Managing System and Application Passwords on an ICS 7750

Document ID: 43005

Introduction

This document helps you manage all of the passwords for the hardware, operating system, and applications that run in a Cisco Integrated Communications System (ICS) 7750. It covers how to change your current password as well as how to recover from situations where the password is lost.

Note: It is not possible to recover from a lost password for the Windows 2000 Server Local Administrator Account on a Systems Processing Engine (SPE). You need to re−image the SPE, reinstall the applications, and restore the application data.

These accounts and passwords are used on a ICS 7750 that has Cisco Unity, Cisco CallManager, and IPCC Express installed.

- Windows 2000 Server Administrator account.
- System switch processor (SSP), analog station interface (ASI), and multiservice route processor (MRP) cards.

    - ♦ Login password (VTY 0 4).
    - ♦ Enable secret password.
    - ♦ Console password.
- ICSConfig Administrator account.

  Note: Uses Windows Administrator account.
- ICS Admin account (for ICS Admin utility).
- Cisco Unity, Cisco CallManager, and System Manager.

    - ♦ SQL System Administrator (SA) database password.
- Cisco CallManager Administrator account.

  Note: Uses Windows Administrator account.
- IPCC Express (CRS/CRA 3.0) Administrator account.
- Cisco Unity Administrator account. (This can be a separate account. You can use a Windows Administrator account.)
- SNMP Community Strings.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- ICS 7750 systems running ICS version 2.5 or later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

ICSConfig Utility

The ICSConfig utility is used to manage the passwords for:

- The ICS System Administration account.
- The Windows 2000 Server Administration user account on SPEs.
- The login and enable passwords for the SSP as well as any MRPs installed in the chassis.
- Simple Network Management Protocol (SNMP) community string.

If you want to change any, or all of these password continue with these steps.

Caution: Do not change any passwords on any card in the chassis using an interface to the card itself

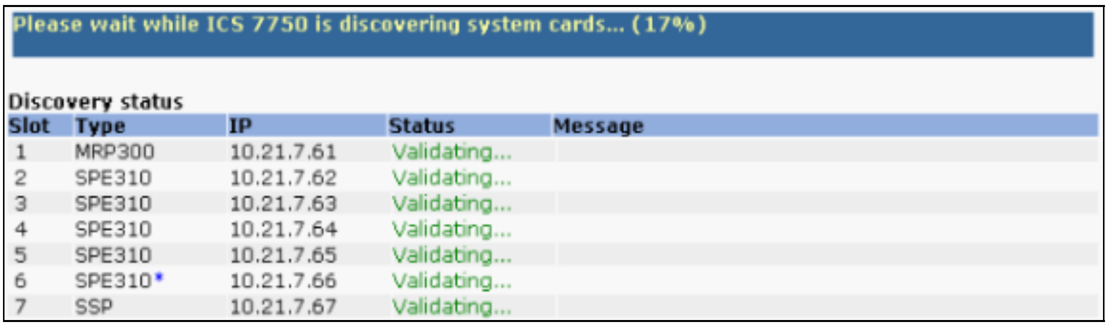
unless you are replacing a card and you need to configure it with the password that is configured for the card

in System Manager. Setting a password to any value that is different from the value stored in the System Manager Database causes the ICS Discovery Process to fail.

1. Start the **ICSConfig utility**.

   This utility is accessible via a browser at URL **http://sm−spe−ip−address/icsconfig** where *sm−spe−ip−address* is the IP address on the SPE running the ICS System Manager software.

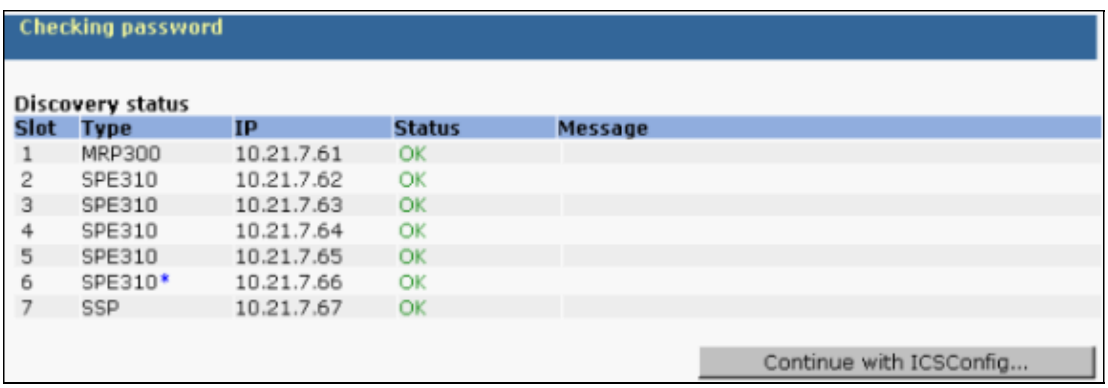
   Note: You may substitute the Domain Name System (DNS) name for this SPE if you have DNS configured.

   Please wait while ICS 7750 is discovering system cards... (17%)

   Discovery status

Slot	Type	IP	Status	Message
1	MRP300	10.21.7.61	Validating...	
2	SPE310	10.21.7.62	Validating...	
3	SPE310	10.21.7.63	Validating...	
4	SPE310	10.21.7.64	Validating...	
5	SPE310	10.21.7.65	Validating...	
6	SPE310*	10.21.7.66	Validating...	
7	SSP	10.21.7.67	Validating...	
2. Once the discovery process is complete. a screen similar to this appears. Click **Continue with ICSConfig**.

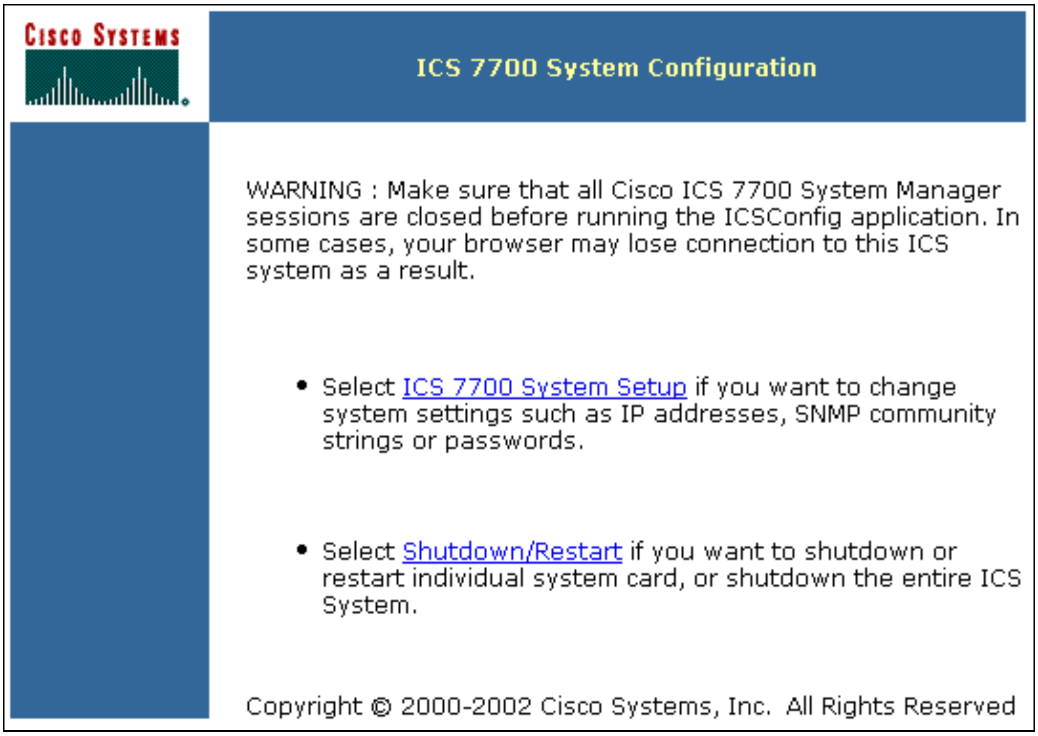
   Checking password

   Discovery status

Slot	Type	IP	Status	Message
1	MRP300	10.21.7.61	OK	
2	SPE310	10.21.7.62	OK	
3	SPE310	10.21.7.63	OK	
4	SPE310	10.21.7.64	OK	
5	SPE310	10.21.7.65	OK	
6	SPE310*	10.21.7.66	OK	
7	SSP	10.21.7.67	OK	

   Continue with ICSConfig...
3. When the ICS 7750 System Configuration screen appears, click **ICS 7700 System Setup**.

   If you do not see this screen because the discovery process failed, refer to the Troubleshoot the Discovery Process section of this document.



4. The configuration menu for all of the ICS 7750 settings appear. A subsection of the options is shown in this image.

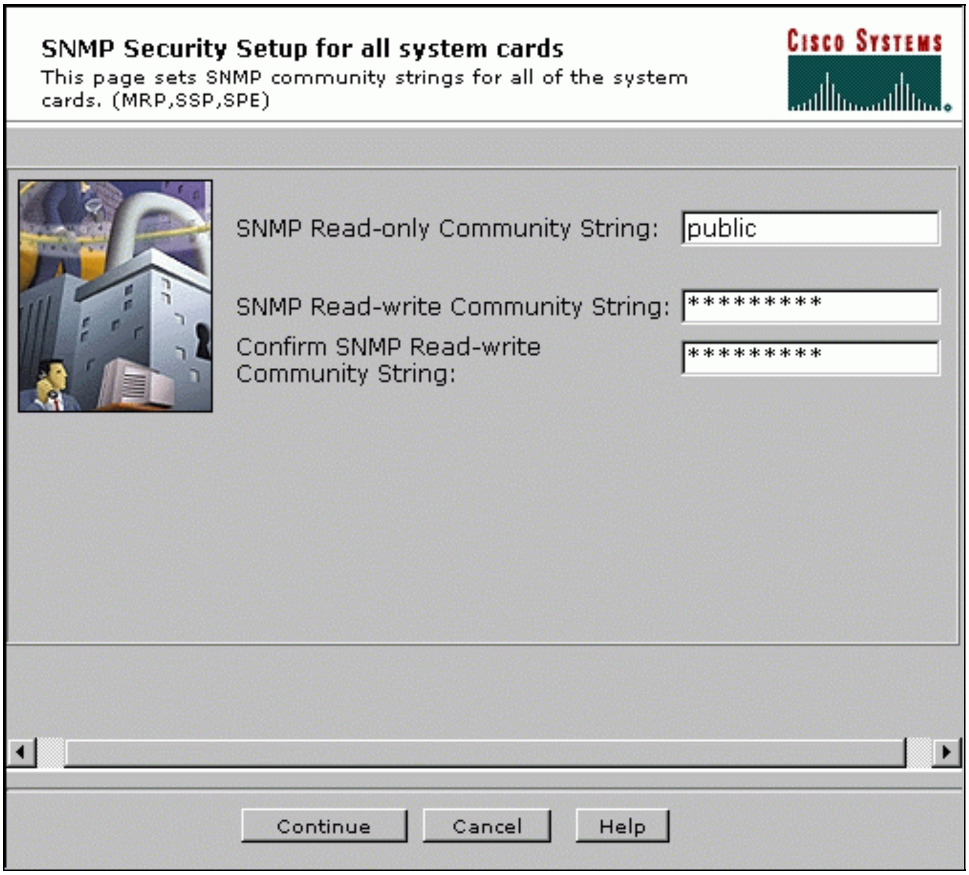
Security Setup for all IOS-based Cards		
Field Name	**Old Value**	**New Value**
Login Password:	******	******
Enable Password:	******	******
SNMP Security Setup for all system cards		
Field Name	**Old Value**	**New Value**
SNMP Read-only Community String:	public	public
SNMP Read-write Community String:	******	******
Security Setup for SPE Cards		
Field Name	**Old Value**	**New Value**
SPE Administrator Password:	******	******
Security Setup for ICS 7700 System		
Field Name	**Old Value**	**New Value**
ICS Super Admin Password:	******	******

5. If you want to change the passwords for the IOS based cards (SSP and MRPs), select **Security Setup for all IOS−based Cards**. Otherwise, proceed with **step 8**.

6. Change the passwords to their new values and click **Continue**.
7. Proceed to **step 8**.

   Note: If you decide not to save your changes you can select the **Cancel** option. This attempts to cancel the entire configuration task, not just the current section you are working on. If you wish to select the Cancel option, see the Cancel Your Changes section of this document.
8. If you want to change the SNMP settings, select **SNMP Security Setup for all system cards**. Otherwise, proceed to **step 10**.
9. Change the password to its new value, click **Continue**, and proceed to **step 10**.

   Note: If you want to cancel your changes, see the Cancel Your Changes section.



10. If you want to change the Windows 2000 Server Administrator Account passwords on the SPEs, select **Security Setup for SPE Cards**. Otherwise, proceed to **step 12**.

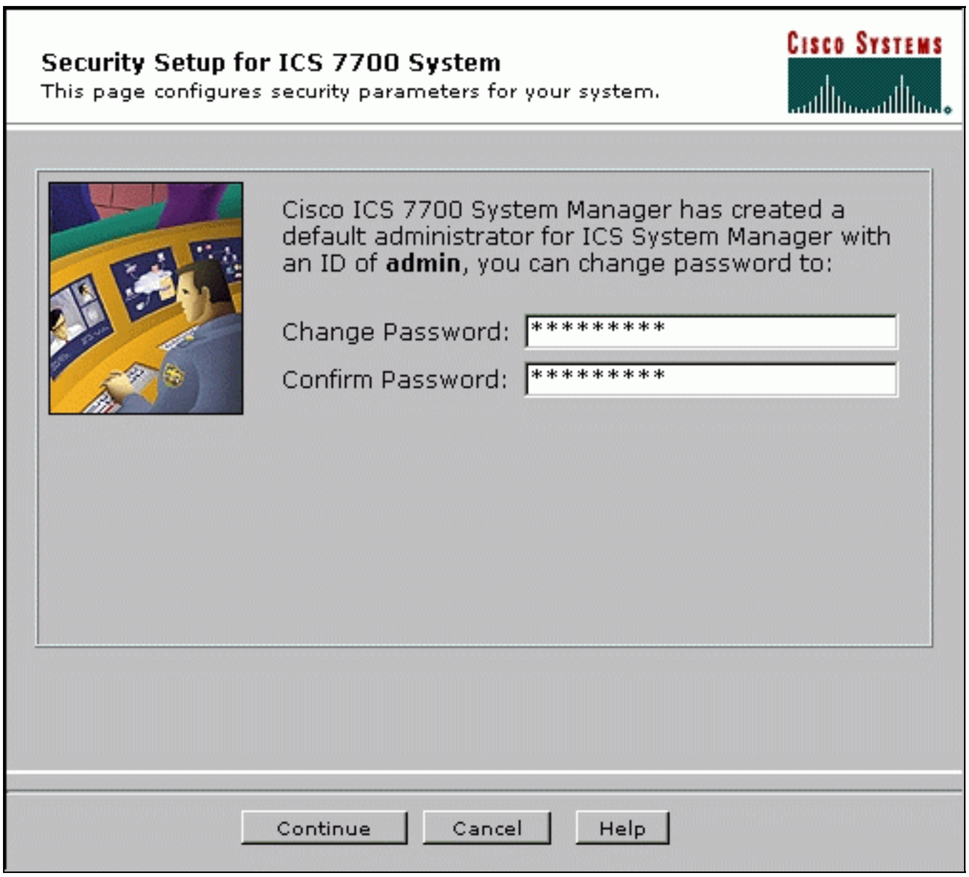
11. Change the password to its new value, click **Continue**, and proceed to **step 12**.

Note: If you want to cancel your changes, see the Cancel Your Changes section.

Caution: Do not lose this password. This is the only password in an ICS 7750 system that is unrecoverable if lost. If you lose this password you need to re−image every SPE in the chassis. Unless you have accounts on the SPEs that allow you to login and create backups prior to re−imaging using an account other than the Windows 2000 Server Local Administrator account, you need to restore the data for each SPE using the most recent backups.

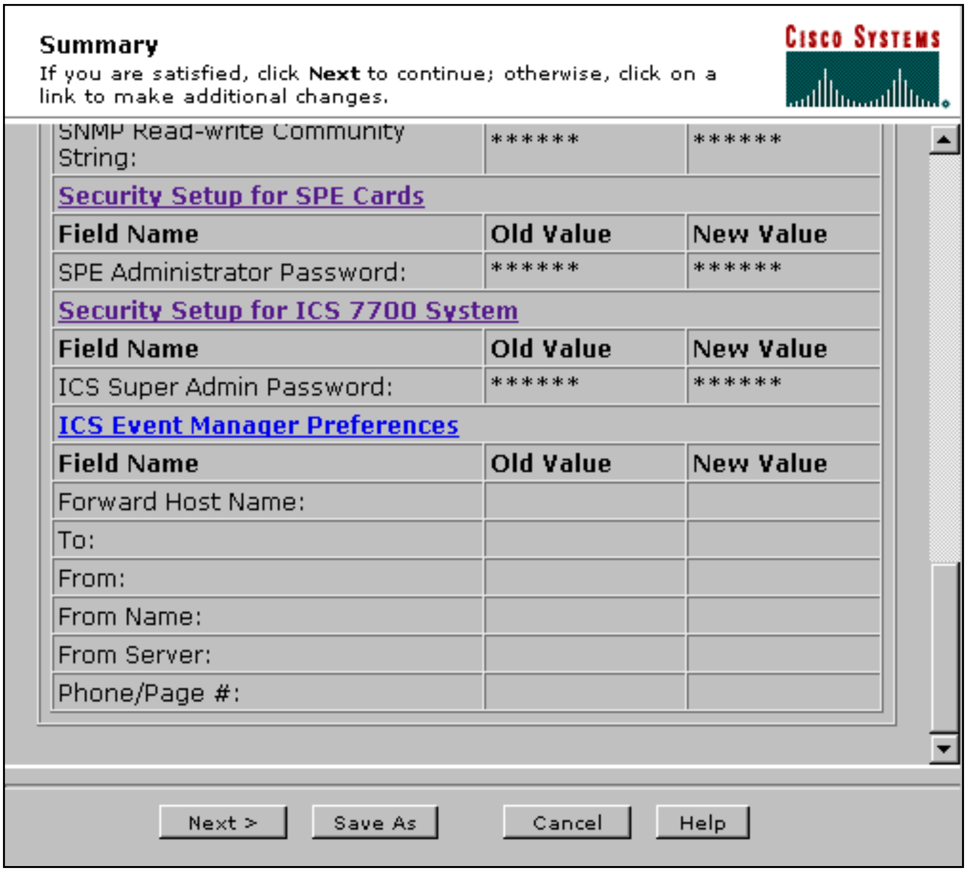
12. If you want to change the password for the ICS 7750 Admin account that is used to log into the ICS 7750 Administration page (http://sm−spe−ip−address/ics), select **Security Setup for ICS 7700 System**. Otherwise, proceed to **step 14**.
13. Change the password to its new value, click **Continue** and proceed to **step 14**.

    Note: If you want to cancel your changes, see the Cancel Your Changes section.



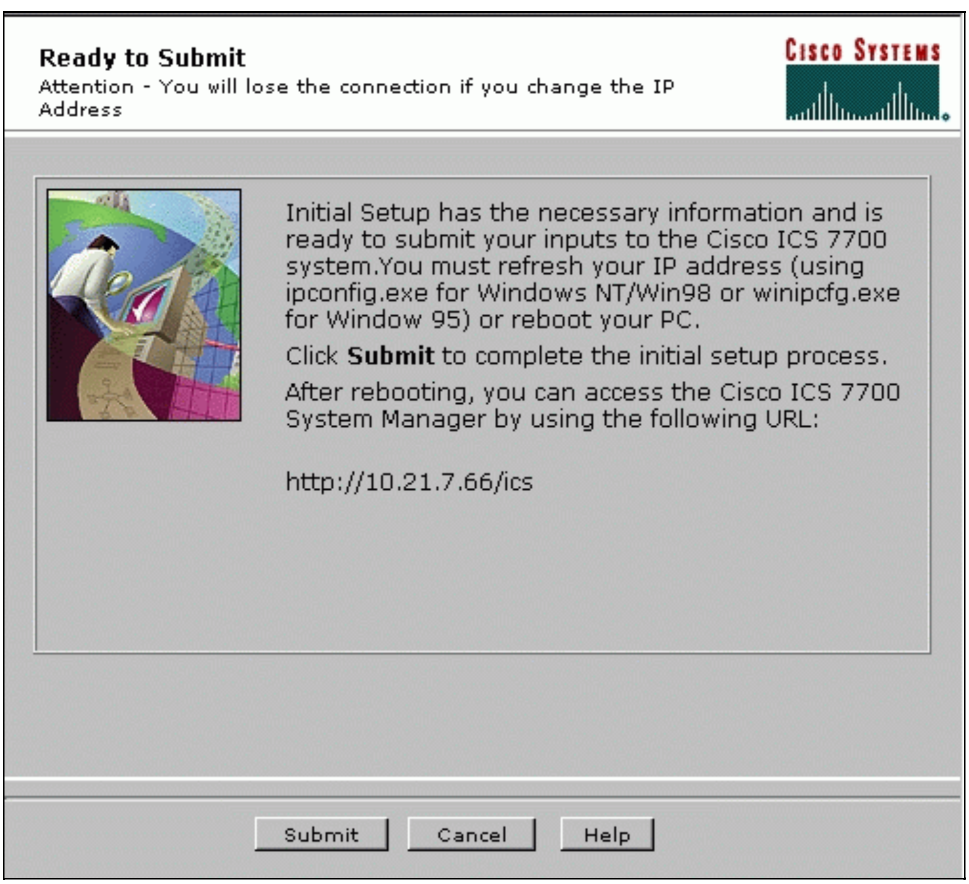
14. When you have finished changing the passwords, click **Next** from the Setup window and proceed to **step 15**.

    Note: If you want to cancel your changes, see the Cancel Your Changes section.



15. Select **Submit** in the window that appears to complete the process of changing the passwords.

Note: If you want to cancel your changes, see the Cancel Your Changes section.

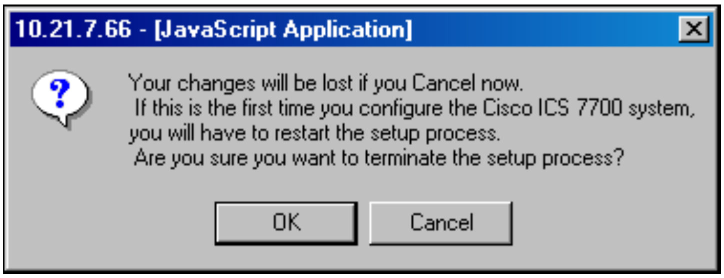


16. When the progress indicator window appears, close the browser when the process has finished.

Cancel Your Changes

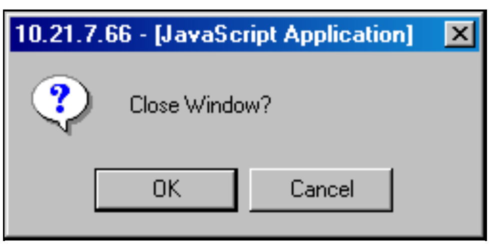
If you decide not to save your changes you can select the **Cancel** option. This attempts to cancel the entire configuration task, not just the current section you are working on. Complete these steps to cancel your changes.

1. Press the **Cancel** option. This popup window appears.

2. Select **OK** to cancel your changes.

   Note: If you select **Cancel** from this popup, you return to the configuration menu. Your only other option at this point is to select **Continue** which saves any changes that you made.
3. From this popup window, click **OK** to terminate your browser session with the ICS 7750.

   Otherwise, click **Cancel** to return to this screen. You can now return to **step 1** to start the task over.

Troubleshoot the Discovery Process

If the discovery process encounters any problems, it is not able to finish. You will see error messages that are linked to probable causes for the problems and possible solutions. You must resolve any problems with the discovery process before you can continue following the steps in this document. Please refer to the ICS 7750 Troubleshooting Documents in the Products and Services area of Cisco.com.

ICS System Manager

The ICS 7750 System Manager interface can be used to change the password for the Administrator (Admin) account on the system as well as making changes to any additional System Manager users that have been added to the system.

Note: This is the ICS Super Admin Password that can also be managed with the ICSConfig Utility.

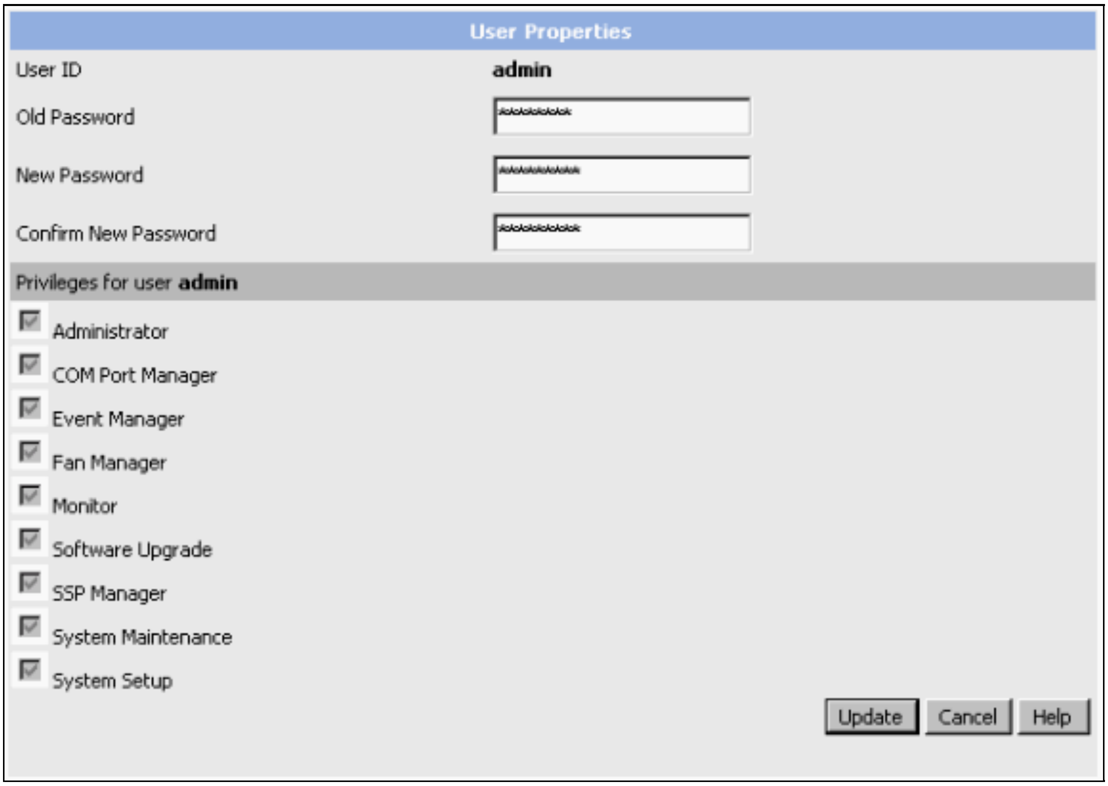
This utility is accessible via a browser at URL **http://sm−spe−ip−address/ics** where *sm−spe−ip−address* is the IP address on the SPE running the ICS System Manager software.

1. Start the **ICS System Manager utility** and login as admin. The default password is **admin**.

   Note: You may substitute the DNS name for this SPE if you have DNS configured.
2. From the ICS System Manager page, select the **Security** tab.

3. Select the **Edit** option next to the account that you want to change the password for. In this case, it is the **admin** account.

   Note: The name "admin" appears here in all lower case. The actual login account name is "Admin" with an uppercase "A".



4. Click **Update** and change any other user passwords as required.
5. Close the browser.

Recovery of a Lost ICS 7750 Administration (Admin) Account Password

Use the ICSConfig Utility as explained in the first task to assign a new password for this account.

Cisco CallManager

Cisco CallManager uses the Windows 2000 Server Local Administrator Account for administrative purposes. The Cisco CallManager installation process changes this password to a blank (no password). You will be prompted to enter a password after the Cisco CallManager installation has finished. You must renter the current password as it is configured in the System Manager.

Caution: Do not place a SPE running Cisco CallManager into an Active Directory Domain. Therefore, you only have the Windows 2000 Server Local Administrator Account available to use for administration purposes.

Recovery of a Lost Cisco CallManager Administration Account Password

Because the Cisco CallManager Administration account is the Windows 2000 Server Local Administrator Account, there is no method available for recovering this password.

Cisco Unity

Administrating administrator account passwords on SPEs running Cisco Unity is different from SPEs running Cisco CallManager because Cisco Unity SPEs are either Active Directory (AD) Domain Controllers or Member Servers in an Active Directory domain. In either case it is a domain level account and not the local account that is used to administrate Cisco Unity.

The account used to administrate Cisco Unity depends on how the person that did the original Cisco Unity installation setup the server. Some users use the Windows 2000 Server Domain Administrator account to administrate Cisco Unity. If this is how your server is setup, change the Windows 2000 Server Administrator Account password at the domain level. The ICSConfig utility cannot do this for you.

It is also possible to setup a dedicated domain account to administrate Cisco Unity. If this is how your server is setup, you need to change the dedicated Cisco Unity Administration Account password at the domain level. The ICSConfig utility cannot do this for you.

Note: The Unity Permissions Wizard utility establishes the required permission levels for the account that was created for administering Cisco Unity.

The Windows 2000 Server Local Administrator Account password on the SPE is managed by the ICSConfig Utility.

Complete these steps to change the password for the Cisco Unity administration Active Directory Domain account.

1. Logon to a PC (or a SPE) that has access to Active Directory Users and Computers.
2. Launch the **Active Directory Users and Computers console**.
3. Locate the Domain user that you want to change the password for.
4. Right−click on the account name.
5. Select **Reset Password**.
6. Enter the new password. Do NOT select the *User must change password at next login* option.
7. Close all of the open windows.

Recovery of a Lost Cisco Unity Administration Account Password

There are no unique procedures for recovering from this situation. Use the procedure above to assign a new password.

IPCC Express (CRA/CRS) and Extended Services

These applications can be co−located on a SPE running Cisco CallManager or they can be installed on a dedicated SPE.

CRA and Extended Services 2.x

CRA 2.x and Extended Services 2.x use the Windows 2000 Server Local Administrator Account to control access to the interface used to configure applications.

The Windows 2000 Server Local Administrator Account password on the SPE is managed by the ICSConfig Utility.

IPCC Express (CRS 3.0)

CRS 3.0 uses a Cisco CallManager user account created in the DC Directory by the Cisco CallManager User Administration interface to administrate the application.

Complete these steps to change the password for the CRS 3.0 administration account.

1. Logon to the **Cisco CallManager System Administration menu** for the Cisco CallManager SPE that you configured the CRS installation to interact with.
2. Select **User** > **Global Directory**.
3. Search for the account that you created to administrate CRS 3.0.
4. Change the password and submit your changes.
5. Close the browser.

Recovery of a Lost CRS 3.0 Administration Account Password

There are no unique procedures for recovering from this situation. Use the procedure above to assign a new password.

DC Directory

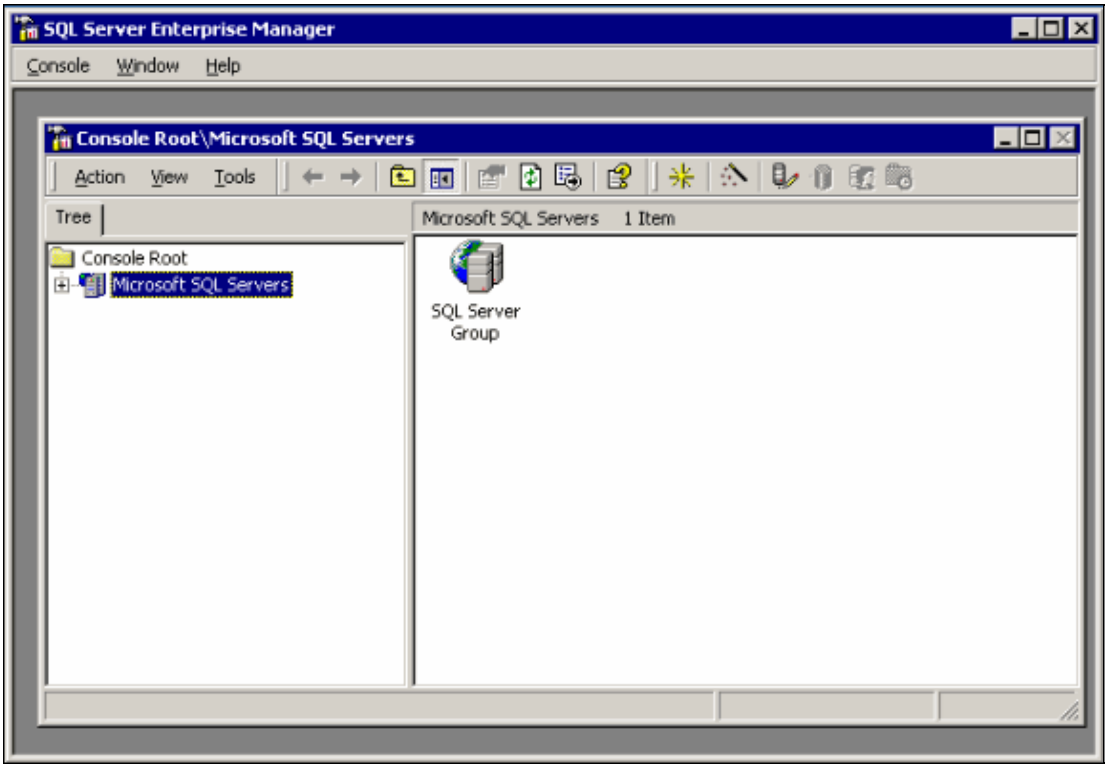
DC Directory has an administration account that is called "Directory Manager" by default. This is not an account that can be used to logon to Windows 2000 on a SPE. Some system administrators periodically change this password for security purposes.

If you want to change the DC Directory Password, refer to How to Change the DC Directory Password.

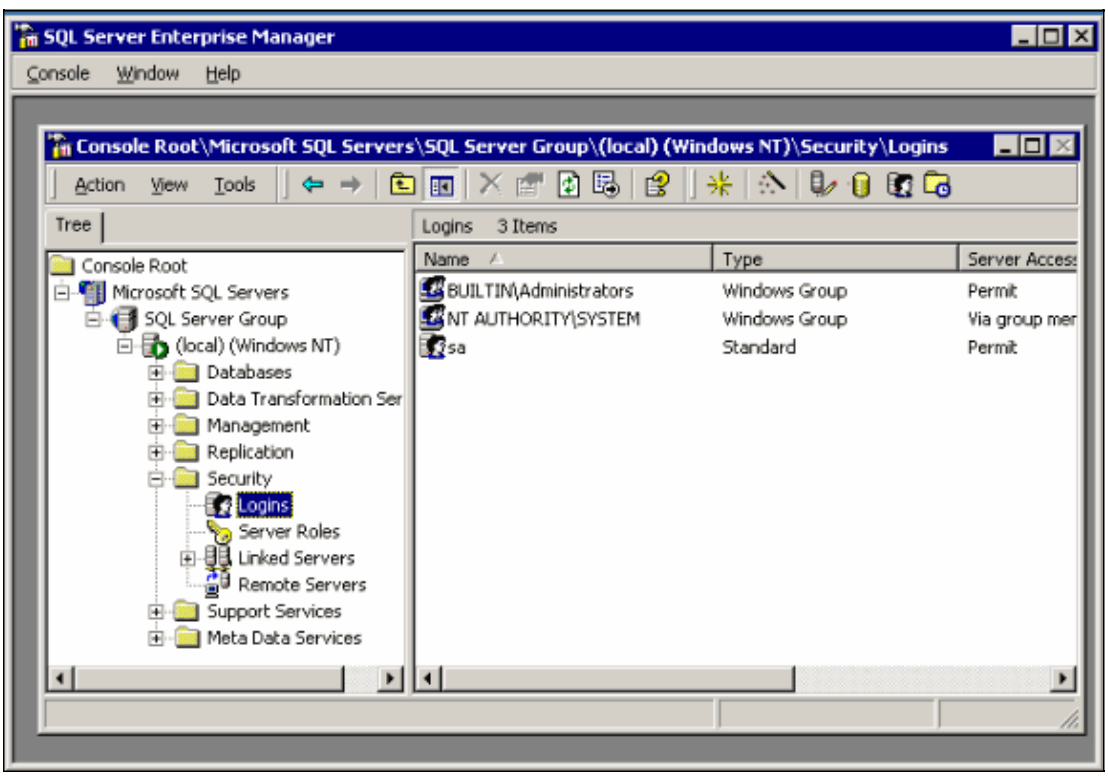
SQL System Administrator (SA) Account

SQL (or Microsoft SQL Desktop Edition (MSDE)) is installed on the SPE running System Manager. It is also installed on SPEs running Cisco CallManager and Cisco Unity, and SPEs that are dedicated to CRS. The procedure for changing the SA password is the same on all of these systems.

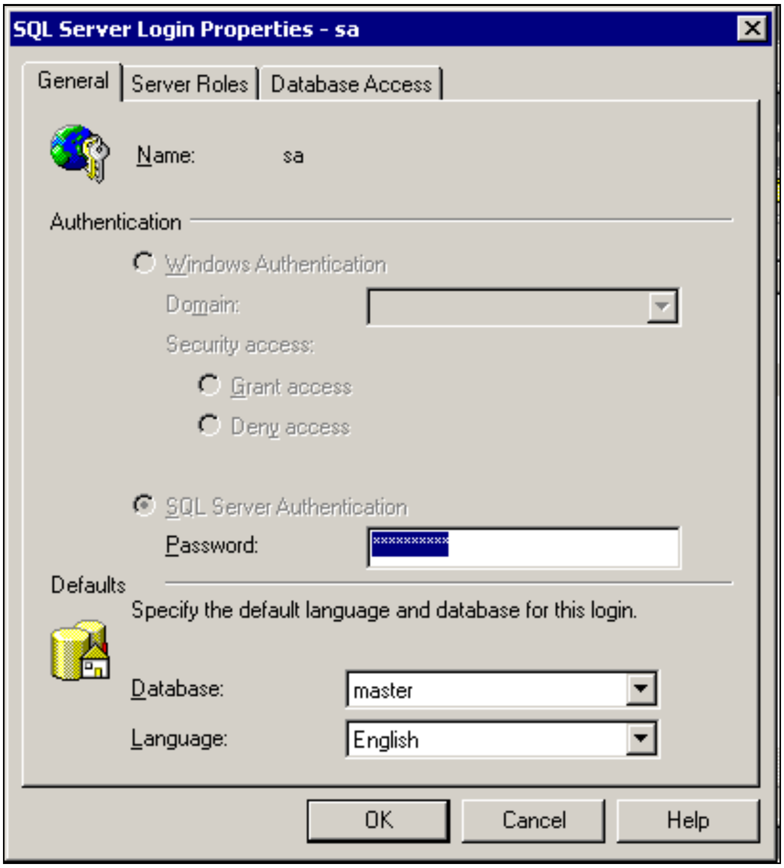
1. Logon to the SPE that you want to change the SA password on.
2. Select **Start** > **Programs** > **Microsoft SQL Server** > **Enterprise Manager**.



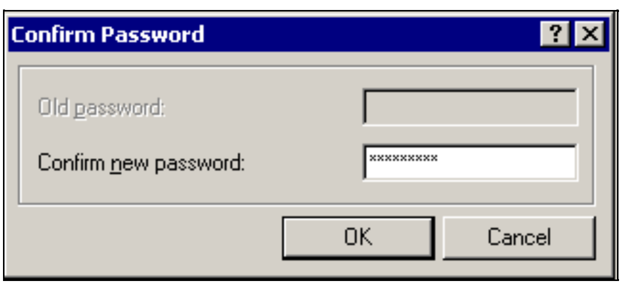
3. Expand the navigation tree as shown here.



4. Double−click on the SA account name in the right−hand window, enter the new password, and click **OK**.



5. Confirm the new password and click **OK**.



6. Close all of the open windows.

Recovery of a Lost SQL System Administrator Account Password

There are no unique procedures for recovering from this situation. Use the procedure above to assign a new password.

SSP Card

Recover from a Lost Password on the SSP

Complete these steps to reset the SSP and change its passwords to their original values.

1. Press the **SHTDN** button on the SSP.

   The STATUS LED on the card starts to blink and turns off after several minutes. Wait for the STATUS LED to turn off before you continue to **step 2**.
2. Put on an ESD−preventive wrist strap and attach it to an unpainted chassis surface.

Caution: To prevent ESD damage, handle cards by the edges only and use an ESD−preventive wrist strap or other grounding device.

3. Completely loosen the card captive screws.
4. Press the upper and lower ejector levers outward at the same time to disengage the card from the backplane.

   Caution: Always use the ejector levers to disengage or seat cards. Failure to use the ejector levers can cause erroneous system error messages that indicate a card failure. Do not use the ejector levers to lift or support the weight of the cards.
5. Grasp the ejector levers, and gently pull the card partially out of the chassis slot until you can grasp the card front panel with one hand. Pull the card out approximately 1 inch (2.5 cm).
6. Make sure that the SSP card is still aligned with the upper and lower card guides in slot 7 of the chassis, and make sure that the ejector levers are in the open position (pointing outward).
7. With the top and bottom edges of the card in the card guides, gently slide the card into the chassis until you feel resistance.

   Because there are grounding clips near the front and rear of the card guides, you might need to increase the force that you use to get the card past the grounding clips. If you encounter extreme resistance, pull the card out slightly, and push it back in again.
8. Press the upper and lower ejector levers inward at the same time until they lock into their slots. This step firmly seats the SSP card into the chassis.
9. While the SSP is booting, use a stylus to press and hold the **SHTDN** button on the SSP front panel.
10. On a PC, open a HyperTerminal session with the SAP card.
11. Press **Ctrl−backslash (\)** and use the SAP card menu to switch to the SSP.
12. Enter the **switch:flash_init** command.

    This command output appears.

    ```
    switch: flash_init
       Initializing Flash...
       flashfs[0]: 109 files, 2 directories
       flashfs[0]: 0 orphaned files, 0 orphaned directories
       flashfs[0]: Total bytes: 3612672
       flashfs[0]: Bytes used: 2672128
       flashfs[0]: Bytes available: 940544
       flashfs[0]: flashfs fsck took 6 seconds.
       ...done Initializing Flash.
    ```
13. Enter the **switch:copy flash:/config.text flash:/configsv.text** command to copy the SSP startup configuration file.

    Output similar to this appears.

    ```
    File "flash:/config.text" successfully copied to "flash:/configsv.text"
    ```
14. Enter the **switch:delete flash:/config.text** command to delete the SSP startup configuration file.
15. Confirm that you want to delete the SSP startup configuration file by entering **y** as shown here.

    ```
    Are you sure you want to delete "flash:/config.text" (y/n)?y
    ```

    Text similar to this displays:

    ```
    File "flash:/config.text" deleted
    ```
16. Enter the **switch:boot** command to enable the SSP to continue booting.

    The SSP reboots and this output appears.

```
Loading
   "flash:c2900XL-c3h2s-mz-120-5.WC5.bin"...##############################
   File "flash:c2900XL-c3h2s-mz-120-5.WC5.bin" uncompressed and installed,
   entry point: 0x3000 executing...
   Restricted Rights Legend
   Use, duplication, or disclosure by the Government is
   subject to restrictions as set forth in subparagraph
   (c) of the Commercial Computer Software - Restricted
   Rights clause at FAR sec. 52.227-19 and subparagraph
   (c) (1) (ii) of the Rights in Technical Data and Computer
   Software clause at DFARS sec. 252.227-7013.
   Cisco Systems, Inc.
   170 West Tasman Drive
   San Jose, California 95134-1706
   Cisco Internetwork Operating System Software
   IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5)WC5,MAINTENANCE
    INTERIM SOFTWARE
   Copyright (c) 1986-2000 by Cisco Systems, Inc.
   Compiled Mon 17-Jul-00 17:35 by ayounes
   Image text-base: 0x00003000, data-base: 0x00301F3C
   Initializing C2900XL flash...
   flashfs[1]: 109 files, 2 directories
   flashfs[1]: 0 orphaned files, 0 orphaned directories
   flashfs[1]: Total bytes: 3612672
   flashfs[1]: Bytes used: 2672128
   flashfs[1]: Bytes available: 940544
   flashfs[1]: flashfs fsck took 7 seconds.
   flashfs[1]: Initialization complete.
   ...done Initializing C2900XL flash.
   C2900XL POST: System Board Test: Passed
   C2900XL POST: Daughter Card Test: Passed
   C2900XL POST: CPU Buffer Test: Passed
   C2900XL POST: CPU Notify RAM Test: Passed
   C2900XL POST: CPU Interface Test: Passed
   C2900XL POST: Testing Switch Core: Passed
   C2900XL POST: Testing Buffer Table: Passed
   C2900XL POST: Data Buffer Test: Passed
   C2900XL POST: Configuring Switch Parameters: Passed
   C2900XL POST: Ethernet Controller Test: Passed
   C2900XL POST: MII Test: Passed
   Cisco ICS7750-SSP80 (PowerPC403GA) processor (revision 0x11)
   with 8192K/1024K    bytes of memory.
   Processor board ID JAD04120G73, with hardware revision 0x00
   Last reset from warm-reset
   Processor is running Enterprise Edition Software
   Cluster command switch capable
   Cluster member switch capable
   8 FastEthernet/IEEE 802.3 interface(s)
   32K bytes of flash-simulated non-volatile configuration memory.
   Base ethernet MAC Address: 00:01:96:5E:02:C0
   Model revision number: B
   Model number: SSP-7750
   System serial number: JAD04120G73
   C2900XL INIT: Complete
   00:00:18: %SYS-5-RESTART: System restarted --
   Cisco Internetwork Operating System Software
   IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5)WC5,
   MAINTENANCE INTERIM SOFTWARE
   Copyright (c) 1986-2000 by Cisco Systems, Inc.
   Compiled Mon 17-Jul-00 17:35 by ayounes
```

When rebooting is complete, the SSP STATUS LED is green, and the SSP ALARM LED is off.

17. When prompted whether you want to continue with the configuration dialog box, enter **no**.

```
Continue with configuration dialog? [yes/no]:no
```

18. Enter privileged EXEC mode by entering the **enable** command.

```
switch>enable
```

19. Display the contents of the SSP Flash memory by entering the **show flash** command.

    This command output appears.

```
Directory of flash:/
   3 −rwx 108 Mar 01 2000 00:59:37 info
   4 −rwx 1645810 Mar 01 2000 01:00:37
   c2900XL−c3h2s−mz−120−5.WC5.bin
   5 drwx 6720 Mar 01 2000 01:01:16 html
   111 −rwx 108 Mar 01 2000 01:01:16 info.ver
   112 −rwx 998 Jan 01 2001 00:01:50 configsv.text
   3612672 bytes total (940544 bytes free)
```

20. Copy the SSP startup configuration file from Flash memory by entering the **copy flash run** command.

```
switch#copy flash run
Source filename []?configsv.text
Destination filename [running−config]?<Enter>
998 bytes copied in 1.69 secs (998 bytes/sec)
```

21. Enter global configuration mode by entering the **configure terminal** command.

```
switch#configure terminal
```

22. Enter these commands to change and save your SSP passwords.

```
switch(config)#line con 0
switch(config)#password your login password
switch(config)#enable password your enable password
switch(config)#
switch(config)#copy run start
Building configuration..
```

MRP Cards with Flash Memory

Recover from a Lost Password on an MRP Card that has Flash

Complete these steps to recover from a lost password on an MRP card that has Flash.

1. On a PC, open a HyperTerminal session with the SAP card.
2. Press **Ctrl−backslash (\)** and use the SAP card menu to switch to the MRP.
3. Put on an ESD−preventive wrist strap and attach it to an unpainted chassis surface.

    Caution: To prevent ESD damage, handle cards by the edges only and use an ESD−preventive wrist strap or other grounding device.
4. Completely loosen the card captive screws.
5. Press the upper and lower ejector levers outward at the same time to disengage the card from the backplane.

    Caution: Always use the ejector levers to disengage or seat cards. Failure to use the ejector levers can cause erroneous system error messages that indicate a card failure. Do not use the ejector levers to lift or support the weight of the cards.
6. Grasp the ejector levers, and gently pull the card partially out of the chassis slot until you can grasp the card front panel with one hand. Pull the card out approximately 1 inch (2.5 cm).
7. Make sure that the card is still aligned with the upper and lower card guides in slot 7 of the chassis

and make sure that the ejector levers are in the open position (pointing outward).

8. With the top and bottom edges of the card in the card guides, gently slide the card into the chassis until you feel resistance.

   Because there are grounding clips near the front and rear of the card guides, you might need to increase the force that you use to get the card past the grounding clips. If you encounter extreme resistance, pull the card out slightly and push it back in again.
9. Press the upper and lower ejector levers inward at the same time until they lock into their slots.

   This step firmly seats the SSP card into the chassis.
10. Press the break key sequence in your terminal software (usually **CTRL Break**).

    This terminates the boot−up sequence and leaves the MRP in ROM Monitor (ROMMON) mode.
11. Enter the **confreg** command to enter the configuration register configuration mode so that you can change the configuration register settings to ignore the configuration in NVRAM.

    ```
    rommon 4 > confreg
    ```
12. You are placed in the configuration register tool which displays the current setting of the configuration registers. In this case 0x2102. The "0" needs to be changed to a **4** to configure the MRP to ignore its configuration the next time it boots up.

    ```
    Configuration Summary
    (Virtual Configuration Register: 0x2102)
    enabled are:load rom after netboot fails
    console baud: 9600
    boot: image specified by the boot system commands
    or default to: cisco2−MRP300h
    ```
13. When prompted to change the current register settings, enter **y** (yes).

    ```
    do you wish to change the configuration? y/n  [n]:y
    ```
14. Enter your responses exactly as shown in this output.

    The only option you want to change is the one for ignoring the system configuration information.

    ```
    enable  "diagnostic mode"? y/n  [n]:
    enable  "use net in IP bcast address"? y/n  [n]:
    disable "load rom after netboot fails"? y/n  [n]:
    enable  "use all zero broadcast"? y/n  [n]:
    enable  "break/abort has effect"? y/n  [n]:
    enable  "ignore system config info"? y/n  [n]:  y
    change console baud rate? y/n  [n]:
    change the boot characteristics? y/n  [n]: [return]
    ```
15. A display of the new settings **0x2142** appears.

    Notice that the "0" is now a "4".

    ```
    Configuration Summary
    (Virtual Configuration Register: 0x2142)
    enabled are:
    load rom after netboot fails
    ignore system config info
    console baud: 9600boot: image specified by the
    boot system commands
    or default to: cisco2−MRP300
    ```
16. When prompted again if you want to change the current register settings, answer **n** for No.

    ```
    do you wish to change the configuration? y/n  [n]:[return]
    ```
17. When you are prompted to reset or power cycle the MRP for the changes to take effect, enter the **reset** command.

```
You must reset or power cycle for new config to take effectrommon 5
> reset
```

18. When the MRP has finished booting, you are prompted to enter the initial configuration dialogue. Answer **n** for No.

```
Router>

      --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: n
```

19. When prompted, press **Return** to get started and to go to the default MRP prompt.

```
Press RETURN to get started!
```

20. Enter enable mode by using the **enable** command.

```
Router> enable
Router#
```

21. Enter the **configure memory** command.

   This loads the configuration in NVRAM over the current running configuration. You are already in enable mode so the fact that you do not know what the enable mode password is in the stored configuration is not a problem. The prompt name changes to the name that was setup in the stored configuration.

```
Router#configure memory
LabMRP#
*Mar 1 00:01:57.811: %SYS-5-CONFIG_I: Configured from memory by console
LabMRP#
```

22. Enter the **configure terminal** command.

```
LabMRP#configure terminal
   Enter configuration commands, one per line. End with CNTL/Z.
```

23. Change the enable secret password.

```
LabMRP(config)#enable secret my_password
```

   Note: The password used must match the password currently configured with ICSConfig. Otherwise, ICS System Manager is unable to manage the MRP.

24. Enter the virtual terminal line configuration mode for Telnet sessions using the **line 0 4** command.

```
LabMRP(config)#line vty 0 4
```

25. Configure the virtual terminal password. Then exit this mode using the **exit** command.

```
LabMRP(config-line)#password my_password
LabMRP(config-line)#exit
```

   Note: The password used must match the password currently configured with ICSConfig. Otherwise, ICS System Manager is unable to manage the MRP.

26. Change the configuration registers so that the MRP reads its stored configuration the next time it reboots. Then exit this mode using the **exit** command.

```
LabMRP(config)#config-register 0x2102
LabMRP(config)#exit
LabMRP#
  *Mar 1 00:02:29.387: %SYS-5-CONFIG_I: Configured from console by console
```

27. Copy the current running configuration over the existing startup configuration using the **copy running−config startup−config** command.

```
LabMRP#copy running-config startup-config
Destination filename [startup-config]?
```

```
Building configuration...
[OK]
```

28. Exit enable mode so that you can enter it again to verify that the password has been changed.

```
LabMRP#exit

LabMRP con0 is now available
Press RETURN to get started.
```

29. Enter enable mode and respond with the password that you just configured.

    The password was accepted. This shows that the new password is in effect.

```
LabMRP>enable
Password:
LabMRP#
```

30. For a final test that the MRP will boot up properly, reload it now. Otherwise, this task is now complete.

```
LabMRP#reload
Proceed with reload? [confirm
```

ASI and MRP Without Flash Memory

Recover from a Lost Password on an MRP Card that does not have Flash Memory

Complete these steps to reset ASI and MRP cards that do not have Flash memory (MRP200, ASI81, and ASI160). Resetting the cards enables them to obtain their passwords from the SPE 310 running System Manager as long as their enable passwords were configured through, and known to, ICSConfig.

Use the SSP hardware module reset Command to Power Cycle the MRP for the Password Recovery Procedure

If you have the passwords for the SSP card, you can use a command line feature to reset any card in the ICS 7750 chassis.

If you do not have this password you must physically reseat the MRP in the ICS chassis. See the Reseat the MRP to Power Cycle It for the Password Recovery Procedure section of this document.

1. Access the command prompt on the SSP using the SAP console connection or via Telnet.
2. Enter configuration (Enable) mode using the **enable** command.
3. Enter this command at the enable mode prompt of the SSP.

```
SSP#hw−module chassis slot 1 restart hold 5 [return]
```

   Where 1 is the ICS−7750 chassis slot number and 5 is a time in seconds to assert reset.

   The MRP resets itself and obtains the correct configuration and passwords from the System Manager SPE.

Reseat the MRP to Power Cycle It for the Password Recovery Procedure

Complete these steps to reseat the MRP to power cycle it for the password recovery procedure.

1. Press the **SHTDN** button on the card.

The STATUS LED on the card starts to blink and then turns off after several minutes. Wait for the STATUS LED to turn off before continuing to step 2.

2. Put on an ESD−preventive wrist strap and attach it to an unpainted chassis surface.

   Caution: To prevent ESD damage, handle cards by the edges only and use an ESD−preventive wrist strap or other grounding device.
3. Completely loosen the card captive screws.
4. Press the upper and lower ejector levers outward at the same time to disengage the card from the backplane.

   Caution: Always use the ejector levers to disengage or seat cards. Failure to use the ejector levers can cause erroneous system error messages that indicate a card failure. Do not use the ejector levers to lift or support the weight of the cards.
5. Grasp the ejector levers and gently pull the card partially out of the chassis slot until you can grasp the card front panel with one hand. Pull the card out approximately 1 inch (2.5 cm).
6. Make sure that the card is still aligned with the upper and lower card guides in slot 7 of the chassis, and make sure that the ejector levers are in the open position (pointing outward).
7. With the top and bottom edges of the card in the card guides, gently slide the card into the chassis until you feel resistance.

   Because there are grounding clips near the front and rear of the card guides, you might need to increase the force that you use to get the card past the grounding clips. If you encounter extreme resistance, pull the card out slightly and push it back in again.
8. Press the upper and lower ejector levers inward at the same time until they lock into their slots.

   This step firmly seats the SSP card into the chassis.

   When the card has finished rebooting it should have downloaded its configuration with the original passwords from the SPE running System Manager.

Related Information

- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Recommended Reading: Troubleshooting Cisco IP Telephony**
- **Technical Support − Cisco Systems**

Updated: Feb 02, 2006 Document ID: 43005