Security and Administration

Overview

This section describes the security and administration for the Centrex IP Client Manager (CICM) component, it describes tools and utilities and provides administration and security procedures.

Administration

Centrex IP Client Manager administration consists of CS2K administration and CICM administration.

Administration for the Centrex IP Client Manager can be done from either the Element Manager hosted web pages or from the Administration PC that allows access to the CICM. The Centrex IP Client Manager does not come equipped with a display or keyboard.

CS2K administration

CS2K administration is undertaken upon installation, with the datafill of hardware data tables to specify connections. Once datafilled, there should be no reason to alter the datafill. Refer to the *Configuration Management* section of this document, and the CS2K documentation.

Centrex IP Client Manager administration

An Administration PC is attached to the service provider's Administration LAN. An Administration PC accesses the CICM Element Manager (EM) via a web interface.

The functions of the Centrex IP Client Manager administration interface are to:

- Display the status of the CentrexIP service
- Start or stop the CentrexIP service
- Configure the CICM and clients
- Collect event logs from the CICM
- Backup and restore the CICM configuration

Device administration

A CentrexIP line can be made busy (BSY), installation busy (INB) or returned to service (RTS) in the same manner as a conventional line. Refer to the CS2K documentation suite for complete procedures.

For information regarding configuration and administration of the IP Phones 200x and m6350 SoftClient, refer to the *Centrex IP Client Manager Series 2.5 IP Phone 200x User Guide* and the *Centrex IP Client Manager m6350 SoftClient User Guide*.

Terminal Handover

The Terminal Handover feature provides a mechanism for terminals on one CICM node to be transferred to the mate node with little or no service interruption. Refer to the *Perform Terminal Handover* procedure in this document.

Terminal Handover overview

When software or hardware maintenance or upgrades are being performed on a CICM node, the node is taken out of service. Terminals on the node to be shut down may be moved to the mate node prior to node shutdown. The mate node is still available to provide service during the node outage (although at a reduced capacity).

The Terminal Handover feature allows the CICM node to shut down in a controlled manner, as follows:

- The administrator selects a shutdown timeout interval (between 5 and 60 minutes, in 5 minute intervals) and initiates the terminal handover.
- Terminals attempting to register new sessions with the CICM node will be automatically redirected to the mate node.
- Terminals with no active user login session are transferred to the mate node immediately when the terminal handover is initiated.
- For terminals with an active user login session:
  - users are presented with a dialog screen informing them that maintenance is being performed, and requesting permission to perform a terminal reboot.
  - Users have the choice to defer the terminal reboot. If they defer the terminal reboot, after several minutes they will again be

presented with a dialog screen requesting permission to perform a terminal reboot.

— Users that repetitively defer the terminal reboot until the end of the shutdown timeout interval will be forced out. The active call is dropped and transferred to the mate node.

— When a terminal is transferred, the terminal loses service for a few seconds.

— The user login session is automatically restored when connectivity is restored on the mate node.

- If all terminals have been moved to the mate node before the timeout occurs, the shutdown will complete at that time instead of waiting for the timeout expiration.

Terminal Handover -- client terminals
This feature applies to both IP Phone 200x and m6350 clients. The handover process is basically the same for both IP Phones 200x and m6350 types of terminals. The differences are primarily in the user interface.

For detailed information on the user interface for IP Phones 200x terminals, refer to the *NN10027-113 CICM Series 2.5 Etherset Installation Guide*. For information on the user interface for the m6350 SoftClient, refer to the *User Manual NN10182-113 CICM Series 2.5 m6350 Client Installation Guide*.

Limitations and restrictions of Terminal Handover
This section provides the limitations and restrictions of the Terminal Handover feature.

Cross-hosted call processing Cross-hosted calls that have terminals with active user sessions on the mate node and are using call processing resources on the node that is shut down, will lose active calls without notice when the node hosting the call processing resources is taken out of service.

Network addressing To move the terminal from one node to the other, the Unistim SwitchServer command is used.

When a terminal connects to the CICM, the CICM queries the terminal's server configuration (which is configured manually on the terminal or via DHCP). The CICM identifies which of the server entries corresponds to its own host address (the client LAN address on the CICM node).

The CICM then identifies which is the failover server. If the failover server is not configured correctly to be the mate node, the terminal transfer will fail. The terminal will eventually reconnect to the node being taken out of service when that node is brought back into service. The CICM does not reprogram the terminal's server configuration.

Example
Failover terminal: If a terminal connected to node B has node A configured for server S0, and node B configured for server S1, then node A is the failover server.

Note: If a static NAT bind is being used to publish private CICM client LAN addresses on a public network, the CICM will be unable to match its own address to either of the addresses configured on the terminal. This will cause unpredictable results when using the Terminal Handover feature.

Terminal server configuration Terminals with S1 and S2 configured as the same server (e.g. both configured with the address of node A) are not candidates for handover to the mate node. In this case, when a terminal handover is being performed, a log is generated for these terminals and the terminal is left connected to the node until the node shuts down completely, at which point it loses service.

Security

The security model for the Centrex IP Client Manager mandates two separate networks: the Administration network (Admin LAN) and the Client network.

Admin and Client LAN security

The Admin LAN is a secure environment owned and managed by the Telco. It is used for carrying operation and administration data and does not carry call control data or media streams. No voice services are available from the Admin LAN.

The Client network also belongs to the Telco customer. The Client LAN is a non-secure network not under the control and management of the Telco. It carries call control and bearer traffic.

For security purposes, the Admin LAN and Client LAN are physically isolated from each other within each CICM cabinet. Routing directly between the Admin and Client LAN is disabled in the CICM. Only the basic services needed for call control are available from the Client LAN connections to the CICM.

Because of the separation between Admin LAN and Client LAN, an administrator would have to do the following to test whether a client PC or IP Phones200x is visible on the client LAN:

- Use **Telnet** to log into the CICM on which the user is registered, or
- Use **ping** or **tracert** command from the Telnet command line to try the reach of the IP address of the client.

Note: **Ping** and **Tracert** commands may not be used for deployment where the CICM and its clients are separated by firewalls and NATs because **Ping** and **Tracert** messages are not able to traverse firewall/NAT.

Access privileges and restrictions

The following access privileges are protected by user names and/or passwords:

- Access to the CICM and Element Manager via the Admin LAN.
- Access to the administration web pages on the Element Manager.
- Login to terminals on the Client LAN.

To access the Element Manager web pages, a user must be a member of the CentrexIP administrators group, which is configured as part of the installation process. As a member of the administrators group, the administrator password can be used for access to the Administration PC, the Element Manager web pages, and for Telnet access.

Refer to the *User Administration Procedures* section of this document for detailed instruction on setting up user and administrator groups and setting privileges.

Element Manager security

Access to the Element Manager is controlled by the Internet Information Server (IIS). For security purposes, authentication is required to obtain access to the EM (by IIS default configuration).

The following options may also be configured for extra security:

- Secure Sockets Layer (SSL) encryption may be configured to provide privacy of sensitive information
- Certificates may be configured for additional authentication
- Auditing may be configured to monitor security activities to prevent unauthorized access

IIS filter access

Internet Information Services (IIS) can filter access to web services based on selected IP addresses or domain names. Having only a small set of client addresses in the filter minimizes the chance of infraction.

Read-only shared resources

The Element Manager is initially configured with three shared directories, one for firmware, one for backup, and one for patching. All of these should be read-only. If directories are created for other purposes, ensure these are made writable for the minimum required period of time.

Authenticated web access

The web server can be configured to only permit access to authenticated NT users within the CICM domain or other domains where trust relationships have been established.

Secure web access

The web server supports secure web access using Secure Sockets Layer (SSL) when provided with a signed Certificate. This requires the administrator to obtain a Certificate from a provider. IIS supports client certificates that are manually distributed to trusted clients and entered into the browser. SSL can be configured using the Internet Service Manager.

Firewall and NAT traversal

Firewalls and Network Address Translation (NAT) devices are widely used by enterprises to maintain their network security and integrity.

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in hardware or software, or a combination of both. All messages entering or leaving the private network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

A NAT needs to be deployed to translate from a private IP address to a public IP address and vice versa (if an enterprise uses private IP addresses internally and public IP addresses externally). A NAT is a software capability residing on a firewall. A NAT essentially hides an enterprise internal private IP address domain and makes it non-reachable from external points of origin, hence providing an additional layer of security.

In a typical deployment where the carrier provides IP Centrex as a carrier-hosted Centrex solution to its various enterprise customers, the

CICM is normally located in the carrier Central Office LAN (CO-LAN), in the carrier's managed IP network and the carrier's IP address space. The IP phones reside on the enterprise LAN in the enterprise private IP address space behind the enterprise firewall and NAT. The IP phones communicate with the CICM over the carrier's managed IP network. The firewalling and NAT functions may be provided via software residing on an enterprise edge router, or a separate device linked to the edge router.

To enable CS2Kto provide Centrex IP as the Succession-hosted Centrex solution to its various enterprise customers, it is critical that the CS2K Centrex IP services are able to traverse enterprise firewalls and NAT devices.

Nortel Networks has developed a comprehensive firewall and NAT traversal solution for CS2K-based Centrex IP Solution utilizing the CICM Series 6.12 and above.

NAT traversal
Nortel Networks' Centrex IP supports all types of NATs regardless if it is a full cone NAT, restricted cone NAT, port-restricted NAT or symmetric NAT. There is no change needed on existing NAT functions or NAT devices of enterprises.

UNIStim signaling NAT traversal Centrex IP UNIStim signaling messages can traverse any type of NAT as UNIStim messages are always initiated by Centrex IP clients from the private side of the enterprise NAT. That initial UNIStim message creates a binding on the NAT to allow UNIStim message traversal from the CICM from the public side of the NAT.

Keep NAT binding alive for UNIStim signaling Each IP Phones 200x is configured with the IP address of its hosting CICM. When the IP Phones 200x powers on, it sends a Resume Connection message to the CICM. A path through the NAT device is set up for UNIStim signaling.

Once the initial connection has been made, the IP Phones 200x starts the Watch Dog timer, with a default value of 2.5 minutes.

To keep the firewall pinhole open for the UNIStim signaling path throughout the user's logon session, the CICM has a built-in global terminal Watch Dog timer that has a default value of 2 minutes.

Every one minute, the CICM sends a UNIStim Reset Watchdog message to the client (i.e. terminal) to reset the Watch Dog timer on the client, and the client responds with an ACK message. This ACK

message goes through the firewall and resets the firewall (NAT) timer, hence keeping the firewall pinhole open and the NAT binding alive.

The configurable NAT binding (firewall) timer value is recommended to be 3 minutes. The guideline is to set the Watch Dog timer about 30 seconds smaller than the firewall timer.

RTP media NAT traversal Two uni-directional RTP media streams are needed to set up a VoIP call. The outgoing RTP media stream from Centrex IP clients to the CICM can traverse the NAT since it is initiated from the private side of the NAT. However, the incoming RTP media stream initiated at the CICM (on the public side of the NAT) and destined to the clients can not traverse the NAT since there is no address binding established at the NAT. Therefore, the call fails.

The real challenge of a NAT on any VoIP application, therefore, is how the incoming RTP media stream traverses the NAT.

Nortel Networks NAT traversal solution

The Nortel Network NAT traversal solution is summarized by the following four factors, which are discussed below.

- CS2K-routed calls
- Intraswitched calls behind a single NAT
- Calls between two enterprises
- Keeping NAT open for RTP media

Unistim Security

This section provides a summary of Unistim security (USEC), and the key webpages used for security administration.

(I)SN07 CICM Unistim Security enhancements

The Unistim Security feature was added in CICM 2.5 MR6 release. For this CICM 7.0 release, there are three new enhancements to CICM Unistim Security:

- The Clearing of Security Objects component
- Securing the UFTP stream component
- Support for Phase 2 sets component

The securing of the UFTP stream and the support for Phase 2 sets are enhancements that are not user visible and require no Telco administrator action.

The Clearing of Security Objects component provides the functionality to move a secured terminal from one CICM to another.

In the initial CICM 2.5 MR6 Implementation of Unistim Security, once a terminal has been connected securely to a CICM, it is tied to that particular CICM. Once in this state, the client is not capable of connecting to a different CICM without manual intervention. This feature enhancement adds an automated procedure to replace the manual intervention. This functionality is administered from the Security webpage of the CICM-EM web pages. Refer to the *Security Configuration* Procedure in the *NN10252-611 CICM Administration and Security* document.

UNIStim Security: Clearing of Security Objects

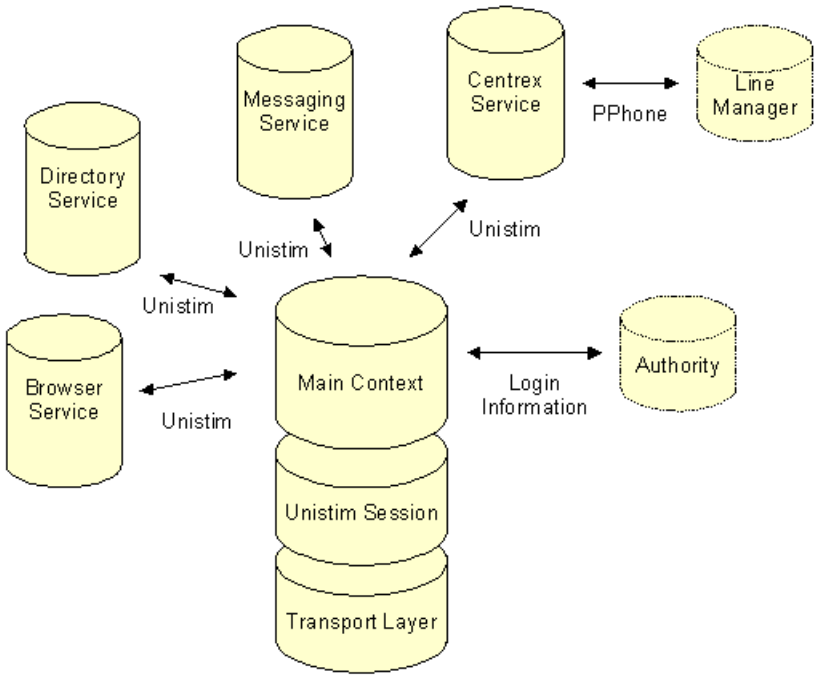
The Clearing of Security Objects component of the Unistim Security feature is new for CICM 7.0 release. This is a new component of the Unistim Security feature that was added in CICM 2.5 MR6 release.

This feature provides the infrastructure for secure signalling communication (i.e. encryption/decryption) between the CICM Server and its clients.

The CICM session manager hosts sessions between end user terminals and the gateway. Terminals can be physical devices, such as the IP Phone 200x, or software applications running on a remote machine like the m6350 softclient. The terminals and the gateway communicate using a stimulus protocol called Unistim. By interacting with the terminal, an end user can use the services that are hosted by the gateway.

The following Figure 4 diagram demonstrates the components of a single session on the CICM Server. The **Unistim Session** and **Transport Layer** shown in the diagram encapsulates the signalling protocol/communication between the terminal clients and the CICM server.

Figure 1 Unistim security

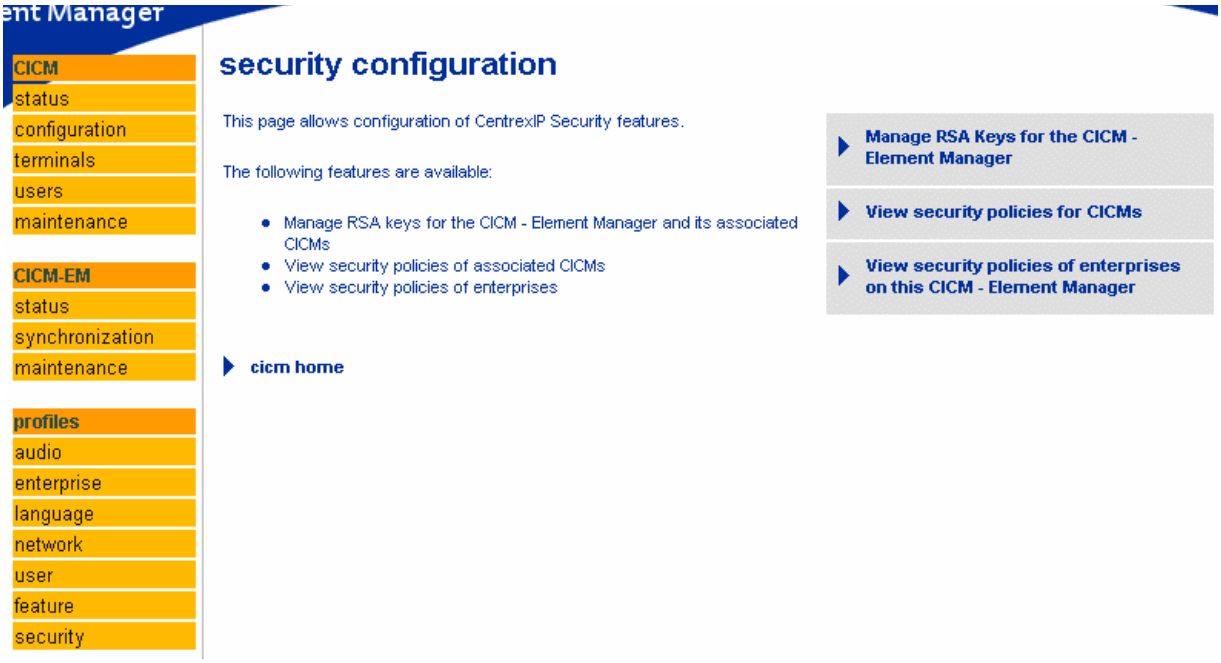


Security configuration

The Security Configuration webpage is new for the CICM 7.0 release. It is illustrated in the following figure. From this page the administrator can:

- Manage RSA keys for the CICM-EM and its associated CICMs
- View the security policy of the associated CICMs
- View the security policies of enterprises

Figure 2 Security configuration

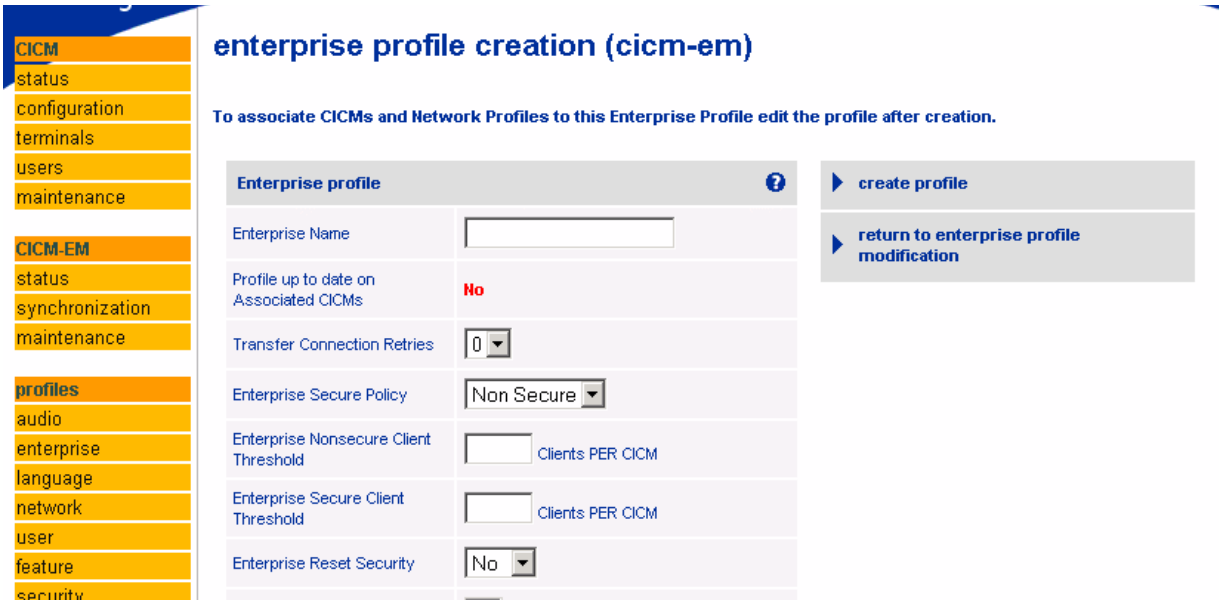


Enterprise Profile webpage

This section reviews the security aspects on the Enterprise Profile webpages.

From the **Enterprise Profile** page, selecting the **Add new profile** option opens the **Enterprise Profile Creation (cicm-em)** webpage, illustrated in the following figure.

Figure 3 Enterprise Profile Creation (cicm-em)



The security fields on this **Enterprise Profile Creation (cicm-em)** webpage are:

- **Enterprise secure policy**
  This field is used to define the security policy of all terminals covered by this Enterprise profile. It can be set to either **Secure** or **Non Secure**. It may be set to Secure only if an RSA key has been generated on the EM.
- **Enterprise Nonsecure Client Threshold**
  The nonsecure client threshold is the number of clients per CICM permitted to connect in a non-secure manner, when the policy for the network is set to **secure**. Basically, the field determies if terminals are allowed to connect non-securely to a secure gateway. Set to zero to disallow.
- **Enterprise Secure Client Threshold**
  This field determines if terminals are allowed to connect securely to a non-secure gateway. Set to zero to disallow.
- **Enterprise Reset Security**
  This field resets the security settings on all terminals that fall under this enterprise profile. This is to allow terminals to connect to different CICM servers securely.

Global Settings webpage

This section reviews the security aspects on the **Global Settings** webpage.

From the **CICM home** page, select **change the global settings for the following CICM** option, which opens the **Global settings modification on <cicm_name>** webpage, illustrated in the following figure.

Figure 4 Global settings modification on <cicm_name>

The security fields on this **Global settings modification on <cicm_name>** webpage are:

- **Default security policy**
  This field is used to define the security policy of all terminals connected to this CICM and not falling under any Enterprise Profile. It can be set to either **Secure** or **Non Secure**.
- **Nonsecure Client Threshold**
  This field determines if terminals are allowed to connect non-securely to a secure gateway. Set to zero to disallow.
- **Secure Client Threshold**
  This field determines if terminals are allowed to connect securely to a non-secure gateway. Set to zero to disallow.
- **Reset Security**
  This field resets the security settings on all terminals that are connected to the CICM and not falling under this enterprise profile. This is to allow terminals to connect to different CICM servers securely.

Terminal audit on <cicm_name> webpage
This section reviews the security aspects on the **Terminal audit on <cicm_name>** webpage.

From the **terminals** webpage, select **terminal audit** option, which opens the **Terminal audit on <cicm_name>** webpage, illustrated in the following figure.

Figure 5 Terminal audit on <cicm_name> webpage

The security fields on this **Terminal audit on <cicm_name>** webpage is:

- **Reset security Setting**
  This field shows the current **Reset Security Setting** for the given terminal.
- **Reset Security State**
  This field shows the current state of the terminal with respect to Security Settings being reset.

Tools and utilities

The Web Interface is the primary user interface to the Centrex IP Client Manager. The CS2K Line Maintenance Manager (LMM) Interface may be used to perform administration and maintenance of the CS2K components that relate to the CICM.

A number of standard administration tools, such as SNMP and WMI, can be used on the Administration PC, in addition to the Web Interface, for remote management of the CICMs.

Web Interface

The Element Manager Web Interface is designed for use with Microsoft Internet Explorer 5.0 or higher and uses standard Microsoft navigation techniques.

> ***Note:*** For the Web Interface to be correctly displayed, a PC with a resolution of at least 800x600 and a color depth of at least 256 colors should be used.

The Web Interface allows you to configure and monitor CICMs via a set of web pages. Web pages are hosted on the Element Manager. They offer configuration and status options to the administrator. These web pages are password protected and can also be accessed from a remote web enabled terminal.

The web interface is made up of two basic components: the navigation bar and the context panel.

The navigation bar is arranged upon installation to offer full administration of the CICM. For example, configuration and status web pages that are applicable to a particular CICM can be selected from the CICM menu on the navigation bar.

The context panel contains different displays depending on which option has been selected on the navigation bar.

LMM Interface

The Line Maintenance Manager (LMM) Interface on the CS2K is the primary interface between administration personnel and the CS2K. The LMM Interface is used to perform administrative and maintenance tasks on the CS2K, including:

- General maintenance
- Network management
- Operational measurements
- Service analysis
- Trunk tests
- Data modification
- Line tests

Refer to the CS2K documentation suite for detailed procedures on the LMM Interface.

CICM SNMP agent

Simple Network Management Protocol (SNMP) is an industry standard management interface. An SNMP agent provides a standard interface for status monitoring and fault reporting.

The CICM provides an SNMP interface for remote status monitoring. Each CICM node will send SNMP traps to a set of management systems when specific events occur (See also the *Event Log* section of the *Security and Administration* module of this document).

An SNMP browser can be used to view the standard MIB-2 mibs as well as the Nortel Networks specific CICM mib.

CICM WMI agent

WMI is a management interface from Microsoft, and is a standard component of the NT-embedded operating system. The WMI management system provides the capability to monitor the status of the CICMs. The WMI Agent does not need configuration.

WMI management systems are available from companies such as Hewlett Packard.

Security and administration procedures

Security and administration procedures are performed by means of the Element Manager Web Interface, a Telnet connection to the Administration LAN, and the Microsoft desktop.

User administration

This section provides procedures for the administration of user accounts on the CICM EM, including the administration of user and administrator privileges. It does not address CICMs.

Since the standard operating system on Series 2.5 EMs is Windows 2000, these procedures are written for a Windows 2000 EM. However, Windows NT is also supported on legacy EMs.

Open the Computer Management tool

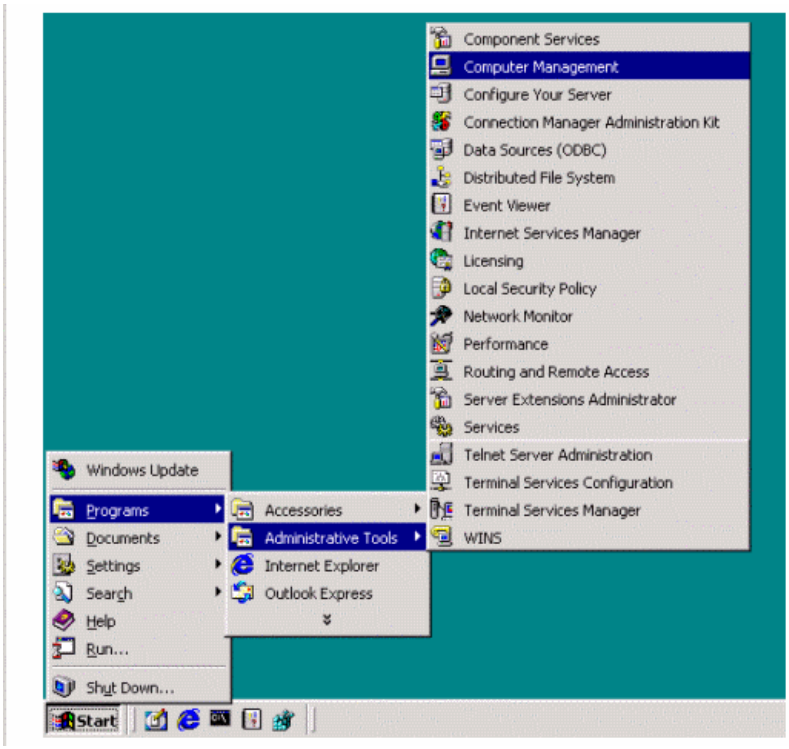
The User Administration procedures use the Computer Management tool, which is a program on Windows 2000 that allows various tasks to be performed, including the management of users. The following procedure demonstrates how to access this tool.

Procedure 1 Open the Computer Management tool

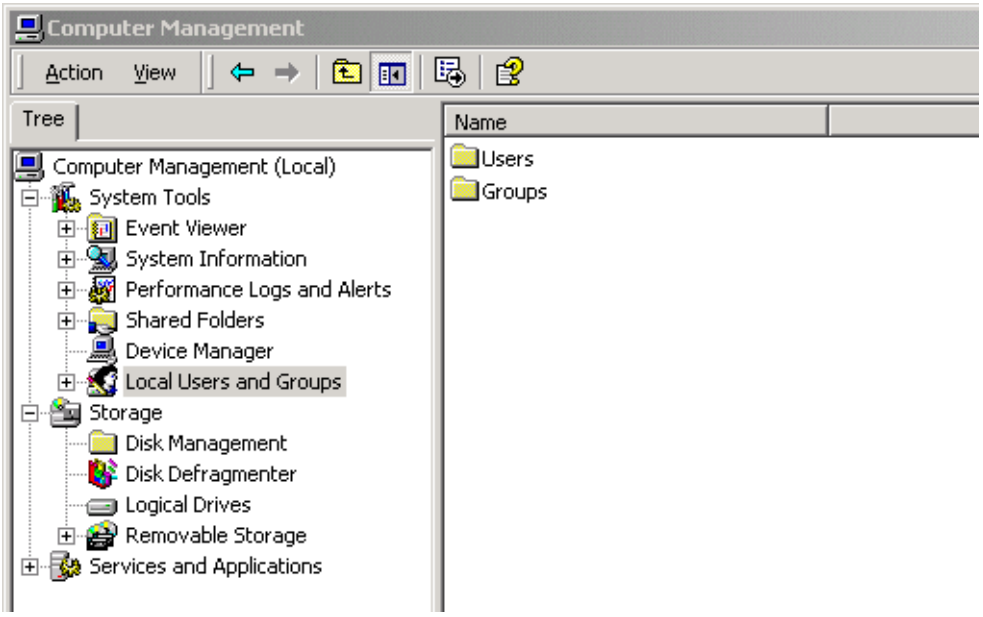
On the EM MS 2000 desktop

1 From the Microsoft Windows Start menu, select **Programs**, then **Administrative Tools**, then **Computer Management**:

Start > Programs > Administrative Tools > Computer Management



Response: The Computer Management window opens.



2 This procedure is complete.

View users on an EM

When the Series 7.0 (or 6.12) CICM software is installed on an Element Manager, a standard set of user accounts is automatically created. The following table provides a description of these automatically created user accounts.

Table 1 Standard User Accounts

User Name	Purpose
IUSR_CENTREXIP-PEM	A built-in account for anonymous access to Internet Information Services (IIS). This user name and password is created and managed by IIS and as such should not be deleted or modified.
IWAM_CENTREXIP-PEM	A built-in account for Internet Information Services to start out of process applications. This user name and password is created and managed by IIS and as such should not be deleted or modified.
Guest	A built-in account for guest access to the computer. This account is not used by CICM and can be disabled if not needed.

Table 1 Standard User Accounts

User Name	Purpose
Administrator	A built-in account for administering the computer with full access permissions. It is used for most operations on the EM. This user password is initially set to “centrexip” but can be changed at any time (see the *Change User Password* procedure below). It is recommended to rename this user name to a less obvious name to enhance security. It is necessary to have an account on the EM with full privileges so all maintenance can be performed.
NortelTAS	This user account allows Nortel Support access to the EM. TAS is the Nortel Technical Assistance Service.
CICM account (site specific, but usually called comuser)	This is an important account that the majority of CICM software runs under. It is created on the EM installation by the preboot command (the install command in 2.4). It should have the same name and password on all CICMs and CICM-EMs that interface with each other. It is not possible to change this account’s password. This account should not be used for general administration purposes.

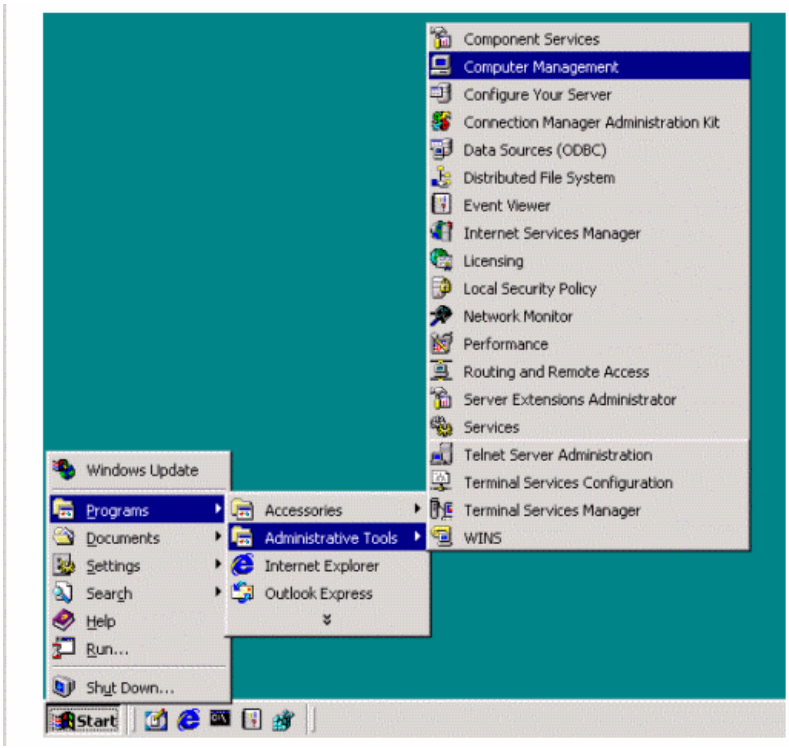
Use the following procedure to view the users on an EM.

Procedure 2 View users on an EM

On the EM MS 2000 desktop

1 Open the Computer Management tool from the Microsoft Windows Start menu:

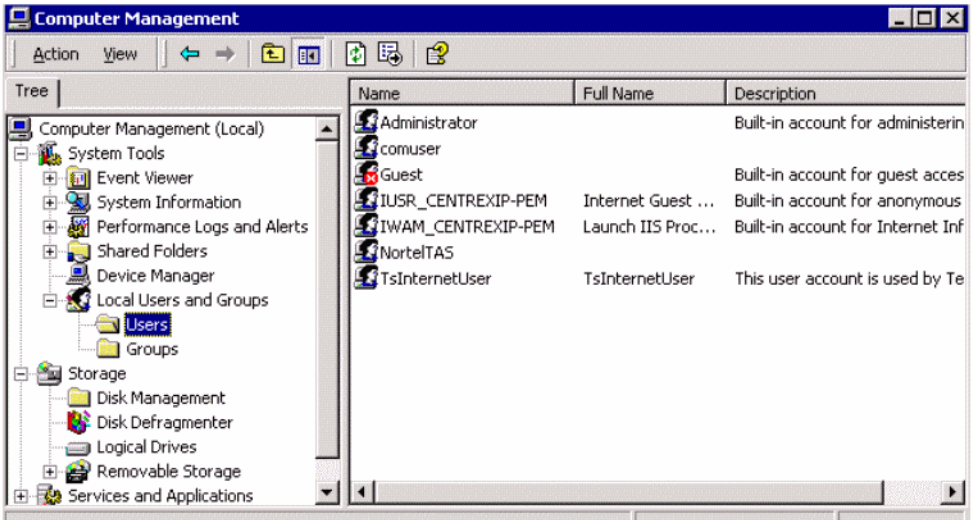
Start > Programs > Administrative Tools > Computer Management



2 In the Computer Management window, expand the **Local Users and Groups** file, then click on the **Users** folder.

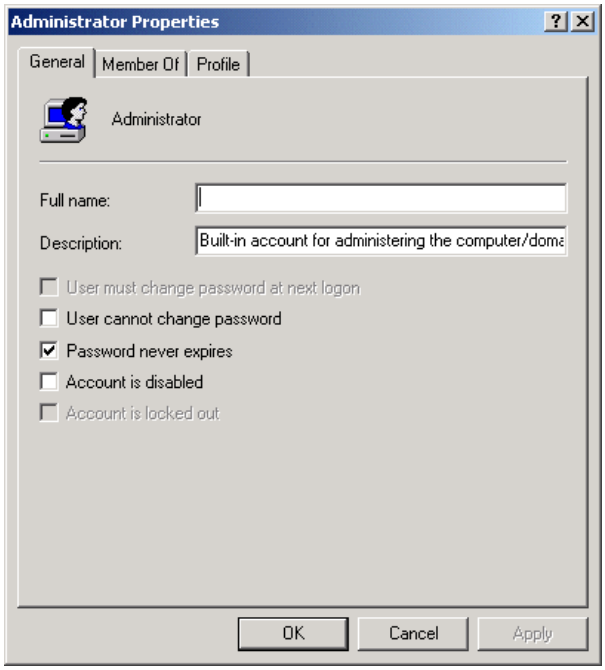
Response: On the right of the Computer Management window is displayed a list of all users on the system.

Note: *The following figure shows the user accounts that are automatically created. Refer to Table 3 above, Standard User Accounts, for a description of these user accounts.*



3 To view the properties of a user, double-click on the user name from the list in the right window.

*Response: The **<Username> Properties** window opens.*



4 This procedure is complete.

Create new users

Use this procedure to create new users on the CICM EM. Only a user with administrator privileges can perform this procedure.

All new users are automatically assigned user privileges. To assign administrator privileges, first create the user, then perform the *Assign Administrator Privileges* procedure below.

Procedure 3 Create new users

On the EM MS 2000 desktop

1 Logon to the EM with a user account with administrator's privileges.

2 Open the Computer Management tool from the Microsoft Windows Start menu:

Start > Programs > Administrative Tools > Computer Management

3 In the Computer Management window, expand the **Local Users and Groups** file by double-clicking on this file.

Response: The Users and Groups sub-folders are displayed in the left window.

4 Click on the **Users** folder.

Response: The right window displays the contents of the Users folder.

5 Click on the **Action** menu, then select the **New User** option.

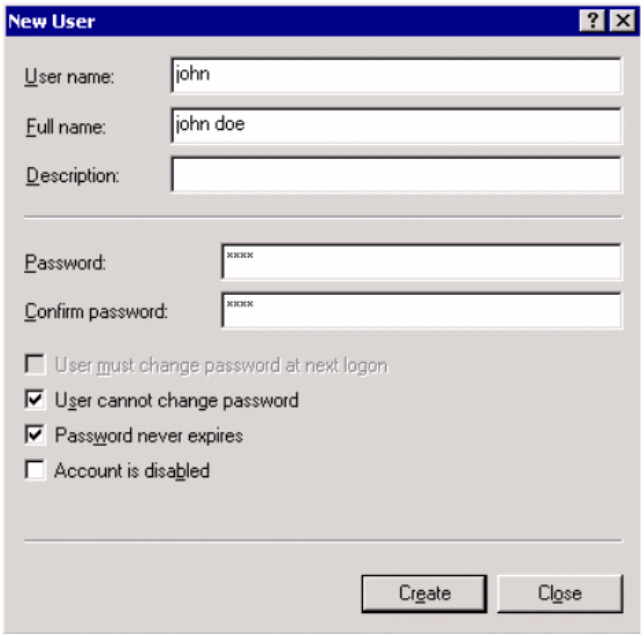
Response: A New User dialog box opens.

6 Datafill the New User dialog box:

a Enter the username and password for the new user.

b Check the boxes as shown in the following figure.

Note: The check boxes normally should be set as shown in the following figure. To set password expiration, see the procedure below, *Set Password Expiration*.



7 Click the **Create** button.

Response: The New User dialog box closes and the new user account appears in the Computer Management window's list of users.

8 This procedure is complete.

Delete or rename a user

Use this procedure to delete or rename a user account. Only a user with administrator privileges can perform this procedure.

Procedure 4 Delete or rename a user

On the EM MS 2000 desktop

1 Logon to the EM with a user account with administrator's privileges.

2 Open the Computer Management tool from the Microsoft Windows Start menu:

Start > Programs > Administrative Tools > Computer Management

3 In the Computer Management window, expand the **Local Users and Groups** file by double-clicking on this file.

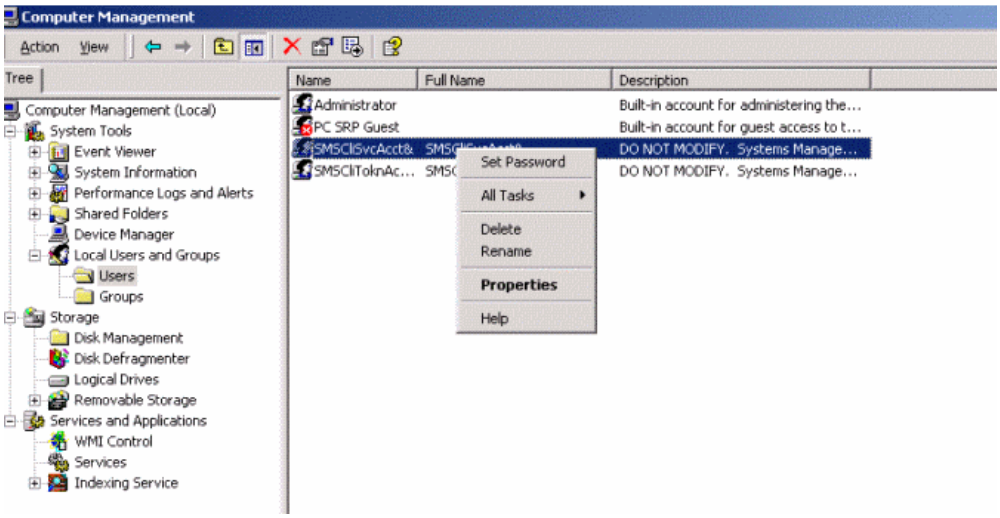
4 Click on the **Users** folder.

Response: The right window displays the contents of the Users folder.

5 From the list of users in the right window, right-click on the user to delete or rename, then

a To delete the user, choose **Delete** from the pop-up menu.

b To rename the user, choose **Rename** from the pop-up menu, then enter the new name and press **Enter**.



6 This procedure is complete.

Set user password

Use either of the following procedures to set or change a user password, or to reset an expired password.

The procedure below changes passwords from the Computer Management tool, and the following procedure changes passwords from the EM Web Interface.

Only a user with administrator privileges can perform these procedures.

Some user account passwords are controlled by IIS and shall not be modified. Refer to Table 3, *Standard User Accounts*, for information on these accounts.

Procedure 5 Set user password (Computer Management tool)

On the EM MS 2000 desktop

1 Logon to the EM with a user account with administrator's privileges.

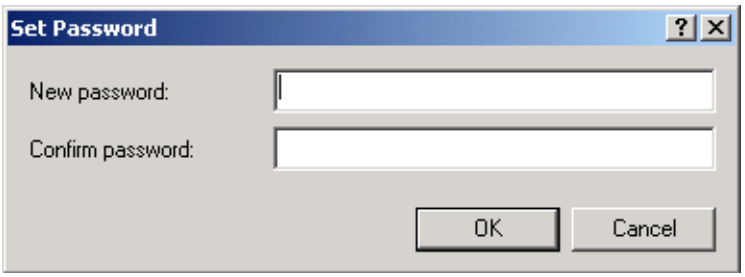
2 Open the Computer Management tool from the Microsoft Windows Start menu:

Start > Programs > Administrative Tools > Computer Management

3 Expand the **Local Users and Groups** file, then the **Users** file.

4 From the list of users in the right window, right-click the user, then select **Set Password** from the pop-up menu.

Response: The Set Password dialog box opens.



5 Enter the new password, confirm it, then press **OK**.

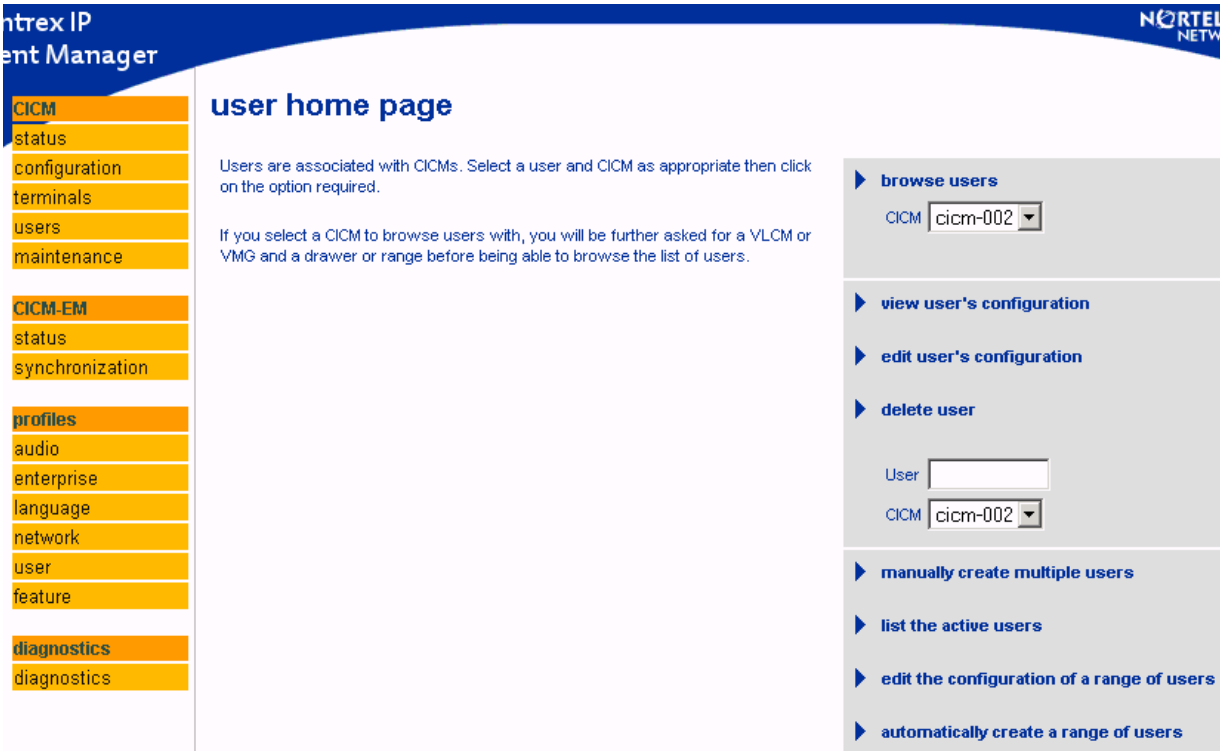
6 This procedure is complete.

Procedure 6 Set user password (EM Web Interface)

At the CICM - Element Manager home page

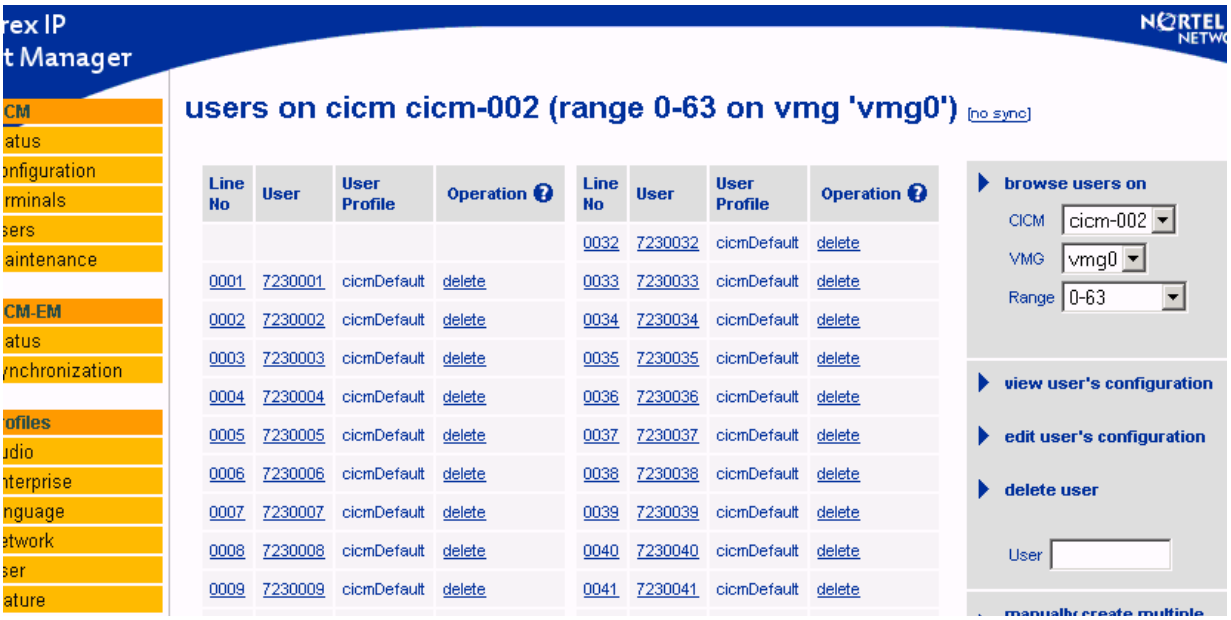
1 Select **users** from the **CICM** section of the left menu bar.

*Response: The **user home page** opens.*



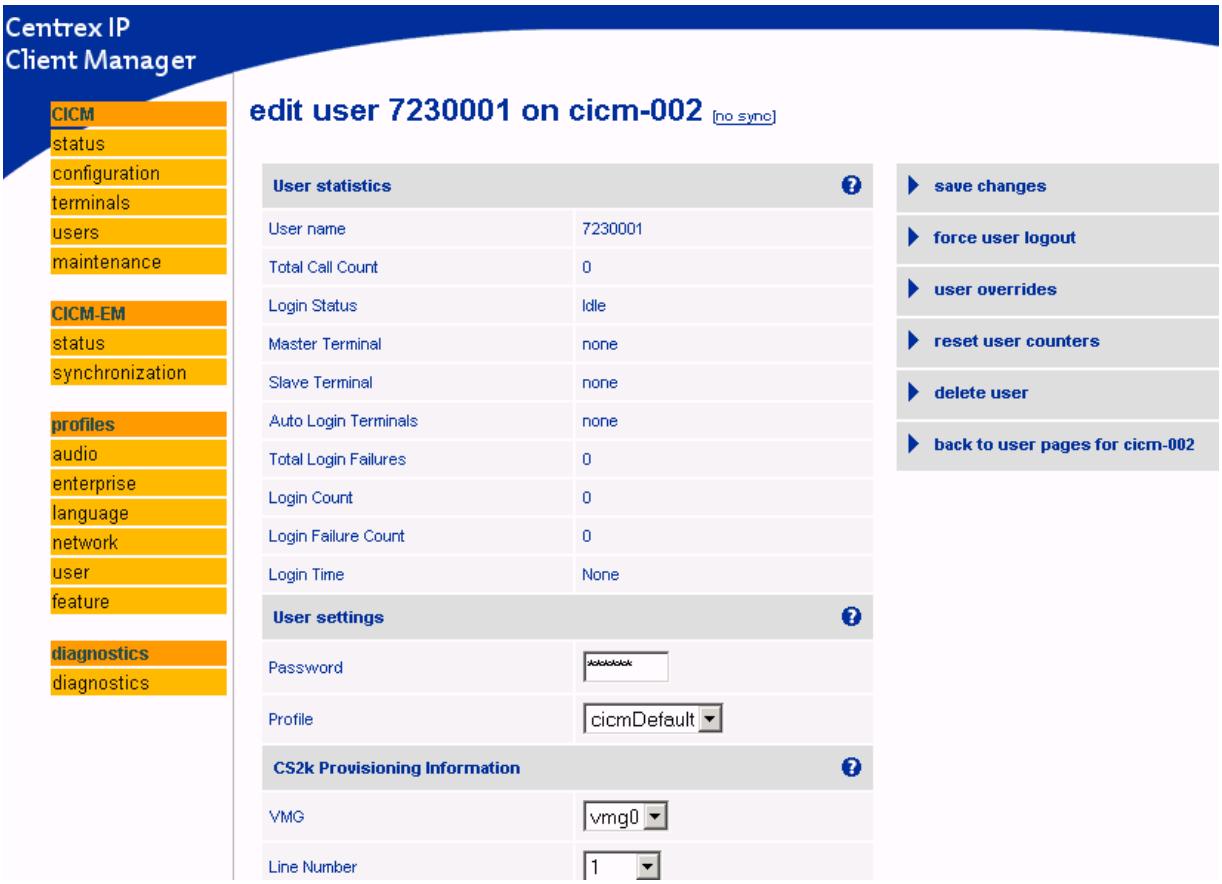
2 Select the CICM from the drop-down menu in the **browse users** option, then click on the **browse users** text.

*Response: The **users on cicm <cicm_name> (range # on vmg_name) page opens.***



3 From the list of users, click on the user name/ID to change the password for.

*Response: The **edit user <name> on <cicm_name>** page opens.*



4 Enter the password in the **Password** field, then click on the **save changes** option.

Note: The user password must be greater than 3 numbers and less than 16 (4-15), numeric characters only. Any more than fifteen numbers entered will be ignored.

Response: A status page opens to confirm the change.

5 This procedure is complete.

Assign/Remove administrator privileges

There are two privilege levels for users: user privileges and administrator privileges.

User privileges applies by default to all new users, who are put into the Users group automatically upon creation.

A user is assigned administrator privileges by adding them to the Administrator group. Administrator privileges are removed by removing the user from the Administrator group.

The user account “Administrator” that is automatically created upon EM configuration is set up as a member of the Administrator’s group.

The following table compares the two privilege levels.

Table 2 User and Administrator Privileges

Operation	User Privileges	Administrator Privileges
Logon locally	Given by default. This privilege can be removed by using the User Rights Assignment in the Local Security Settings program.	Given by default. Can be removed using the User Rights Assignment in the Local Security Settings program.
Telnet	Yes	Yes
FTP	Yes	Yes
CICM web page access	Yes	Yes
Certain operations such as installing some types of software, changing network settings, etc.	Restricted	Yes
Running **preboot** or **swupgrade** on the EM	No	Yes
Change other user’s passwords	No	Yes

Only a user with administrator privileges can perform this procedure to assign or remove administrator privileges.

Procedure 7 Assign/Remove administrator privileges

At the EM MS2000 desktop

1 Logon to the EM with a user account with administrator’s privileges.

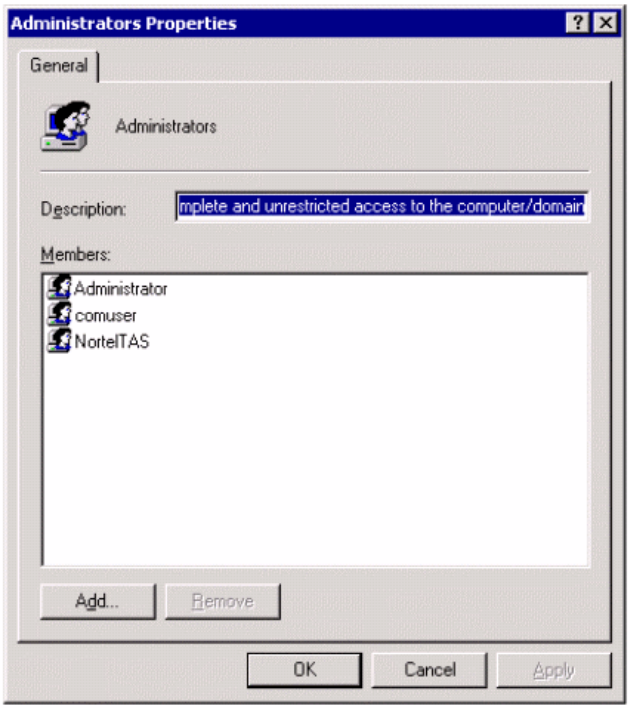
2 Open the Computer Management tool from the Microsoft Windows Start menu:

Start > Programs > Administrative Tools > Computer Management

3 Expand the **Local Users and Groups** file, and then the **Groups** file.

4 Double-click on **Administrators** from the list of groups in the right window.

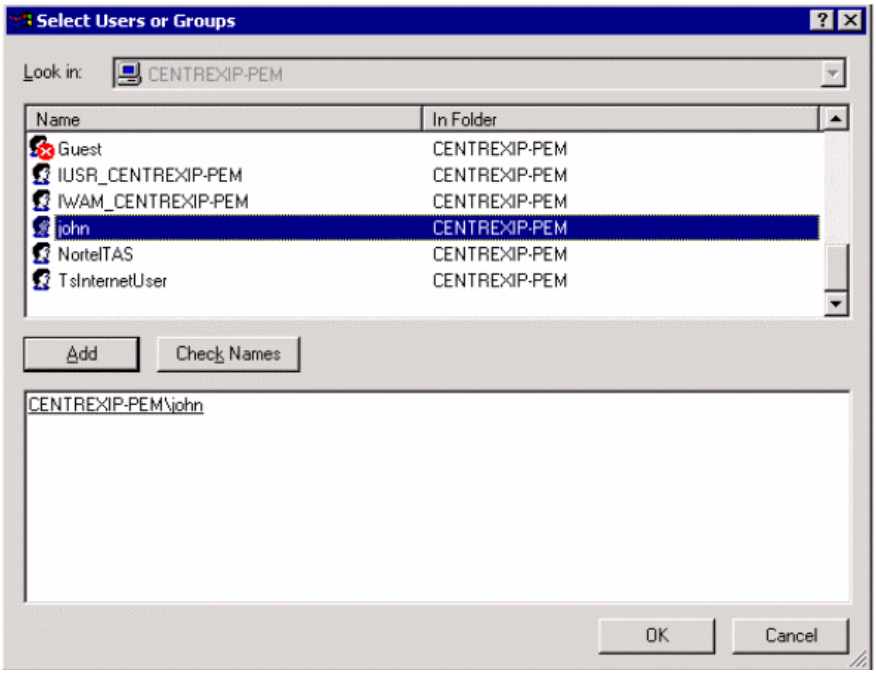
Response: The Administrator's Properties dialog box opens with a list of the Administrator's group members.



5 To add a user to the Administrator group and assign them administrator privileges:

a In the Administrator's Properties window, click on the **Add** button

Response: The Select Users or Groups dialog box opens.



b Search for and select the user to add from the list in the top half of the dialog box, or type the username into the bottom window of the dialog box,

c Then click on the **Add** button.

Response: The name added moves to the bottom half of the dialog box.

d Continue to select and add until you have completed your list,

e Then click **OK** to save your changes.

6 To remove a user's administrator's privileges:

a From the **Administrator's Properties** window's list of administrators, click on the user name to remove,

b Then click on the **Remove** button.

c Continue to remove user names until complete,

d Then click on **OK** to save your changes.

7 This procedure is complete.

Set password expiry

Microsoft Windows has a build-in method to manage password expiry. This is turned off on the EM to stop certain accounts from expiring,

which could affect the running of the CICM. Before turning on password expiration, you must make sure the CICM account is set to never expire.

Only a user with administrator privileges can perform this procedure.

Procedure 8 Set password expiry

On the EM MS 2000 desktop

1 Logon to the EM as an Administrator.

2 From the Microsoft Windows Start menu, open the Computer Management tool by selecting:

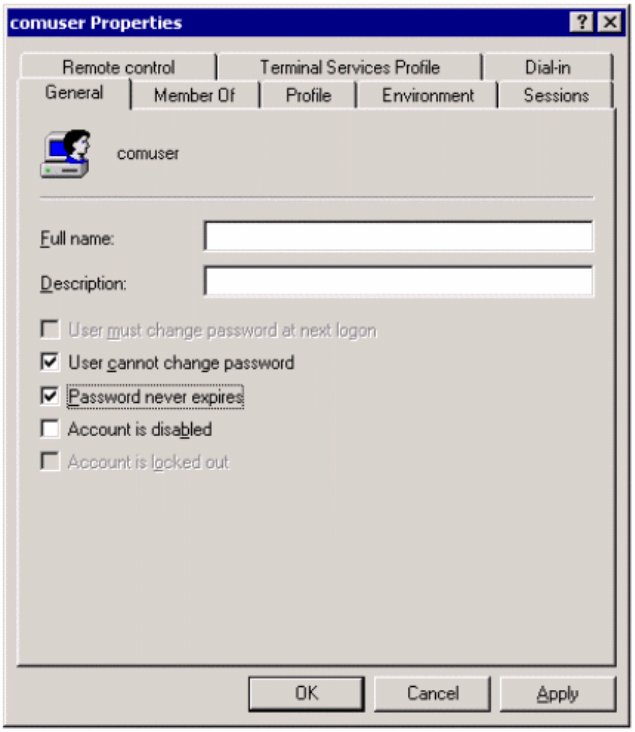
Start > Programs > Administrative Tools > Computer Management

3 In the Computer Management window, expand the **Local Users and Groups** file, then the **User** file.

4 Double-click on the CICM user account from the list of Users.

Note: The CICM user account is site-specific, but it is usually named **comuser**.

*Response: The **<CICM user account> Properties** dialog box opens.*

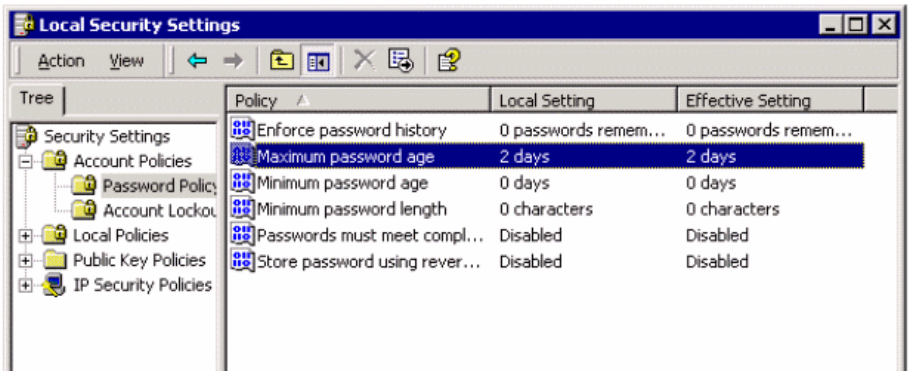


5 In the **user Properties** dialog box, check the **User cannot change password** and **Password never expires** options, then click **OK**.

6 To turn on password expiry, it is necessary to first change a system setting. From the Microsoft Windows Start menu, open the Local Security Settings dialog box by selecting:

Start > Programs > Administrative Tools > Local Security Policy

Response: The Local Security Settings dialog box opens.

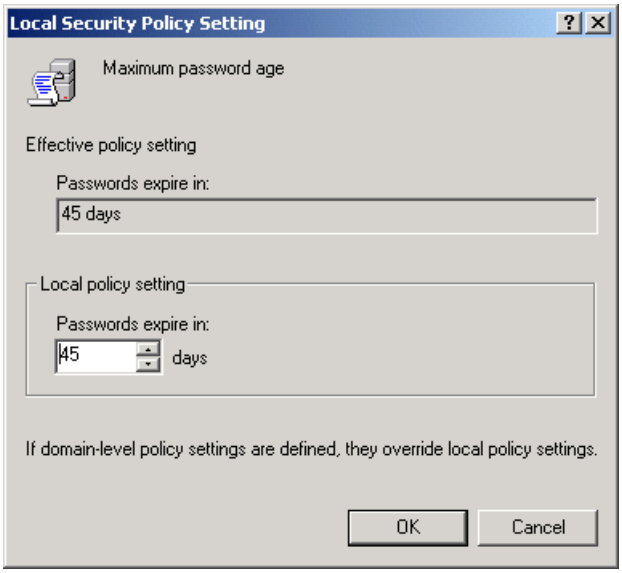


7 From the **Local Security Settings** window, expand the **Account Policies** file, then expand the **Password Policy** file.

Response: The right window displays a list of settings that affect passwords.

8 It is recommended to only change the Maximum Password Age setting. To change this setting, double-click on **Maximum Password Age** from the list of settings in the right window of the **Local Security Settings** window.

*Response: The **Local Security Policy Setting** dialog box opens.*



9 To change the expiry setting:

a To disable expiry, set the Maximum Password Age in the **Passwords expire in:** field to 0, then click **OK**.

b To enable expiry, set the Maximum Password Age in the **Passwords expire in:** field to the number of days you want passwords to be valid, then click **OK**.

10 *(OPTIONAL: FOR EXPIRED PASSWORDS)*
Once a user password is close to the expiry time, when the user logs into the EM the user will receive a warning message telling them to change their password. If their password is not changed and expires, they will not be able to login or use the EM web pages. Upon attempting to login, a **Change Password** dialog box opens, which must be completed before they can proceed.

11 This procedure is complete.

Prevent user logon to local EM

Use this procedure to prevent a particular user from logging on locally to the EM. Users with or without administrator privileges can both be denied logon privileges. Only a user with administrator privileges can perform this procedure.

Procedure 9 Prevent user logon to local EM

On the EM MS 2000 desktop

1 Logon to the EM as an Administrator.

2 From the Microsoft Windows Start menu, open the Local Security Settings window by selecting:

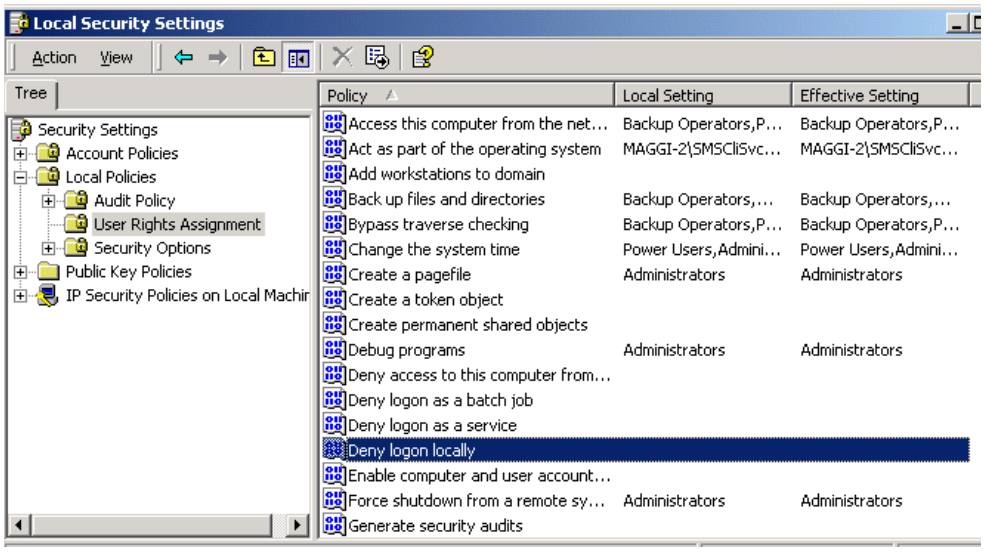
Start > Programs > Administrative Tools > Local Security Policy

Response: The Local Security Settings window opens.

3 In the left window of the Local Security Settings window, expand the **Local Policies** file.

4 Click on **User Rights Assignment**

Response: The right window displays the list of User Rights policies.

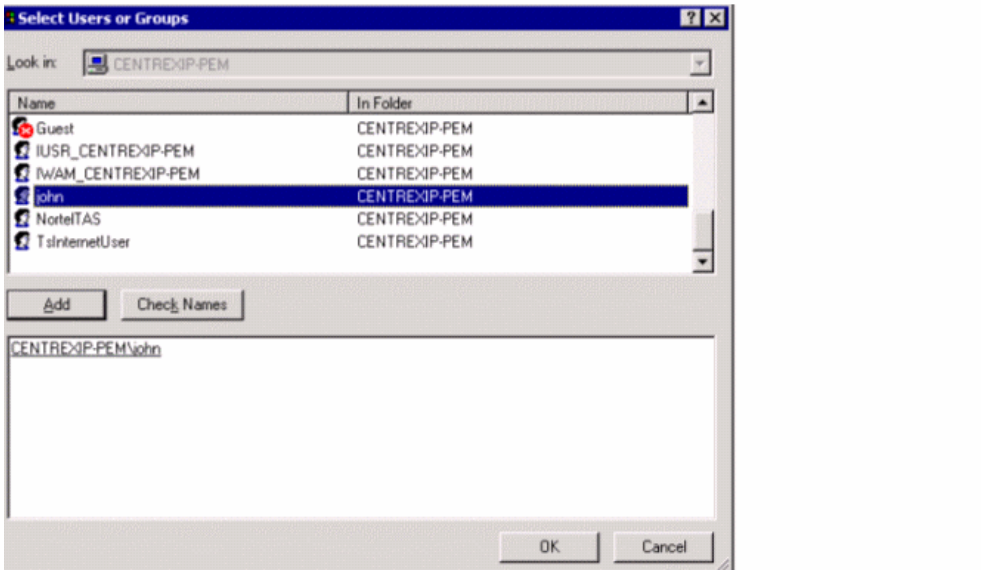


5 In the right window, double-click on **Deny logon locally**.

Response: The Local Security Policy Settings dialog box opens to display the current list of users denied logon.

6 Click the Add button in the Local Security Policy Setting dialog box.

*Response: The **Select Users or Groups** dialog box opens.*



7 Search and select from the top window, or type in the bottom window the username to deny access to, then click **OK**.

8 This procedure is complete.

Disable the Telnet service

Use this procedure to disable the Telnet service. This will stop all users from using it. Only a user with administrator privileges can perform this procedure.

Procedure 10 Disable the Telnet service

On the EM MS 2000 desktop

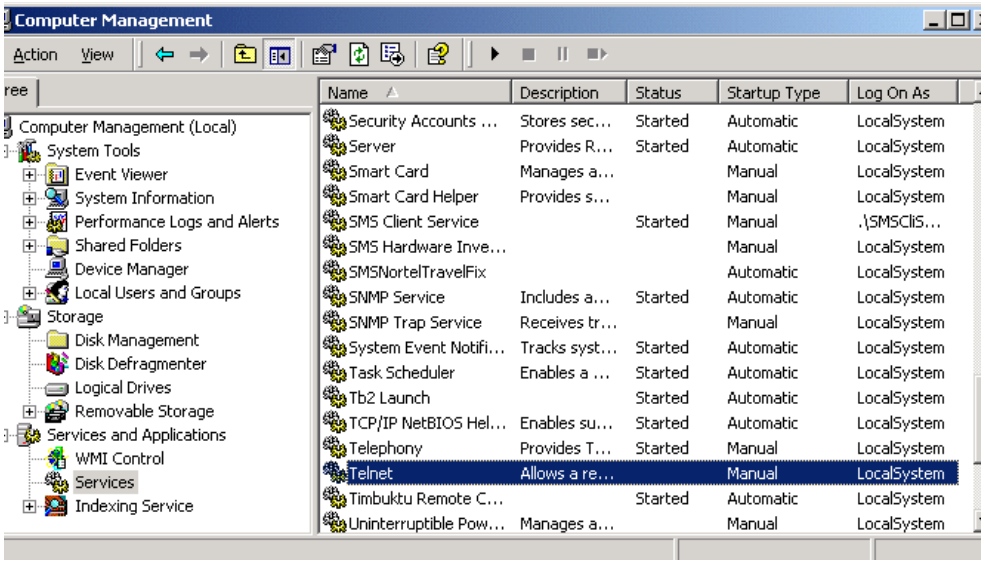
1 Logon to the EM as an Administrator.

2 From the Microsoft Windows Start menu, open the Computer Management window by selecting:

Start > Programs > Administrative Tools > Computer Management

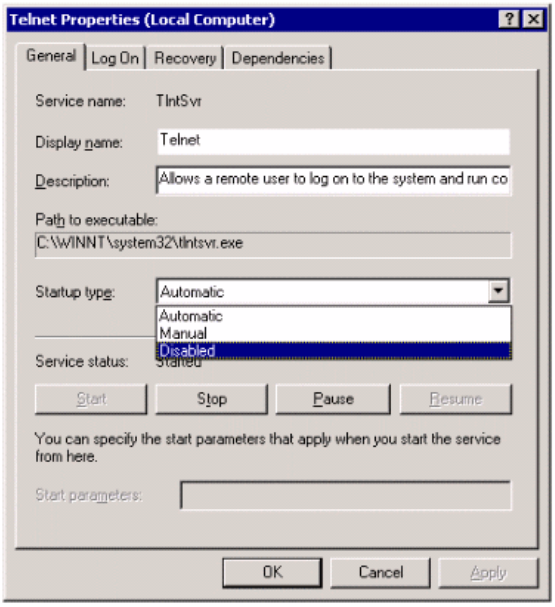
3 Expand the **Services and Applications** file.

4 Click on **Services**.



5 In the list in the right window, double-click on the **Telnet** service.

The Telnet Properties dialog box opens.



6 Change the **Startup type** to disabled, then click the **Stop** button, then click **OK** to save the changes.

7 This procedure is complete.

Element Manager web pages procedures

This section provides procedures based on the Element Manager web pages. For all procedures provided in this document, it is required to use administrator userids and passwords to login to the Element Manager.

Access Element Manager Home page

The Element Manager Home page consolidates access to all of the user administration procedures. It is accessed from a PC running Internet Explorer 5.0 or above. From this home page, the following administrative web pages may be accessed:

- CICM home
- CICM - element manager home
- Configuration (see the *CICM Configuration Management* document)
- Terminals (see the *CICM Configuration Management* document)
- Users (see the *CICM Configuration Management* document)
- Maintenance
- Audio Profiles (see the *CICM Configuration Management* document)

- Language Profiles (see the *CICM Configuration Management* document)
- Network Profiles (see the *CICM Configuration Management* document)
- User Profiles (see the *CICM Configuration Management* document)
- CICM upgrades (see the *CICM Upgrade* document)
- synchronization
- diagnostics

Procedure 11 Access CICM home page

At the Internet Explorer address line

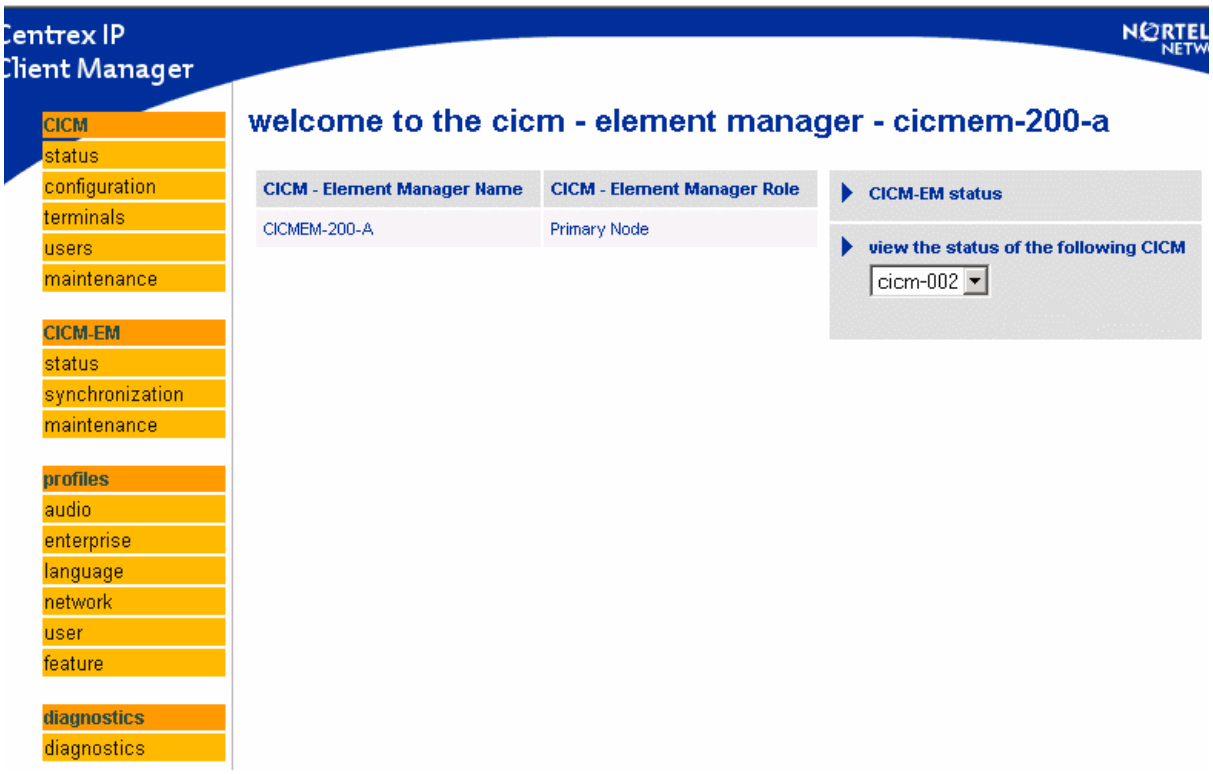
1 Type the IP address of the Element Manager, followed by **/centrexip/**, then press Enter.

Example
http://47.73.240.176/centrexip/

Response: A prompt for the user name and password opens.

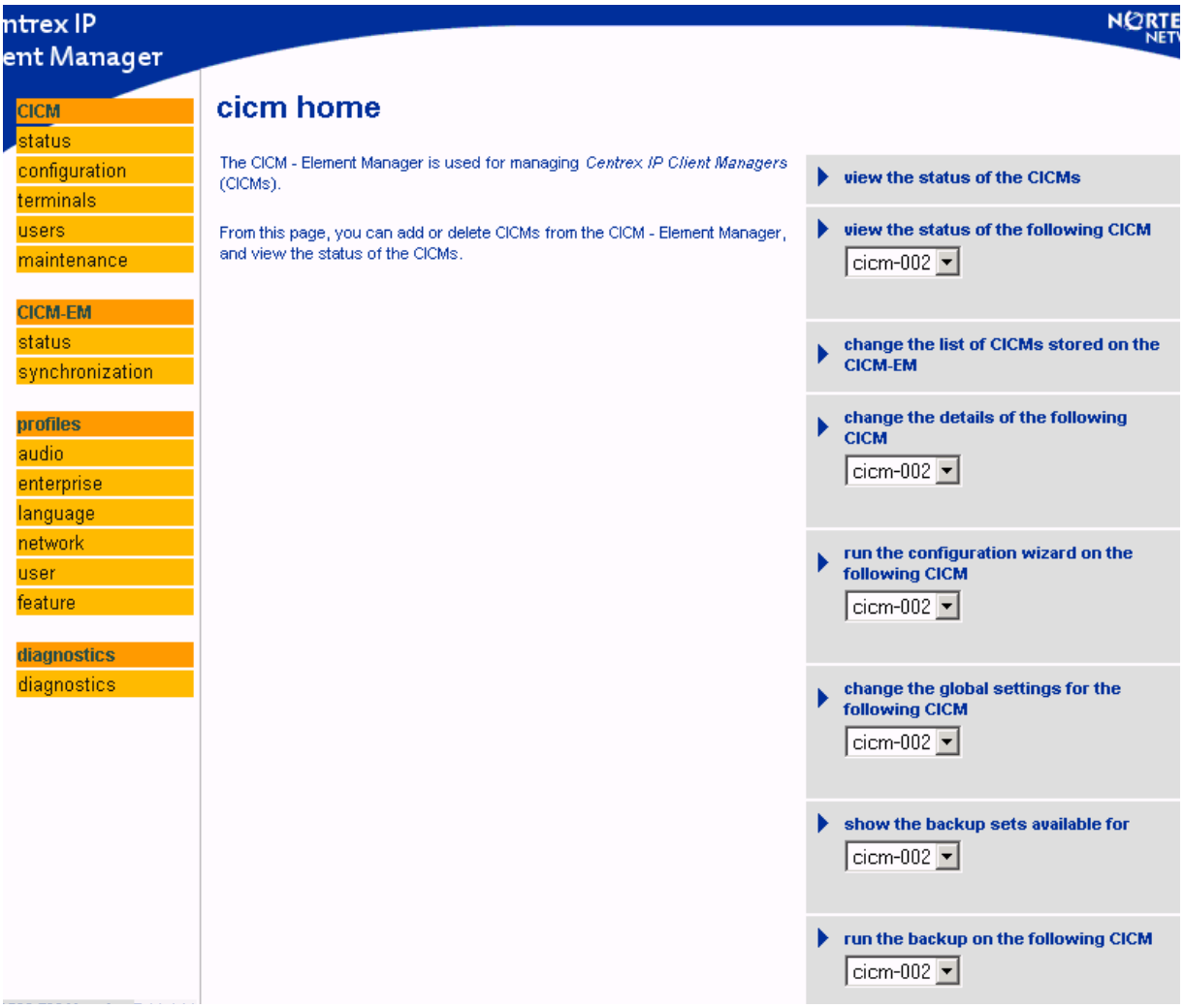
2 Type your Administrator user name and password, then press Enter.

*Response: The **welcome to the cicm - element manager - <cicmname>** page opens.*



3 Click on the **status** option in the **CICM** section of the left menu bar.

*Response: The **cicm home** page opens.*



4 This procedure is complete.

Monitor the status of a CICM

Use this procedure to monitor the status of a CICM.

The **CICM status** page is an emulation of the alarm bar panel on the physical CICM. Any alarms that are seen on the alarm bar will be seen within 30 seconds on the Element Manager **CICM Status** page. From this page you can view the status of individual cards and information about their configuration.

This **CICM Status** web page is the best tool to monitor the CICM status. However, it is recommended to also periodically monitor the event logs of both nodes and the Element Manager. The details of event logs

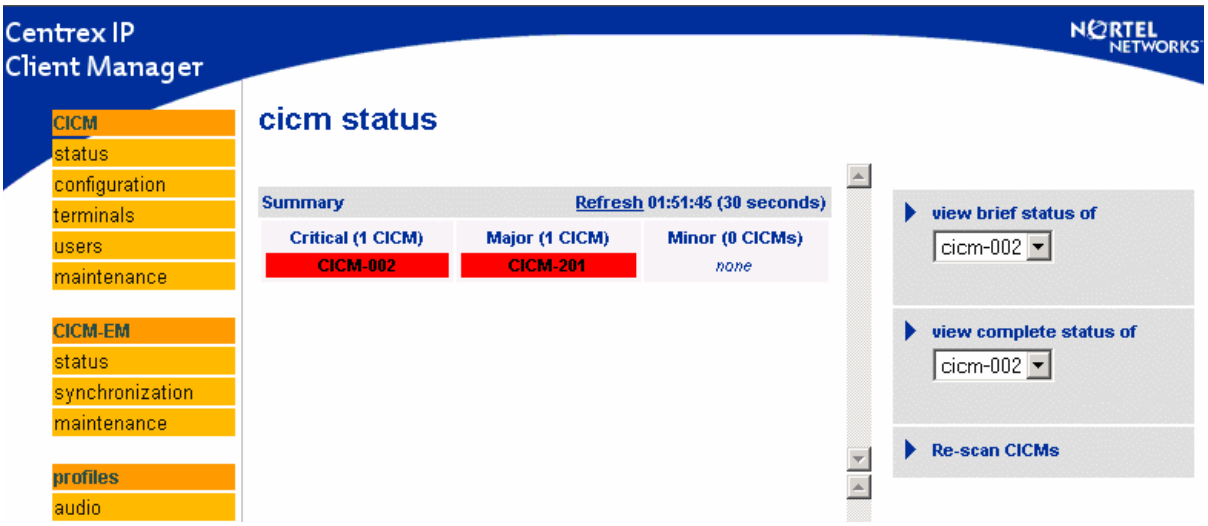
should also be viewed if an error occurs to identify the cause of the fault. Refer to the *View Event Logs* procedure of this document.

Procedure 12 Monitor the status of a CICM

At the CICM home page on the Element Manager web interface

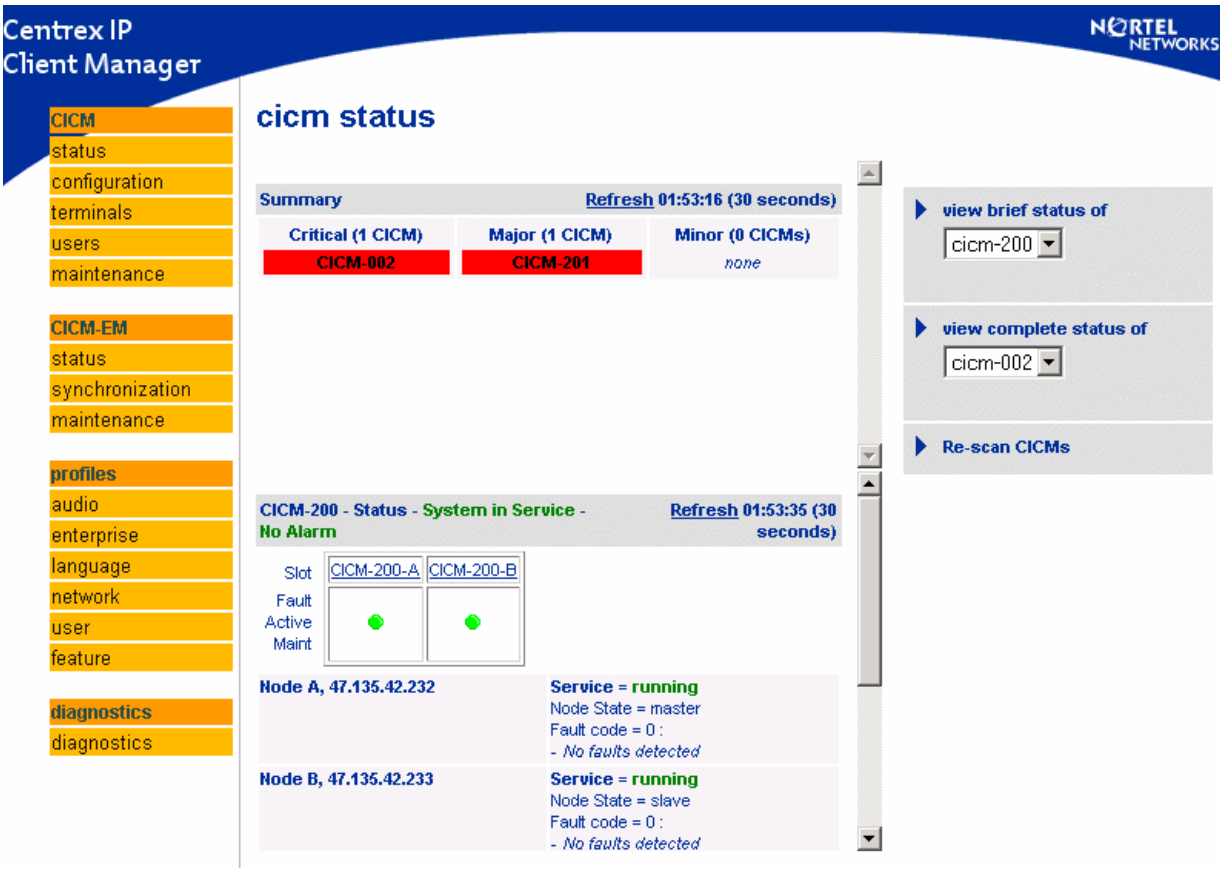
1 Select **View the status of the CICMs** from the menu bar on the right.

*Response: the **cicm status** page displays a summary of critical, major, and minor faults on the CICM.*



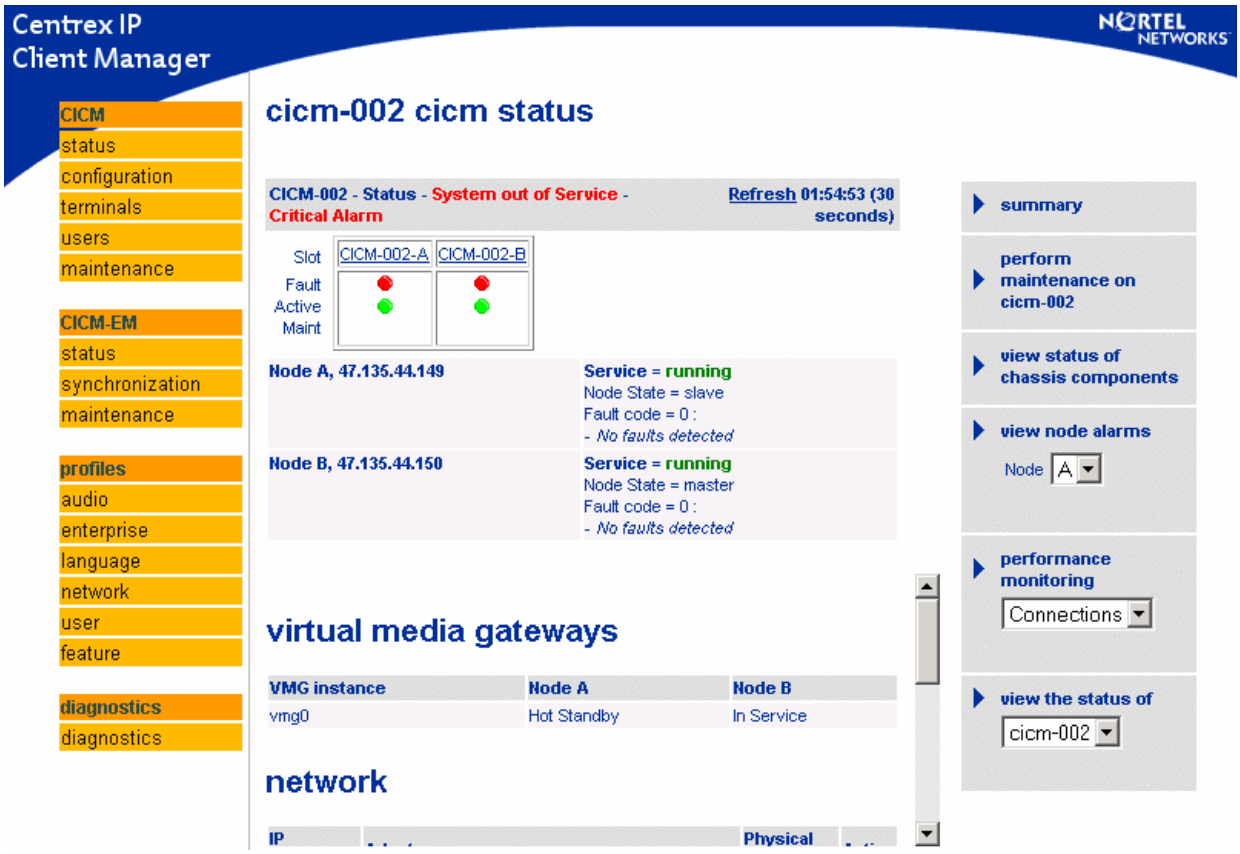
2 To view additional details of the CICM status, click on the **view brief status of** text box on the right.

*Response: The **cicm status** page updates to add additional node and card status information for the CICM.*



3 To view the complete CICM status, click the **view complete status of** text box on the right menu.

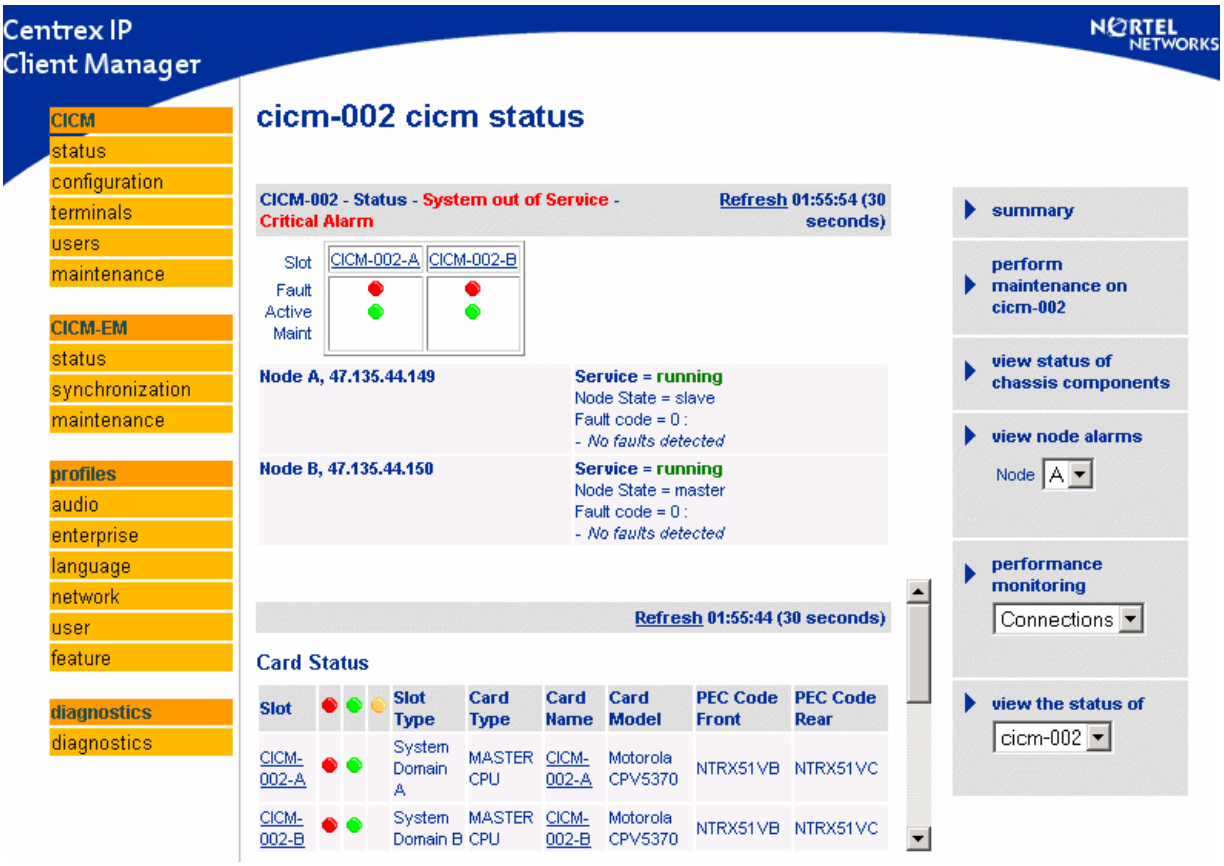
*Response: The **<cicm_name> cicm status** page updates to add additional VMG, node, and network information, and to provide options to view additional detail (See step 4).*



Note: You must scroll down in the details sub-window to view all information.

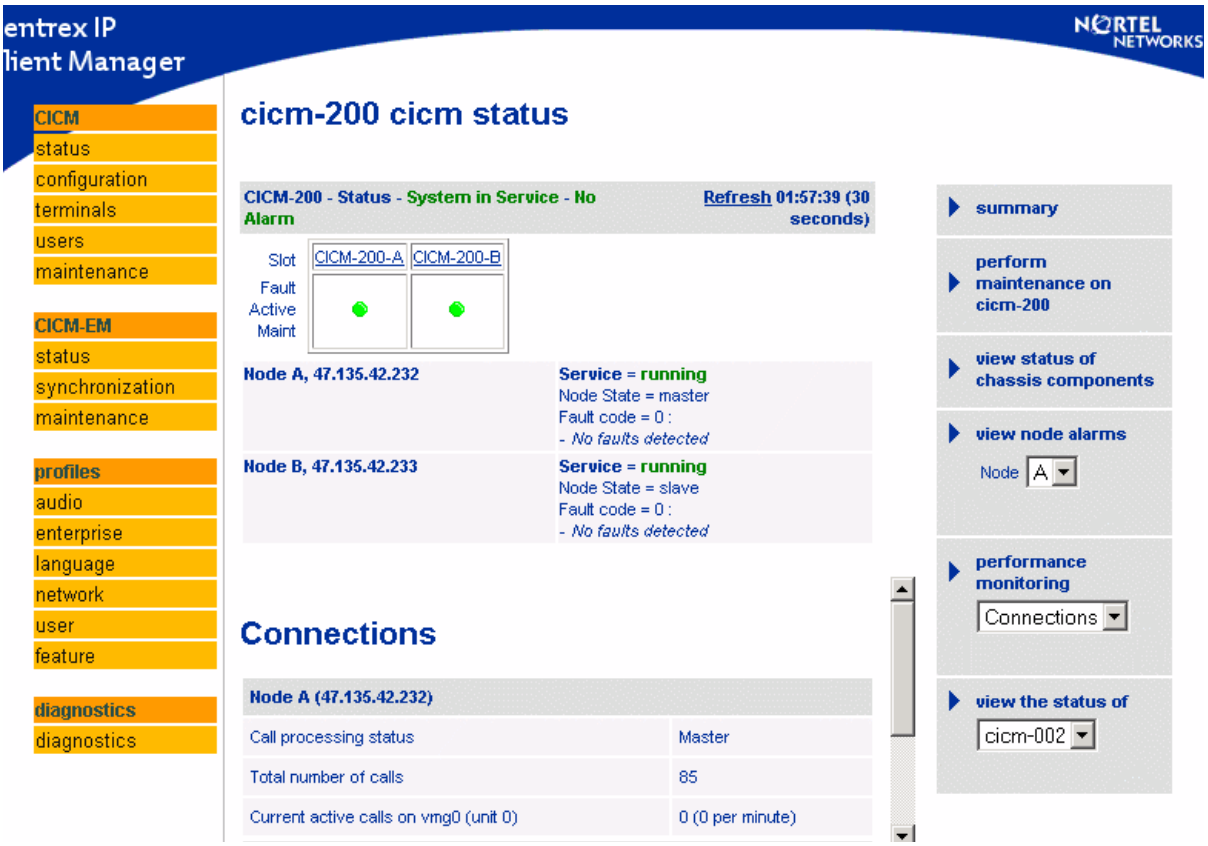
4 To view details of the chassis components, select the **view status of chassis components** text for each options on the right menu bar.

*Response: The **<cicm name> cicm status** page updates with the additional detail selected.*



5 For performance monitoring of connections or terminals, from the **<cicm_name> cicm status** page, select **Connections**, **Terminals**, or **Packets** from the drop-down menu in the **performance monitoring** option on the right menu, then click on the **performance monitoring** text.

*Response: the **<cicm_name> cicm status** page updates to display the information. The figure below displays connections information.*



6 This procedure is complete.

Add a CICM

Use this procedure to add a CICM to an Element Manager.

Procedure 13 Add a CICM

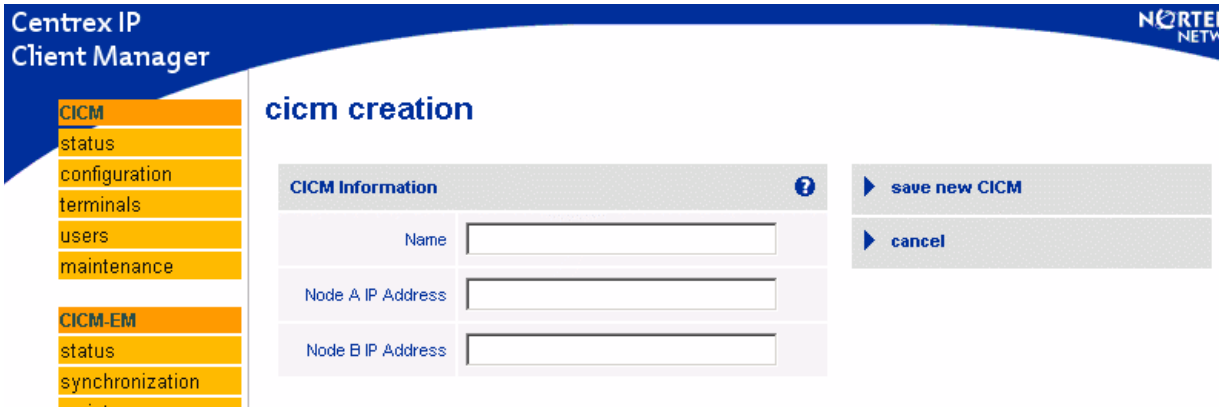
At the cicm home page

1 Click on the **Change the list of CICMs stored on the CICM-EM** text bar on the right navigation bar.

*Response: The **cicm modification** page opens.*

2 Click on the **add new CICM** option on the right.

*Response: The **CICM creation** page opens.*



3 Type the CICM name in the **Name** field,

Where

CICM name
refers to both sides of the CICM.

Then enter the IP addresses in the **node A IP address** and **node B IP address** fields,

Where

nodes
are the names of each side of a CICM.

Then click on the **save new CICM** option.

*Response: The **CICM creation** page displays the status of the creation, and confirms completion.*

4 This procedure is complete.

Delete a CICM

This procedure is used only under Nortel support direction to delete a CICM from the Element Manager.

Procedure 14 Delete a CICM

WARNING
Loss of all service
Completing this procedure will delete a CICM and result in loss of all CentrexIP service on that CICM.
This procedure shall only be performed under Nortel Support direction.

At the CICM Home page of the element manager web pages

1 Click on the **Change the list of CICMs stored in the CICM-EM** text in the menu on the right.

*Response: The **CICM modification** page opens.*

2 On the list of CICMs displayed, click the **delete** (trash can) icon for the CICM to be deleted.

Response: A status window displays the status of the deletion operation, and provides notification when complete.

3 This procedure is complete.

Edit CICM nodes

Use this procedure to edit the CICM nodes.

Procedure 15 Edit CICM nodes

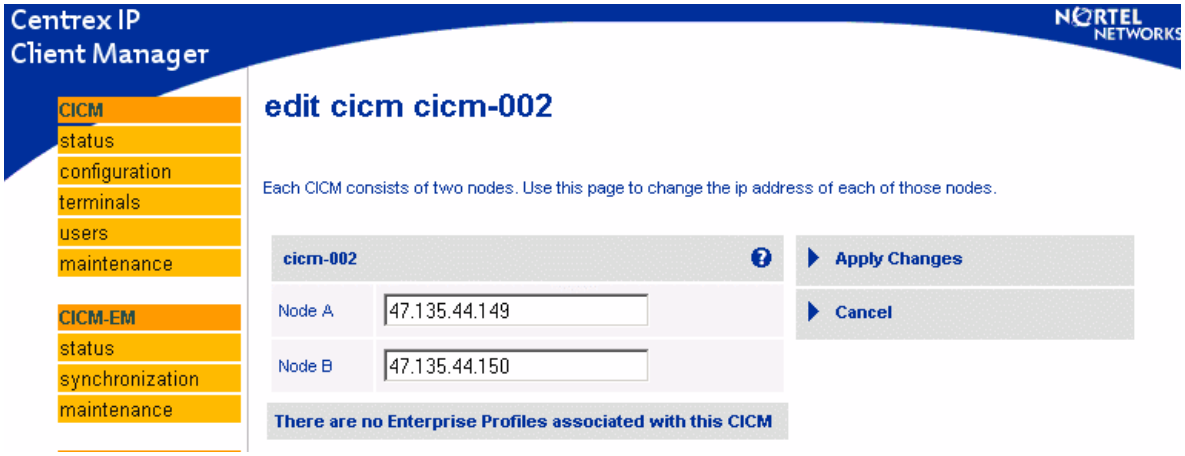
At the cicm home page of the element manager web pages

1 Click on the **Change the list of CICMs stored in the CICM-EM** text in the menu on the right.

*Response: The **cicm modification** page opens.*

2 On the list of CICMs displayed, click on the CICM to be changed.

*Response: The **edit cicm <cicm_name>** page opens.*



3 Enter the node IP address for Node A and/or Node B,

Note 1: The nodes of a CICM correspond to the IP address of each side of the CICM (Unit 0 = Node A, Unit 1 = Node B). The IP addresses must be exactly correct, as the CICM-EM accesses the CICM using the IP address.

Note 2: The CICM name is a reference only and is not used for communication with the CICM.

4 Click on the **Apply Changes** option on the right.

5 This procedure is complete.

View Element Manager synchronization

Use this procedure to view and check the synchronization between the Primary and Backup Element Managers.

Procedure 16 View Element Manager synchronization

At the cicm - element manager home page

1 Select **synchronization** from the **CICM-EM** section of the left navigation bar.

*Response: The **cicm - element manager synchronization** page opens.*

2 This procedure is complete.

View Language Profiles on a CICM

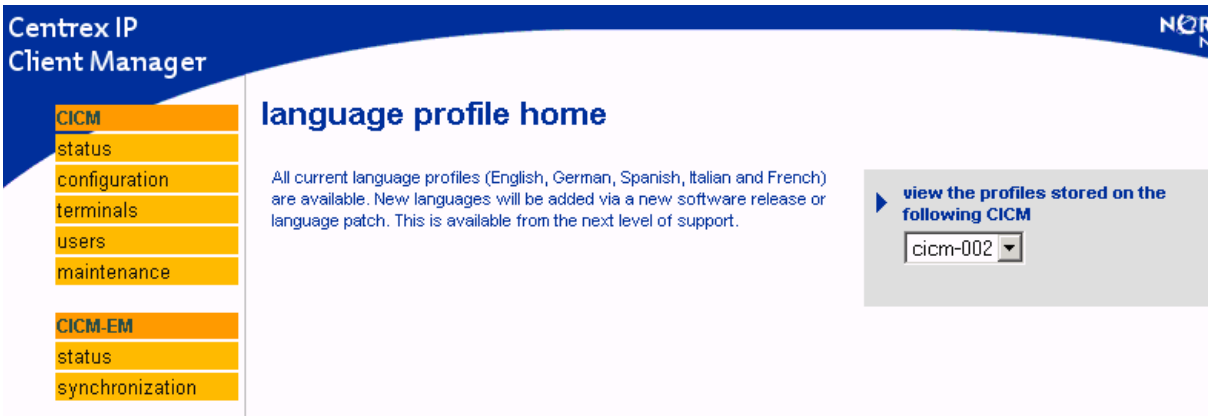
Use this procedure to view the Language Profiles applied to a CICM. Current Language Profiles available are English, German, Spanish, Italian, and French. New Language Profiles will be added via new software releases.

Procedure 17 View Language Profile on a CICM

At the cicm - element manager home page

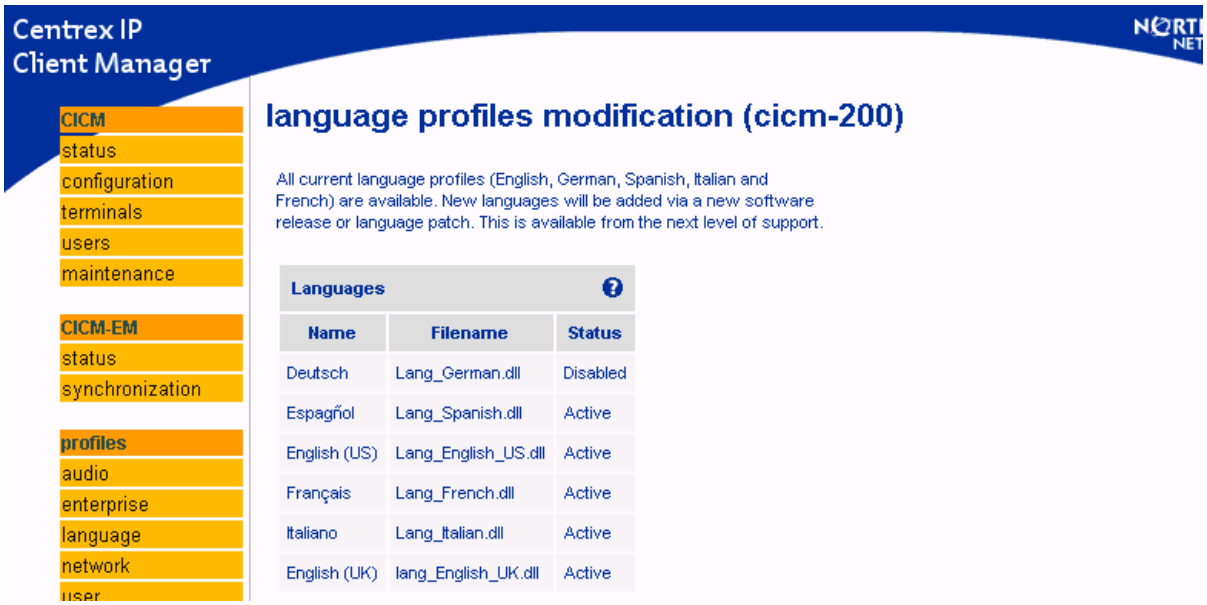
1 Select the **language** option form the **profiles** section of the left menu.

*Response: The **language profile home** page opens.*



2 To view the language profiles stored on a CICM, select the CICM from the drop-down menu, then click on the **view the profiles stored on the following CICM** option on the right menu.

*Response: The **language profiles modification (<cicm_name>)** page opens and displays the list of language profiles on the CICM.*



3 This procedure is complete.

Perform sanity check on a CICM

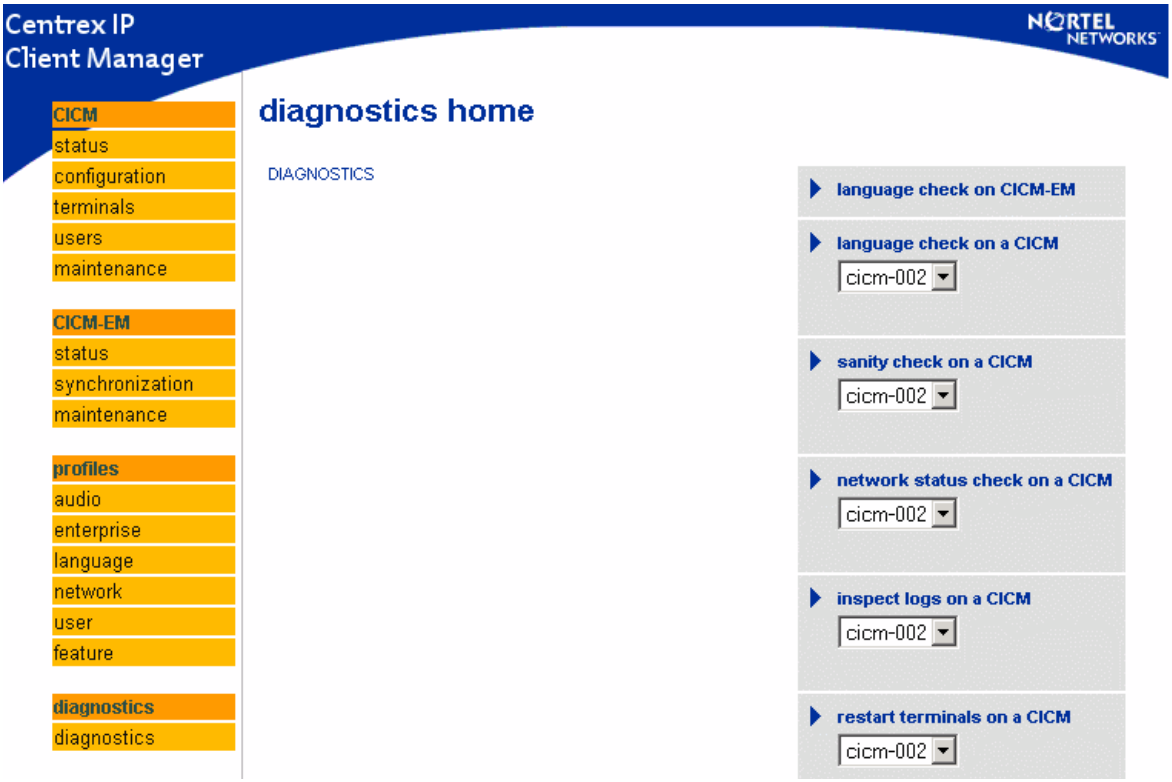
Use this procedure to perform a sanity check on a CICM. It will result in a display of the software release version.

Procedure 18 Perform sanity check on a CICM

At the cicm home page of the element manager web pages

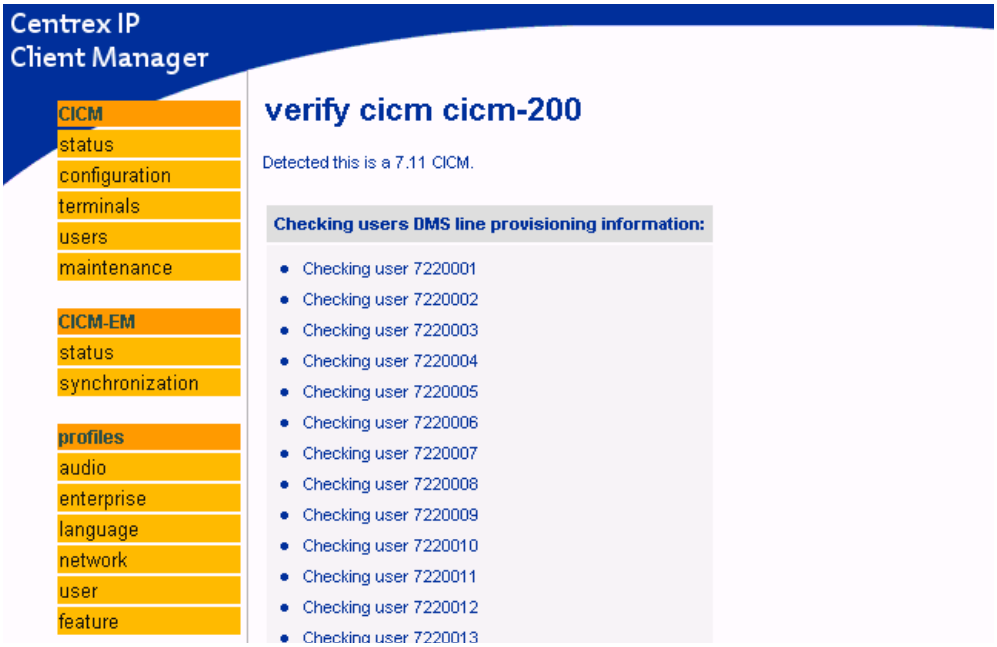
1 Select the **diagnostics** option on the left navigation bar.

*Response: The **diagnostics home** page opens.*



2 Choose the CICM from the drop-down menu in the **sanity check on a CICM** option on the right navigation bar, then click on the **sanity check on a CICM** text.

*Response: the **verify CICM <CICM name>** page opens and displays the results of the sanity check.*



3 This procedure is complete.

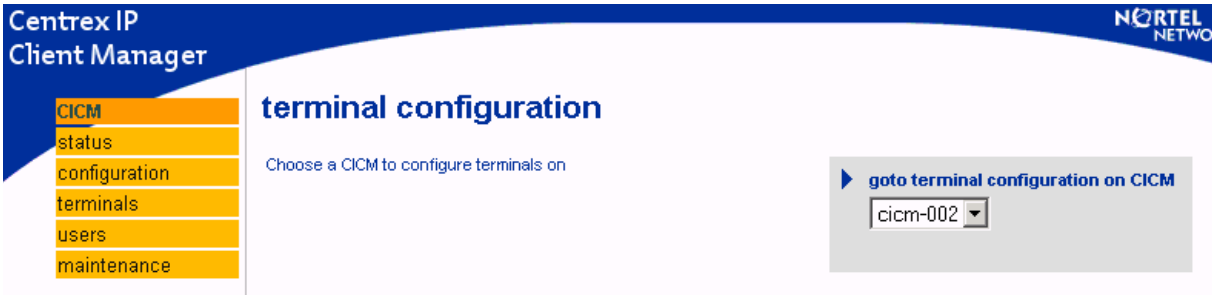
View terminal status
Use this procedure to view a terminal status

Procedure 19 View terminal status

At the CICM - element manager home page

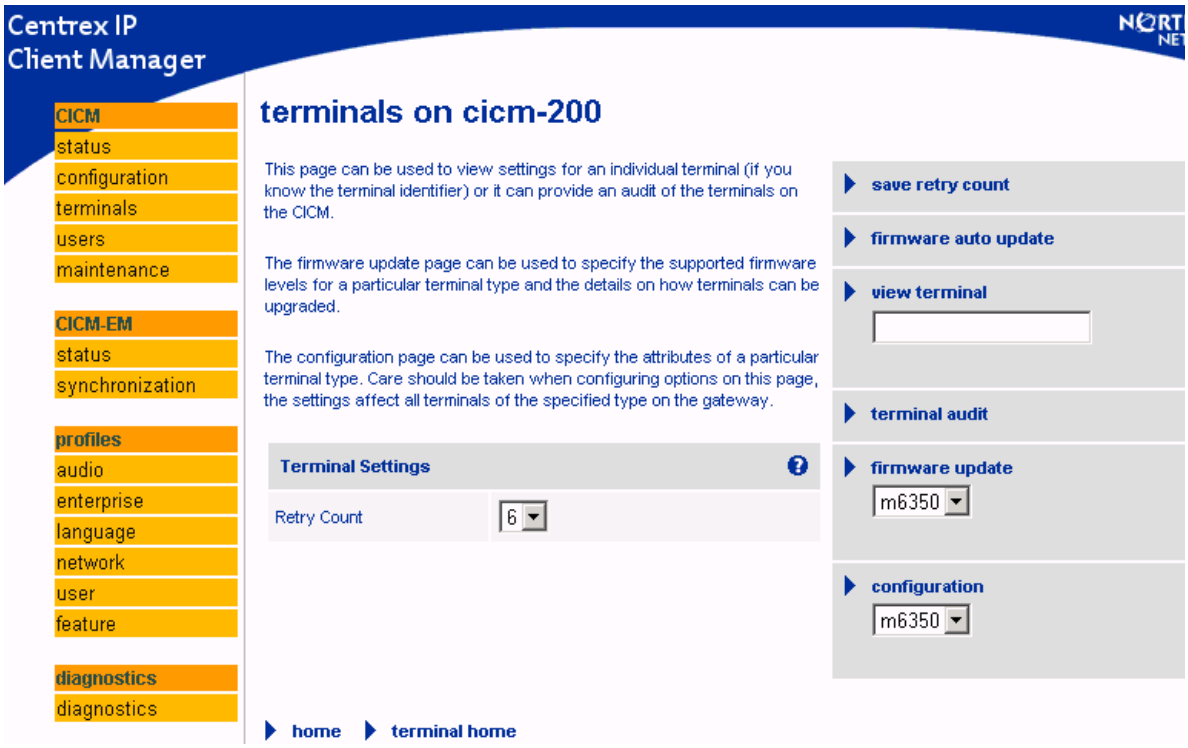
1 Select **terminals** from the left navigation bar.

*Response: The **terminal configuration** page opens.*



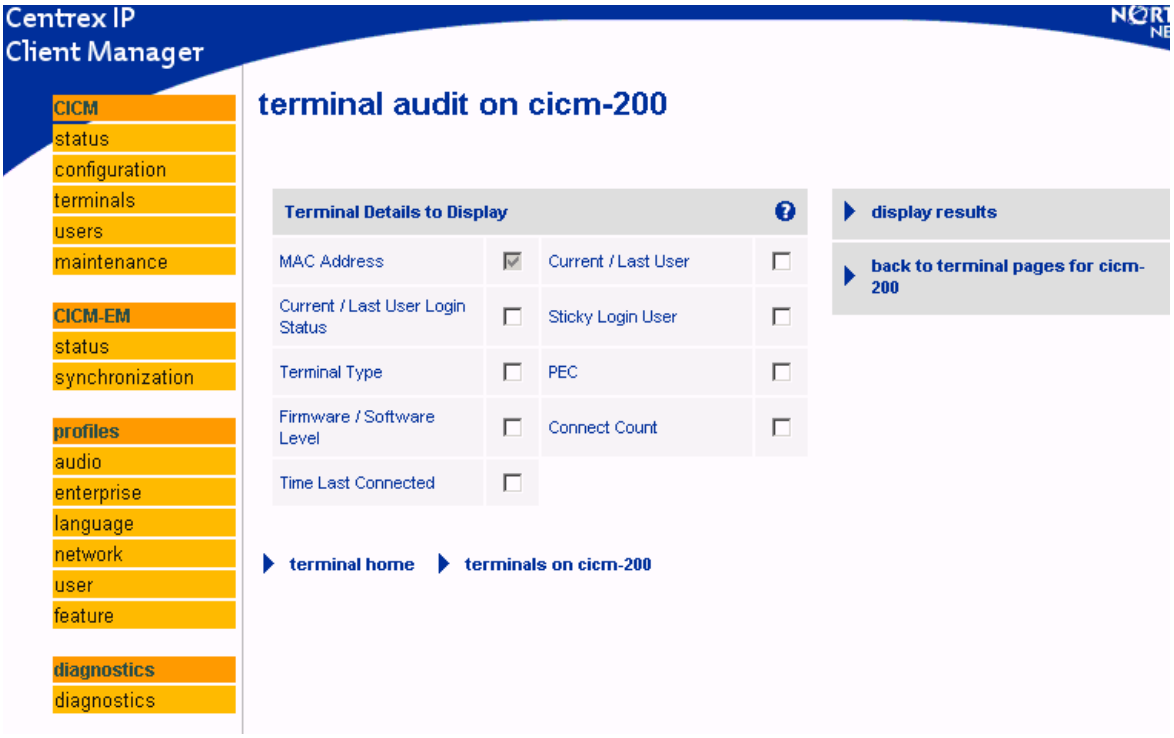
2 Select the CICM from the drop-down menu in the **go to terminal configuration on CICM** option on the right, then click on the **go to terminal configuration on CICM** text.

*Response: The **terminals on <CICM name>** page opens.*



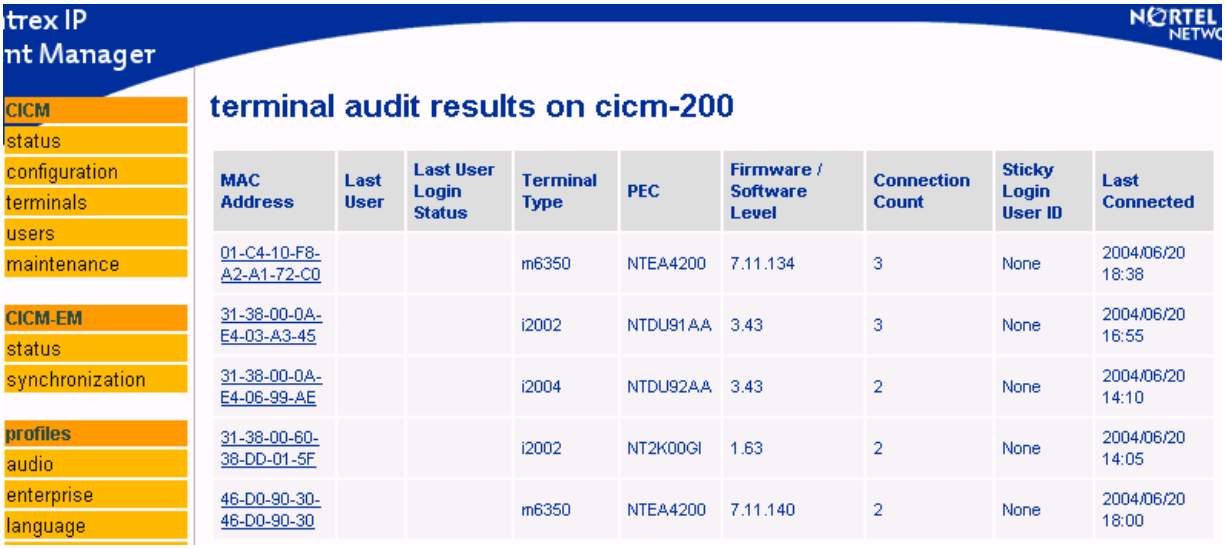
3 Click on the **terminal audit** option on the right menu bar.

*Response: The **terminal audit on <cicm_name>** page opens.*



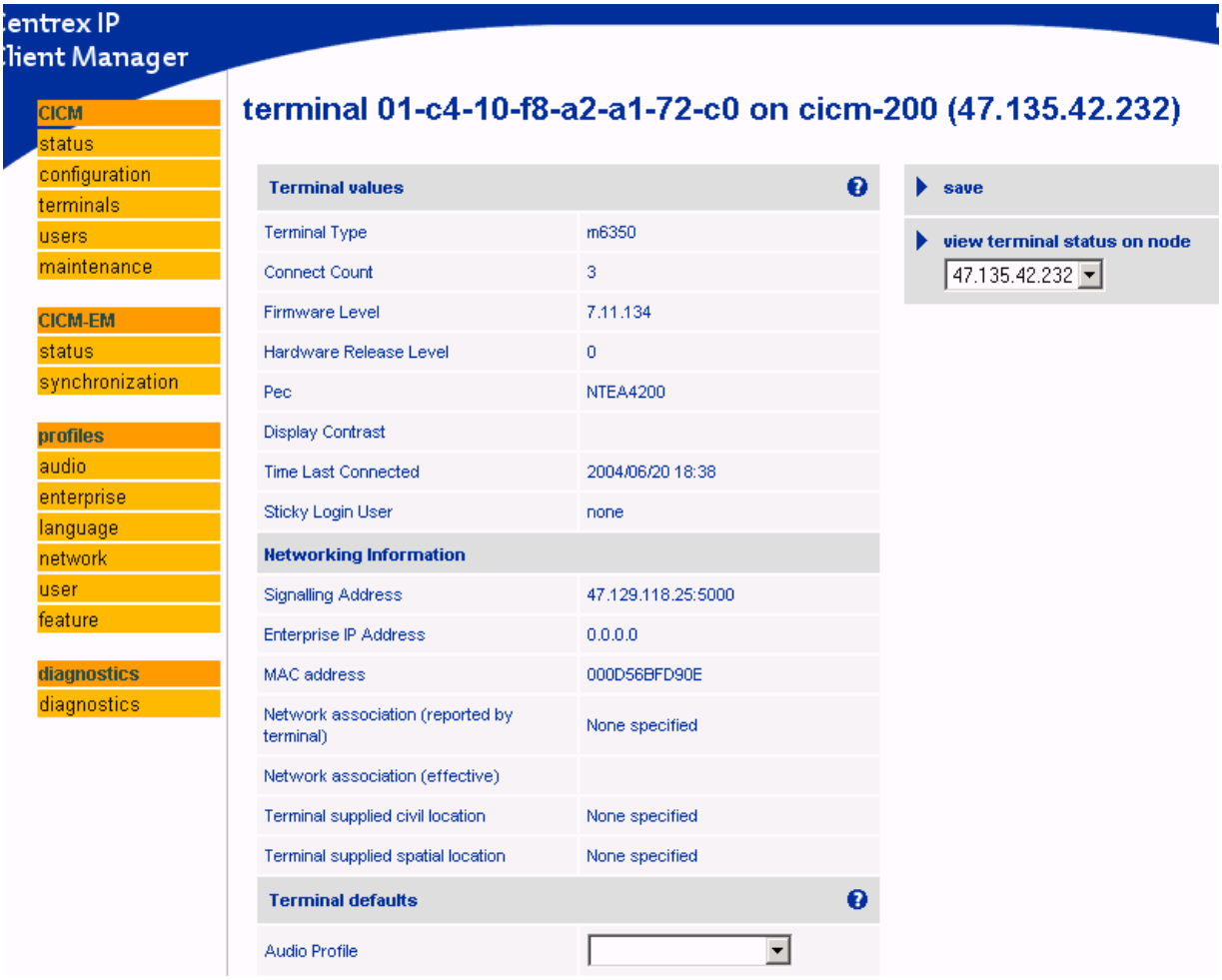
4 Select the terminal details to display in the audit by checking each box, then click on the **display results** option.

*Response: The **terminal audit results on <cicm_name>** page opens.*



5 To view terminal values, networking information, and terminal defaults for a specific terminal, click on the terminal ID (MAC Address) on the list.

*Response: The **terminal <name> on <cicm name> (<IP address>)** page opens.*



6 This procedure is complete.

View CICM information at the node level

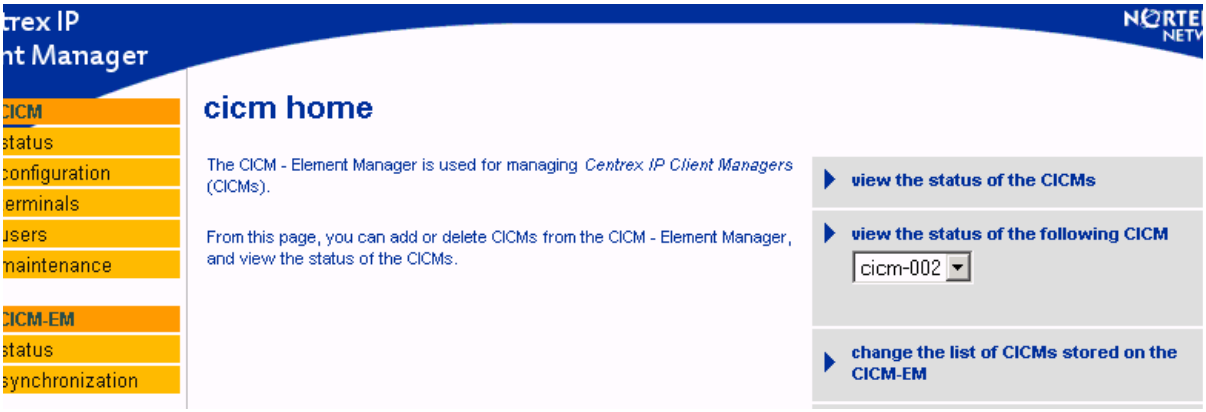
The Web Interface can be used to collect statistics about the number of calls that are handled by the CentrexIP International Gateway. These statistics are collected and displayed on a per-node basis.

Procedure 20 View CICM information at the node level

At the cicm - element manager home page

1 Select the **status** link from **CICM** section of the left navigation bar.

*Response: The **cicm home** page opens.*

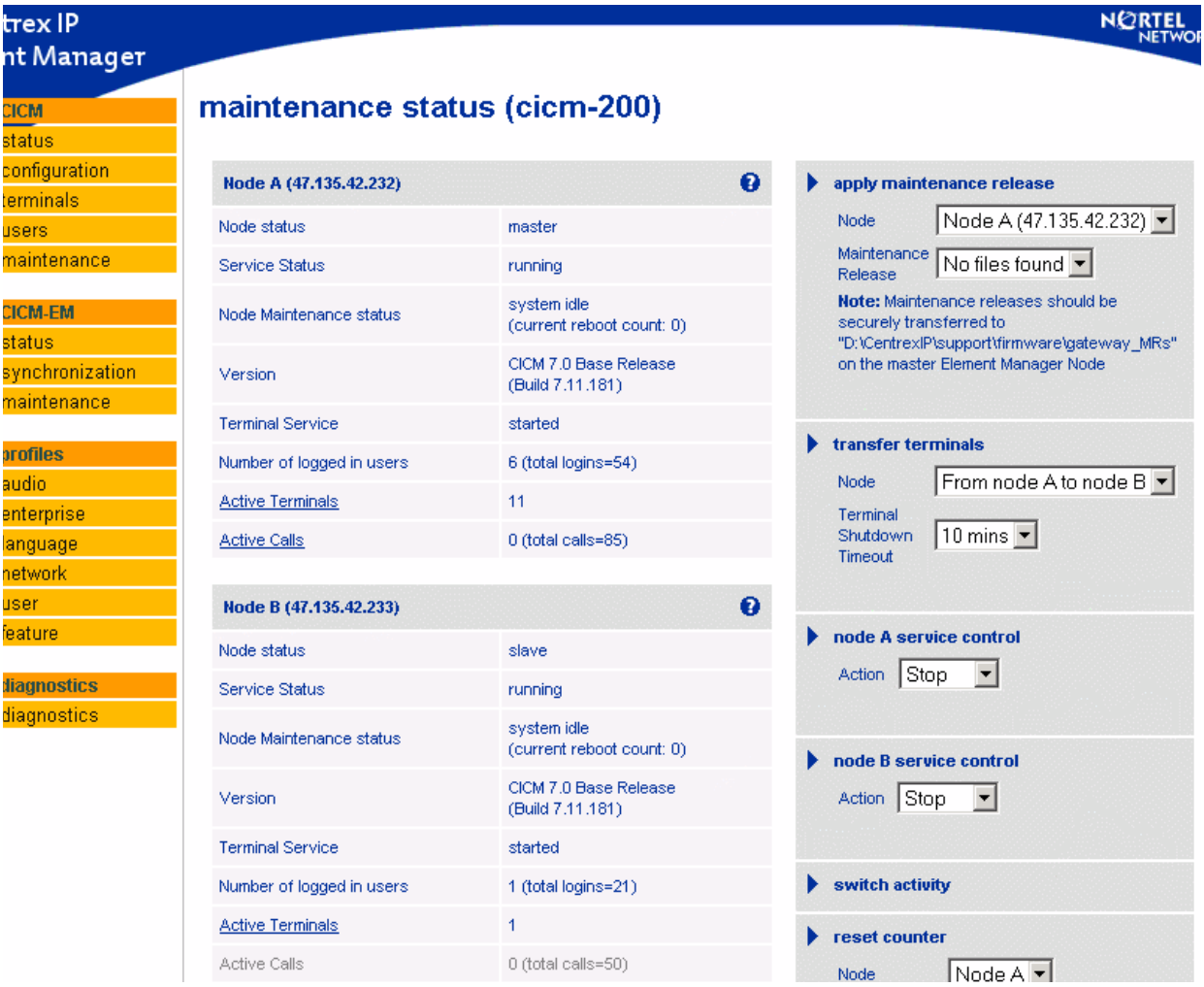


2 Select the CICM to be viewed from the drop-down menu on the **view the status of the following CICM** option on the right menu, then click on the **view the status of the following CICM** text.

*Response: The **<cicm_name> cicm status** page opens.*

3 Select the **perform maintenance on <cicm_name>** option on the right menu.

*Response: The **maintenance status <cicm_name>** page opens. Below is an example.*



4 This procedure is complete.

View the record of backup sets for a CICM

Use this procedure to view the record of backup sets (backup execution times) for a CICM.

Procedure 21 View the record of backup sets for a CICM

At the CICM home page of the Element Manager web pages

1 Select the cicm name from the drop-down menu in the **show the backup sets available for** option on the right menu, then click on the **show the backup sets available for** text.

*Response: The **<CICM name> backup sets on <cicm-em_name>** page opens and displays a table of backup sets for the CICM.*

2 This procedure is complete.

Perform a terminal handover

Use the following procedure to perform a controlled terminal handover. This procedure is performed to minimize service impact during upgrade or maintenance, by transferring service from one CICM node to its mate node.

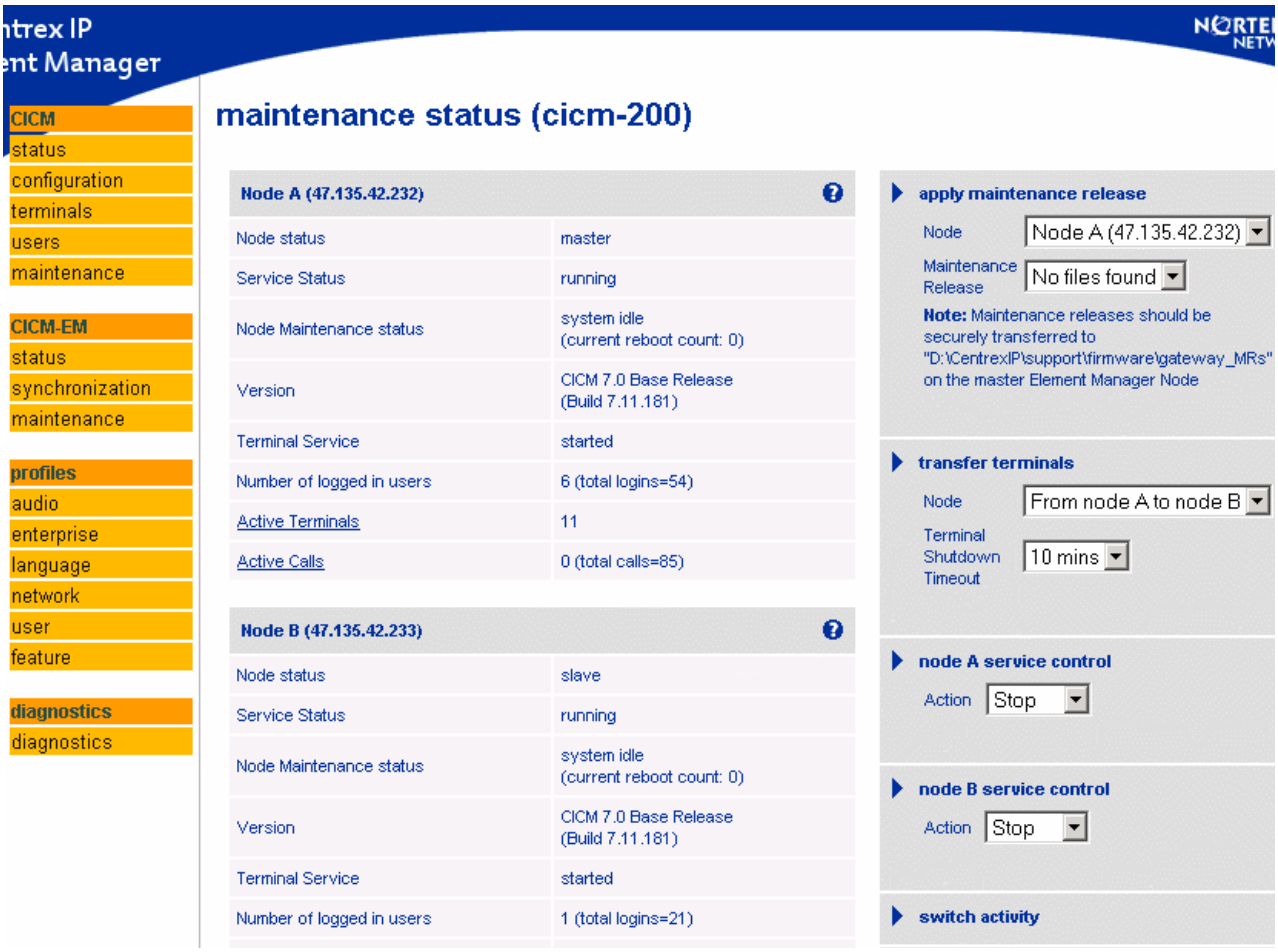
Terminal handovers are initiated and monitored from the CICM Element Manager.

Procedure 22 Perform a terminal handover

At the CICM-EM home page of the Element Manager web pages

1 Select maintenance from the CICM section of the left menu bar.

*Response: The **maintenance status (<cicm_name>)** page opens.*



2 View the terminal status on the **maintenance status (<cicm_name>)** page.

The following information relevant to terminal handover is displayed on this page:

- **Number of logged in users (**for each node)
- **Active terminals** This field shows the number of terminals that will suffer an outage if terminals are transferred from this node.
- **Terminal Service**
  This field shows the status of terminal service on each node. It is shown as **started** when terminal handover is not taking place. It is shown as **stopped** when the node is stopped and the terminal handover to the mate node has occurred.

  Note: Terminal handovers are not initiated on a node already shut down. If a shutdown has occurred, the terminals that were connected have already been automatically redirected to the mate node.

- **Transfer Terminals**
  This menu option is visible when both nodes are active and have connected terminal(s). This option is not shown when a node is already shut down and it is not possible to initiate a terminal transfer.
  - **Node** drop-down menu. Choose the nodes to transfer terminals from and to.
  - **Terminal Shutdown Timeout** drop-down menu. Select a time value between 5 and 60 minutes, by 5-minute intervals, to schedule the timeout. This is the time displayed to the user to give them time to complete active calls.

3 To initiate a terminal handover,
In the **transfer terminals** text box on the right menu:

a Choose the node to transfer from and to by selecting **From node A to node B** or **From node B to node A** from the drop-down menu,

b Then select the **terminal shutdown timeout** time from the drop-down menu,

c Then click on the **transfer terminals** text.

*Response: The **maintenance status <CICM name>** page updates with a prompt to confirm the terminal transfer.*

4 From the right menu, select **Confirm terminal transfer** OR **cancel** the transfer.

5 Verify that the terminal service has stopped.
From the **maintenance status (<cicm_name>)** page, monitor the progress of the transfer by selecting the **start auto refresh** or **refresh now** text boxes on the right menu.

*Response: The progress of the terminal handover taking place is shown. The **Terminal Service** field for the node displays the percentage of time elapsed since the handover commenced. **Note**: this is not the percentage of terminals.*

*When the terminal handover has completed, the state of the **terminal service** will be shown as **stopped**.*

6 (**OPTIONAL STEP**)
To abort a terminal handover in progress, click on the **abort terminal transfer on node <#>** on the **maintenance status <CICM name>** page's right menu.

7 Restart the terminal service (after upgrade or maintenance).
When the terminal handover is complete and the state of the terminal service is shown as **stopped**,
restart the terminal service on the node by selecting **restart** from the drop-down menu in the **Node A/B service control** menu option on the right.

Note 1: Stopping and starting the terminal service without restarting the rest of the system has no impact on call processing on either node, except that users on active calls when the terminal handover completes will be forcefully redirected to the mate node (where new calls may immediately begin).

Note 2: Some terminals cannot be transferred during a handover (e.g. older versions of the m6350 or terminals that are not configured correctly). These terminals are left connected to the node and are able to initiate new calls until the node is shut down. In this case the status of the terminal service is shown as "stop pending -- xxx terminals remaining"

*Response: When the terminal service has restarted, the status changes to **started**.*

8 This procedure is complete.

Start or stop the CICM Service
Stopping a node on the CICM may be necessary when upgrading or during routine maintenance such as changing cables. The procedures

to start or stop the CICM Service (the CICM nodes) are only used under Nortel Support direction, or according to documented procedures.

It is recommended to perform terminal handover prior to stopping or restarting the CICM service, in order to minimize service outage. Refer to the *Perform Terminal Handover* procedure above.

Procedure 23 Start the CICM Service

CAUTION
Loss of service
Using the ***Restart*** button can result in loss of service if terminal handover is not performed prior to this procedure.
This procedure shall only be performed under Nortel Support direction.

At the CICM-EM home page of the Element Manager web pages

1 Complete the *Perform Terminal Handover* procedure above, through step 5.

2 Click on the **status** option on the **CICMs** section of the left navigation bar.

*Response: The **cicm home** page opens*

3 Select the CICM to view from the drop-down list under the **view the status of the following CICM** text on the right menu bar, then click on the **view the status of the following CICM** text.

*Response: The **<cicm name> cicm status** page opens.*

4 Select **perform maintenance on <cicm_name>** option on the menu on the right.

*Response: The **maintenance status <cicm_name>** page opens*

5 In the **Node A Service Control** or **Node B Service Control** options on the right menu, select **Restart** from the drop-down menu for the applicable node.

Response: A confirmation prompt is displayed.

6 At the confirmation prompt, enter **Yes** to confirm restart (or **no** to decline).

Response:
With confirmation, the CICM resets and attempts to start the service on the node.

*The **Service Status** field updates to display the current service state. Possible states are: Stopped, Start Pending, Running, and Stop Pending.*

***Note:** The node will be in the state "Start Pending" while the hardware is being initialized.*

7 Monitor the node service status from the **maintenance status (<cicm name>)** page.

When the **service state** changes to **running** the service has correctly started.

8 Repeat this procedure to start the second node.

9 This procedure is complete.

Note: If the service fails to start, refer to the CS2K documentation *Remote Line concentrating Module Maintenance Guide* to bring the CentrexIP into service.

Procedure 24 Stop the CICM Service

WARNING
Loss of service
Completing this procedure to will result in loss of CentrexIP service on that node if terminal handover is not performed prior to this procedure.
This procedure shall only be performed under Nortel Support direction.

At the Element Manager home page

1 Complete the *Perform Terminal Handover* procedure above, through step 5.

2 Click on the **status** option of the **CICMs** section of the left navigation bar.

*Response: The **cicm home** page opens*

3 Select the CICM to view from the drop-down list on the right, then click on the **view the status of the following CICM** text.

*Response: The **<cicm_name> cicm status** page opens.*

4 On the **<cicm_name> cicm status** page, **select perform maintenance on <cicm_name>** option on the right menu.

*Response: The **maintenance status (<cicm_name>)** page opens*

5 On the **maintenance status (<cicm_name>)** page, select the **node A service control** or **node B service control** field. **Stop** should be displayed on the drop-down menu (if the node is running, the **Restart** option will be displayed). Click on the **node A service control** or **node B service control** option as applicable.

Response: The node begins the shutdown process, and the results of the action is displayed.

6 On the **maintenance status (<cicm_name>)** page, the Service Status field displays **stop pending** for the node selected. The node will be in the **Stop Pending** state while the hardware is shutting down.

7 Monitor the node service state from the **maintenance status (<cicm_name>)** page.

When the service state changes to **stopped** the service has correctly been shut down.

Note: Stopping the CentrexIP service will result in alarms being raised. To prevent these alarms, offline the CICM at the CS2K before powering down the CICM. Refer to the Nortel Networks documentation *Remote Line Concentrating Module Maintenance Guide*.

8 Repeat this procedure to stop the second node.

9 This procedure is complete.

Backup and restore process

In (I)SN07 release the CICM and CICM-EM have been enhanced to provide a Backup & Restore functionality for the CICM, by means of scheduled and on demand backups. This backup feature makes it possible to restore a CICM configuration that was backed up earlier.

This feature is useful in the following types of circumstances:

- When an unexpected system failure of one or both nodes occurs and it is necessary to re-image the CICM node(s) with a fresh load.
- When some parts of the CICM configuration are lost or accidentally deleted, the backup/restore feature makes it possible to avoid manually re-running all the configuration steps.

This feature provides the ability to perform a backup of the CICM data periodically or on demand. This functionality is provided under an individual application on the CICM, controlled by a scheduler and the CICM-EM.

The backup process stores all elements of the MIB Registry that are considered to be static data (i.e. non-volatile), and that are directly relevant to the configuration of the CICM.

Although there is no specific restriction on the time when backups can be executed, they can only be restored on CICM nodes mounting the exact same version of the CICM software.

The configuration data to be copied falls into the following categories:

- Global / Local Settings
- Hardware configuration
- Virtual Media Gateways
- Users configuration
  - Passwords
  - Locality preferences
  - Contacts
- Terminals
  - Locality preferences
  - Autologin preference
- Lines
  - Features
- Profiles (endpoint equipment profiles)
  - Global Profile Overrides stored on CICM

The MIB branches copied during the backup process are highlighted in the MIB hierarchy shown in the following figure.

Backups can be created at a regularly scheduled time, or on demand by an operator (e.g. prior to a CICM installation). On-demand backups are triggered via the CICM-EM, while scheduled backups will require no manual intervention once configured.

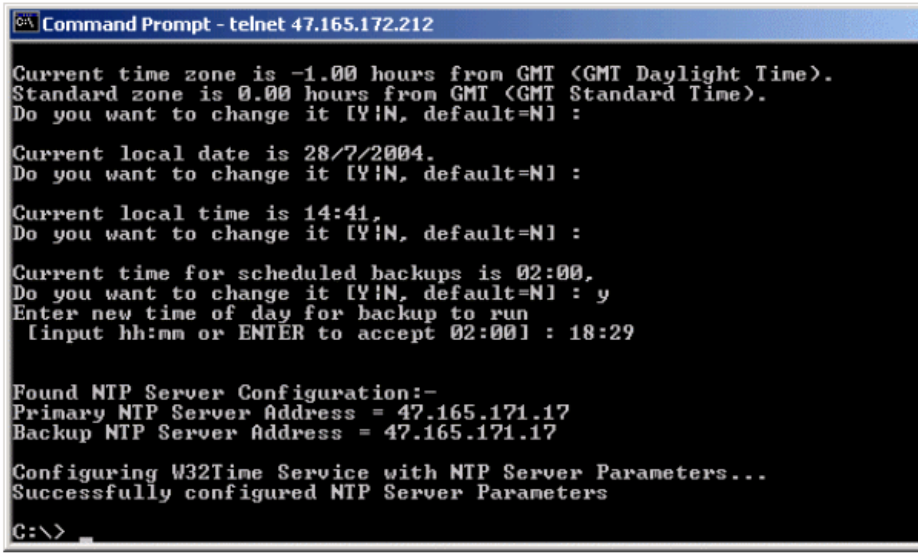
In both scheduled and on-demand backups, the result is an XML file, which is sent to the CICM-EM through anonymous FTP and stored locally in the following folder:
DC:\CentrexIP\support\backups\<cicm_node>,
where **<cicm_node>** is the full name of the node.

The node-specific folder is automatically created the first time a backup (of either kind) is run for that node. Although both backups are designed to occupy a limited amount of disk space on the CICM-EM, it is entirely up to the administrator to actually manage the files, for example by moving them periodically to a separate secure location.

Scheduled Backups

Scheduled backups are automatically run on a daily basis by each CICM node and require no further intervention by the operator once they have been successfully set up during preboot.

The **time** portion of **preboot** (also accessible by typing **preboot time /interactive**) has been expanded to prompt for a base time for scheduled backups, expressed in hours and minutes. The default value for the base time is 2AM. The command line interface is illustrated in the following figure:

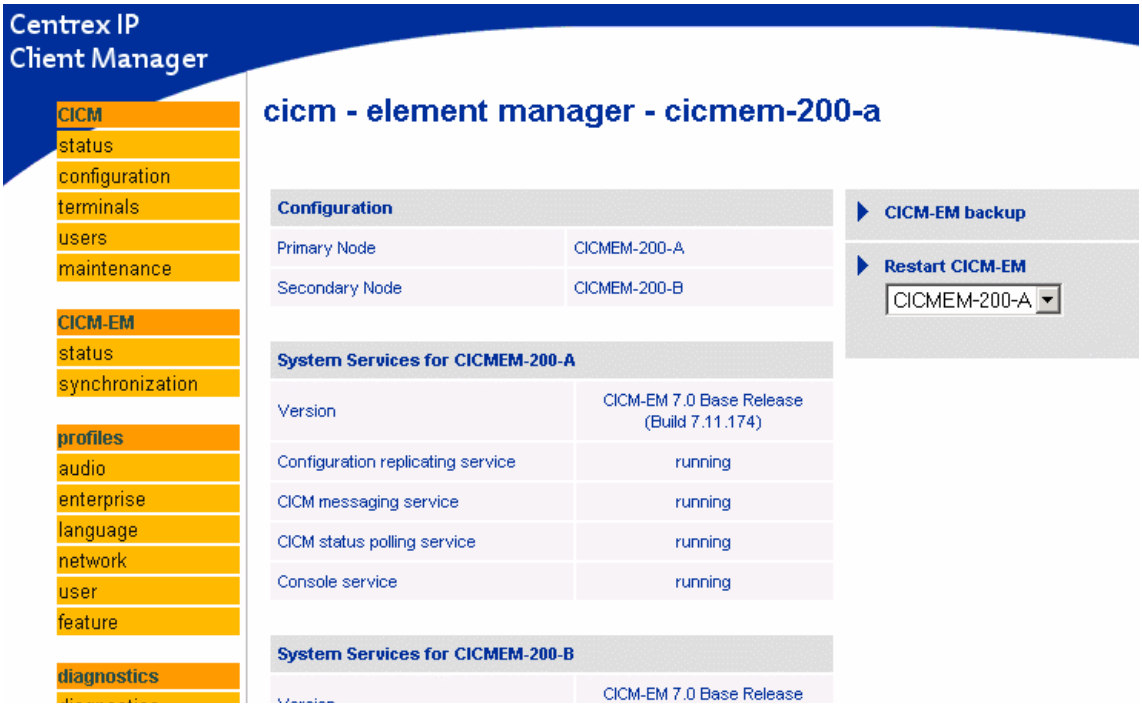


Once the base time has been chosen or the default value confirmed, a new scheduled job is allocated on the CICM to perform the actual backup and then FTP the result to the CICM-EM at the specified time, as can be seen in the figure above. The backup job is designed to send the XML file to the IP address of the Primary and Backup Element Managers (PEM, BEM), alternating between them on a daily basis to ensure a balanced usage of their disk space.
The fixed name for the backup file is
backupconfig_<day>.xml
where **<day>** is the day of the month (e.g. **backupconfig_25.xml**). As backup files are automatically overwritten, this naming convention ensures that the PEM / BEM has to store only a limited set of automatic backup files (up to a maximum of 31) for any CICM node it manages.

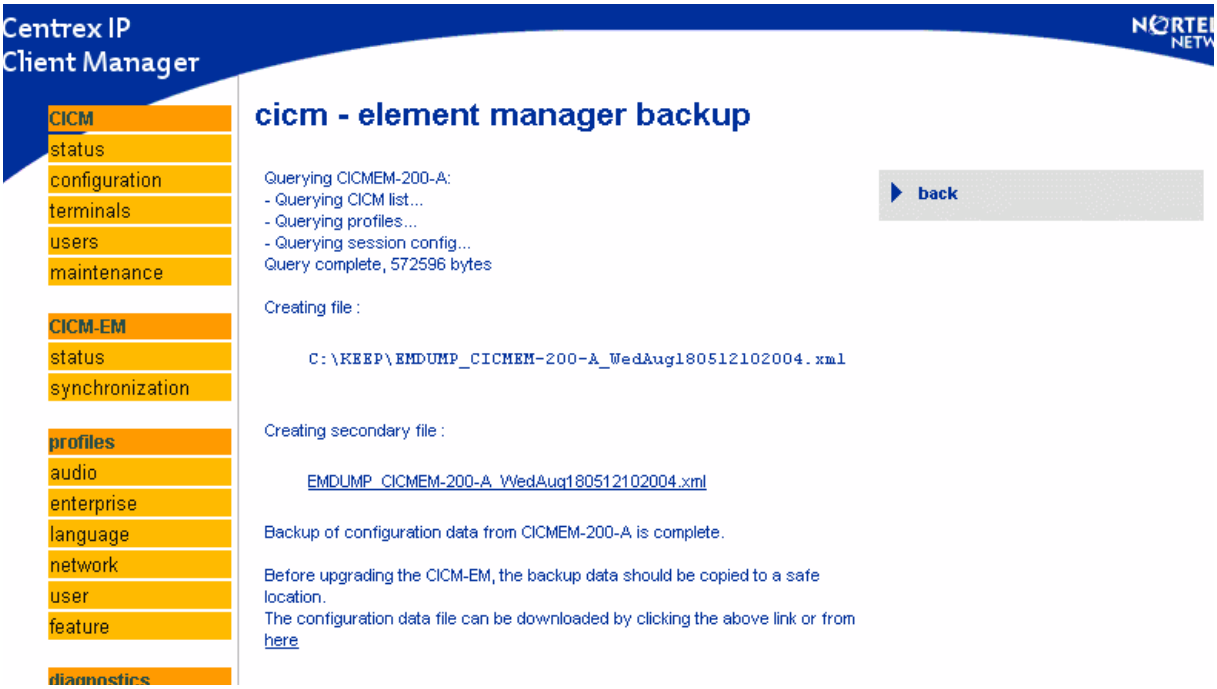
Scheduled backups can be turned off, if necessary. By running the **at** command on the CICM command line, the ID associated with the scheduled job will be output, just as it is automatically done by preboot. Then the following command is entered:
At <task_id> /delete
where **<task_id>** is the ID previously identified.

On demand backups

On-demand backups can be initiated at any time from any CICM-EM that manages the given CICM node. It is not necessary that the CICM-EM be the PEM or the BEM, just as for scheduled backups. The backup/restore functionality is accessed through the **CICM-EM backup** button, as illustrated in the following figure.



This backup action results in he backup page shown in the following figure.



Once either node has been chosen, a task is run on that CICM node to carry out the backup and FTP the resulting XML file to the CICM-EM, which normally takes a few seconds, depending on the size of the MIB itself. The fixed name for the backup file is:
backupconfig_<day>_em.xml
where **<day>** is the day of the month (e.g. **backupconfig_25_em.xml5**). As backup files are automatically overwritten, this naming convention ensures that the CICM-EM has to store only a limited set of automatic backup files (up to a maximum of 31) for any CICM node it manages, despite the fact that on-demand backups can be triggered an unlimited number of times each day.

Although the backup files are stored in the same directory as the scheduled backups, the naming convention ensures there is no overlap between them. However, it is up to the administrator to make sure that the backup file for a given day is saved to a different location before it is automatically replaced, which happens in the event of another backup being triggered on the same day, or on the same day of a later month.

Restore

Although there is no specific restriction on the time when backups can be executed (whether they are scheduled or on demand), they can only

be restored on CICM nodes mounting the exact same version of the CICM software, and specifically only in the two following scenarios:

- Upon accidental loss or deletion of portions of the MIB (on a pair of fully configured CICM nodes)
- Upon fresh re-image of both CICM nodes, after having fully run preboot on one node.

This means that the use of the restore functionality is NOT supported and hence strongly discouraged in the following scenarios:

- Across software upgrades within the same product series (e.g. 7.11 to 7.12)
- Software upgrades across two different product series (e.g. 7.11 to Series 8)

A version check is built into the restore facility purposely to prevent accidental usage of a backup file outside the scope intended by this feature (and specifically across any kind of software upgrade).

Moreover, this functionality does not provide direct support for automated restores of CICM backups. This means that, in order to apply any previously saved configuration, the operator must connect directly to both the CICM-EM and the CICM, as the CICM-EM itself will not include a restore interface.

Specifically, the following two steps must be performed:

- Locate the applicable XML file on the CICM-EM and copy or FTP it to the CICM node
- Telnet to the CICM and run the following command:
  cxiprestore <xml_backup_file> /norestart <xml_backup_file>
  or
  cxiprestore <xml_backup_file> /restart <xml_backup_file>
  where **<xml_backup_file>** is the configuration file,
  /norestart is specified to restore on fully configured CICM nodes, and **/restart** is used for freshly re-imaged CICM nodes (following completion of preboot).

In the case the **/restart** option is chosen, the main CICM services will be stopped prior to re-applying the actual data, to be restarted upon completion of the restore operation. Conversely, the **/norestart** option has no impact on the services running at the time the restore is performed.

Note 1: For the restore procedure to succeed on freshly re-imaged CICM nodes (i.e. when using the **/restart** option), the node being

restored must be the only one currently running, which means it must be the Master node of the pair, with no Slave presently connected to the network or switched on. This is essential to ensure that the newly restored MIB content will not be accidentally deleted by a premature synchronisation with the mate node, and that it will be properly replicated across following the re-imaging of the Slave at a later stage.

Note 2: When using the **/restart** option, the restart of the main CICM services will mean that all networks adapters for the node will be re-initialised, and as a result the Telnet connection will be dropped.

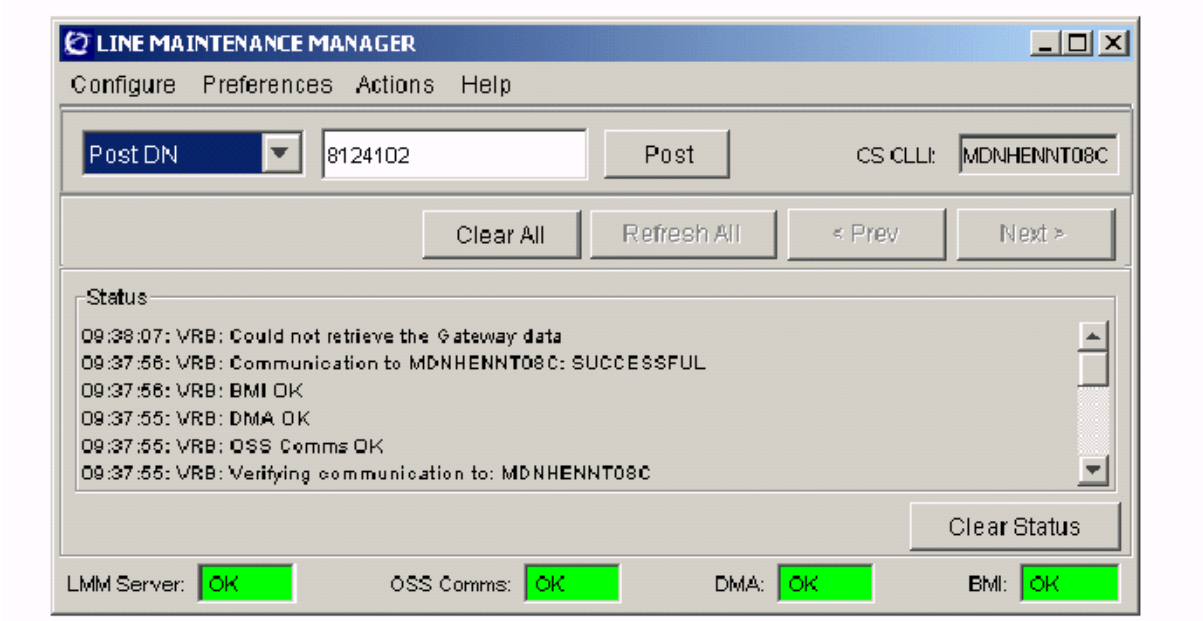
Note 3: Although there are other command line options available for the **cxiprestore** tool, they are not documented here as they are not relevant to this activity, and as such their usage should be avoided.

Note 4: A version check is built into the restore facility, purposely to prevent accidental usage of a backup file outside the scope intended by this feature (and specifically across any kind of software upgrade).

Line Maintenance Manager

The Line Maintenance Manager (LMM) is a GUI provided by the CS2000 Management Server to replace/emulate the functionality provided by the MAPCI tool on the CS2000 Core.

Example: Line Maintenance Manager



The LMM provides for the following commands:

- BSY
- RTS
- FRLS
- INB

The LMM also provides the functionality to post a gateway in addition to individual lines.