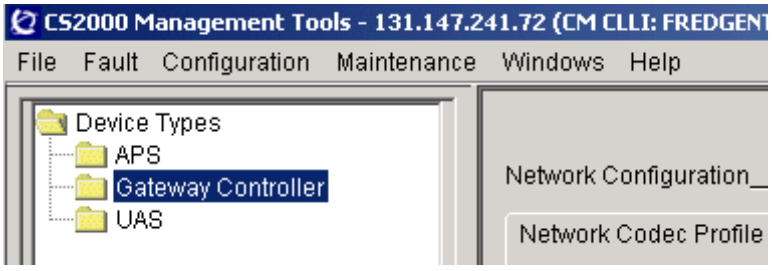
The following prerequisites apply:

- 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) on page 29.
- 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 on page 17, after you have performed the steps in this procedure.

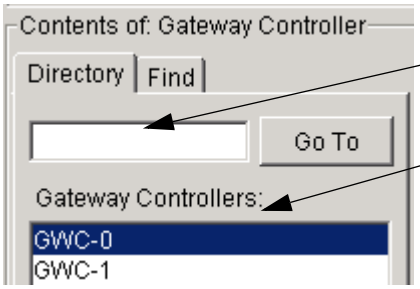
Action

At the CS 2000 GWC Manager workstation

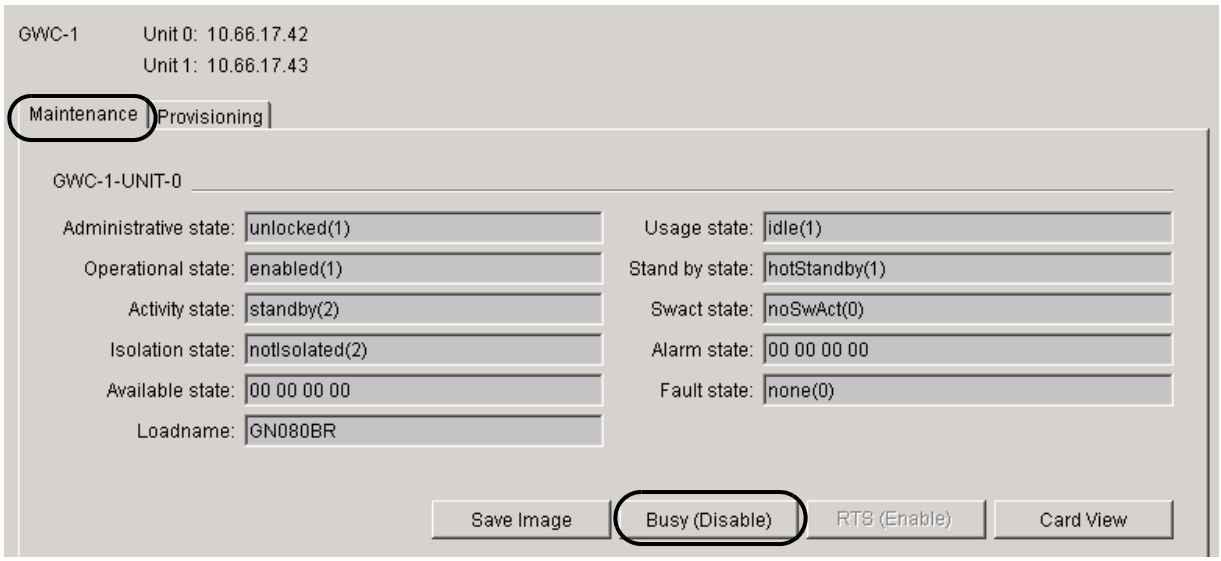
1 At the CS 2000 Management Tools Selector window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



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 This procedure is complete.

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.

Note: To restart services on both GWC cards in a node refer to procedure “Manually return a GWC node to service” found in the *Gateway Controller Configuration Management* NTP, NN10205-511.

When to use this procedure

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

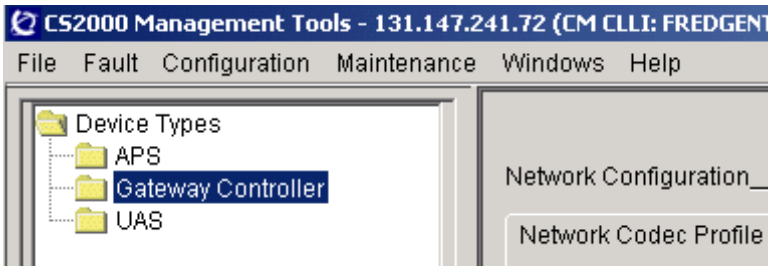
Prerequisites

The services on the GWC card must be in a busied state. Use procedure Disable (Busy) GWC card services on page 37 to perform this task.

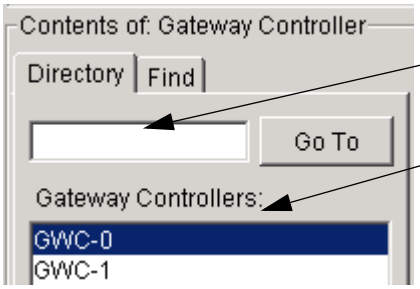
Action

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.



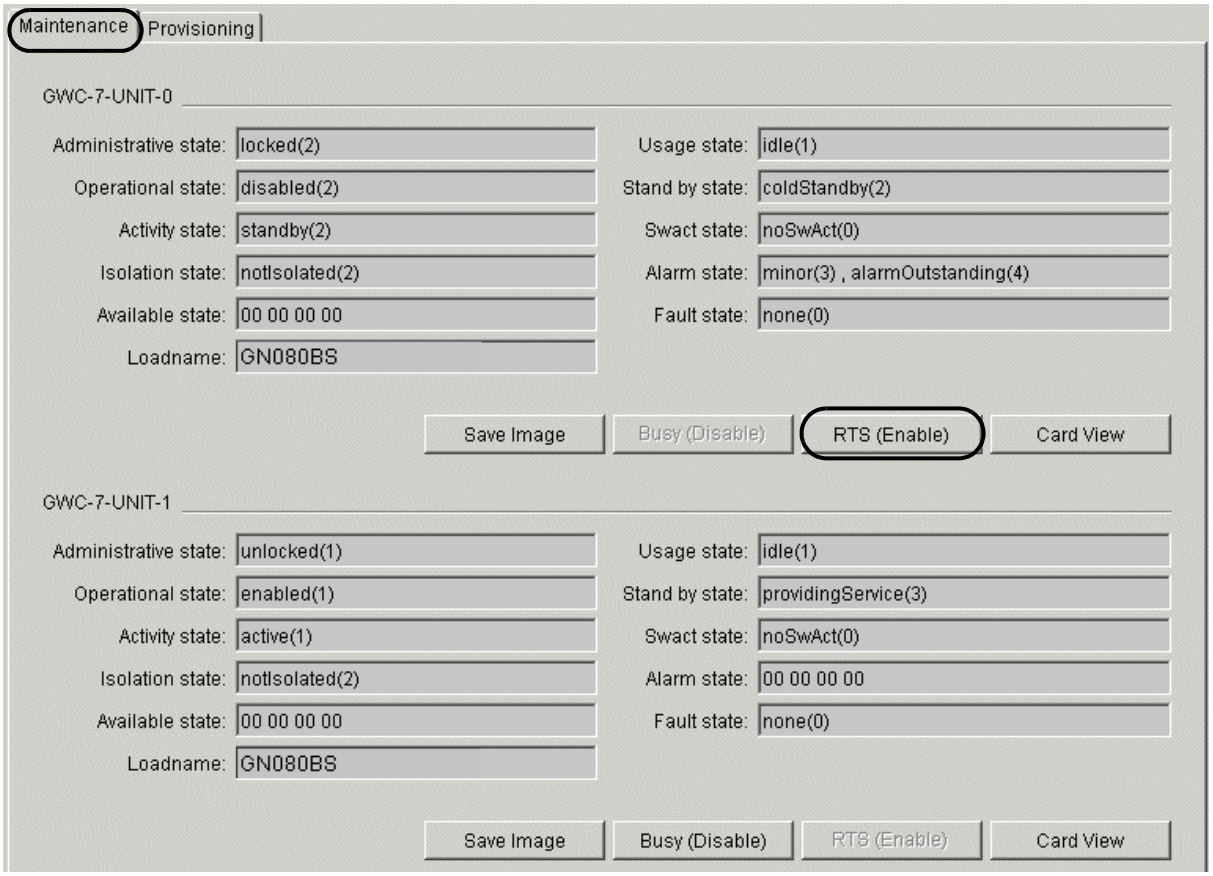
2 From the Contents of: GatewayController frame, select the GWC node that you wish to perform an RTS on.



3 Select the **Maintenance** tab.

4 Determine which GWC card in the node has services busied. If both card's services busied, refer to procedure "Manually return a GWC node to service" found in the *Gateway Controller Configuration Management* NTP, NN10205-511.

5 Click the **RTS (Enable)** button for the standby card.



6 This procedure is complete.

Configure IPSec Profile

Purpose of this procedure

This procedure provides the steps required to configure 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.

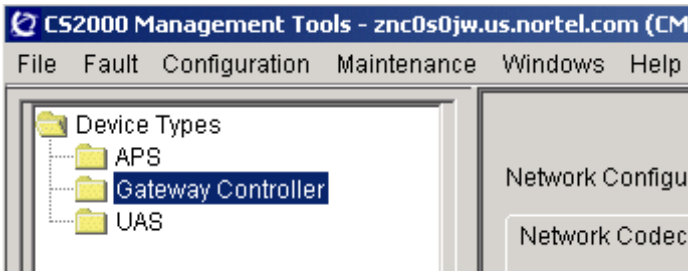
Prerequisites

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

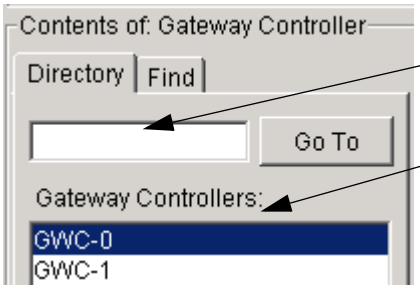
Action

At the CS 2000 GWC Manager client

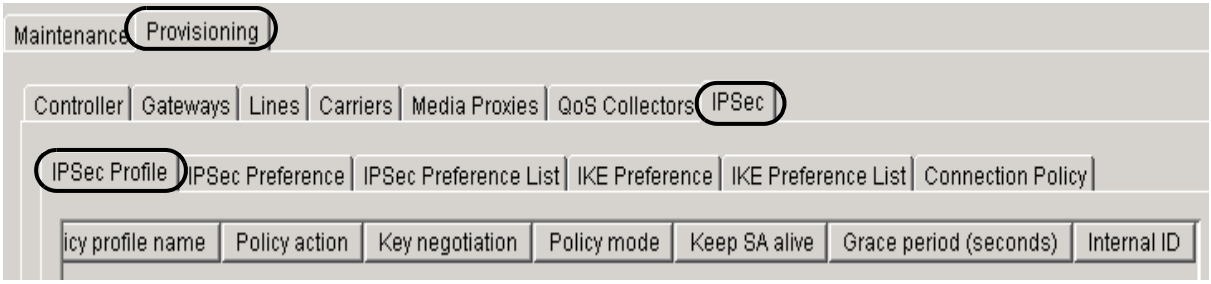
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



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

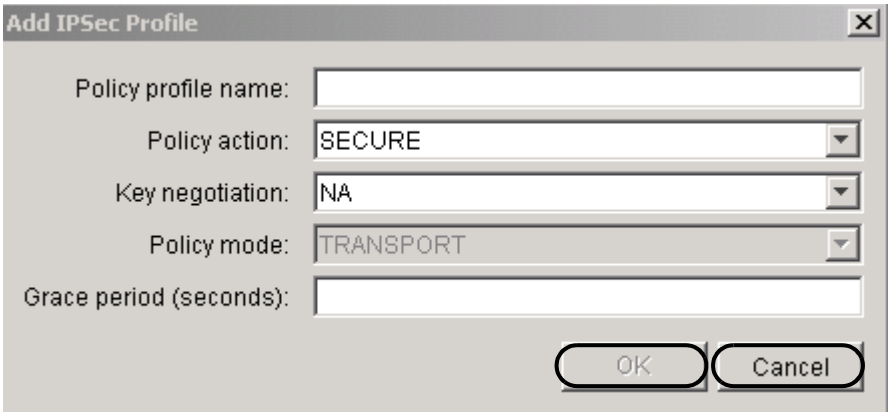


3 Click the **Provisioning** tab, then the **IPSec** tab, then click the **IPSec Profile** tab.



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

Note: 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.



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 (Sheet 1 of 2)

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	No IPSec processing will be applied to all packets matching the policy.
	DISCARD	All packets matching the policy 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.
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.		

IPSec Profile configuration fields (Sheet 2 of 2)

Field	Value	Description
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. ***Note:*** If you chose the 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 ***Note:*** IPSec in tunnel mode is not supported in SN08.
Grace period (seconds)	0 to 2419200	Enter an integer value (in seconds) representing 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. ***Note:*** The recommended value is 60.

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

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

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

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

8 The procedure is complete.

Configure IKE Preference and Preference List

Purpose of this procedure

This procedure provides the steps required to configure 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).

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:*** Note that only main mode is supported on the GWC (aggressive mode is not supported). Also, only pre-shared key authentication is supported (digital signature authentication or public key encryption authentication are not supported).

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 when you wish 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.

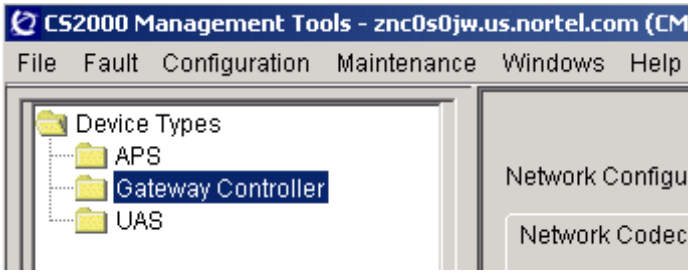
Prerequisites

None

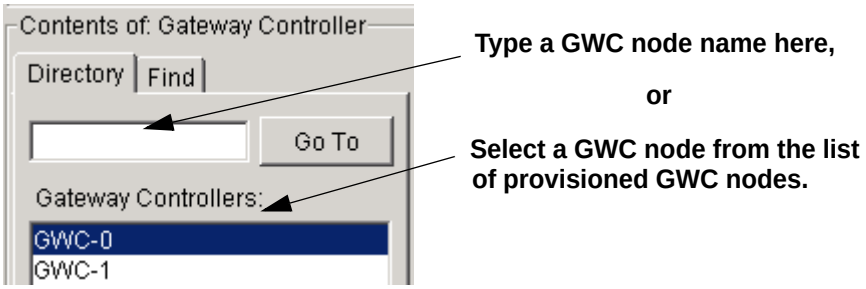
Action

At the CS 2000 GWC Manager client

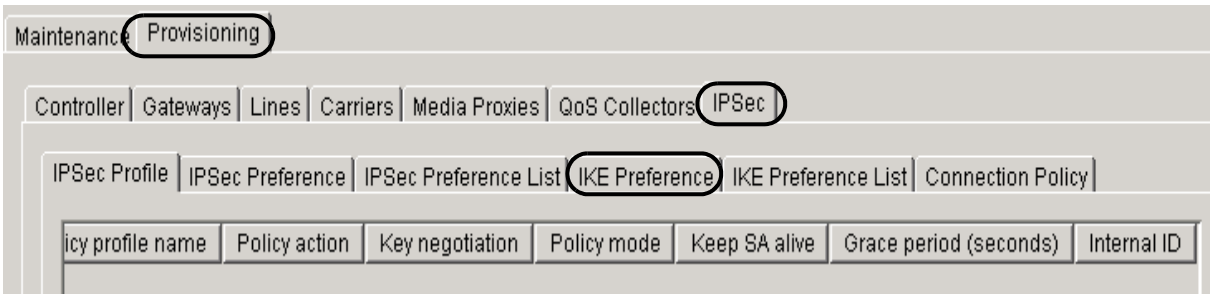
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



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

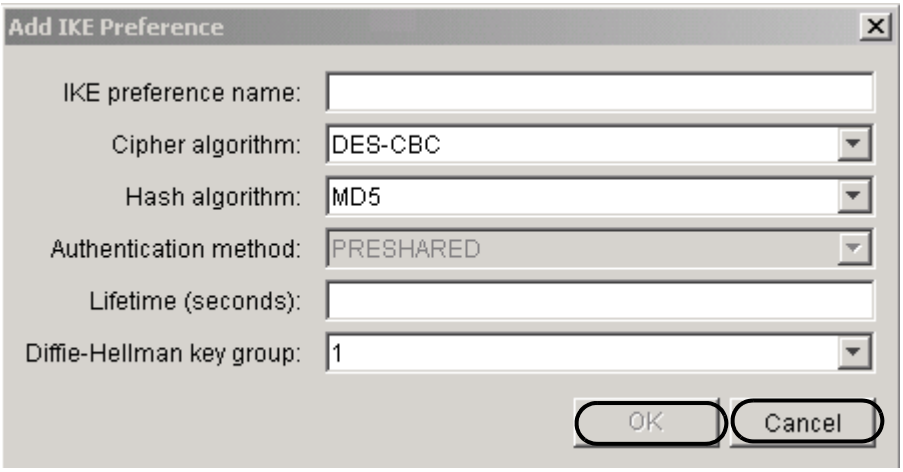


3 Click the **Provisioning** tab, then the **IPSec** tab, then click the **IKE Preference** tab.



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

Note: 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.



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 (Sheet 1 of 2)

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. ***Note 1:*** 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. ***Note 2:*** This algorithm must match the algorithm configured on the remote gateway. If necessary, refer to the appropriate gateway documentation or contact your network administrator.

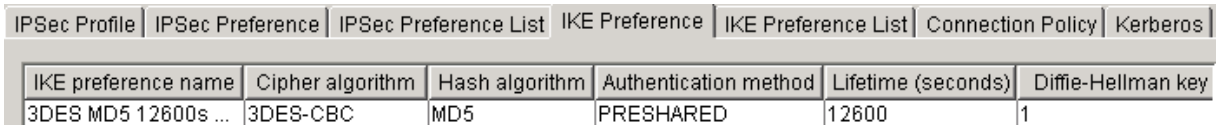
IKE Preference configuration fields (Sheet 2 of 2)

Field	Values	Description
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. ***Note:*** This algorithm must match the algorithm configured on the remote gateway. If necessary, refer to the appropriate gateway documentation or contact your network administrator.
Authentication method:	PRESHARED	This field indicates the authentication method to be used with this IKE preference. This field is pre-defined with the value of PRESHARED, which means that the same key is pre-installed on each host.
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. ***Note:*** Ensure that the same lifetime value is configured on the GWC and on the remote gateway. Contact your network administrator to determine this value.
Diffie-Hellman key group:	1 2	This field indicates the Oakley group to be used for a Diffie-Hellman key exchange during phase 1 negotiation (establishing IKE SA).

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

Observe that the newly defined data appears in the IKE Preference table.

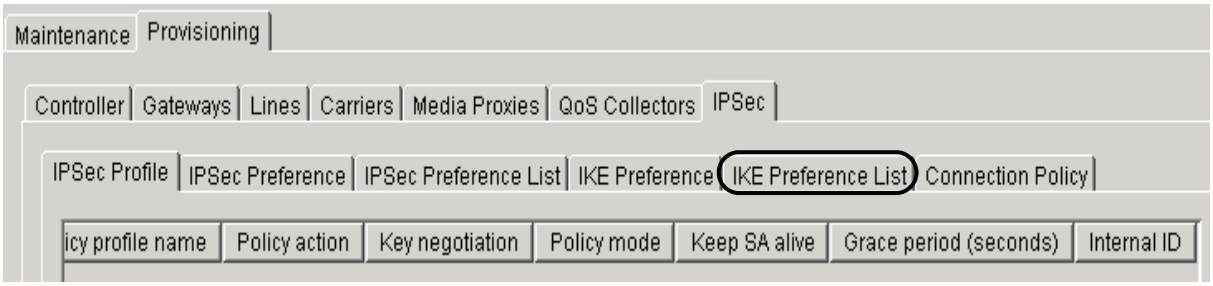
Note: If you need to remove the new entry, click the appropriate row to highlight it, then click the **Delete** button. A Confirm deletion window appears. Click the **Yes** button to delete the entry.



7 Use the following table to determine your next step.

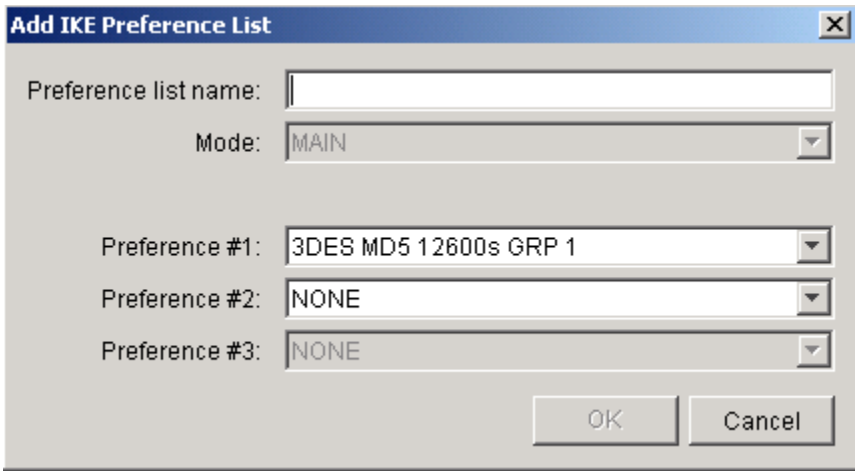
If you wish to	Do
add more IKE preferences	repeat steps 4 to 7
configure IKE Preference List table	go to step 8

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.

Note: 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.

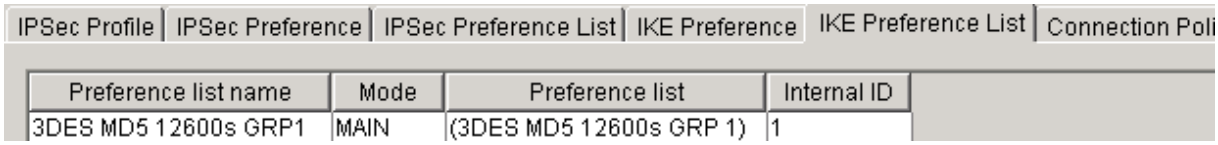
If you want to add more items, repeat this step for the remaining two fields. Otherwise, go to step 12.

Note: 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.

12 Click the **OK** button.

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

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



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

14 The procedure is complete.

Configure IPSec Preference and Preference List

Purpose of this procedure

This procedure provides the steps required to configure IPSec Preference and IPSec Preference List tables.

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. The IPSec SAs define how two network components will use IPSec to communicate securely.

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.

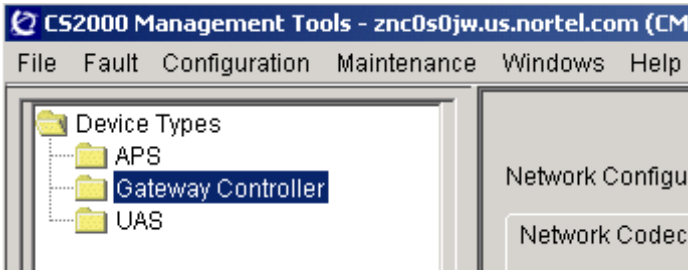
Prerequisites

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

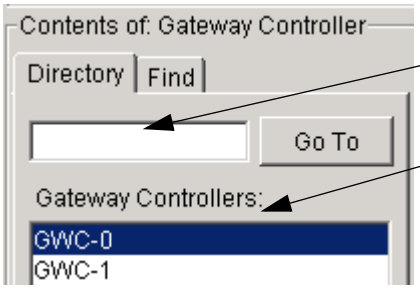
Action

At the CS 2000 GWC Manager client

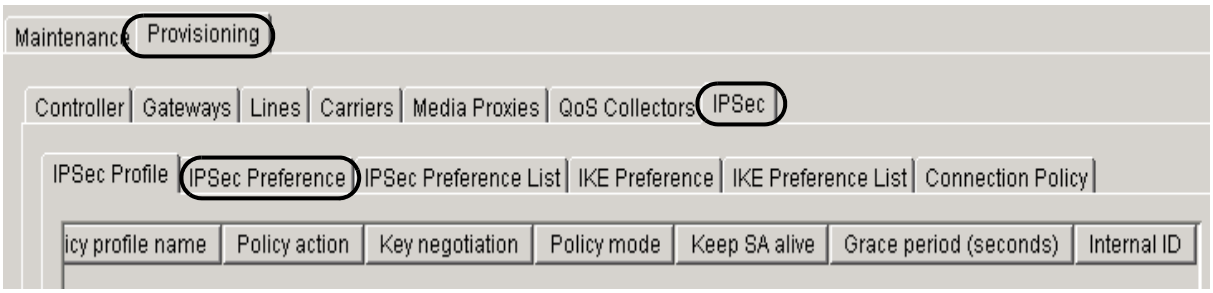
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



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

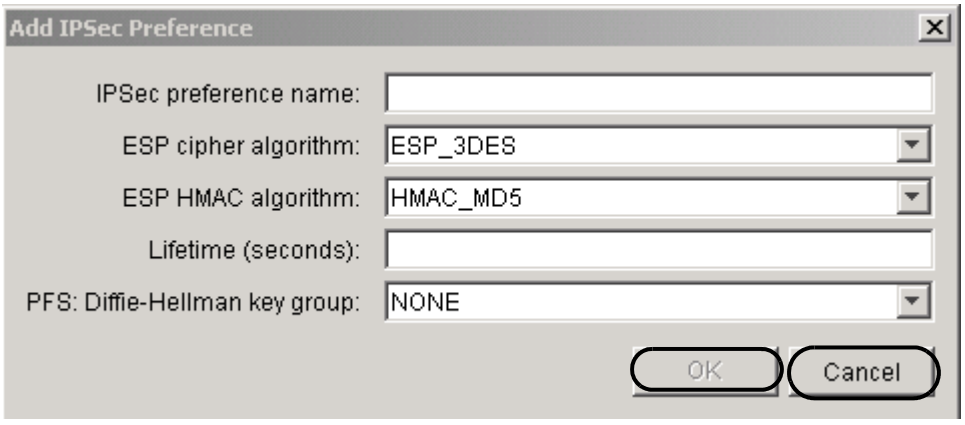


3 Click the **Provisioning** tab, then on the **IPSec** tab, then click the **IPSec Preference** tab.



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

Note: 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.



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

IPSec Preference configuration fields (Sheet 1 of 2)

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. ***Note 1:*** Triple DES (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 cannot be supported by the remote gateway. NULL provides no encryption to the data, but does retain data integrity and authentication. ***Note 2:*** If IKE is used as the key management protocol, ensure that the same algorithm is configured on the remote gateway. If necessary, refer to the appropriate gateway documentation or contact your network administrator.
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. ***Note:*** If IKE is used as the key management protocol, ensure that the same algorithm is configured on the remote gateway. If necessary, refer to the appropriate gateway documentation or contact your network administrator.

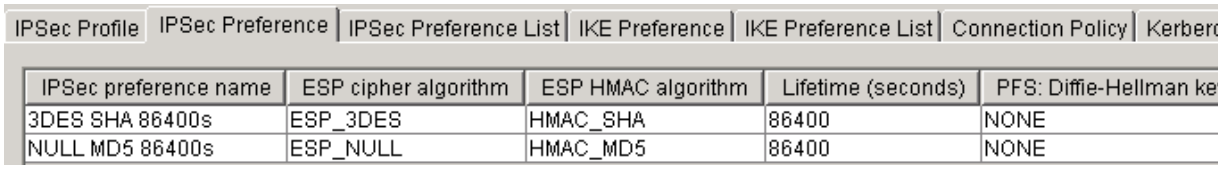
IPSec Preference configuration fields (Sheet 2 of 2)

Field	Values	Description
Lifetime (seconds)	0 to 2419200	Specify (in seconds) the desired lifetime of an IPSec SA established using this preference. ***Note 1:*** The recommended value is 86400 (1 day). ***Note 2:*** If IKE is used as the key management protocol, ensure that the same lifetime is used on the GWC and on the remote gateway.
PFS: Diffie-Hellman key group:	NONE 1 2	When Kerberos is used as the key management, this value must be set to NONE. When IKE is used as the key management, this field indicates what Oakley group will be used for a Diffie-Hellman key exchange during phase 2 negotiation (establishing IPSec SAs pair). For packet cable solutions, the recommendation is not to use Perfect Forward Secrecy (PFS), so select NONE when configuring IPSec between the GWC and a CMTS, and between the GWC and a TGCP trunk gateway.

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

Observe that the newly defined data appears in the IPSec Preference table.

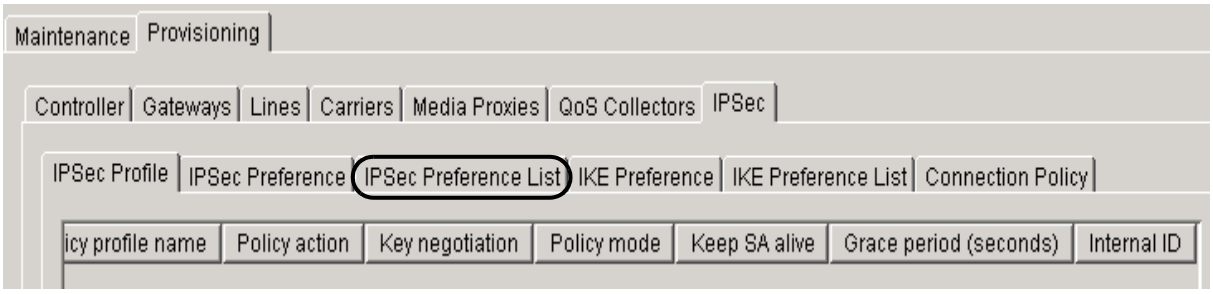
Note: If you need to remove the new entry, click the appropriate row to highlight it, then click the **Delete** button. A Confirm deletion window appears. Click the **Yes** button to delete the entry.



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 table	go to step 8

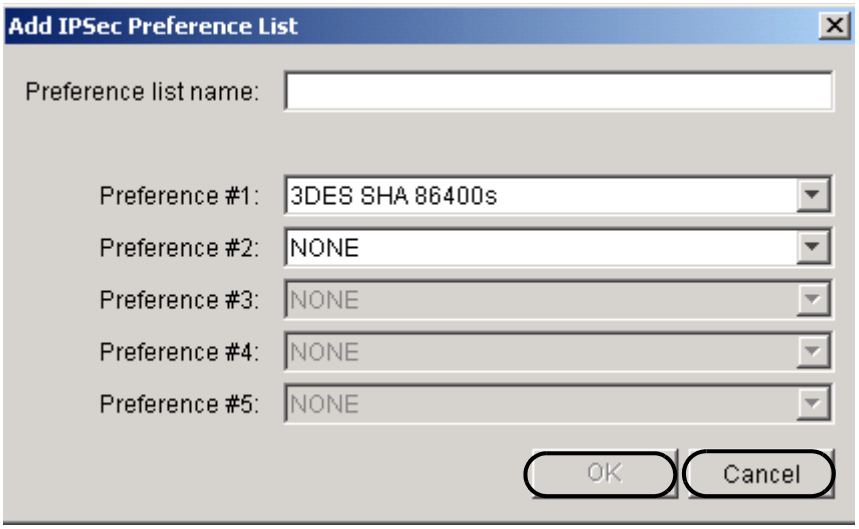
8 Click the **IPSec Preference List** tab.



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.

Note: 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.

Note 3: 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.

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.

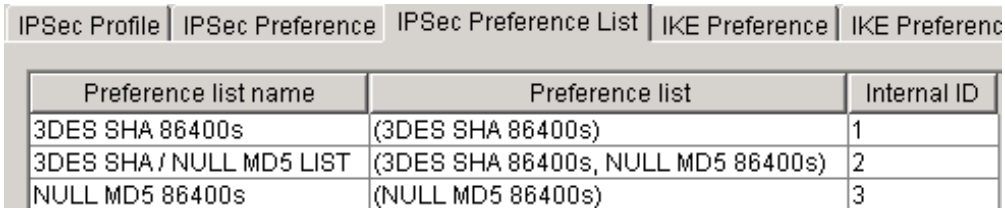
If you want to add more items, repeat this step for the remaining fields. Otherwise, go to step 12.

Note: 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 the **OK** button.

Observe that the newly defined data appears in the IPSec Preference List table.

Note: 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 the **Yes** button to delete the entry.



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

14 The procedure is complete.

Configure Kerberos key management

Purpose of this procedure

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

- SMALL_LINENA
- SMALL_LINEINTL

Note: 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.

Note: 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

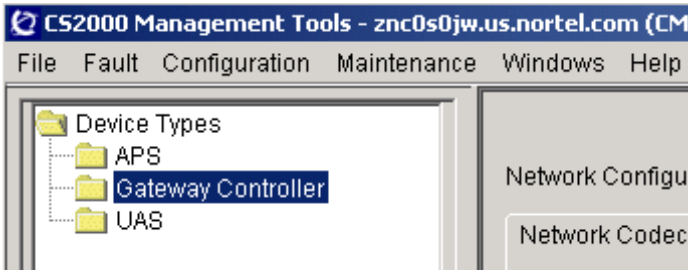
authentication tickets to the MTA. These tickets are used to authenticate an MTA to a GWC, and to establish a pair of IPSec SAs on both nodes. The KDC is third-party equipment and must be integrated with the network.

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.

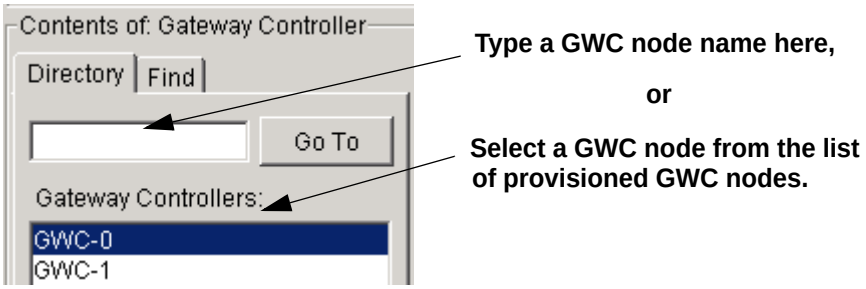
Action

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.

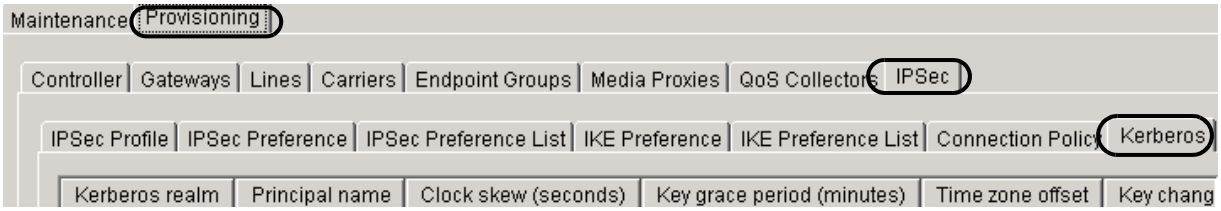


2 From the Contents of: GatewayController frame, select the appropriate GWC node.



3 Click the **Provisioning** tab, then on the **IPSec** tab, then click the **Kerberos** tab.

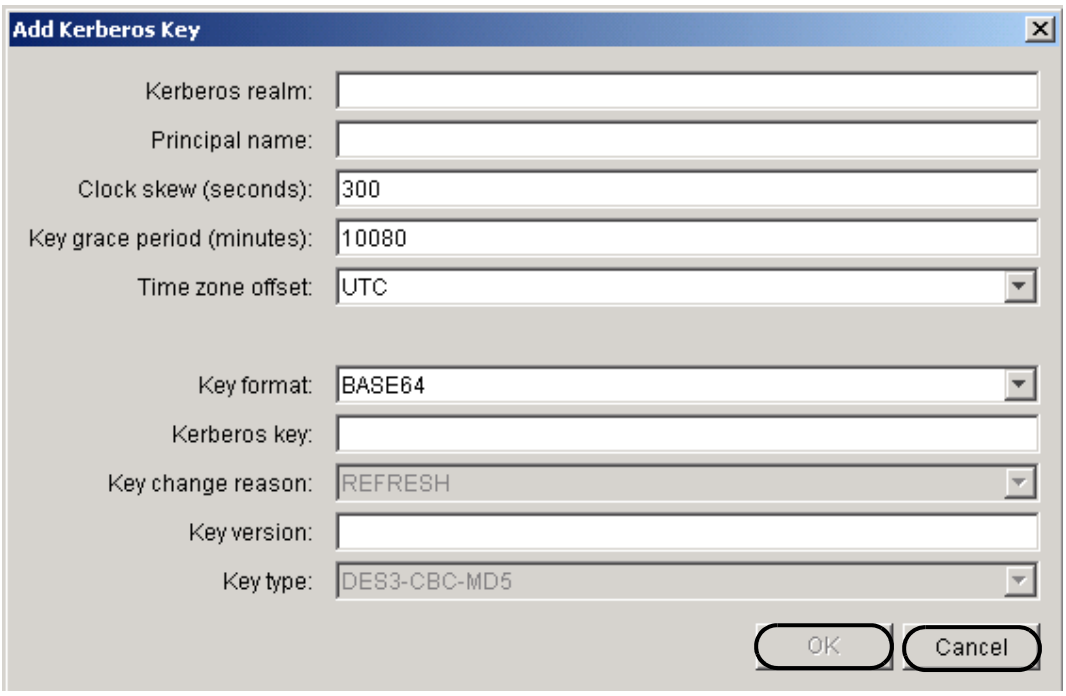
Note: The IPSec and Kerberos tabs are visible only when you select a GWC service profile with the Kerberos capability. Refer to the list of GWC service profiles at the beginning of this procedure.



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

Note 1: 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 refer to procedure Modify Kerberos service key on page 113.

Note 2: 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.



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 (Sheet 1 of 4)

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. ***Note:*** Valid realm name must have at least one dot (.). Make sure that this realm is also defined on the KDC. ***Note:*** 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.
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. ***Note:*** 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.

Kerberos key configuration fields (Sheet 2 of 4)

Field	Values	Description
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 encrypted with 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. ***Note 1:*** 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. ***Note 2:*** 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).
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 configuration fields (Sheet 3 of 4)

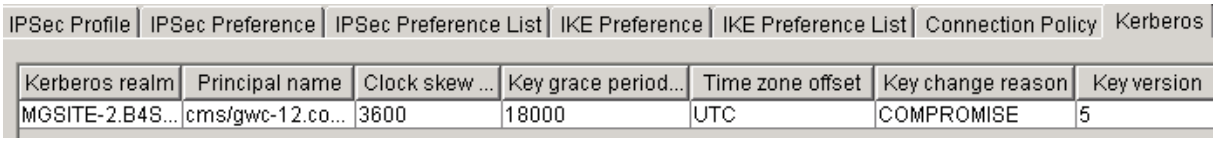
Field	Values	Description
Kerberos key:	<user-defined>	Enter the Kerberos service key that the GWC will use to decrypt Kerberos tickets sent by the MTA. These tickets (obtained by the MTA from the KDC) are encrypted using the same key. The expected key size is • for BASE64 key format: 32 BASE64 digits ***Note:*** The acceptable range of characters is: <a-z, A-Z, 0-9, /+>. • for HEX key format: 48 HEX digits ***Note:*** 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 is required 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. ***Note:*** 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.

Kerberos key configuration fields (Sheet 4 of 4)

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.

Observe that the newly defined Kerberos key data appears in the Kerberos table.



7 The procedure is complete.

Configure a BYPASS connection policy

Purpose of this procedure

This procedure provides the steps required 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 network component (defined by the IP address, a range of addresses, or a netmask) are not secure.

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 are 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 refer to procedure Disable or enable IPSec between two nodes using BYPASS policy on page 103.

Prerequisites

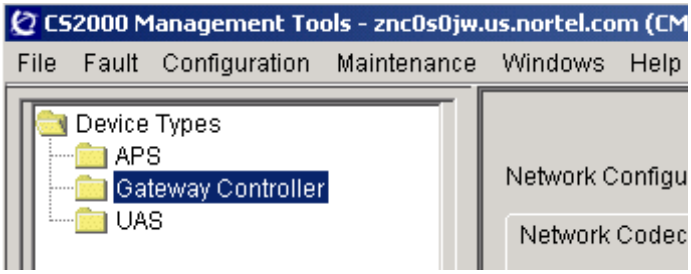
CAUTION
Possible communication disruption
Adding a BYPASS policy can cause a communication disruption between the GWC and a gateway that requires IPSec. Proceed with caution.

This procedure requires that the IPSec profile with the BYPASS policy action is configured first. If required, complete procedure Configure IPSec Profile on page 41.

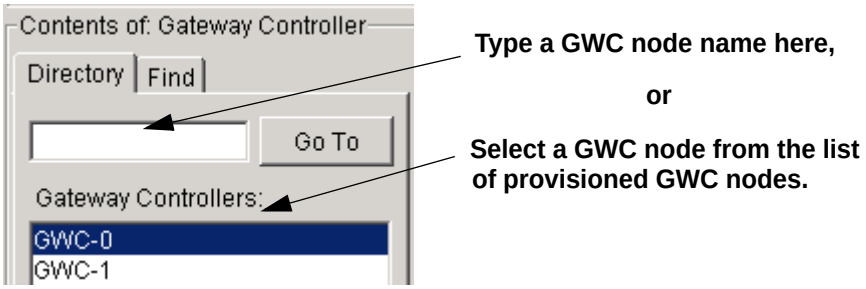
Action

At the CS 2000 GWC Manager client

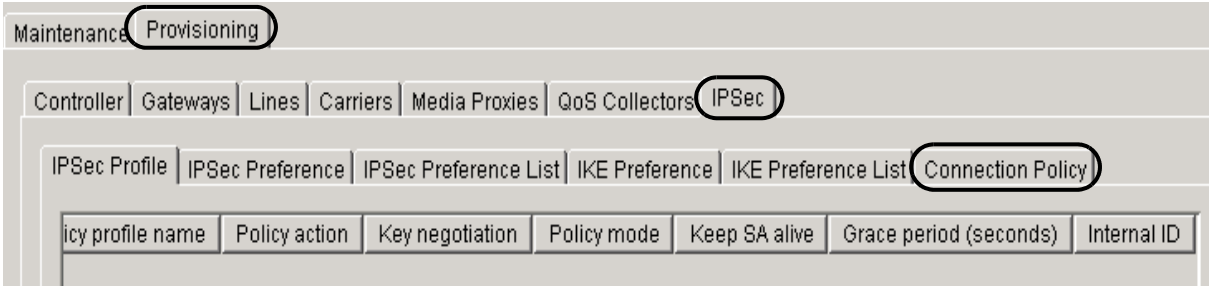
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



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

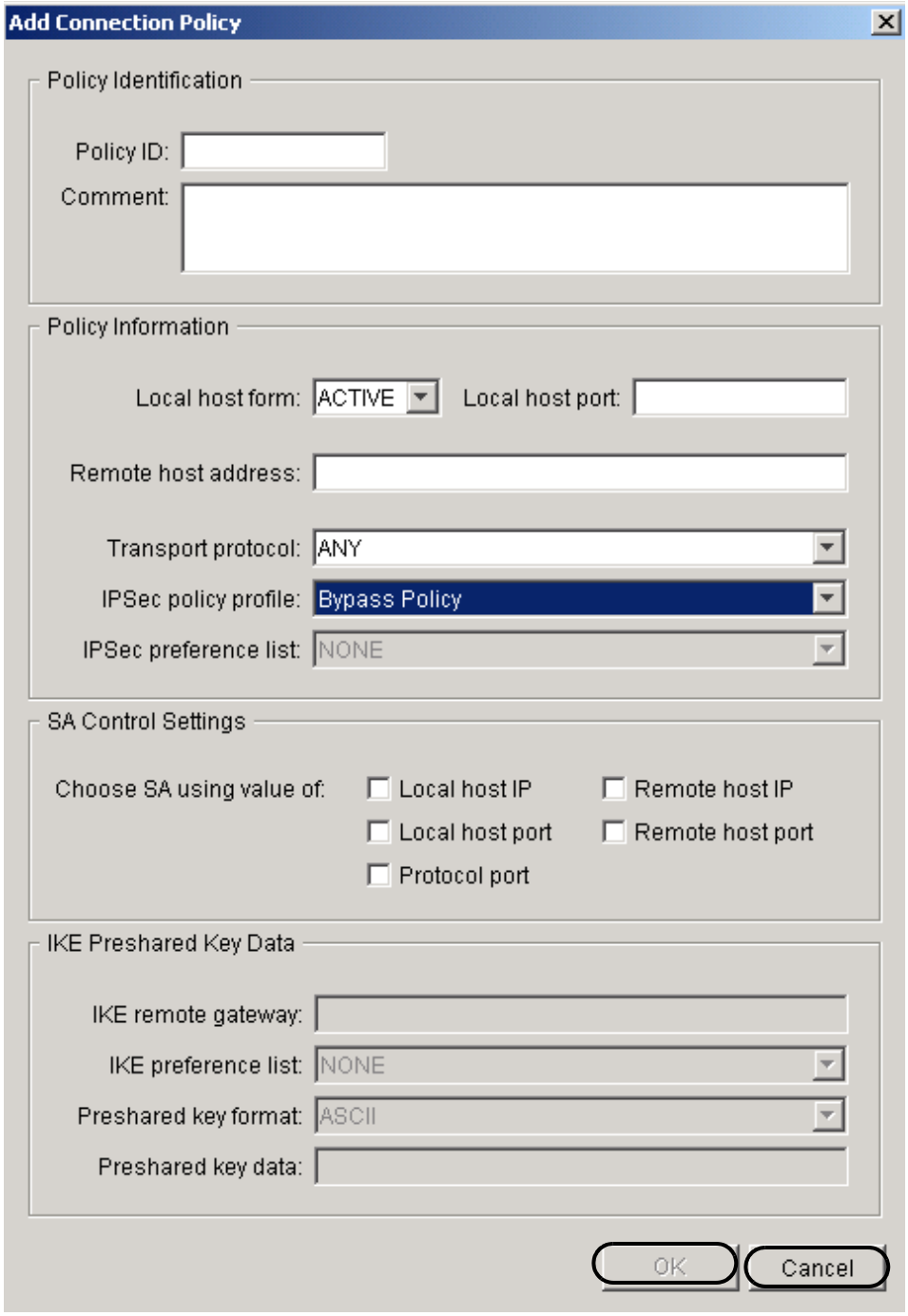


3 Click the **Provisioning** tab, then on the **IPSec** tab, then click the **Connection Policy** tab.



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

Note: 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.



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 (Sheet 1 of 2)

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 means any port.

BYPASS connection policy configuration fields (Sheet 2 of 2)

Field	Values	Description
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) ***Note:*** 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 for every packet received from or sent to the specified IP address, range of addresses, or sub-network, security will not be applied. ***Note:*** 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. ***Note 1:*** The entry of ANY means any protocol. ***Note 2:*** 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. ***Note:*** 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.

7 Observe that the newly defined policy appears in the Connection Policy table.

Note: 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.

IPSec Profile | IPSec Preference | IPSec Preference List | IKE Preference | IKE Preference List | Connection Policy | Kerberos

Policy ID	Comment	Local host...	Local host port	Remote host address	Transport...	IPSec policy profi
100	Bypass for CO-LAN	ACTIVE	0	10.10.0.0/16	ANY	BYPASS
200	Secure Policy for DQOS	ACTIVE	0	11.11.11.11	TCP	IKE SECURE 60s

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

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

9 The procedure is complete.

Configure a DISCARD connection policy

Purpose of this procedure

This procedure provides the steps required to configure a DISCARD connection policy for a selected Gateway Controller (GWC) node. This policy means that all messages sent by the GWC to the specified network device, or received by the GWC from that device, are discarded.

When to use this procedure

Configure a DISCARD-type policy to prevent the GWC from being disturbed by specific devices. It is a good practice to configure a DISCARD-type 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.

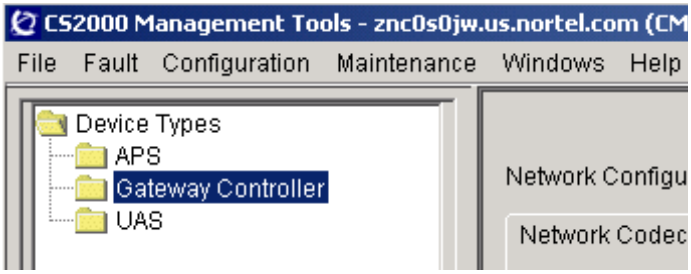
Provision IPSec only if a secure gateway exists in your network.

This procedure requires that the IPSec profile with the DISCARD policy action is configured first. If required, complete procedure Configure IPSec Profile on page 41.

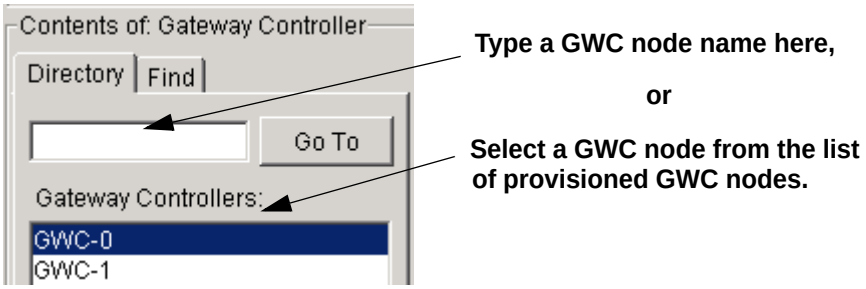
Action

At the CS 2000 GWC Manager client

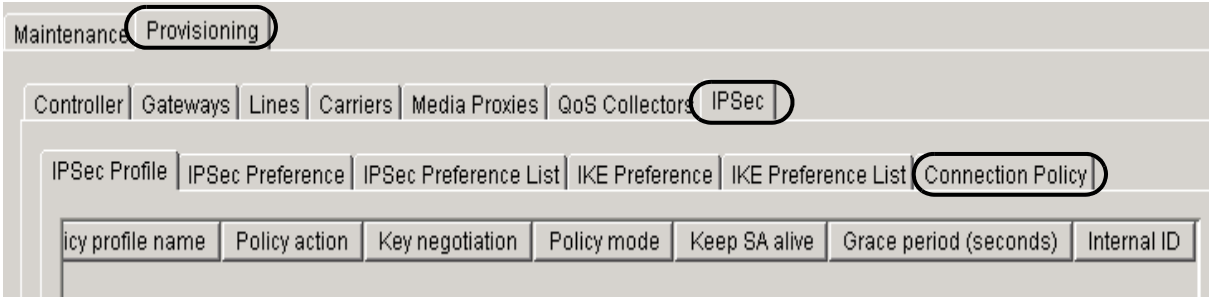
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



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

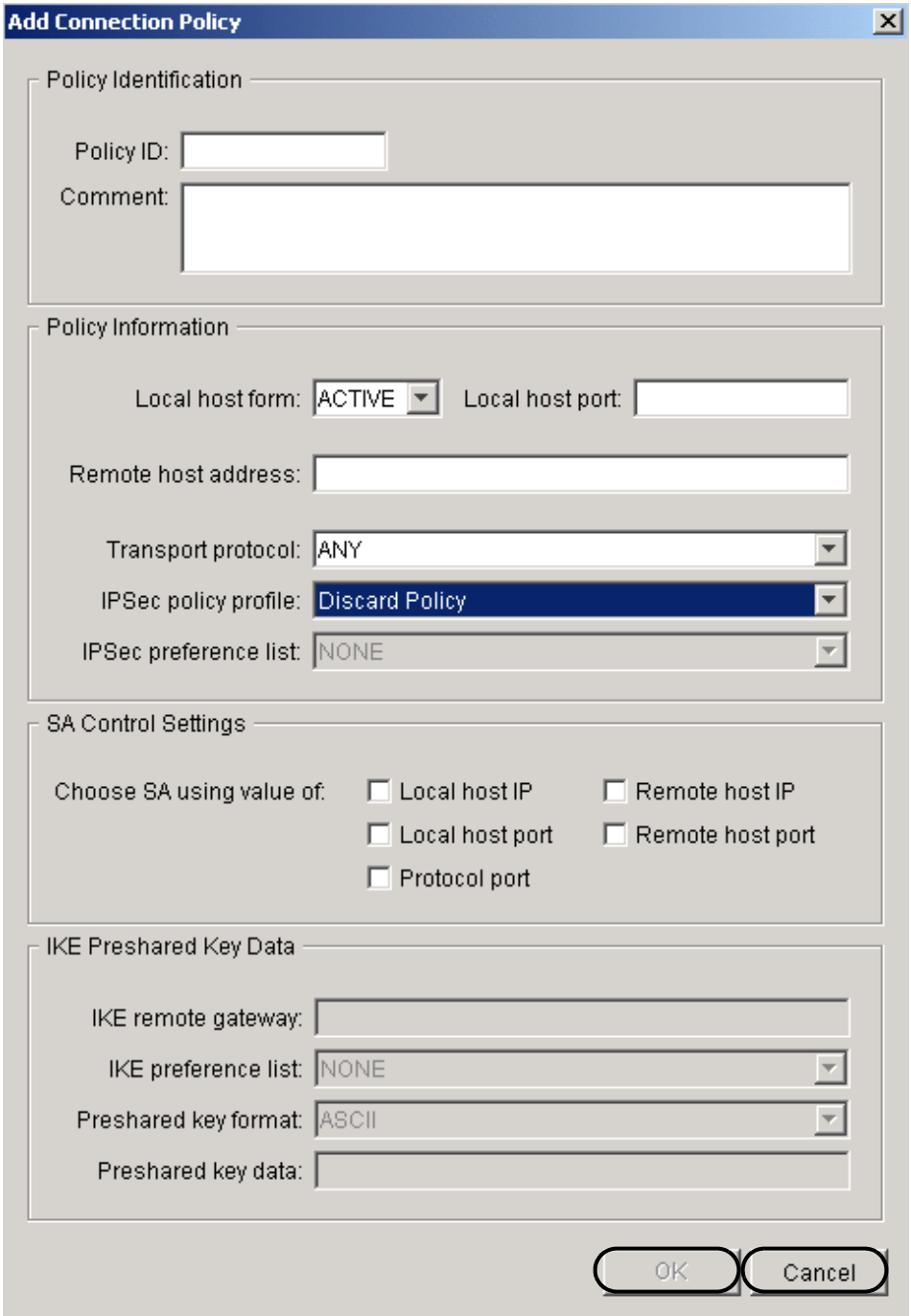


3 Click the **Provisioning** tab, then on the **IPSec** tab, then click the **Connection Policy** tab.



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

Note: 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.



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 (Sheet 1 of 2)

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 means any port.

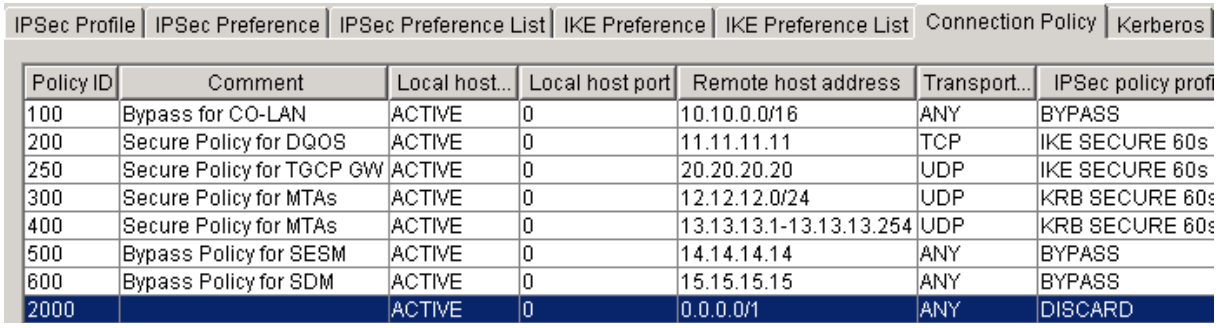
DISCARD connection policy configuration fields (Sheet 2 of 2)

Field	Values	Description
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) ***Note:*** 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.
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.
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. ***Note:*** 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.

Observe that the newly defined policy appears in the Connection Policy table.

Note: 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.



Policy ID	Comment	Local host...	Local host port	Remote host address	Transport...	IPSec policy profi
100	Bypass for CO-LAN	ACTIVE	0	10.10.0.0/16	ANY	BYPASS
200	Secure Policy for DQOS	ACTIVE	0	11.11.11.11	TCP	IKE SECURE 60s
250	Secure Policy for TGCP GW	ACTIVE	0	20.20.20.20	UDP	IKE SECURE 60s
300	Secure Policy for MTAs	ACTIVE	0	12.12.12.0/24	UDP	KRB SECURE 60s
400	Secure Policy for MTAs	ACTIVE	0	13.13.13.1-13.13.13.254	UDP	KRB SECURE 60s
500	Bypass Policy for SESM	ACTIVE	0	14.14.14.14	ANY	BYPASS
600	Bypass Policy for SDM	ACTIVE	0	15.15.15.15	ANY	BYPASS
2000		ACTIVE	0	0.0.0.0/1	ANY	DISCARD

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

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

8 The procedure is complete.

Configure IPSec SECURE or FLEX connection policy with IKE

Purpose of this procedure

This procedure provides the steps required 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.

> ***Note:*** For MTAs, use the Kerberos/PKINIT protocol as the key management system. For more information, refer to procedure Configure IPSec SECURE or FLEX connection policy with Kerberos on page 89.

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, refer to the *ATM/IP Solution-level Security and Administration* NTP, 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. For more information on how to activate or de-active IPSec using FLEX policy, refer to procedure Activate or de-activate IPSec using FLEX policy on page 99.

Once all gateways are configured with IPSec, change the FLEX policy to the appropriate SECURE policy. Refer to procedure Change the policy action for an existing IPSec connection policy on page 121.

ATTENTION

After a connection policy with IKE is provisioned, you will only be able to change the following parameters: pre-shared key format, pre-shared key data, and the 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 (refer to procedure De-activate IPSec using FLEX policy on page 101), then re-activate security with the new configuration values (refer to procedure Activate IPSec using FLEX policy on page 100).

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.

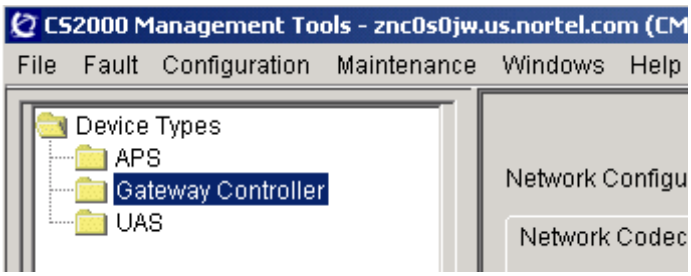
This procedure requires that the following tables are configured first:

- IPSec Profile (if required, complete procedure Configure IPSec Profile on page 41)
- IKE Preference and IKE Preference List (if required, complete procedure Configure IKE Preference and Preference List on page 45)
- IPSec Preference and IPSec Preference List (if required, complete procedure Configure IPSec Preference and Preference List on page 53)

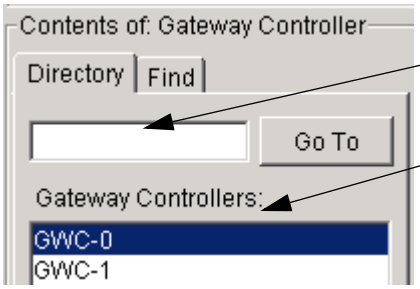
Action

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.

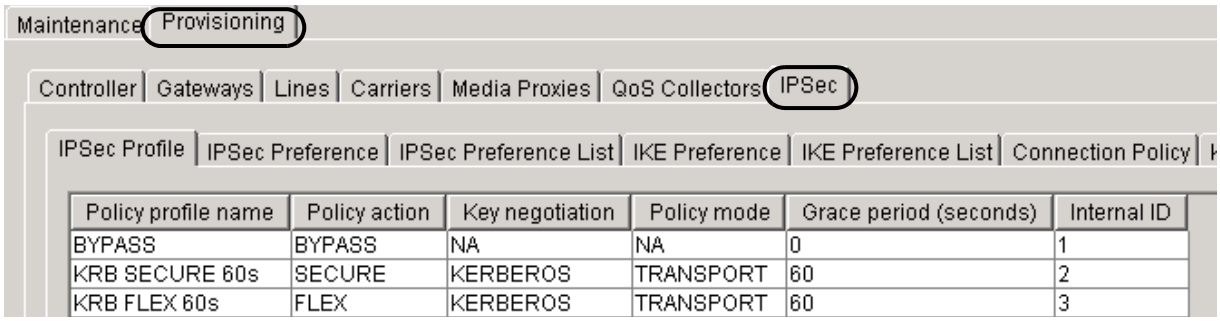


Type a GWC node name here,

or

Select a GWC node from the list of provisioned GWC nodes.

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

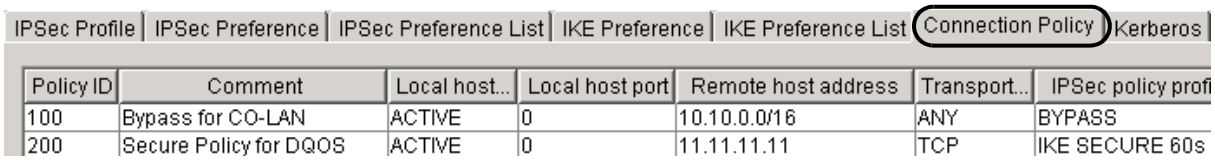


4 The tables displayed under each tab show the currently configured data. You can use the existing data to add a new connection policy. However, if you still need to add data to any of the required tables, use the following table to determine your next step, then continue with step 5.

If you need to configure	Do
IPSec Profile table	Configure IPSec Profile on page 41
IPSec Preference and IPSec Preference List tables	Configure IPSec Preference and Preference List on page 53
IKE Preference and Preference List tables	Configure IKE Preference and Preference List on page 45

5 Click the **Connection Policy** tab.

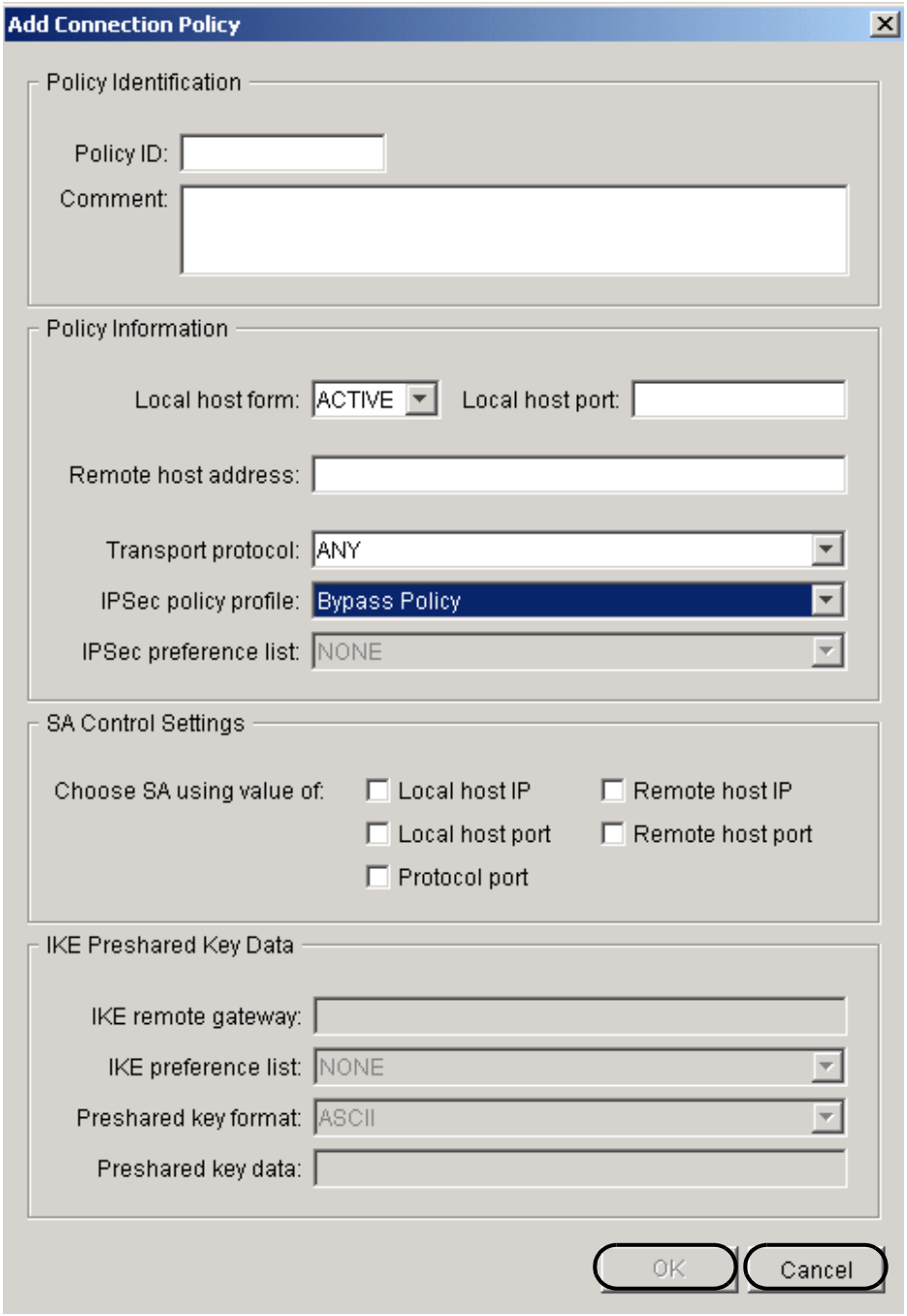
The Connection Policy table is displayed showing all currently configured policies.



Policy ID	Comment	Local host...	Local host port	Remote host address	Transport...	IPSec policy profi
100	Bypass for CO-LAN	ACTIVE	0	10.10.0.0/16	ANY	BYPASS
200	Secure Policy for DQOS	ACTIVE	0	11.11.11.11	TCP	IKE SECURE 60s

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

Note: 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.



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 (Sheet 1 of 4)

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) ***Note:*** 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 means any port. ***Note:*** Refer to the appropriate gateway documentation to obtain this value.

Connection Policy configuration fields (Sheet 2 of 4)

Field	Values	Description
Remote host address:	<gateway IP address>	Enter a unique IP address to identify the remote host (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>). ***Note:*** Some gateways are configured to require the port number to be included in the IP address. Refer to 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. The recommended configuration is: • UDP - for Nortel Media Gateway 3200 and TGCP trunk gateways • TCP - for CMTS (COPS messages) • ANY - for all other gateways • ICMP Refer to 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 that you want to use for this policy. ***Note:*** If no IPSec profile is defined, the following message is displayed in this field: `NO PROFILES DEFINED.`

Connection Policy configuration fields (Sheet 3 of 4)

Field	Values	Description
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. ***Note 1:*** The lifetime of all preferences in the selected list must be greater than the grace period of the previously selected policy profile. ***Note 2:*** 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.
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>	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.

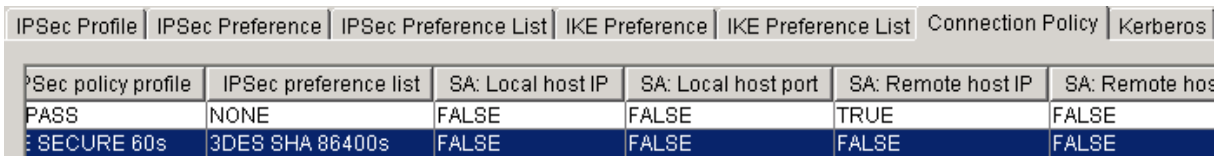
Connection Policy configuration fields (Sheet 4 of 4)

Field	Values	Description
In the IKE Preshared Key Data panel: ***Note:*** You cannot configure two policies defining an IKE pre-shared key for the same IP address. You must configure a separate policy for each gateway.		
IKE remote gateway:	<gateway IP address>	Enter the exact IP address of the remote gateway.
IKE preference list:	<names of the previously defined IKE preference lists>	This field identifies the IKE preference list for this connection policy. By default, the system displays the first preference list name from the IKE Preference List table. Click the drop-down menu and select the name of the IKE preference list that you want to use for this policy.
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 with this IKE policy. 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. ***Note:*** The value entered in this field must match the preshared key configured on a gateway. For more information, contact your network administrator.

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

Observe that the newly defined policy data appears in the Connection Policy table.

Note: 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 with IKE.

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

10 The procedure is complete.

Configure IPSec SECURE or FLEX connection policy with Kerberos

Purpose of this procedure

This procedure provides the steps required to configure 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) 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 on

how to activate or de-active IPSec using FLEX policy, refer to procedure Activate or de-activate IPSec using FLEX policy on page 99.

ATTENTION
Once IPSec is enabled on the remote gateway, change the FLEX policy on the GWC to the appropriate SECURE policy using procedure Change the policy action for an existing IPSec connection policy on page 121. 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.

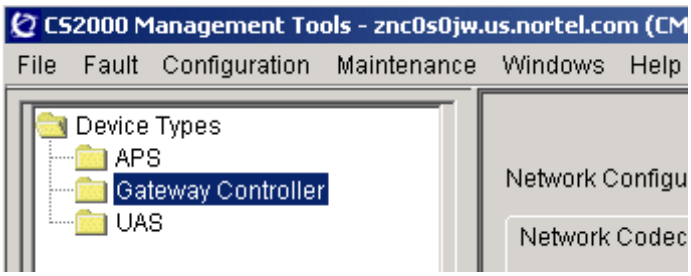
This procedure requires that the following tables are configured first:

- IPSec Profile (if required, complete procedure Configure IPSec Profile on page 41)
- IPSec Preference and IPSec Preference List (if required, complete procedure Configure IPSec Preference and Preference List on page 53)
- Kerberos (if required, complete procedure Configure Kerberos key management on page 59)

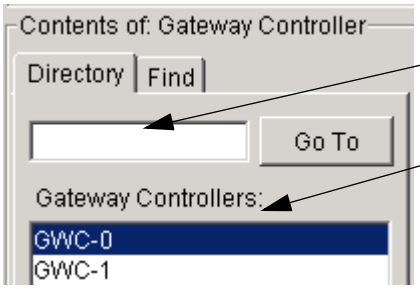
Action

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.

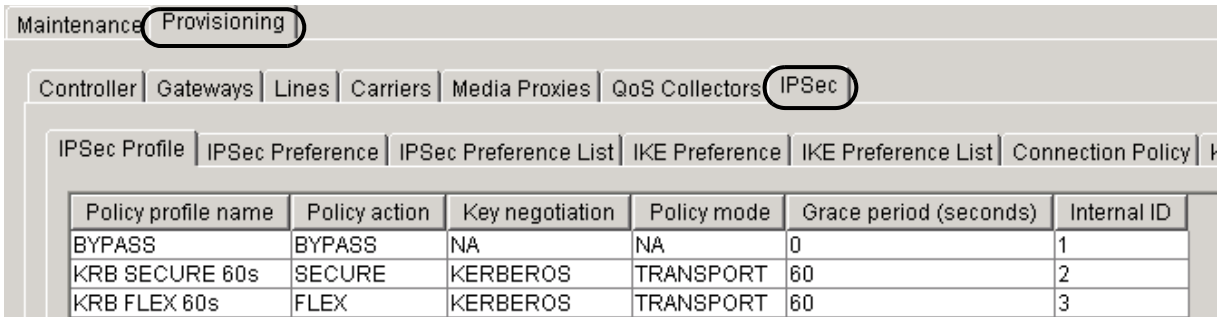


Type a GWC node name here,

or

Select a GWC node from the list of provisioned GWC nodes.

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

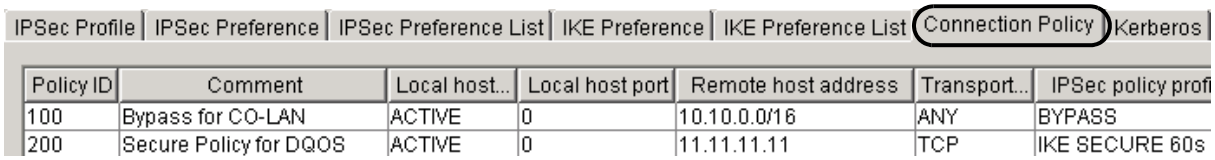


4 The tables displayed under each tab show the currently configured data. You can use the existing data to add a new connection policy. However, if you still need to add data to any of the required tables, use the following table to determine your next step, then continue with step 5.

If you need to configure	Do
IPSec Profile table	Configure IPSec Profile on page 41
IPSec Preference and IPSec Preference List tables	Configure IPSec Preference and Preference List on page 53
Kerberos	Configure Kerberos key management on page 59

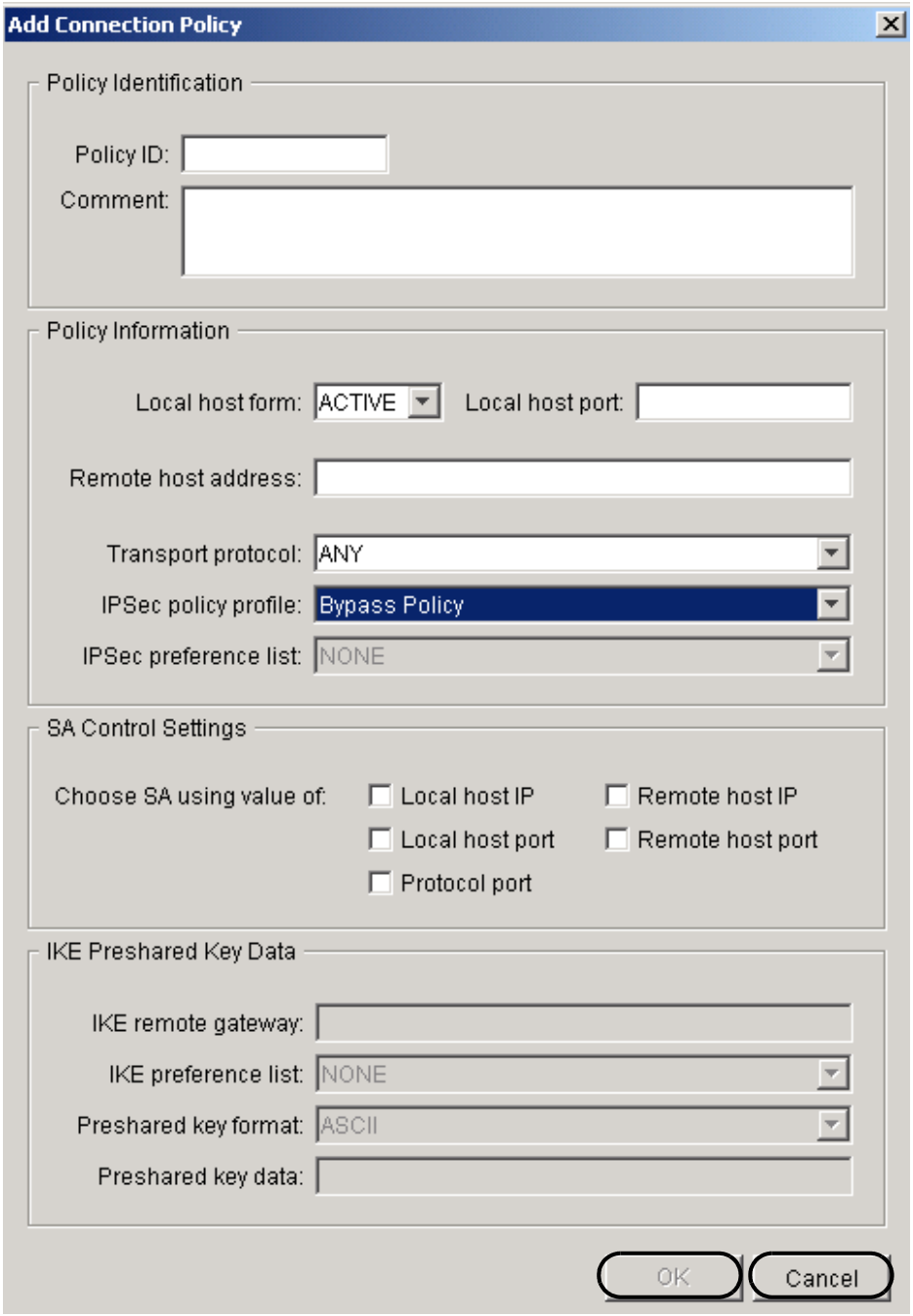
5 Click the **Connection Policy** tab.

The Connection Policy table is displayed showing 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.

Note: 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.



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 (Sheet 1 of 4)

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) ***Note:*** 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 means any port. ***Note:*** Refer to the appropriate gateway documentation to obtain this value.

Connection Policy configuration fields (Sheet 2 of 4)

Field	Values	Description
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>) ***Note:*** Some gateways are configured to require the port number to be included in the IP address. Refer to 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) ***Note:*** 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 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. ***Note:*** 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. Refer to the appropriate gateway documentation to determine the value for this field.

Connection Policy configuration fields (Sheet 3 of 4)

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 that you want to use for this policy. ***Note:*** 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. ***Note 1:*** The lifetime of all preferences in the selected list must be greater than the grace period of the previously selected policy profile. ***Note 2:*** 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.
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.

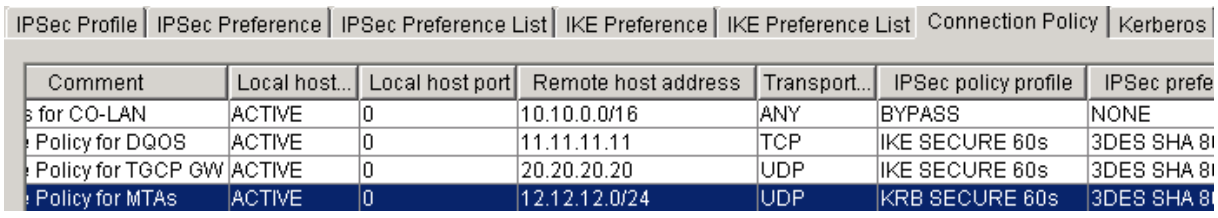
Connection Policy configuration fields (Sheet 4 of 4)

Field	Values	Description
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.
All remaining fields do not apply to a SECURE or FLEX policy with Kerberos key management, and are disabled. Do not attempt to configure them.		

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

Observe that the newly defined policy data appears in the Connection Policy table.

Note: 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.

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

10 The procedure is complete.

Activate or de-activate IPSec using FLEX policy

Purpose of this procedure

This procedure provides the steps required to activate or de-activate IPSec between the Gateway Controller (GWC) and the specified remote gateway - using a FLEX connection policy.

When to use this procedure

Use this procedure when you wish to activate or de-activate IPSec 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 using FLEX policy on page 100
- De-activate IPSec using FLEX policy on page 101

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 using FLEX policy

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

At the CS 2000 GWC Manager client

1 Add a FLEX policy covering the IP address of the remote gateway for which you want to activate IPSec. Follow one of the following procedures:

- Configure IPSec SECURE or FLEX connection policy with Kerberos on page 89 - for multimedia terminal adapter (MTA) line gateways in packet cable solutions

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

- Configure IPSec SECURE or FLEX connection policy with IKE on page 79 - for all other gateways

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 gateway. Refer to the appropriate gateway documentation to complete this step. If required, contact your network administrator for assistance.

Note: 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 Change the policy action for an existing IPSec connection policy on page 121.

Note: If you need to add an appropriate IPSec profile with the Policy action: SECURE, follow procedure Configure IPSec Profile on page 41.

4 The procedure is complete.

De-activate IPSec using FLEX policy

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

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

At the CS 2000 GWC Manager client

1 Change the SECURE policy to a FLEX policy covering the IP address of the remote gateway for which you want to de-activate IPSec. Follow procedure Change the policy action for an existing IPSec connection policy on page 121.

Note: If you need to add an appropriate IPSec profile with the Policy action: FLEX, follow procedure Configure IPSec Profile on page 41.

The GWC and the gateway continue to communicate securely.

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

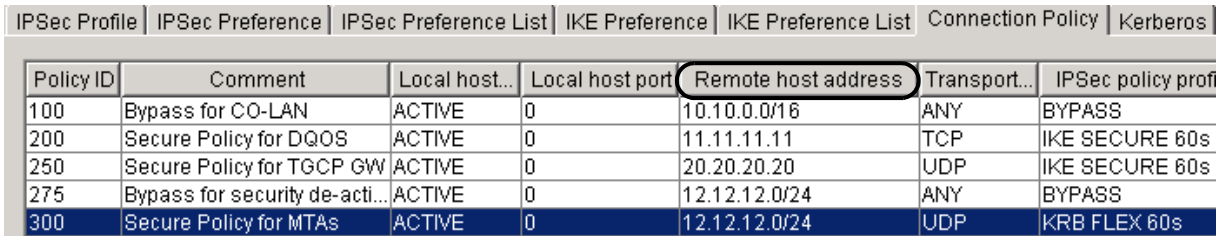
Note: As soon as IPSec is disabled on the gateway, the remote gateway terminates its SA. GWC stops applying IPSec services to all packets sent to and received from the remote gateway. Depending on the characteristics of a gateway, the two nodes either continue to communicate, or the communication stops 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, refer to procedure Configure a BYPASS connection policy on page 67.

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).



Policy ID	Comment	Local host...	Local host port	Remote host address	Transport...	IPSec policy profi
100	Bypass for CO-LAN	ACTIVE	0	10.10.0.0/16	ANY	BYPASS
200	Secure Policy for DQOS	ACTIVE	0	11.11.11.11	TCP	IKE SECURE 60s
250	Secure Policy for TGCP GW	ACTIVE	0	20.20.20.20	UDP	IKE SECURE 60s
275	Bypass for security de-acti...	ACTIVE	0	12.12.12.0/24	ANY	BYPASS
300	Secure Policy for MTAs	ACTIVE	0	12.12.12.0/24	UDP	KRB FLEX 60s

b Click the **Delete** button. A Confirm deletion window appears. Click the **Yes** button to delete the policy.

5 The procedure is complete.

Disable or enable IPSec between two nodes using BYPASS policy

Purpose of this procedure

This procedure provides the steps required to disable or enable the IPSec processing between the 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 the GWC node and the specified gateway, using a BYPASS policy.

You can also use this procedure to re-establish a SECURE policy that has been 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 on page 104
- Enable IPSec by removing a BYPASS policy on page 107

Prerequisites

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

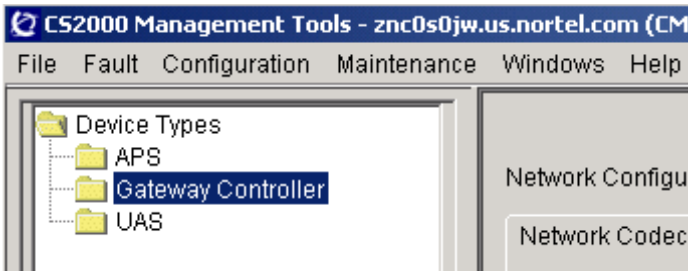
Make sure that an appropriate IPSec profile with Policy action: BYPASS is configured for the selected GWC node. If required, add a new profile (with Policy action: BYPASS) using procedure Configure IPSec Profile on page 41.

Action

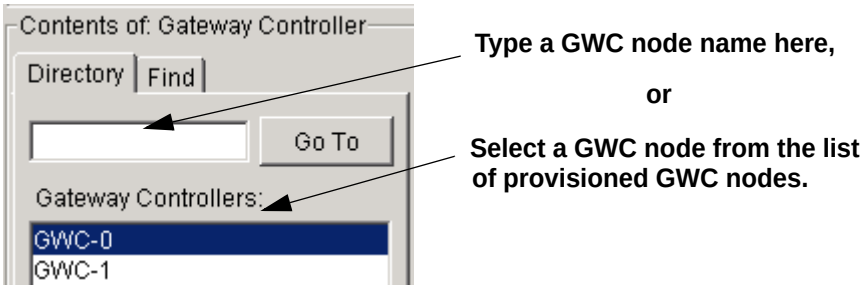
Disable IPSec using BYPASS policy

At the CS 2000 GWC Manager client

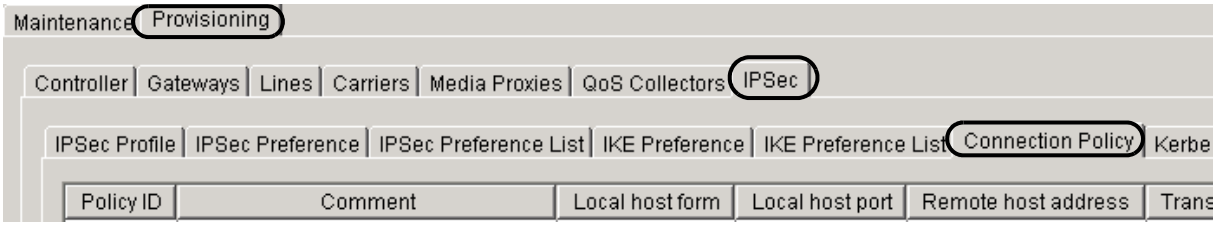
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



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



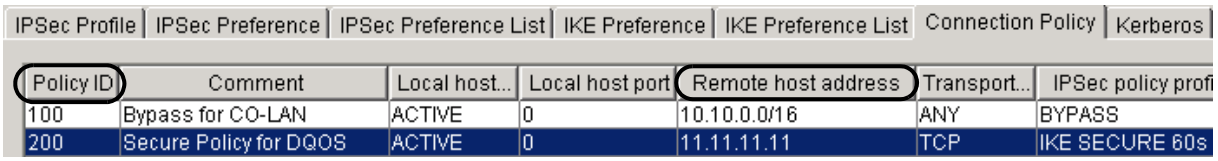
3 Click the **Provisioning** tab, then on the **IPSec** tab, then click the **Connection Policy** tab to display connection policies currently configured for this GWC node.



4 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, refer to procedure Change the policy action for an existing IPSec connection policy on page 121.

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

Note: 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.

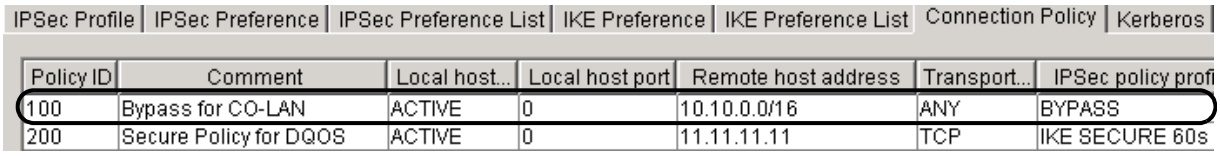
8 Enter (or select from the drop-down menu) provisioning values for each field described in the following table.

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 Observe that 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.

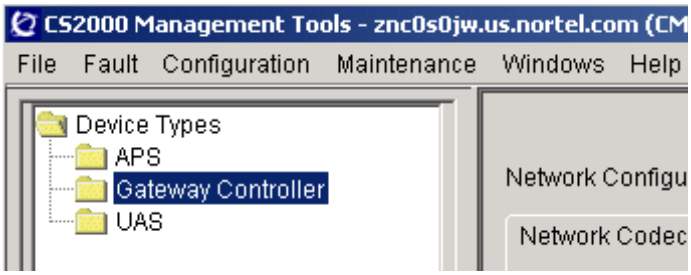


11 The procedure is complete.

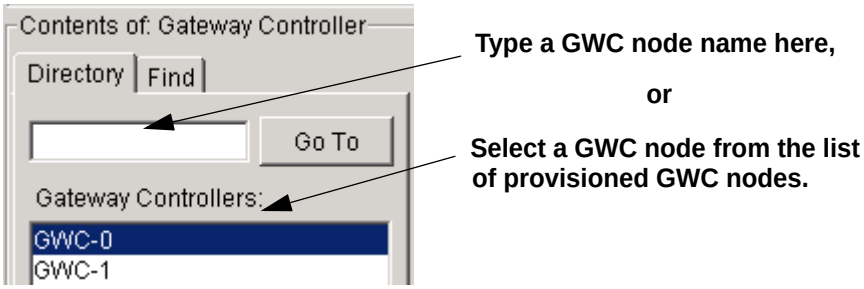
Enable IPSec by removing a BYPASS policy

At the CS 2000 GWC Manager client

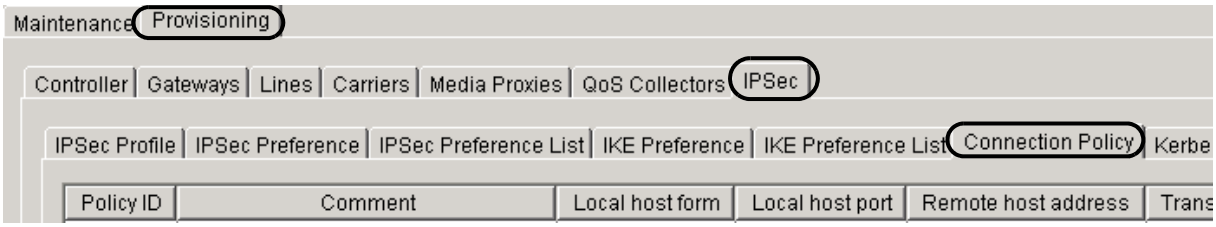
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



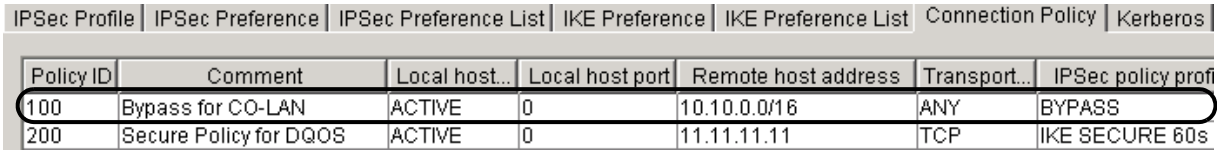
2 From the Contents of: GatewayController frame, select the appropriate GWC node.



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 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. A Confirm deletion window appears. Click the **Yes** button to delete the policy.

6 The procedure is complete.

Modify IKE pre-shared keys

Purpose of this procedure

This procedure provides steps required to change the IKE pre-shared keys for an existing IPSec connection policy with the IKE protocol as the key management mechanism.

When to use this procedure

Use this procedure when you wish to modify the IKE pre-shared keys information for an existing IPSec connection policy.

Prerequisites

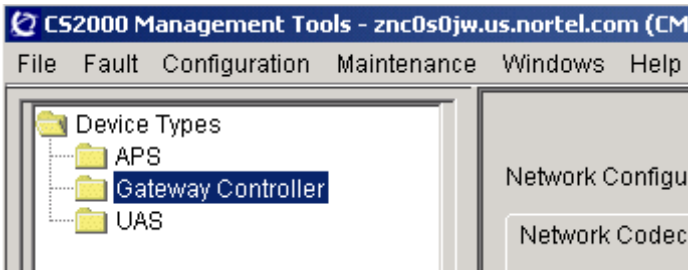
This procedure assumes that a SECURE connection policy (with IKE key management) exists between the GWC and another network device.

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.

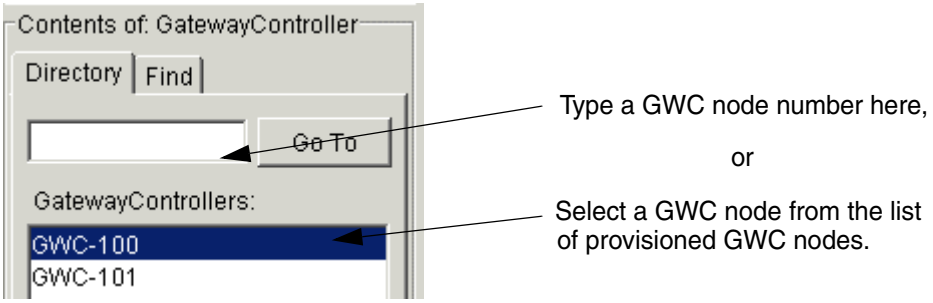
Action

At the CS 2000 GWC Manager client

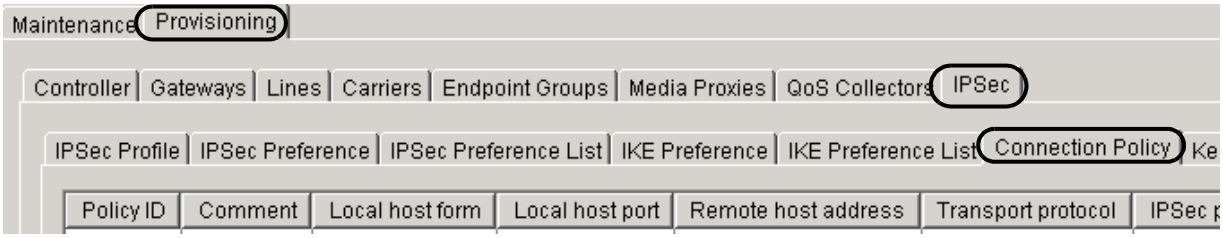
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



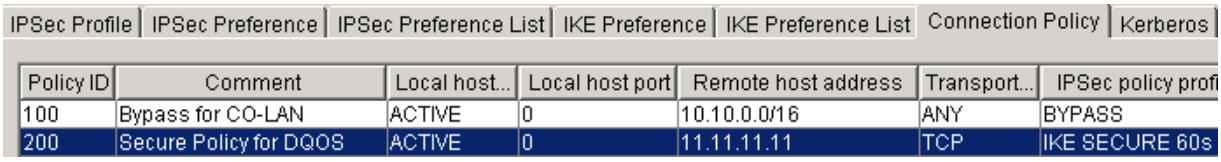
2 From the Contents of: GatewayController frame, select the appropriate GWC node.



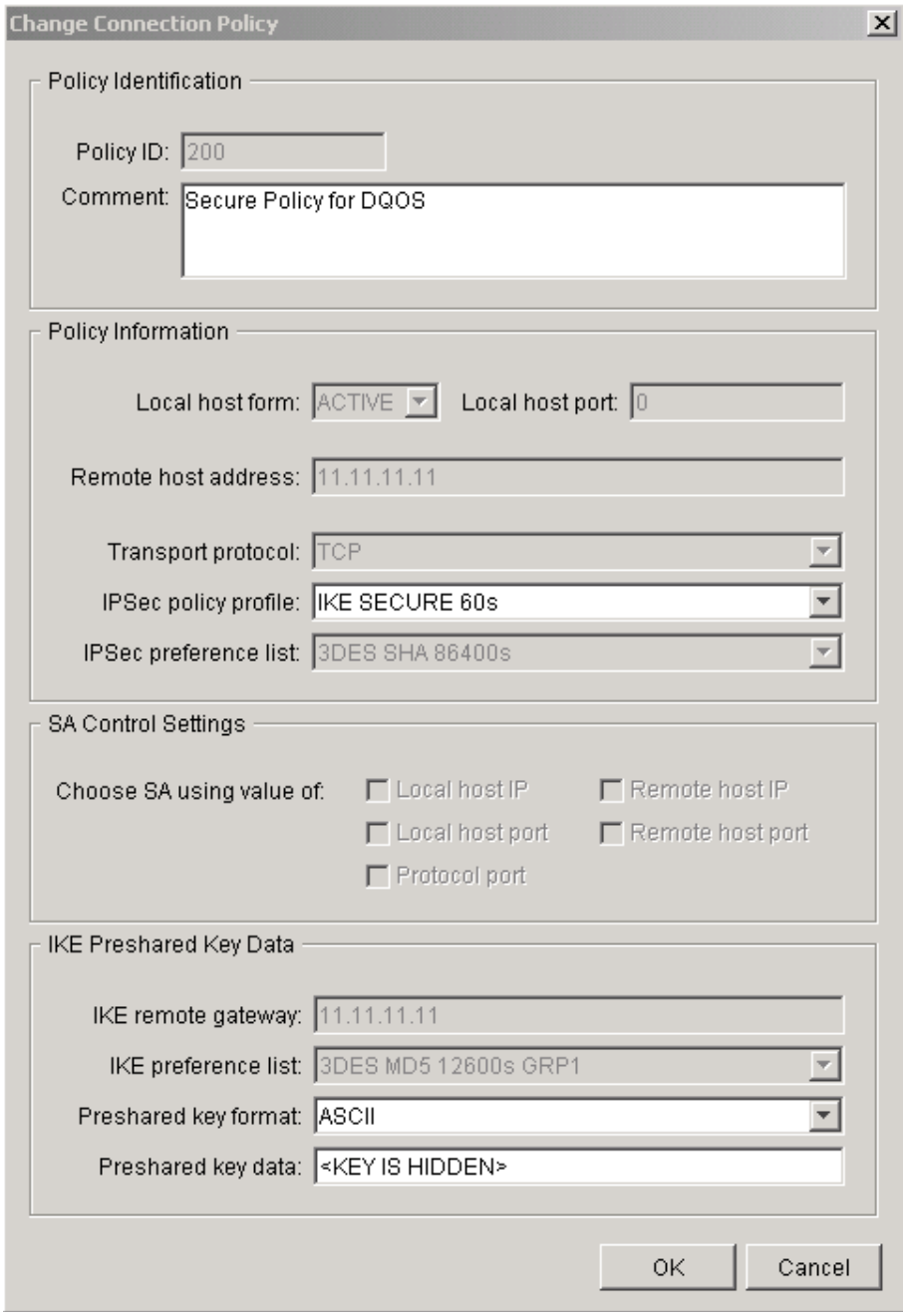
3 Click the **Provisioning** tab, then on the **IPSec** tab, then click the **Connection Policy** tab to display connection policies currently configured for the selected GWC node.



4 Click the SECURE IKE policy that you want to modify to highlight it.



5 Click the **Change** button to display the Change Connection Policy 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) that will be used with this IKE policy. 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.

Note: 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.

9 The procedure is complete.

Modify Kerberos service key

Purpose of this procedure

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

- SMALL_LINENA
- SMALL_LINEINTL

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.

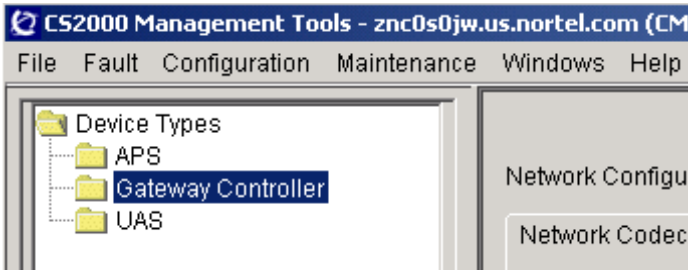
Prerequisites

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.

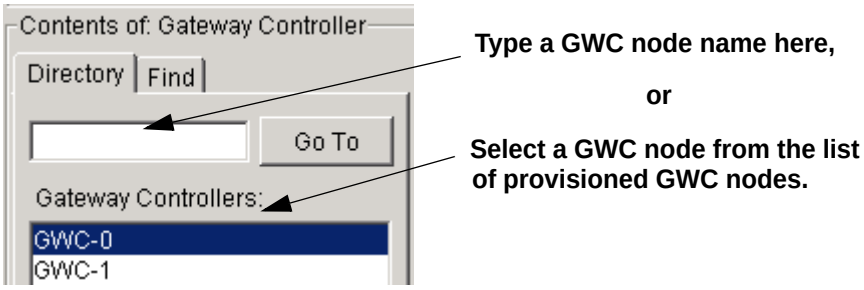
Action

At the CS 2000 GWC Manager client

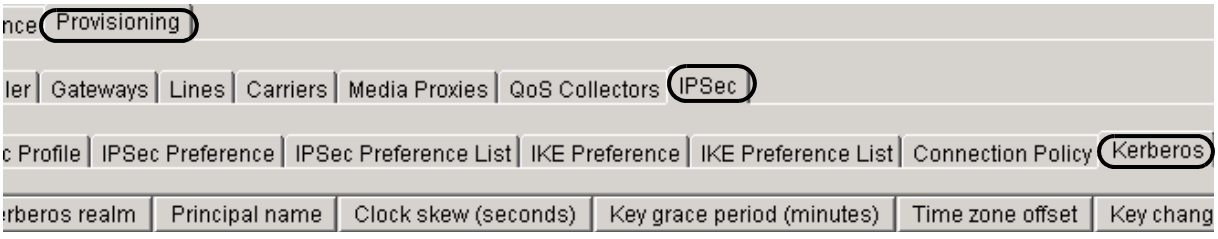
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



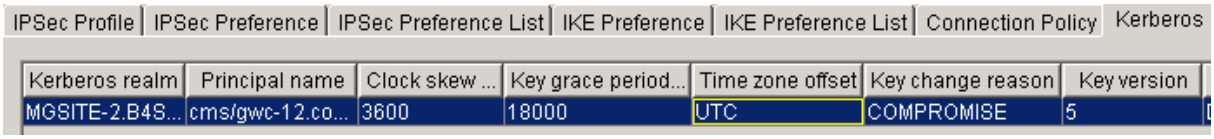
2 From the Contents of: GatewayController frame, select the appropriate GWC node.



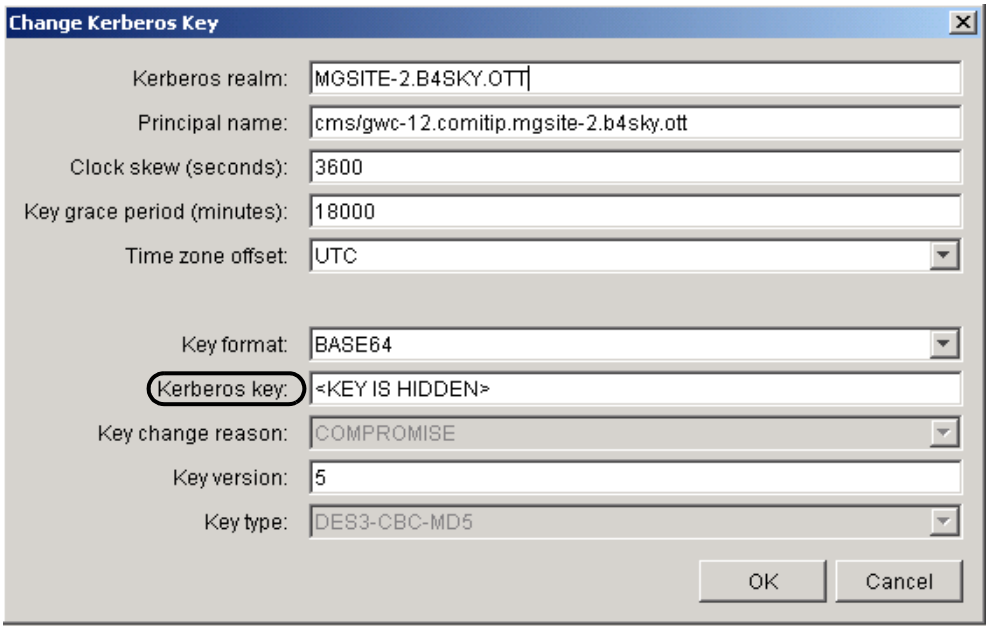
3 Click the **Provisioning** tab, then on the **IPSec** tab, then click the **Kerberos** tab to display the existing single entry in this table.



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.

Note 1: The key is generated at KDC, then the extracted key must be provisioned (by copying and pasting) at the GWC.

Note 2: Make sure that you enter the valid number of characters. Otherwise, the system displays the following error message:

The expected key size is:

- for BASE64 key format: 32 BASE64 digits

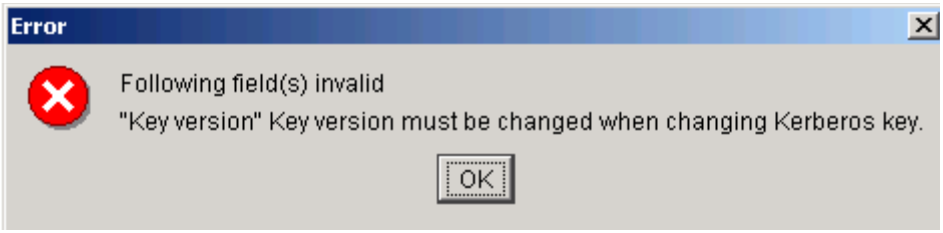
  Note: The acceptable range of characters is: <a-z, A-Z, 0-9, /+>.

- 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 the following 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.

Disable Kerberos key management

Purpose of this procedure

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

- SMALL_LINENA
- SMALL_LINEINTL

When to use this procedure

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

Note: 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.

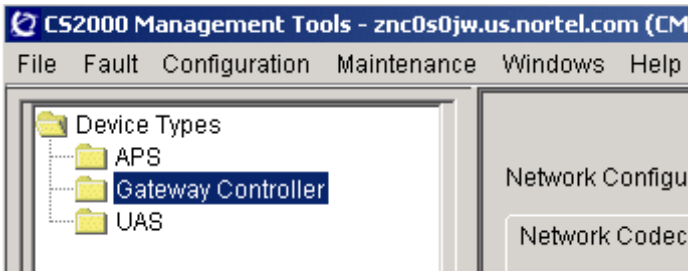
Prerequisites

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.

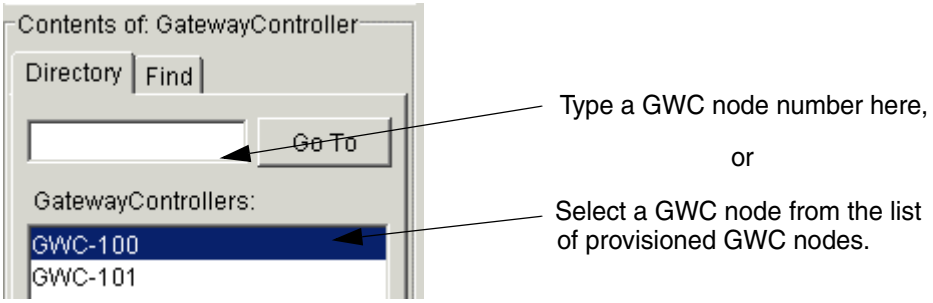
Action

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.



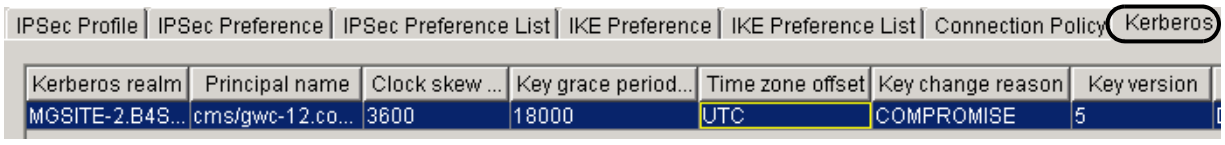
2 From the Contents of: GatewayController frame, select the appropriate GWC node.



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.

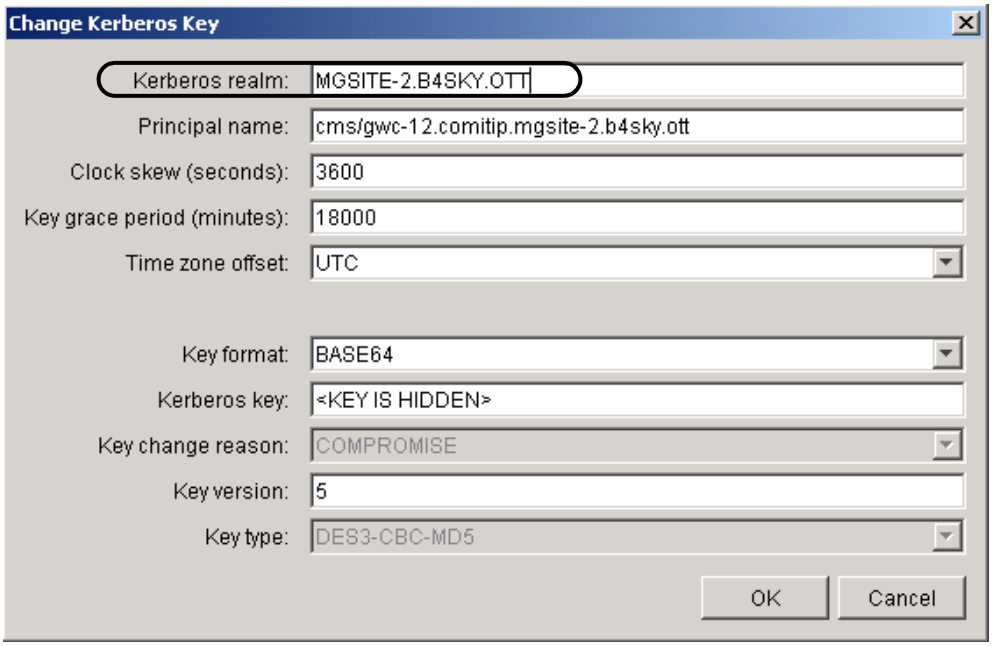
4 Identify all FLEX and SECURE connection policies with the Kerberos key management. Add a BYPASS policy in front (with a lower Policy ID number) of each of these policies. Refer to procedure Disable or enable IPSec between two nodes using BYPASS policy on page 103.

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



6 Click this entry to highlight it.

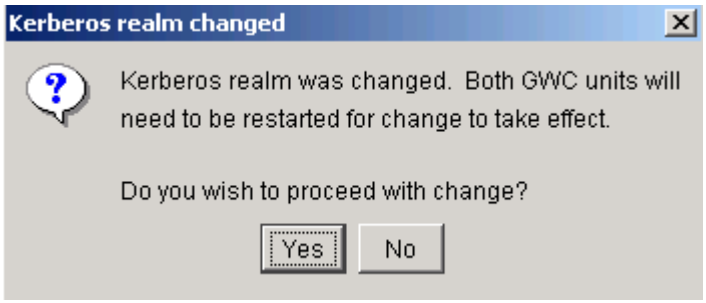
7 Click the **Change** button to display the Change Kerberos Key dialog box.



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

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

The system displays the following message:



10 Click the **Yes** button to confirm.

11 Restart the GWC node using the following steps:

a Busy the inactive unit. Follow procedure Disable (Busy) GWC card services on page 37 in this NTP.

b Return the inactive unit to service. Follow procedure Enable (RTS) GWC card services on page 39 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) on page 29 in this NTP.

Note: 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.

Note: Observe that the entry in the Kerberos table cannot be deleted. It remains displayed, even though the Kerberos functionality has been disabled.

Change the policy action for an existing IPSec connection policy

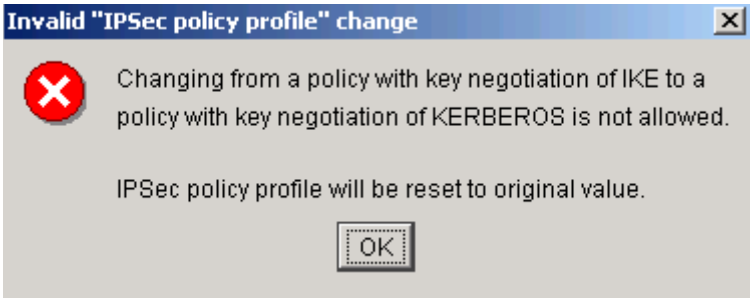
Purpose of this procedure

This procedure describes how you can change the type of action that an existing connection policy applies to incoming and outgoing packets, without configuring a new policy. 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

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

Note: 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, for example:



When to use this procedure

Use this procedure when you want to change the type of action that an existing connection policy applies to messages exchanged between the Gateway Controller (GWC) and a gateway, but you do not want to configure a new policy.

Note: Refer to the table above for the list of allowed changes.

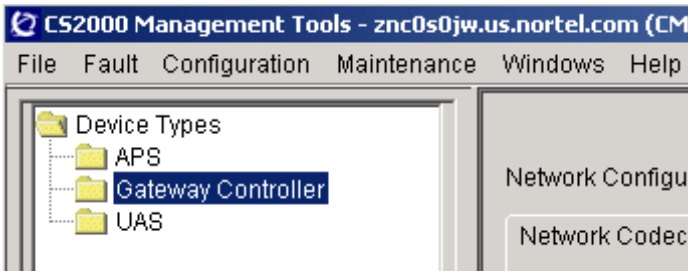
Prerequisites

This procedure requires that the IPSec profile with the appropriate policy action (which you want to use for the selected policy) is configured first. If required, complete procedure Configure IPSec Profile on page 41

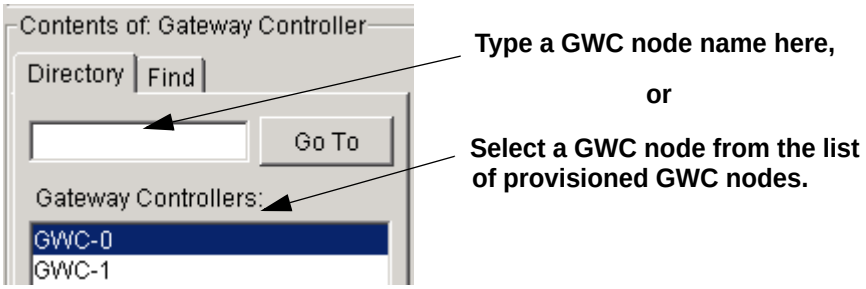
Action

At the CS 2000 GWC Manager client

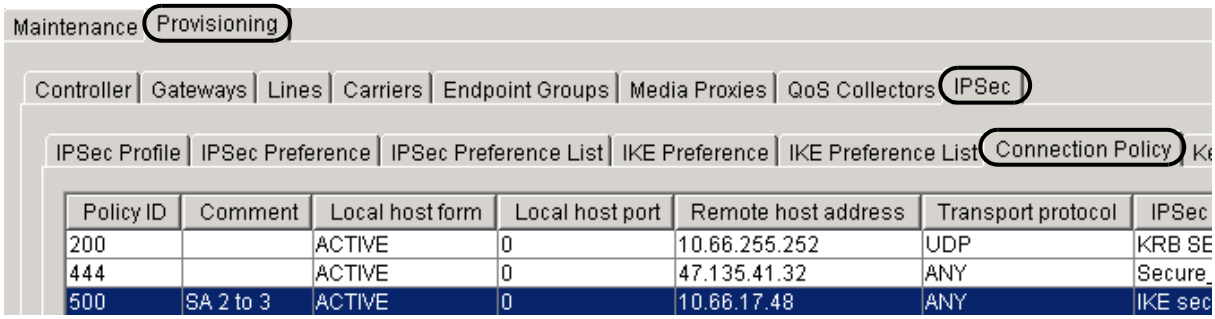
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



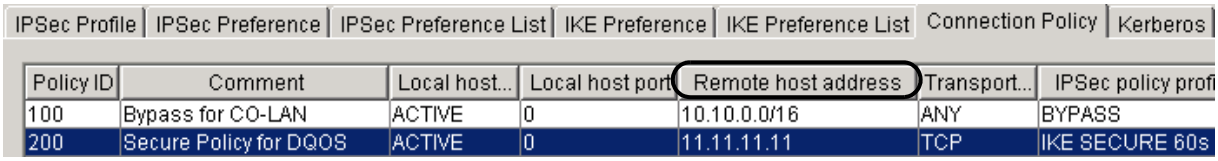
2 From the Contents of: GatewayController frame, select the appropriate GWC node.



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.

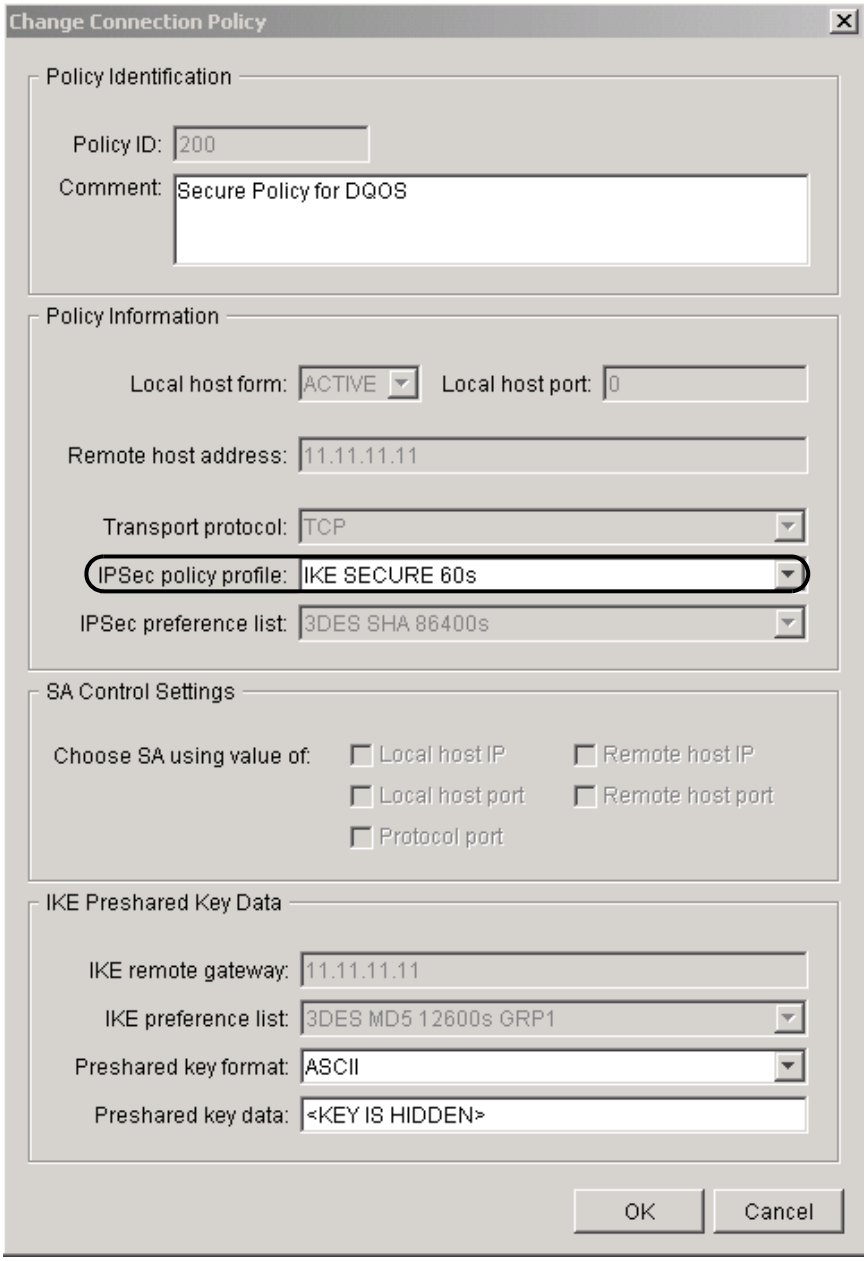


4 In the Remote host address (gateway IP address) column, identify the policy that you want to modify. Click that entry to highlight the policy.



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 the **OK** button). To do that, click the **Cancel** button.



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

Note: Only certain changes are acceptable. Refer to the table at the beginning of this procedure for the list of allowed changes.

7 Use the following table to determine you next step.

If your change is	Do
from BYPASS to FLEX or SECURE (with IKE key negotiation)	step 8
anything else	step 9

8 Configure the IKE Preshared Key Data parameters as described in the following table.

IKE Preshared Key Data parameters (Sheet 1 of 2)

Field	Values	Description
In the IKE Preshared Key Data panel: ***Note:*** You cannot configure two policies defining an IKE pre-shared key for the same IP address. You must configure a separate policy for each gateway.		
IKE remote gateway:	<gateway IP address>	Enter the exact IP address of the remote gateway.
IKE preference list:	<names of the previously defined IKE preference lists>	This field identifies the IKE preference list for this connection policy. By default, the system displays the first preference list name from the IKE Preference List table. Click the drop-down menu and select the name of the IKE preference list that you want to use for this policy.

IKE Preshared Key Data parameters (Sheet 2 of 2)

Field	Values	Description
Preshared key format:	ASCII or HEX	Select ASCII or HEX to indicate the format of the preshared key.
Preshared key data:	<user-defined key; 1 to 48 characters>	Enter the 1- to 48-character long preshared key that will be used with this IKE policy. 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. ***Note:*** The value entered in this field must match the preshared key configured on a gateway. For more information, contact your network administrator.

9 Click the **OK** button.

10 The procedure is complete.

Delete an IPSec connection policy

Purpose of this procedure

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

When to use this procedure

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

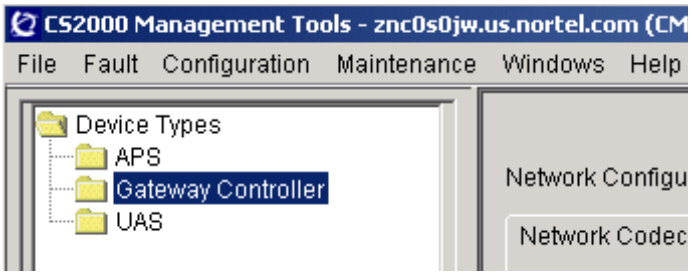
Prerequisites

An IPSec connection policy must be configured on a GWC.

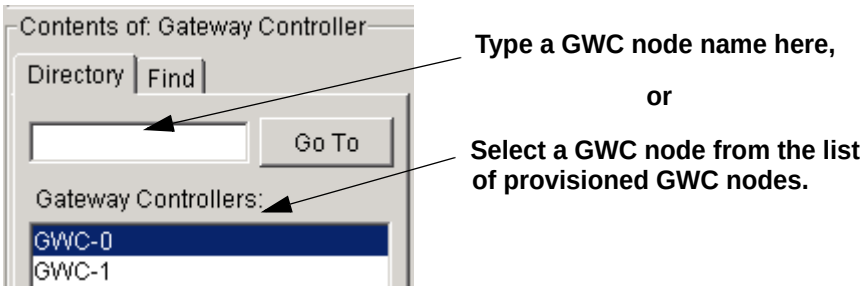
Action

At the CS 2000 GWC Manager client

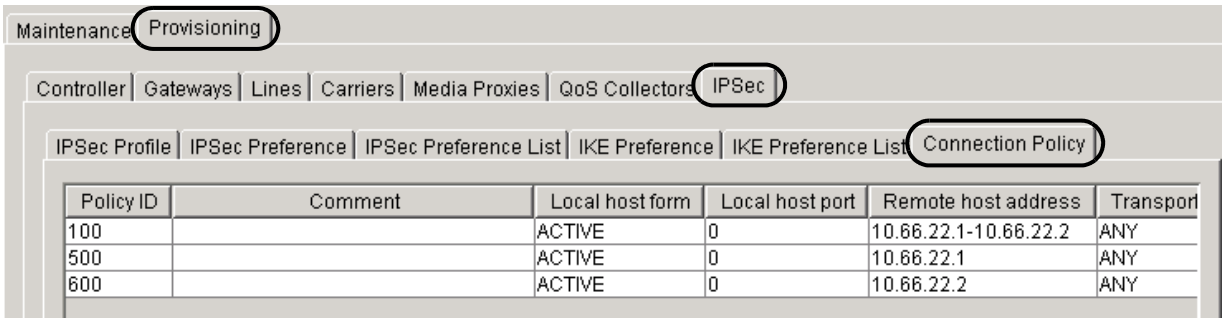
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types menu.



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



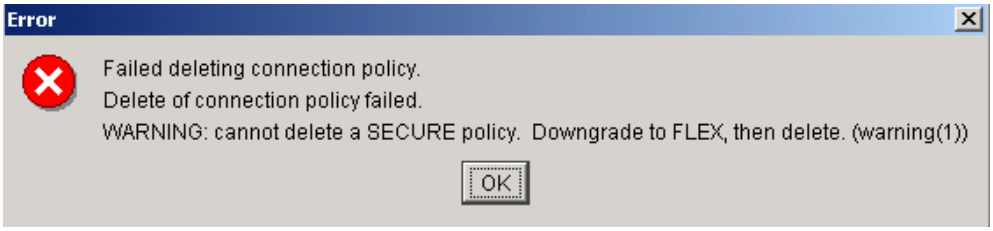
3 Click the **Provisioning** tab, then on the **IPSec** tab, then click the **Connection Policy** tab to display connection policies currently configured for the selected GWC node.



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 Change the policy action for an existing IPSec connection policy on page 121.

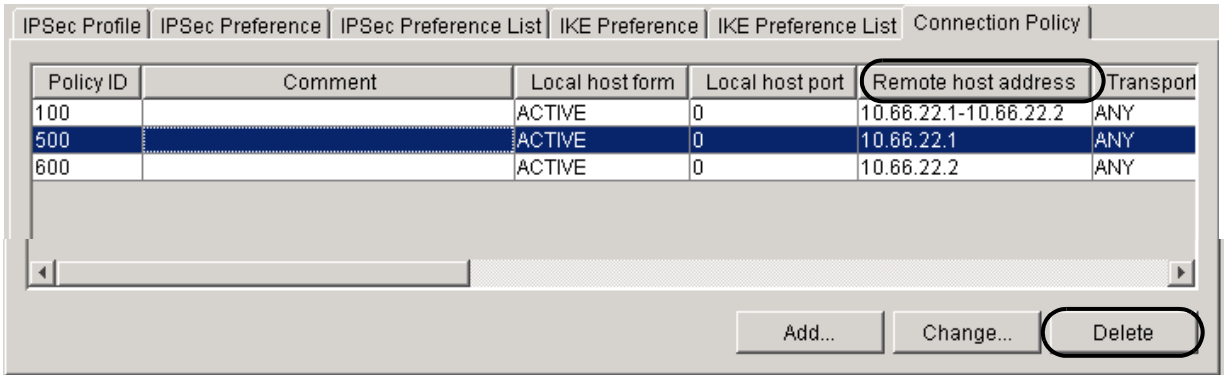
b Continue with step step 5.

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.

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 A Confirm deletion window appears. Click the **Yes** button to delete the selected policy.

9 The procedure is complete.