1.0 DCAF Security

1.1 Installing the Security Components

DCAF security enables you to safeguard your target workstations against unauthorized control.

This chapter provides the following:

- A description of how DCAF security works
- The main tasks that you perform to set up and maintain DCAF security
- Instructions for installing the security components

1.1.1 How DCAF Security Works

The administrator workstation, the only one in the network, gathers and maintains information about authorized controllers, their access to secure targets, and the authenticators for the whole network, and stores it in security databases. It distributes these databases to the authenticators. The authenticators use the information to ensure that only authorized users can control the secure targets for which they are authorized.

Authorized controllers access basic and secure targets on the LAN through a secure gateway or LAN directory. The gateway or LAN directory verifies with the authenticator that the controllers are authorized to access the secure targets. When the authenticator confirms that the controller is authorized, the gateway or LAN directory enables the session to start.

1.1.1.1 Determining a Controller′s Access to Secure Targets

For the controllers, you create various access levels, which enable varying degrees of control over the secure targets. Then you create access level tables that specify which privileges the controller exercises over the targets. You associate an access level table with each secure target and an access level with each controller. The combination of the controller′s access level and the target′s access level table determines the degree of access that the controller has to the secure target.

A controller′s access level can vary from one target to another, and two controllers can access the same target at different levels.

Because authorized controllers identify themselves with a user ID and pass phrase, the authenticator recognizes them from any controller workstation in the network.

1.1.1.2 Protecting Information during a Secure Session

DCAF encrypts the information, including security databases, that is stored on the security components or sent across the network during secure sessions. To do this, DCAF uses a master key and key-encrypting key (KEK) that it generates from your input.

The security components use either the IBM 4755 Cryptographic Adapter card or an encryptor included in the DCAF software.

1.1.2 Setting up DCAF Security: Main Tasks

Setting up DCAF security involves the following activities:

- Planning DCAF network topology.

  Consider the following: How many targets do you need to safeguard on a LAN? How many secure LANs do you need? Where can you install a security checkpoint (secure gateway or LAN directory) so that it is present on a LAN of secure targets? How do your workstations connect to each other? Does DCAF support my network's topology (Figure 12 in topic 1.2)?

- Installing the DCAF components. A list of the components required for the simplest secure network follows. See "The DCAF Components" in the Installation and Configuration Guide for a more detailed description of the components.

  - Administrator
  - Authenticator
  - Controller
  - LAN directory and secure gateway or the LAN directory alone
  - Secure target

  This chapter includes instructions on how to install the administrator and authenticator. To install the other components, follow the instructions in the chapter "Installing the DCAF on OS/2 Workstations" in the Installation and Configuration Guide.

- Personalizing the DCAF components.

  Required for the following components:

  - Administrator. (personalize when you install)
  - Authenticator. (personalize when you install)
  - Gateway. You can make the gateway secure only during installation. See "Updating the Authenticator Name for Secure Workstations" in the Installation and Configuration Guide.
  - LAN directory. See "Personalizing the LAN Directory" in the Installation and Configuration Guide.
  - Target. You can make the target secure only during installation. See the chapter "Personalizing the DCAF Targets" in the Installation and Configuration Guide.

- Configuring the communications on the workstations for the following purposes:

  - To enable a secure session
  - To distribute the security databases to the authenticators "Configuring the Communications for Secure Sessions" in topic 1.2 provides instructions for both.
  - To send a new pass phrase from the controller to the administrator See "Configuring the Workstations for Pass Phrase Updates" in topic 1.3.

- Configuring the workstation directory on the controllers. The chapter "Configuring the Workstation Directory" in the Installation and Configuration Guide and "Defining the Administrator on the Controller" in topic 1.3.1 provide instructions.

- Creating the security databases. See "Setting up the Security Databases" in topic 1.4.

- Distributing the security databases to the authenticators. See ″Transferring Security Databases to the Authenticators″ in topic 1.4.6.

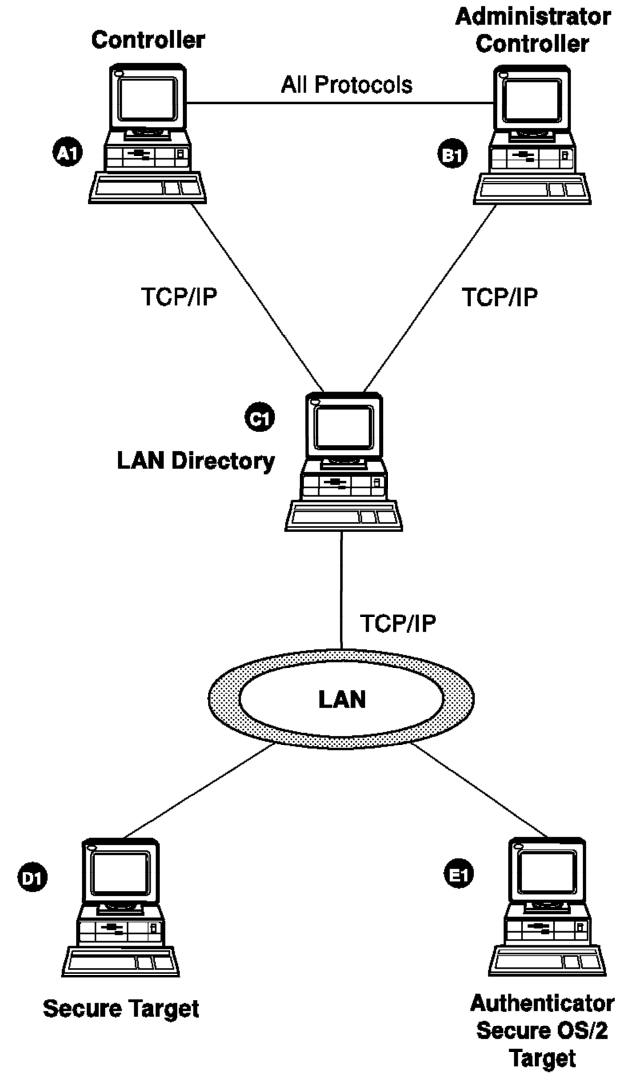
- Updating the security information whenever it changes. See ″Keeping DCAF Security Up to Date″ in topic 1.5.

1.1.2.1 Planning the DCAF Network Topology

Before you install the security components, analyze your network and identify the workstations (targets) that need to be safeguarded. Divide this network into logical LANs and identify the communications that tie the LANs together.

Designate a central point (the administrator) where you can manage security information. Decide where the checkpoints (secure gateways and LAN directories) for each LAN should reside. The gateway is necessary only when the controller uses a protocol that is different from the protocol that connects the secure LAN. The LAN directory is always necessary. Also decide where to install an authenticator for each logical LAN. You can concentrate the checkpoints (gateway, LAN directory, and authenticator) on a secure OS/2 target workstation. If a secure OS/2 target is on a LAN by itself, you must use this arrangement.

Figure 1 shows an example of a simple secure DCAF environment.



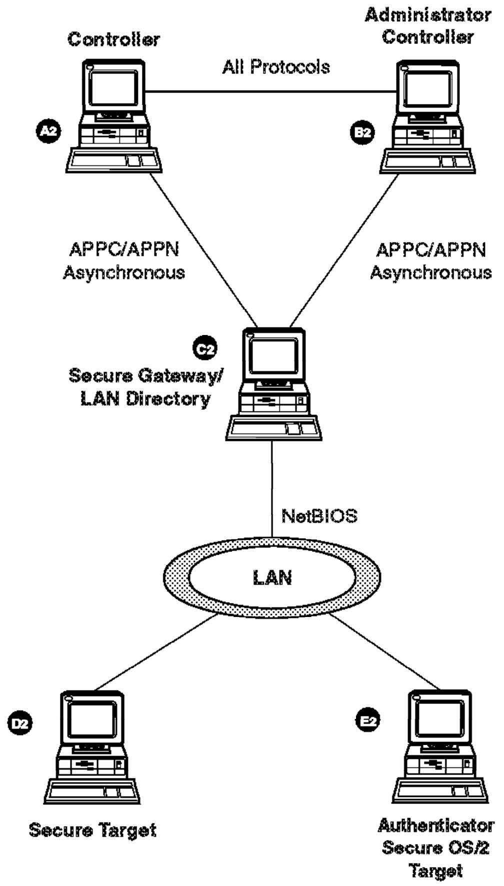
PICTURE 1

Figure 1. Example 1 of a Secure Environment

| The controller (A1) uses any protocol (APPC/APPN, asynchronous, NetBIOS, or TCP/IP) to send pass phrase updates to the administrator/controller (B1). The administrator uses TCP/IP to send security information to the authenticator (E1) through the LAN directory (C1). The controller (A1) uses TCP/IP to connect to the secure target (D1) through the LAN directory. The LAN directory lists the available targets for the controller.

Because all segments of the connection to the secure target use the same protocol, the gateway is not needed to convert one protocol to another. | This example also applies to NetBIOS connections. If your network uses these protocols, you can configure your workstations to match this example.

Figure 2 shows another example of how the components are connected in a simple secure DCAF environment.



PICTURE 2

Figure 2. Example 2 of a Secure Environment

In this environment, the controller (A2) uses any protocol (APPC/APPN, | asynchronous, NetBIOS, or TCP/IP) to send pass phrase updates to the administrator/controller (B2). It sends security information to the | authenticator (E2) through a secure gateway and LAN directory (C2). | Similarly, the controller (A2) connects to the secure target (D2) through | a secure gateway and LAN directory.

The gateway (C2) is important because it converts the APPC/APPN or asynchronous connections to NetBIOS for the LAN. The LAN directory lists the available targets for the controller. If your network connectivity resembles this environment, configure your workstations to match this example.

1.1.2.2 Installing the Security Components

These instructions explain how to install the administrator and the | authenticator directly. You can also use the CID method (see the chapter | "Installing the DCAF Using the CID Method" in the Installation and | Configuration Guide).

In most cases, you install the administrator on the same workstation as a controller, and the authenticator on the same workstation as a secure target. The authenticator is known as a remotely administered authenticator.

If, however, you have only one authenticator in your network and it is installed on the same workstation as the administrator workstation, you do not need to install the controller and target on the workstation. An authenticator that is installed on the administrator workstation is known as a locally administered authenticator.

If you plan to use the IBM 4755 Cryptographic Adapter card, ensure that it is ready to use before you start to install the components.

The following instructions begin at the DCAF Installation window ("Installing the DCAF on OS/2 Workstations" in the Installation and Configuration Guide explains how to get there). To interrupt installation, close the DCAF installation program. The **Cancel** push button is disabled.

1.1.2.2.1 Installing the Administrator

To install the administrator, complete the following steps:

1. On the DCAF Installation window, select Administrator and choose **Include component...** from Install on the menu bar. "Ready to install" is displayed under Status.

   If you are installing the authenticator on the same workstation, you must do it now. Repeat this step for the authenticator.

2. Choose **Install included component(s)...** from Install on the menu bar. The DCAF Installation Path window is displayed.

3. Enter the path where you want the DCAF product to be installed. The default path is C:\DCAF13. If the directory that you specify does not exist, then the directory will be created on the workstation's hard disk.

   - The path is 1-50 characters in length.
   - For character guidelines, follow OS/2 conventions for paths.

   Enter the name for the backup CONFIG.SYS file.

   - Follow OS/2 file name conventions.
   - The format of the file name depends on whether your hard disk has been formatted for HPFS or FAT.
   - The default is CONFIG.BAK.

   Press the **OK** push button.

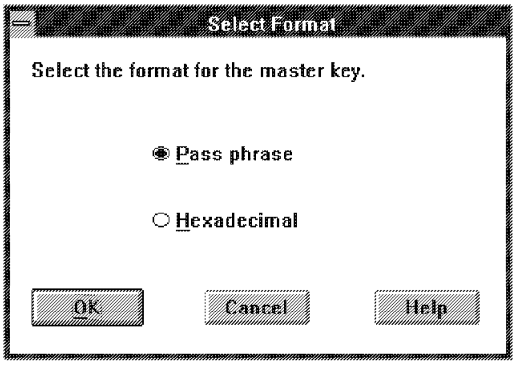
4. The following message is displayed:

   Are you going to use the IBM 4755 Cryptographic Adapter?

   If you choose **Yes**, the Select Format window for the KEK (Figure 6) is displayed. Continue the steps in "Supplying the Format for the Administrator Key-Encrypting Key."

   If you choose **No**, continue here.

5. The Select Format window (Figure 3) for the master key is displayed.



PICTURE 3

Figure 3. Select Format for Master Key

6. On the Select Format window, select one of the following formats to create the master key:

   - Pass phrase
   - Hexadecimal string

   Press the **OK** push button.

   - If you select **Pass phrase:**

     a. The Set Master Key window (Figure 4) is displayed.

PICTURE 4

Figure 4. Set Master Key with Pass Phrase Format

In the **Key** field enter your pass phrase. It can be 4-80 characters in length, including:

- Upper- or lowercase letters (A-Z, a-z)
- Digits (0-9)
- Special characters: #, @, $, or blank

b. In the **Key confirmation** field enter the same pass phrase again. Press the **OK** push button.

- If you select **Hexadecimal:**

a. The Set Master Key window (Figure 5) is displayed.

PICTURE 5

Figure 5. Set Master Key with Hexadecimal Format

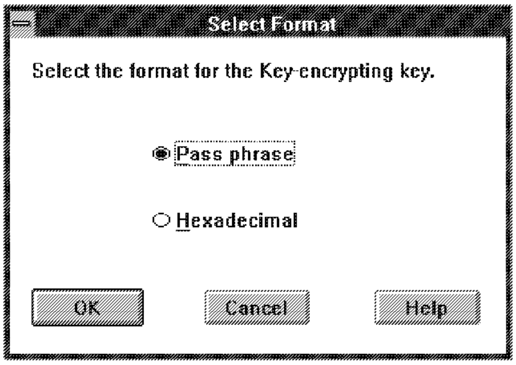
In the **Key** field enter a hexadecimal string. It is exactly 32 characters in length, including:

- Upper- or lowercase letters (A-F, a-f)
- Digits (0-9).

b. In the **Key confirmation** field enter the same hexadecimal string again. Press the **OK** push button.

7. The Select Format window for the KEK (Figure 6) is displayed. Continue with the instructions in "Supplying the Format for the Administrator Key-Encrypting Key."

Supplying the Format for the Administrator Key-Encrypting Key: Whether or not you are using the 4755 Cryptographic Adapter card, complete the following steps:



PICTURE 6

Figure 6. Select Format for Key-Encrypting Key

1. On the Select Format window, select one of the following formats to create the KEK:

- Pass phrase
- Hexadecimal string

Press the **OK** push button.

- If you select **Pass phrase:**

  a. The Set Key-encrypting Key window (Figure 7) is displayed.

PICTURE 7

Figure 7. Set Key-Encrypting Key with Pass Phrase Format

In the **Key** field enter your pass phrase. It is 4-80 characters in length, including:

- Upper- or lowercase letters (A-Z, a-z)
- Digits (0-9)
- Special characters: #, @, $ or blank

  b. In the **Key confirmation** field enter the same pass phrase again. Press the **OK** push button.

- If you select **Hexadecimal:**

  a. The Key-encrypting Key window (Figure 8) is displayed.

PICTURE 8

Figure 8. Set Key-Encrypting Key with Hexadecimal Format

In the **Key** field enter a hexadecimal string. It must be exactly 32 characters in length, including:

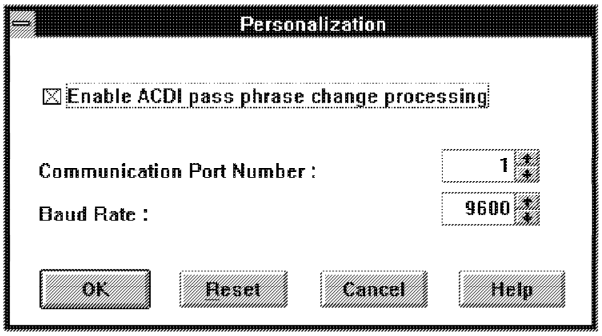
- Upper- or lowercase letters (A-F, a-f)
- Digits (0-9)

b. In the **Key confirmation** field enter the same hexadecimal string again. Press the **OK** push button. The DCAF Pass Phrase Change Personalization window is displayed.

> **Reminder**
>
> Keep a record of the KEK that you typed. You will use the same KEK when you create the Authenticator database on the administrator.

Continue with ″Completing the Administrator Installation.″

Completing the Administrator Installation: On the DCAF Pass Phrase Change Personalization window (Figure 9), you can autostart asynchronous comunication between the administrator and the controllers when they change their pass phrases. To enable other communications protocols after you install the administrator, see ″Enabling Communications Protocols on the Administrator″ in topic 1.3.3.



PICTURE 9

Figure 9. Pass Phrase Change Personalization

To finish installing the administrator, perform the following steps:

1. Select the Enable ACDI pass phrase change processing check box. The selected check box enables the other fields.

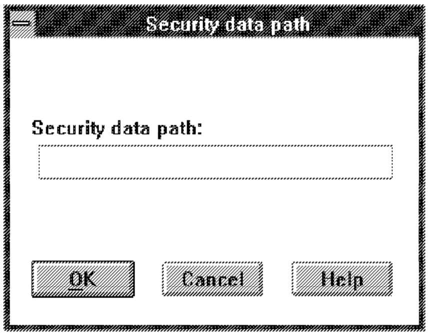
2. Choose the communication port number for the asynchronous serial port where the modem is attached. The values are 1-3. The default is 1.

3. Choose the baud rate (modem transmission rate). The choices are 1200, 2400, 4800, 9600, 19200. The default is 9600.

4. Press the **OK** push button.

5. If you are installing an authenticator on the same workstation, skip

to "Installing the Authenticator" in topic 1.1.2.2.2. If you are not installing an authenticator on the same workstation, the Security data path window (Figure 10) is displayed.



PICTURE 10

Figure 10. Security Data Path for the Administrator

6. Enter the path where the files of security information will be stored on the administrator.

   - The path is 1-50 characters in length.
   - No blank spaces between characters.
   - For character guidelines, follow the OS/2 conventions for paths.

   Press the **OK** push button. Follow the instructions online.

You have completed installation of the administrator. Now you are ready to install the authenticator if you are installing it separately.

1.1.2.2.2 Installing the Authenticator

If you want to install the authenticator on a workstation on which the administrator is already installed, you need to do the following:

1. Reinstall the administrator with the authenticator.
2. Update the KEKs for each authenticator in the authenticator database and the pass phrases for each user in the user database on the administrator. See "Setting up the Security Databases" in topic 1.4 for instructions.

Otherwise, to install a remote authenticator on its own, complete the following steps:

1. On the DCAF Installation window, select Authenticator and choose **Include component...** from Install on the menu bar. "Ready to install" is displayed under Status.

2. Choose **Install included component(s)...** from Install on the menu bar. The DCAF Installation Path window is displayed.

3. Enter the path where you want the DCAF product to be installed. The default path is C:\DCAF13. If the directory that you specify does not exist, then the it will be created on the workstation's hard disk.

   - The path is 1-50 characters in length.
   - For character guidelines, follow OS/2 conventions for paths.

   Enter the name for the backup CONFIG.SYS file.

- Follow the OS/2 file naming conventions.

- The format of the file name depends on whether your hard disk has been formatted for HPFS or FAT.

- The default is CONFIG.BAK.

Press the **OK** push button.

4. The following message is displayed:

   Are you going to use the IBM 4755 Cryptographic Adapter?

   If you choose **Yes**, the Select Format window for the KEK (Figure 6 in topic 1.1.2.2.1) is displayed. Continue the steps in ″Supplying the Format for the Authenticator Key-Encrypting Key.″

   If you choose **No**, continue here.

5. The Select Format window (Figure 3 in topic 1.1.2.2.1) for the master key is displayed.

6. On the Select Format window, select one of the following formats to create the master key:

   - Pass phrase
   - Hexadecimal string

   Press the **OK** push button.

   - If you select **Pass phrase:**

     a. The Set Master Key window (Figure 4 in topic 1.1.2.2.1) is displayed.

        In the **Key** field enter your pass phrase. It can be 4-80 characters in length, including:

        - Upper- or lowercase letters (A-Z, a-z)
        - Digits (0-9)
        - Special characters: #, @, $, or blank

     b. In the **Key confirmation** field enter the same pass phrase again. Press the **OK** push button.

   - If you select **Hexadecimal:**

     a. The Set Master Key window (Figure 5 in topic 1.1.2.2.1) is displayed.

        In the **Key** field enter a hexadecimal string. It is exactly 32 characters in length, including:

        - Upper- or lowercase letters (A-F, a-f)
        - Digits (0-9).

     b. In the **Key confirmation** field enter the same hexadecimal string again. Press the **OK** push button.

7. The Select Format window for the KEK (Figure 6 in topic 1.1.2.2.1) is displayed. Continue with the instructions in ″Supplying the Format for the Authenticator Key-Encrypting Key.″

Supplying the Format for the Authenticator Key-Encrypting Key: Whether or not you are using the 4755 Cryptographic Adapter card, complete the following steps:

1. On the Select Format window, select one of the following formats to create the KEK:

   - Pass phrase
   - Hexadecimal string

   Press the **OK** push button.

   - If you select **Pass phrase:**

     a. The Set Key-encrypting Key window (Figure 7 in topic 1.1.2.2.1) is displayed.

        In the **Key** field enter your pass phrase. It is 4-80 characters in length, including:

        - Upper- or lowercase letters (A-Z, a-z)
        - Digits (0-9)
        - Special characters: #, @, $ or blank

     b. In the **Key confirmation** field enter the same pass phrase again. Press the **OK** push button.

   - If you select **Hexadecimal:**

     a. The Key-encrypting Key window (Figure 8 in topic 1.1.2.2.1) is displayed.

        In the **Key** field enter a hexadecimal string. It must be exactly 32 characters in length, including:

        - Upper- or lowercase letters (A-F, a-f)
        - Digits (0-9)

     b. In the **Key confirmation** field enter the same hexadecimal string again. Press the **OK** push button.

2. If you are using the IBM 4755 Cryptographic Adapter card, continue the steps in "Completing the Security Authenticator Installation." Otherwise, the Set Random Seed Values window is displayed.

3. The authenticator uses how you enter data on the Set Random Seed Values window to encrypt its security information. Enter any input at random as long as you use the following guidelines:

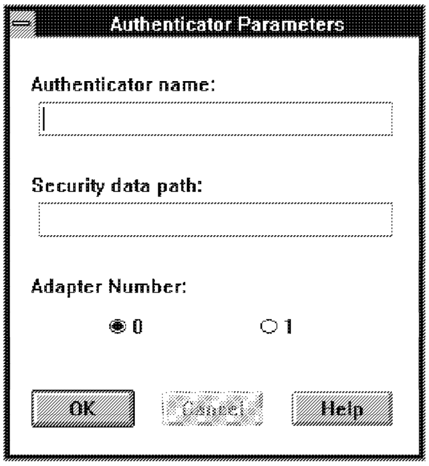
   - Enter at least eight characters in each field.
   - Pause at least half a second between keystrokes.
   - Complete all four fields.

   Press the **OK** push button. The Authenticator Personalization window (Figure 11) is displayed.

Continue with the steps in "Completing the Security Authenticator Installation."

Completing the Security Authenticator Installation: On the Authenticator Personalization window (Figure 11), you can enable the NetBIOS

comunication for the authenticator. To enable other communications
| protocols after you install the authenticator, see "Personalizing the
| Authenticator" in the Installation and Configuration Guide.



PICTURE 11

Figure 11. Authenticator Personalization Window

To finish installing the authenticator, perform the following steps:

1. Enter an Authenticator name following these guidelines:

   - It can be 1-12 characters in length.
   - All characters are valid except a single asterisk (*) or all blanks.
   - It is not case sensitive even if it is displayed in uppercase.
   - It must match the authenticator name you typed when you personalized the DCAF gateway or LAN directory.

2. For Security Data Path, enter the path (for example, C:\DCAF13) in which the security data files will be stored on the security authenticator. Ensure that the authenticator can access the path.

   - The path is 1-50 characters in length.
   - For character guidelines, follow the OS/2 conventions for paths.

   Reminder

   Keep a record of the path that you enter here. You will use the same security data path when you create the security authenticator database on the administrator.

3. For Adapter Number, select 0 or 1. The default is 0.

4. Press the **OK** push button.

You have completed installation of the authenticator.

After you are done

Now you are ready to configure the communications. See "Configuring the Communications for Secure Sessions" in topic 1.2 for configuration scenarios that you can copy.

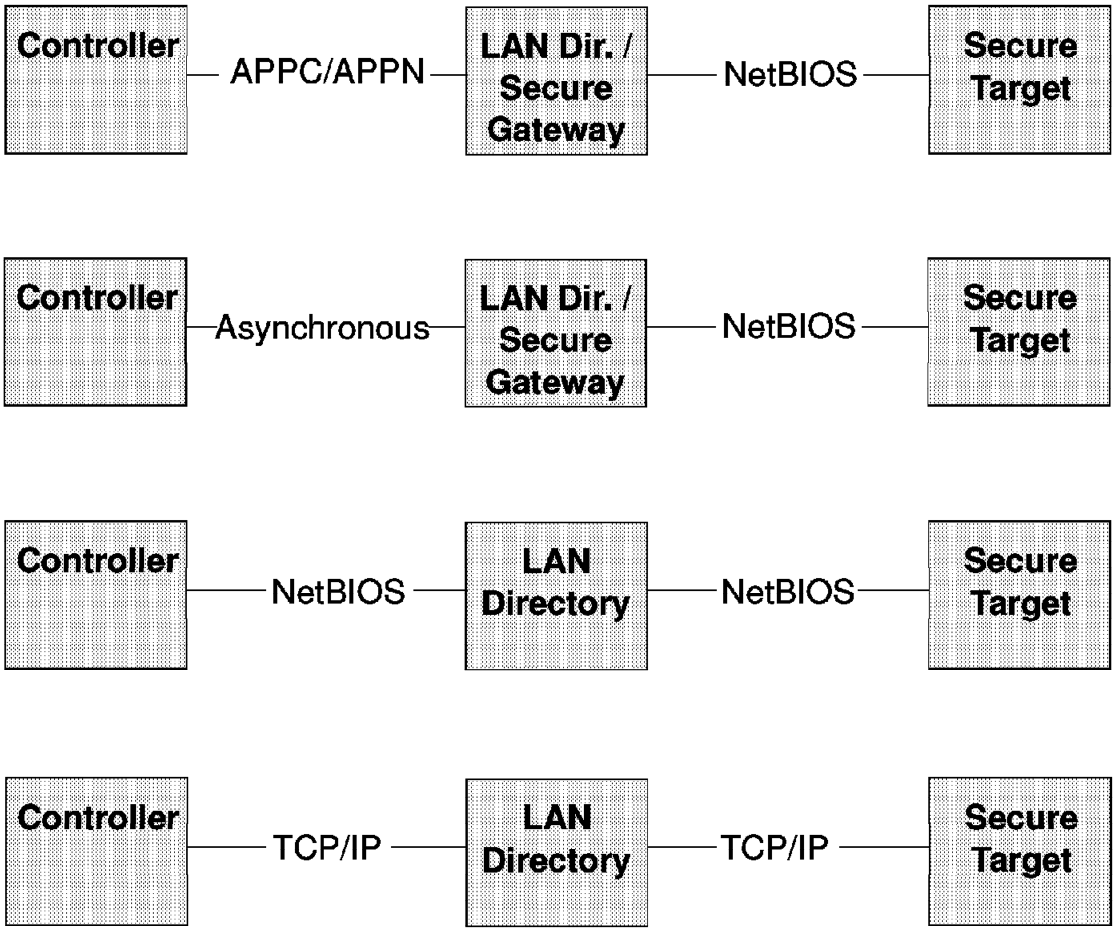
1.2 Configuring the Communications for Secure Sessions

Figure 12 shows all the combinations of connections for secure sessions. You need to configure for secure sessions for two purposes: for controllers to access and work on secure targets and for the administrator to distribute the security databases to remote authenticators. Because it is the controller on the administrator workstation that transfers the databases to the secure target on the authenticator workstation, you configure the workstations as for secure sessions.

Reminder

Remember to enable on the authenticator the protocols with which the other workstations connect it. If you did not do this during installation, look up ″Personalizing the Authenticator″ in the Installation and Configuration Guide to do it now, and then return here to continue.

Choose an arrangement that corresponds to your network.



PICTURE 12

Figure 12. Types of Connections for Secure Sessions

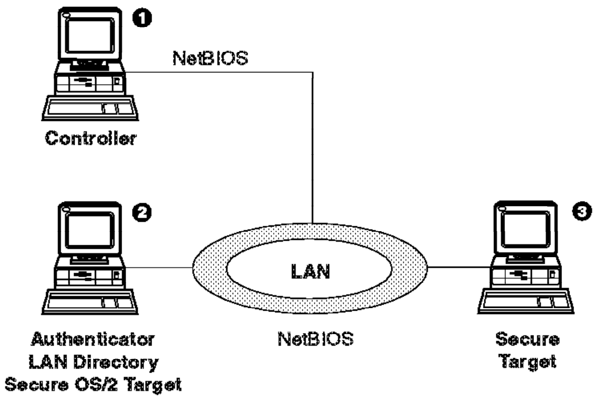
The first two connections consist of two segments: from the controller to the gateway and from the gateway to the target. For the first segment, you can follow any controller to gateway scenario from Part 3. "Configuring" in the Installation and Configuration Guide. For the second segment, follow the instructions in the chapter "Gateway to a Target via NetBIOS on a Logical LAN" in the Installation and Configuration Guide.

The next three connections use a single protocol from the controller all the way to the target. This chapter includes instructions for these three simple LAN connections:

- "Secure Session: Controller to Target via NetBIOS" in topic 1.2.1
- "Secure Session: Controller to Target via TCP/IP" in topic 1.2.2

1.2.1 Secure Session: Controller to Target via NetBIOS

This scenario describes how to set up a NetBIOS connection between a controller and a secure target. Figure 13 shows a typical setup. However, you can distribute the components on the LAN any way you want on the LAN as long as the authenticator is with a secure target.



PICTURE 13

Figure 13. Example of a Secure Controller/Target Connection Using NetBIOS

1.2.1.1 Before You Start

The instructions in this example assume that OS/2 is installed in drive C: and that the LAN Protocol Support (LAPS) is installed in default directory **c:\ibmcom**. If you installed LAPS in a different drive and directory, modify all the instructions accordingly. This example uses token-ring adapters.

Make sure that the following programs (see Table 1) are installed on the workstations.

Table 1. Software Needed for Secure NetBIOS Configuration

Workstation 1	Workstation 2	Workstation 3
• OS/2 Version 2.1 (or later) • LAPS • DCAF 1.31 with CSD level UB09850 controller	• OS/2 Version 2.1 (or later) • LAPS • DCAF 1.31 with CSD level UB09850 LAN directory, authenticator, and secure OS/2 target	• One of the following: - OS/2 Version 2.1 for OS/2 targets - DOS 6.3 (or later) for DOS and Windows t.s - MS-Windows Version 3.1 for Windows targets • LAPS for OS/2 targets • LAN Support Program for DOS or Windows targets • DCAF 1.31 with CSD level UB09850 secure OS/2, Windows, or DOS target

1.2.1.2 Updating LAPS for the OS/2 Workstations

Update the following LAPS parameters on the OS/2 workstations:

1. At an OS/2 prompt, enter **c:\ibmcom\laps** and press the **Enter** push button. The IBM LAN Adapter and Protocol Support logo window appears.

2. Press the **Configure...** push button. The Configuration dialog box appears.

3. Select the Configure LAN transports radio button and press the **Continue...** push button. The Configure Workstation window appears.

4. Ensure that IBM Token-Ring Network Adapter and IBM OS/2 NetBIOS appear in the Current Configuration list box.

5. To add IBM Token-Ring Network Adapter, from the Network Adapters list box, select IBM Token-Ring Network Adapter, and press the **Add** push button.

6. To add IBM OS/2 NetBIOS, from the Protocols list box again, select IBM OS/2 NetBIOS, and press the **Add** push button.

7. From the Current Configuration list box, select IBM OS/2 NetBIOS and press the **Edit** push button. The Parameters for IBM OS/2 NetBIOS window appears. If you have the gateway and target on the same workstation, skip the next step.

8. **For targets only:** In the Universally administered address reversed field, enter **No**.

9. Increase the NetBIOS resources by the sum of the resources that are required for each component that is on the same workstation. Increase the values in the following fields:

   - Maximum sessions
   - Maximum commands
   - Maximum names

   Add the minimum values for DCAF to the values that you already have for your NetBIOS environment. Refer to Table 19 in the Installation and Configuration Guide to determine the minimum value of NetBIOS resources required for each component.

10. Press the **OK** push button. The Configure Workstation window reappears.

11. Press the **OK** push button. The IBM LAN Adapter and Protocol Support logo window reappears.

12. Press the **Exit** push button. The CONFIG.SYS Updates window appears.

13. In the Drive to Update list box, select **C**. Press the **Continue...** push button. The message CONFIG.SYS updated appears.

14. Press the **OK** push button. The Exiting LAPS window appears.

15. Press the **Exit** push button.

16. Stop all applications on the workstation and shut down the workstation.

You have completed the configuration for the OS/2 workstations.

After you are done

Perform the steps in the next section only if you have a DOS or Windows target. Then add the LAN directory to the workstation directory on the controller. See the chapter "Configuring the Workstation Directory" in the Installation and Configuration Guide.

1.2.1.3 Updating the NetBIOS Resources for the DOS or Windows Target

For the DOS or Windows target, update the CONFIG.SYS in the native DOS environment. Perform the following steps:

1. Edit the CONFIG.SYS file.

2. At the DXMT0MOD.SYS statement, increase the values for sessions, commands, and names in the Maximum sessions, Maximum commands, and Maximum names fields by adding the minimum values for DCAF to the

values that you already have for your NetBIOS environment. DCAF requires the following minimum values:

- Maximum sessions: 1
- Maximum commands: 5
- Maximum names: 2

3. If you are using IBM LAN Support Program Version 1.30.1 on the Windows target, you can improve mouse performance during a session by including the following parameter in the DXMT0MOD.SYS statement: **PBA=0**. Otherwise, go to the next step.

4. Save and close the CONFIG.SYS file.

5. Stop all applications on the workstation and shut down the workstation.

You have completed the configuration for this scenario.

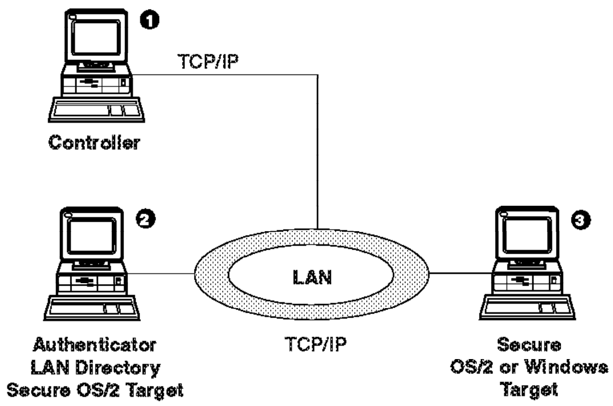
After you are done

Now you are ready to add the LAN directory to the workstation directory on the controller. See the chapter "Configuring the Workstation Directory" in the Installation and Configuration Guide.

For diagnosis and problem solving for this scenario, see "Diagnosis" in the Installation and Configuration Guide.

1.2.2 Secure Session: Controller to Target via TCP/IP

This scenario describes how to set up a TCP/IP connection between a controller and a secure target. Figure 14 shows a typical setup. However, you can distribute the components any way you want on the LAN as long as the authenticator is with a secure target.



PICTURE 14

Figure 14. Example of Secure Connection Using TCP/IP

1.2.2.1 Before You Start

In this scenario TCP/IP is installed in default directory **c:\tcpip**. If you installed it in a different drive and directory, modify all the instructions accordingly.

The maximum transmit unit value is 4400 for a 16MB token-ring adapter. If you have a different token-ring adapter, use the maximum transmit unit value for your token-ring adapter.

Make sure that the following programs (see Table 2) are installed on the workstations.

Table 2. Software Needed for Secure TCP/IP Configuration

Workstation 1	**Workstation 2**	**Workstation 3**
• OS/2 Version 2.1 (or later) • DCAF 1.31 with CSD level UB09850 controller • TCP/IP for OS/2 2.0 (or later)	• OS/2 Version 2.1 (or later) • DCAF 1.31 with CSD level UB09850 LAN directory, authenticator, and secure target • TCP/IP for OS/2 2.0 (or later)	• One of the following: - OS/2 Version 2.1 for OS/2 targets - DOS 6.3 (or later) for Windows targets - MS-Windows Version 3.1 for Windows targets • DCAF 1.31 with CSD level UB09850 secure OS/2 or Windows target • TCP/IP for OS/2 2.0 (or later) for OS/2 targets or TCP/IP 2.1.1 for Windows targets

On each workstation, do the following configuration tasks:

- Update the network configuration
- Update the service configuration
- Create or update the HOSTS file (optional)

1.2.2.2 Updating the Network Configuration

To update the network configuration, complete the following steps:

1. At an OS/2 prompt, enter

   c:\tcpip\bin\tcpipcfg

   The TCP/IP configuration notebook appears.

2. Select the Enable LAN adapter 0 check box.

3. In the IP address field, enter IP address of your workstation. This is a unique number that you (or your network administrator) assigns to each workstation in the network. It is a string composed of four numerical substrings, separated by periods (nnn.nnn.nnn.nnn.). The range for each substring is 0-255.

4. In the MTU field, enter **4400**. Now update the Services configuration.

1.2.2.3 Updating the Services Configuration

To update the services configuration,

1. Select the Services tab. The Services notebook page appears.

2. In the This machine's hostname field, enter the hostname of your workstation, assigned by your system administrator.

3. If you know the domain server address, enter it in the Domain Nameserver(s) (address) field.

4. In the Domain Name field, enter domain name of your workstation.

5. To validate your changes and close the TCP/IP notebook, press **Alt+F4**.

6. Select Save.

If you completed step 3, you have finished configuring the workstations. Otherwise, continue with the next task.

After you are done

Now you are ready to add the LAN directory to the workstation directory on the controller. Use the same entries that you used here for the LAN directory. See the chapter "Configuring the Workstation Directory" in the Installation and Configuration Guide.

1.2.2.4 Creating the HOSTS File

Do this task only if you did not complete Step 3 in topic 1.2.2.3 in "Updating the Services Configuration" in topic 1.2.2.3, or if you do not know the IP address of the target. Create or update a simple ASCII text file, called a HOSTS file, that contains the IP address and name of the workstations that need to communicate in the TCP/IP configuration. Complete the following steps:

1. At an OS/2 prompt, enter **c:\tcpip\etc** and press the **Enter** push button.

2. In the HOSTS file, enter a line for each workstation in the following format:

   IPaddress hostname /*Comment* ./

IPaddress hostname /*Comment* ./

3. Select Save and close.

4. Close all the applications running on the controller and shut down the controller.

You have finished configuring the workstations.

After you are done

Now you are ready to add the LAN directory to the workstation directory on the controller. Use the same entries that you used here for the LAN directory. See the chapter ″Configuring the Workstation Directory″ in the Installation and Configuration Guide.

For diagnosis and problem solving for this scenario, see ″Diagnosing Common Problems″ in the Installation and Configuration Guide.

1.3 Configuring the Workstations for Pass Phrase Updates

When controllers change their pass phrases, they send the new ones to the administrator workstation. To enable the controller workstations to communicate with the administrator, you need to do these tasks:

- Configure the communications on the administrator and controllers.
- Add the administrator to the workstation directory of each controller.
- Enable the communications for the connection on the administrator. Perform this task if you did not enable the protocols during installation.

Choose a scenario that resembles the connection between your controller | and administrator from the following list of chapters in the Installation | and Configuration Guide and follow the configuration instructions. Then, return to this chapter to complete the other two tasks.

| - Chapter 17, "Controller to a Target via APPN on a Token-Ring LAN". | Replace the target with the administrator in the instructions.

| - Chapter 22, "Controller to the Security Administrator via APPC on a | Token-Ring LAN".

| - Chapter 24, "Controller to a Security Administrator via Asynchronous".

| - Chapter 27, "Controller to a Target Directly via NetBIOS". Replace | the target with the administrator in the instructions.

| - Chapter 29, "Controller to a Target via TCP/IP". Replace the target | with the administrator in the instructions.

1.3.1 Defining the Administrator on the Controller

After you configure the controller and administrator workstations to communicate with each other, you need to define the administrator in the workstation directory on each controller.

To change an administrator definition that already exists, first remove the administrator (see "Changing or Removing an Administrator" in topic 1.3.2) and then redefine it.

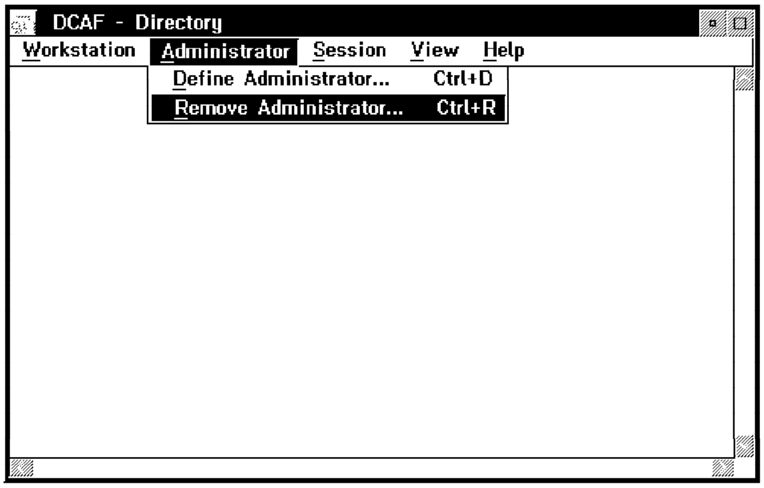
To define the administrator, you need to both provide a general and a protocol description.

1.3.1.1 General Description

To define the general description of the administrator, perform the following steps:

1. To start the DCAF controller, first choose the DCAF folder from the desktop, and then choose the DCAF Controller icon. First, the IBM logo, then the Distributed Console Access Facility - Controller window | appears.

2. From Session on the menu bar of the Distributed Console Access Facility - Controller window, choose Open a Workstation Directory.... The DCAF - Directory window appears.

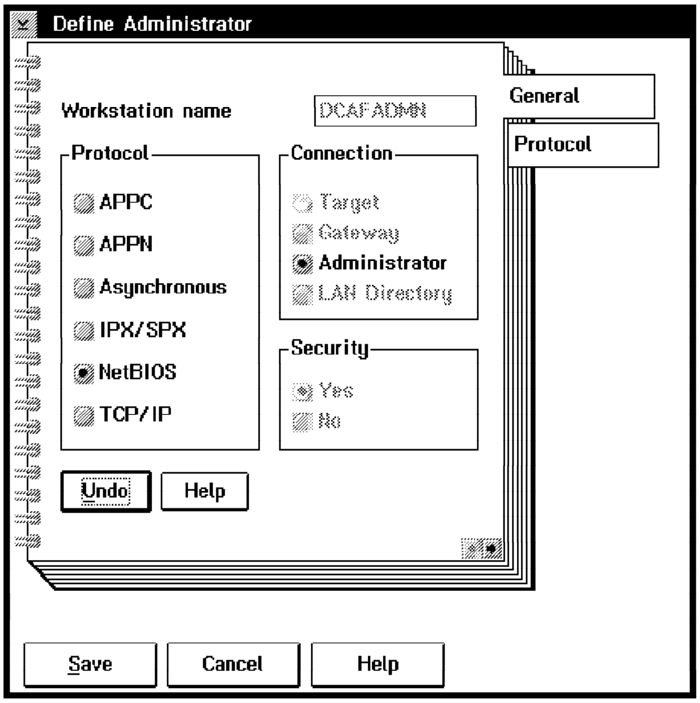


PICTURE 15

Figure 15. Defining the Administrator

3. From Administrator on the menu bar (Figure 15), choose Define Administrator....

   The Define Administrator notebook (Figure 16) appears.



PICTURE 16

Figure 16. Define Administrator General Notebook

   In the Workstation name field, DCAFADMN is already displayed because the DCAF environment has only one administrator. In the Connection field, Administrator is already selected. In the Security field, Yes is already selected.

4. From the Protocol list box, select the communications protocol that you use to connect to the workstation.

You are ready to provide the protocol description.

1.3.1.2 Protocol Description

Provide a protocol description for the communication type that you use to connect to the administrator. From the Define Administrator notebook, select the Protocol tab. If, on the General notebook page, you selected:

- APPC, the APPC page (Figure 17 in topic 1.3.1.2.1) appears.

- APPN, the APPN page (Figure 18 in topic 1.3.1.2.2) appears.

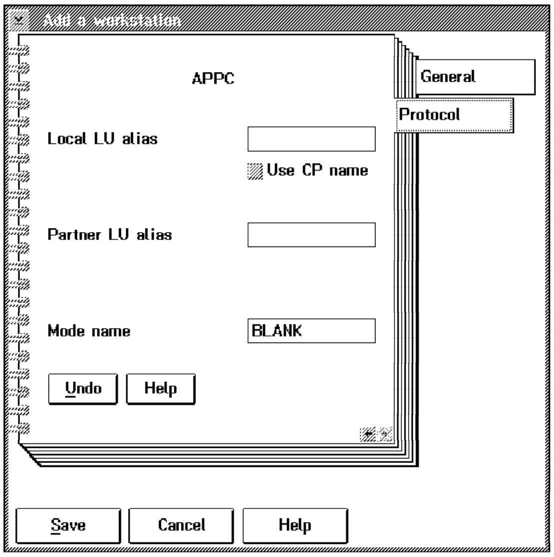
- Asynchronous, the Asynchronous page (Figure 19 in topic 1.3.1.2.3) appears.

- NetBIOS, the NetBIOS page (Figure 20 in topic 1.3.1.2.4) appears.

- TCP/IP, the TCP/IP page (Figure 21 in topic 1.3.1.2.5) appears.

1.3.1.2.1 APPC Protocol Description

Define the following APPC parameters for the workstation.



PICTURE 17

Figure 17. APPC Protocol Page

Complete the following steps:

1. If you are using the CP name (local node name) of the workstation, select the Use CP Name check box. When the check box is selected, the Local LU Alias field is unavailable. Skip to Step 3. Otherwise, leave it unselected.

2. In the Local LU Alias field, enter your controller LU name.

Character guidelines:

- It is 1-8 characters in length.

- It can be any combination of characters, except left parenthesis, right parenthesis, comma, semicolon, blank.

- It cannot start with @.

3. In the Partner LU Alias field, enter the LU name of the workstation to which you are connecting.

   Character guidelines:

   - It is 1-8 characters in length.

   - It can be any combination of characters, except left parenthesis, right parenthesis, comma, semicolon, blank.

   - It cannot start with @.

4. In the Mode Name field, enter the mode name for DCAF in your network. Valid characters are the same as for the local LU alias.

5. Press the Save push button.

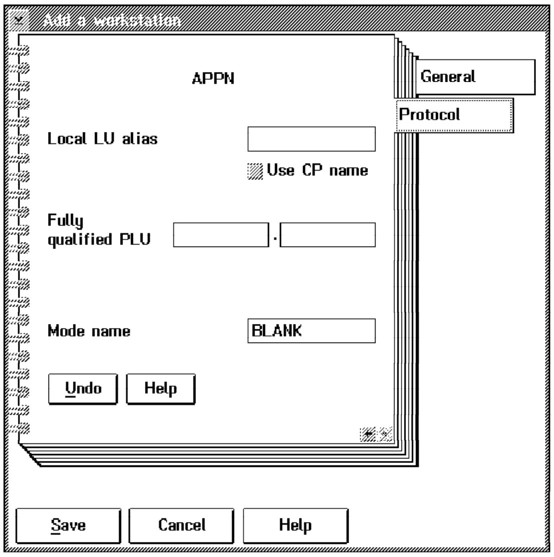
6. Close the notebook. The administrator appears in the workstation directory list.

After you are done

Now you are ready to set up the security databases. See "Setting up the Security Databases" in topic 1.4 for instructions.

1.3.1.2.2 APPN Protocol Description

Define the following APPN parameters for the workstation.



PICTURE 18

Figure 18. APPN Protocol Page

Complete the following steps:

1. If you are using the CP name (local node name) of the workstation, select the Use CP Name check box. When the check box is selected, the Local LU Alias field is unavailable. Skip to Step 3. Otherwise, leave it unselected.

2. In the Local LU Alias field, enter your controller LU name.

Character guidelines:

- It is 1-8 characters in length.
- It can be any combination of characters, except left parenthesis, right parenthesis, comma, semicolon, blank.
- It cannot start with @.

3. In the Fully Qualified PLU field, enter your node ID and the destination workstation LU name

   Character guidelines are the same as for the local LU alias.

4. In the Mode Name field, enter the mode name for DCAF in your network.

5. Press the Save push button.

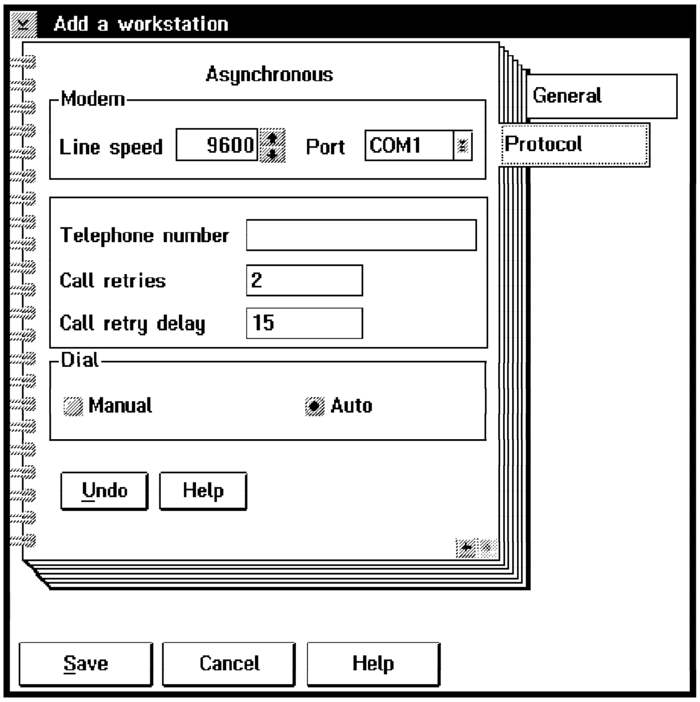
6. Close the notebook. The administrator appears in the workstation directory list.

After you are done

Now you are ready to set up the security databases. See "Setting up the Security Databases" in topic 1.4 for instructions.

1.3.1.2.3 Asynchronous Protocol Description

Define the following asynchronous parameters for the workstation.



PICTURE 19

Figure 19. Asynchronous Protocol Page

Complete the following steps:

1. From the Modem list box, in the Line Speed field, select the modem transmission rate in bits per second. For asynchronous connections, use the highest line speed supported by your modem for best performance.

   The default is 9600.

2. In the Port field, select the asynchronous communication port number that the destination workstation uses.

   The range is 1-3. The default is 1.

3. In the Telephone Number field, enter the modem telephone number of the workstation.

   The maximum number of characters is 250.

4. In the Call Retries field, type the number of times you want DCAF to redial the telephone number if it cannot make the connection immediately. The range is 0-20. The default is 2.

5. In the Call Retry Delay field, type the pause in between retries in seconds. The range is 1-1200. The default is 15.

6. In the Dial box, select the kind of dialing, automatic or manual, for the workstation modem.

7. Press the Save push button.

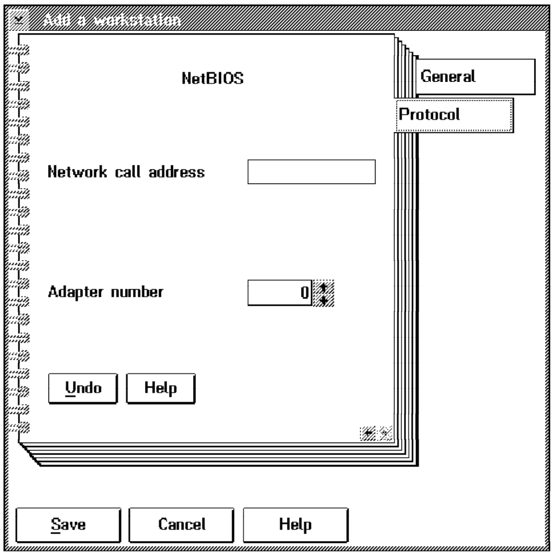
8. Close the notebook. The administrator appears in the workstation directory list.

After you are done

Now you are ready to set up the security databases. See "Setting up the Security Databases" in topic 1.4 for instructions.

1.3.1.2.4 NetBIOS Protocol Description

Define the adapter number of the administrator.



PICTURE 20

Figure 20. NetBIOS Protocol Page

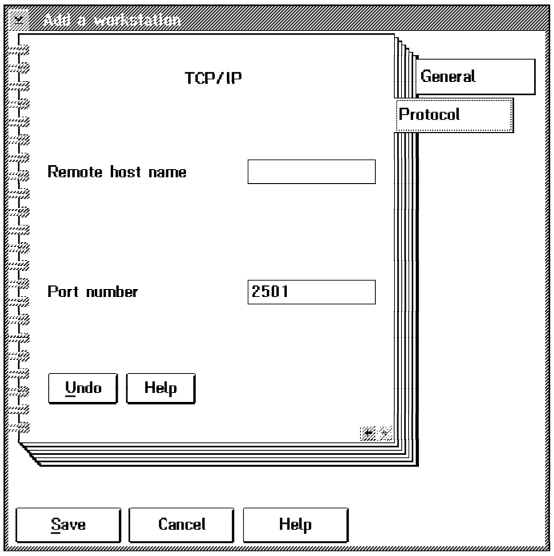
1. In the Network call address field, the administrator name DCAFADMN is displayed. The field is grayed out because the DCAF network has only one administrator.

2. In the Adapter number field, select the adapter number of the workstation.

   The range is 0-3. The default is 0.

1.3.1.2.5 TCP/IP Protocol Description

Define the following TCP/IP parameters for the workstation:



PICTURE 21

Figure 21. TCP/IP Protocol Page

1. In the Remote Host Name field, enter host name or the IP address of

the administrator. Use the host name only if you are sure that the workstation and IP address of the administrator are listed in the HOSTS file on your workstation.

Character guidelines for host name:

- It is 1-256 characters in length.
- Upper- or lowercase letters (A-Z, a-z).
- Digits (0-9).
- All special characters except blanks.

The IP address is a string composed of four substrings of numbers, divided by a period (nnn.nnn.nnn.nnn.). The range for each substring is 0-255.

2. In the Port Number field, enter the port number of the administrator. For DCAF, the range is 1024-65534. The default is 2504.

3. Press the Save push button.

4. Close the notebook. The administrator appears in the workstation directory list.

After you are done

Now you are ready to set up the security databases. See "Setting up the Security Databases" in topic 1.4 for instructions.

1.3.2 Changing or Removing an Administrator

To change the administrator definition, you need to first remove and then redefine it.

To remove an administrator, perform the following steps:

1. Ensure that the controller is running.

2. From Session on the menu bar of the Distributed Console Access Facility - Controller window, choose Open a Workstation Directory.... The DCAF - Directory window appears.

3. From Administrator on the menu bar (Figure 15 in topic 1.3.1.1), choose Remove Administrator.... A message requesting confirmation to delete the administrator appears.

4. Press the Yes push button. DCAF removes the administrator.

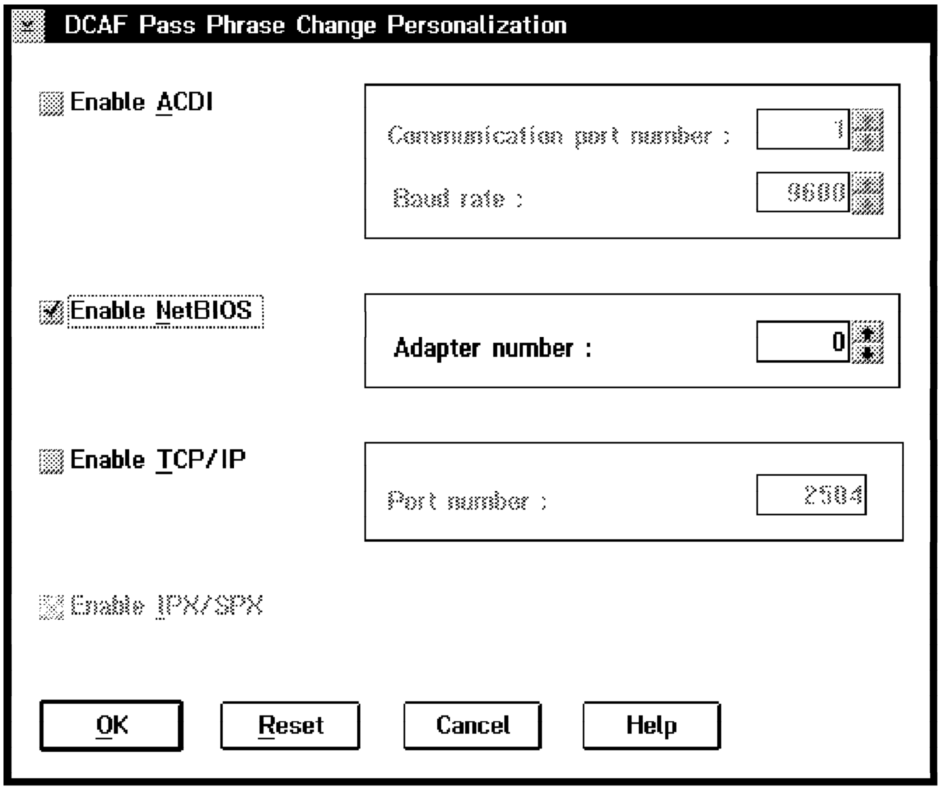
1.3.3 Enabling Communications Protocols on the Administrator

You must enable the protocols with which the controllers communicate their new pass phrases. You can enable the following protocols:

- ACDI
- NetBIOS
- TCP/IP

Perform the following steps:

1. Choose **Personalization...** (or Ctrl+P shortcut key) from the **Options** pull-down menu on the DCAF Security Administrator main window. The DCAF Pass Phrase Change Personalization window (Figure 22) appears.



PICTURE 22

Figure 22. Enabling Protocols for Pass Phrase Changes

2. To enable a protocol, select its check box and provide the parameters requested, if any:

   Enable ACDI
   For Communication Port Number, the values are 1-3.

   For Baud Rate, the values are 1200, 2400, 4800, 9600, 19200, 38400, 48000, 56000, 578000, or 64000. The default is 9600.

   Enable NetBIOS
   For Adapter Number, select 0 or 1. The default is 0.

   Enable TCP/IP
   For Port Number, the range is 1024-65534. The default is 2504.

3. Press the **OK** push button.

1.4 Setting up the Security Databases

Before you begin, ensure that you have already installed the required components, configured the communications, and configured the workstation directory on the controllers. If you have not, then do it now. You can find instructions in "DCAF Security" in topic 1.0.

Setting up the security databases consists of the following tasks:

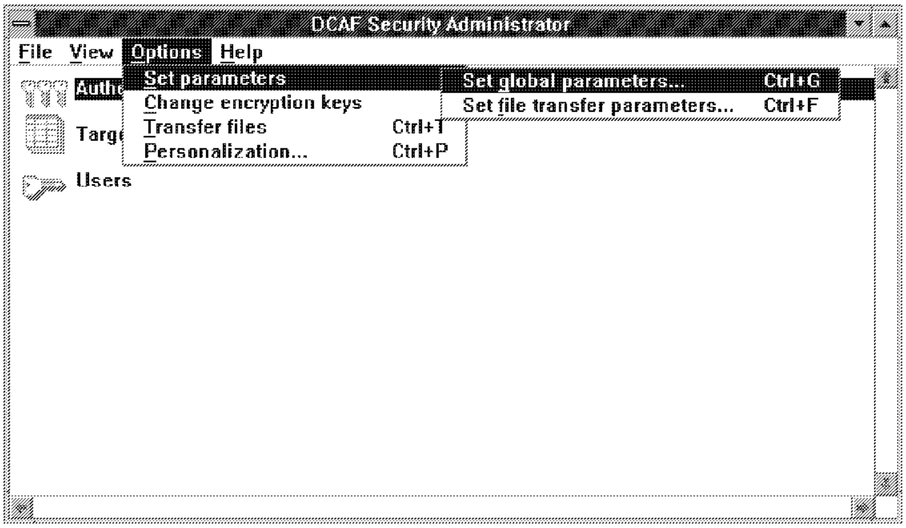
- Defining global parameters for user classes and pass phrases
- Defining the levels of access to the target
- Creating user profiles for the controllers
- Defining the authenticators for the administrator
- Assigning the secure target to the authenticators
- Transferring the security databases to the authenticators

1.4.1 Defining General Parameters

Before you can create the security databases, you must define some general parameters, such as the number of user access levels.

To define the global parameters, complete the following steps:

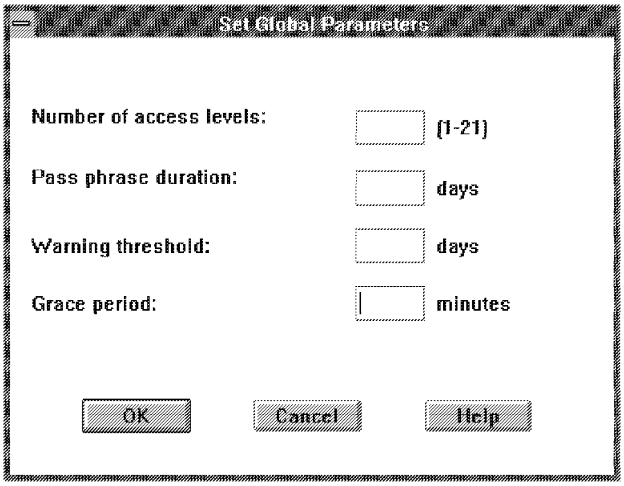
1. To start the security administrator, choose the Distributed Console Access Facility icon from the desktop. Then choose the **DCAF Administrator** icon. The Security Administrator window (Figure 23) is displayed.



PICTURE 23

Figure 23. Security Administrator Main Window with Options Pull-Down Menu

2. From the Options pull-down menu, choose **Set parameters...** and then choose **Set global parameters...**. The Set Global Parameters window (Figure 24) appears.



PICTURE 24

Figure 24. Set Global Parameters

3. In the Number of access levels field, enter the number of categories of users that can access the secure target. Include the security administrator level (with the most authority). The range is 1-21.

4. In the Pass phrase duration field, enter the interval for which pass phrases are valid. The range is 1-32 768 days.

5. In the Warning threshold field, enter the number of days that users are notified before their pass phrases expire. The range is 1-32 767 days. The value must be lower than the value you enter for Pass phrase duration.

6. In the Grace period field, enter the period that users can use and update their pass phrase after it expires. When the grace period is over, users must contact the network administrator to reset their pass phrase. The range is 1-32 768 minutes.

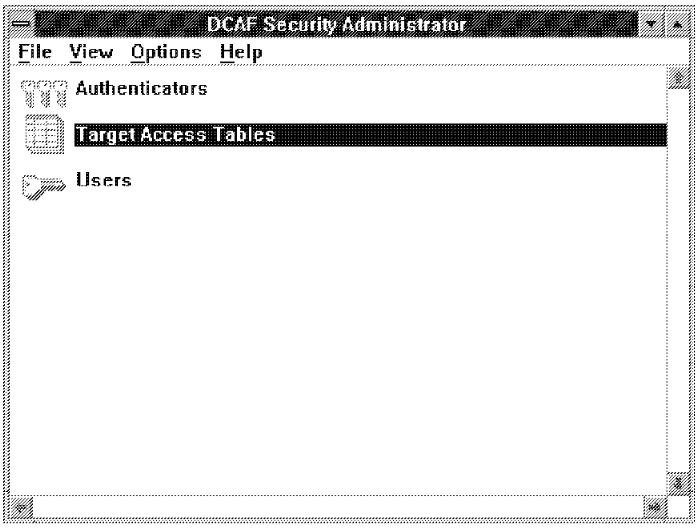
7. Press the **OK** push button to return to the DCAF Security Administrator window.

You have set the user classes. Now you are ready to define access levels for the targets.

1.4.2 Defining Access Levels for the Targets

The target access table determines the actions that the controller can perform on a secure target. You can create a table for each target profile and associate the table with the targets for which the limits apply.

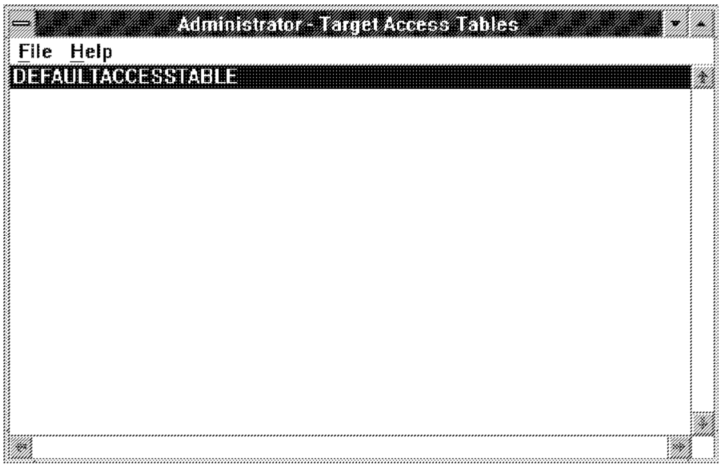
To create a target access table, complete the following steps:



PICTURE 25

Figure 25. DCAF Security Administrator Main Window

1. Choose **Target Access Tables** from the DCAF Security Administrator window (Figure 25). The Administrator - Target Access Tables window (Figure 26) is displayed.

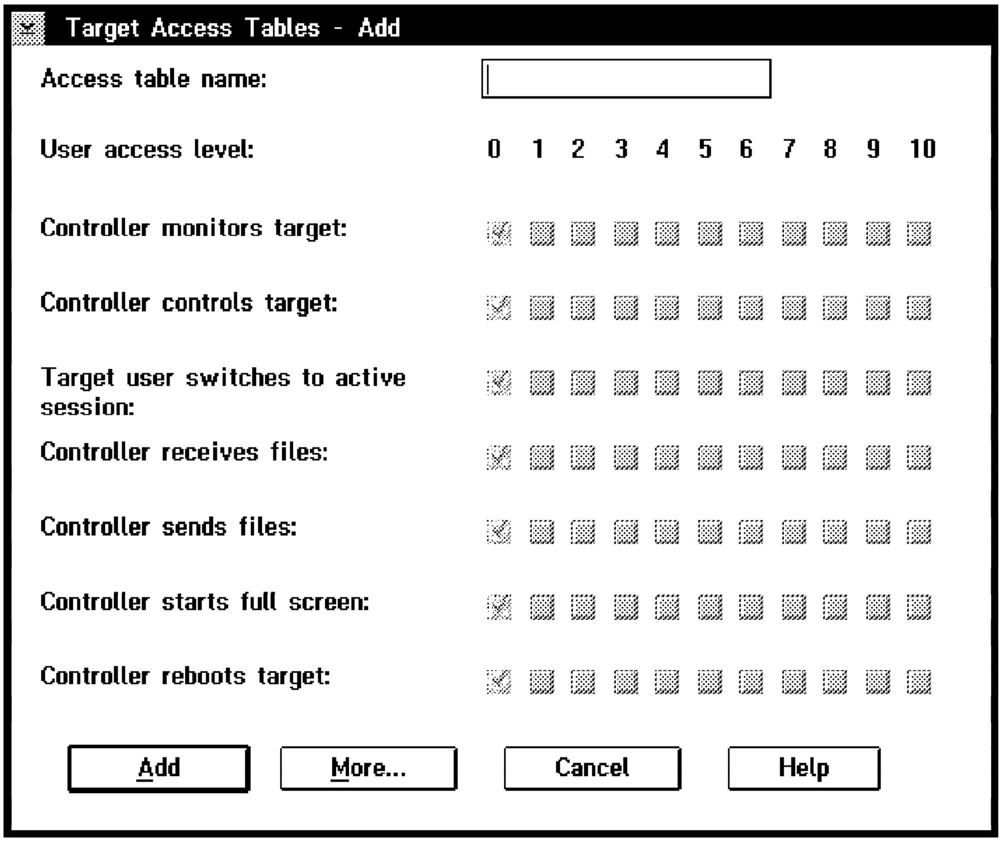


PICTURE 26

Figure 26. Target Access Tables

The window contains a predefined table, **DEFAULTACCESSTABLE**, which you can use or change, but not delete.

2. Choose **Add...** from the File pull-down menu. The Target Access Tables - Add window is displayed.



PICTURE 27

Figure 27. DCAF Adding a Target Access Table

3. In the Access table name field, enter a name that identifies the table. The access table name can be 1-60 characters in length, including:

   - Upper- or lowercase letters (A-Z, a-z)
   - Digits (0-9)
   - Special characters #, @, and $
   - No blanks between characters

   You can create up to 21 levels (from 0 to 20).

4. After you complete the table, press the **Add** push button. The Administrator - Target Access Tables window is displayed.

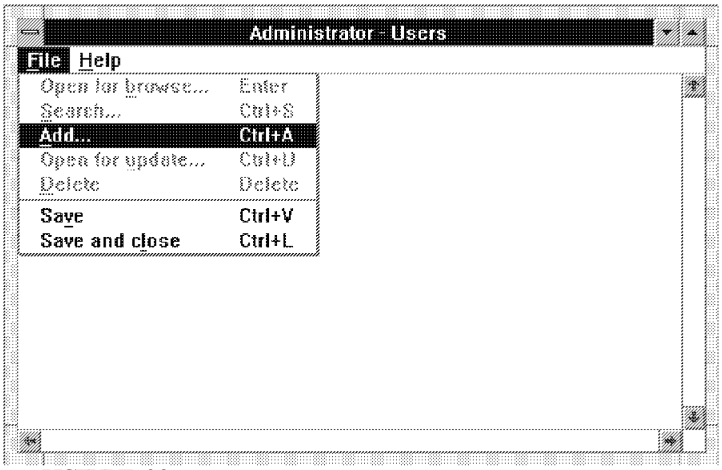
5. Choose **Save** or **Save and close** from the File pull-down menu. Now you are ready to create user profiles for the controllers.

1.4.3 Creating User Profiles for Authorized Controllers

In the user profiles, you specify which targets users can access and when, and their access levels.

To create the user profiles, complete the following steps:

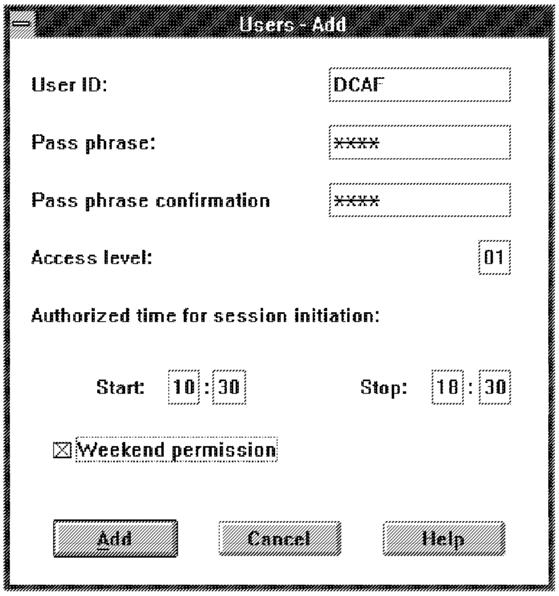
1. From the Security Administrator main window (Figure 25 in topic 1.4.2), choose **Users**. The Administrator - Users window (Figure 28) is displayed.



PICTURE 28

Figure 28. Administrator - Users Window

2. From the File pull-down menu, choose **Add...**. The Users - Add window (Figure 29) is displayed.



PICTURE 29

Figure 29. Example of Users - Add Window

3. In the User ID field, enter the user's ID.

   The user ID can be 1-8 characters in length, including:

   - Upper- or lowercase letters (A-Z, a-z)
   - Digits (0-9)
   - Special characters: #, @, or $

4. In the Pass phrase field, enter an initial pass phrase that users can change the first time they log on for a secure session.

   The pass phrase can be 4-80 characters in length, including:

   - Upper- or lowercase letters (A-Z, a-z)

- Digits (0-9)
- Special characters: #, @, $ or blank

5. In the Pass phrase confirmation field, enter again the pass phrase you just typed.

6. In the Access level field, enter the level of access for the user. You defined the access levels in "Defining Access Levels for the Targets" in topic 1.4.2. Level 0 enables the user (usually, the administrator of your network) to perform all actions on the target. At least one user must have level 0 access.

7. In the Start and Stop fields, enter the interval, in hours and minutes, during which the user can access the target. The range is:

   - For hours: 00 - 23
   - For minutes: 00 - 59.

   For 24-hour access, enter **00:00** in both Start and Stop fields.

8. To give the user access on Saturdays and Sundays, select the Weekend permission check box.

9. Press the **Add** push button. The Administrator - Users window is displayed. Repeat the previous steps to add more users.

10. After you finish adding the users, select **Save** or **Save and close** from the File pull-down menu.

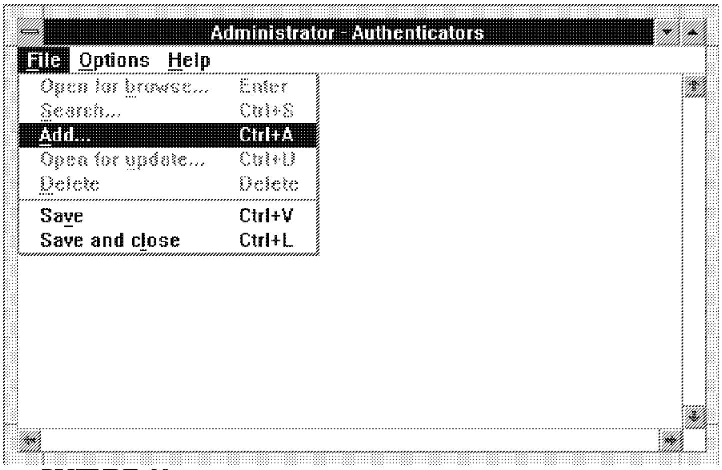
You have created user profiles for authorized controllers of targets. Now you are ready to define the authenticators for the administrator.

1.4.4 Defining the Authenticators for the Administrator

You must define all the authenticators in the network so that the administrator can transfer the security information you typed to the authenticators.

To define the authenticators, complete the following steps:

1. From the DCAF Security Administrator window (Figure 25 in topic 1.4.2), choose **Authenticators**. The Administrator - Authenticators window (Figure 30) is displayed.



PICTURE 30

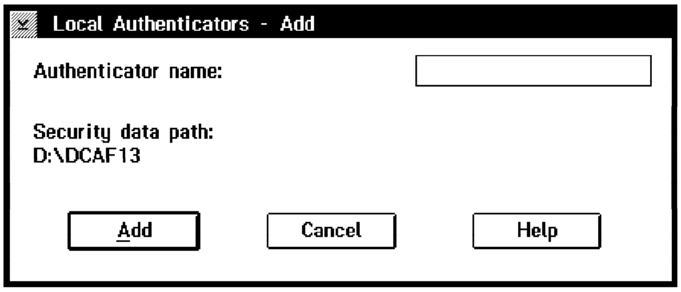
Figure 30. Authenticators with File Pull-Down Menu

2. From the File pull-down menu, choose **Add...**. The following message is displayed:

   Will this security authenticator
   be administered locally?

   - Select **Yes** only if your network has only one authenticator and if the authenticator is on the same workstation as the administrator.

     a. If you select **Yes**, the Local Authenticator - Add window (Figure 31) is displayed.



PICTURE 31

Figure 31. Local Authenticators - Add Window

   In the Authenticator name field, enter a descriptive name. It can be 1-12 characters long and must be unique for the administrator.

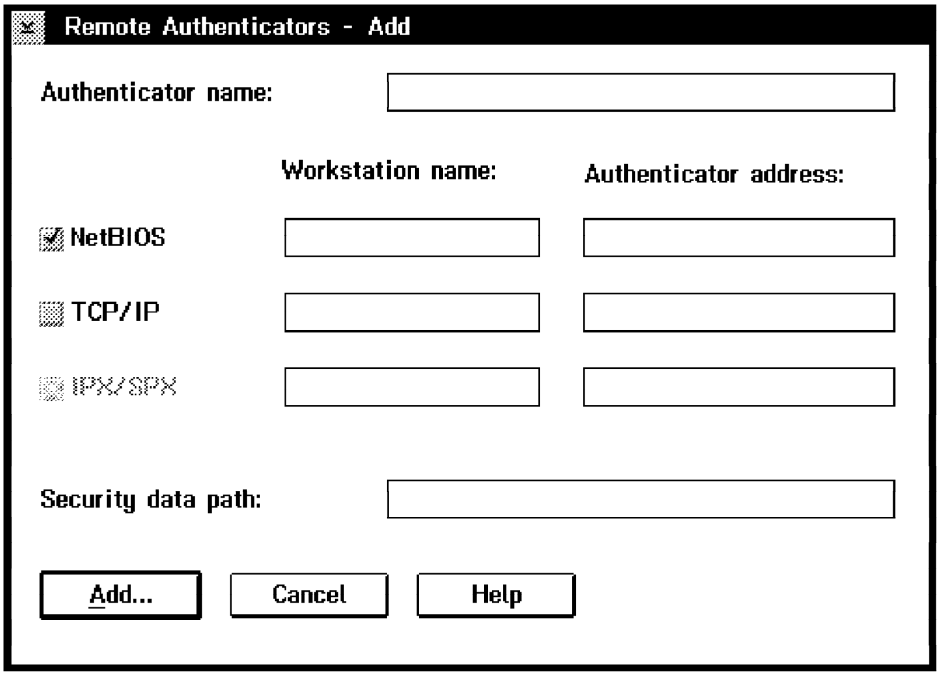
   The Security data path field displays the path that you typed when you installed the authenticator. The administrator stores the security information in this path.

     b. Press the **Add** push button. The Administrator - Authenticators window is displayed.

     c. Choose **Save** from the File pull-down menu.

   - Select **No** in all other cases.

     a. If you select **No**, the Remote Authenticators - Add window (Figure 32) is displayed.



PICTURE 32

Figure 32. Remote Authenticators - Add Window

b. In the Authenticator name field, enter a descriptive name that helps you to recognize the authenticator in your network. It can be 1-12 characters in length and must be unique for the administrator.

c. Select the check box for the protocols that the controller uses for secure sessions through this authenticator. Then provide the parameters requested:

NetBIOS

In the Workstation name field, enter the name that you typed when you added the LAN directory or secure gateway to the DCAF directory on the controller/administrator workstation.

In the Authenticator Address field, enter the LAN adapter address of the authenticator workstation.

TCP/IP

In the Workstation name field, enter the name that you typed when you added the LAN directory to the DCAF directory on the controller/administrator workstation.

In the Authenticator Address field, enter the IP address of the authenticator workstation. It is a string composed of four substrings of numbers, divided by a period (nnn.nnn.nnn.nnn.). The range for each substring is 0-255. You can find it in the configuration notebook in c:\tcpip\bin\tcpipcfg.

d. In the Security data path field, enter the path that you typed when you installed the authenticator (see "Completing the Security Authenticator Installation" in topic 1.1.2.2.2). The administrator sends the security information to this path on the authenticator.

The path can be 50 characters long and must not contain any blanks between characters. Do not use wildcard characters.

e. Press the **Add** push button. The Select Format for the key-encrypting key window is displayed.

Reminder
The KEK must match the KEK that you typed when you installed the authenticator.

Continue with the instructions in ″Supplying the Format for the Administrator Key-Encrypting Key″ in topic 1.1.2.2.1.

3. After you add the authenticator, the Administrator - Authenticators window is displayed. Repeat the procedure to define any other authenticators in your network. Then choose **Save** from the File pull-down menu.

You have defined the authenticators for the administrator. Now you are ready to assign the targets to the authenticator.

1.4.5 Assigning Targets to the Authenticators

When you assign a target to an authenticator, you provide the information that enables the authenticator to authenticate a connection with the target. Remember that you need to assign the target on the authenticator workstation as well as any other secure targets on the LAN. If, when you | installed the secure target you provided different LAN addresses for a primary authenticator and for a backup secondary authenticator, be sure to assign the target to both authenticators.

You can assign targets to the authenticator in one of the following ways:

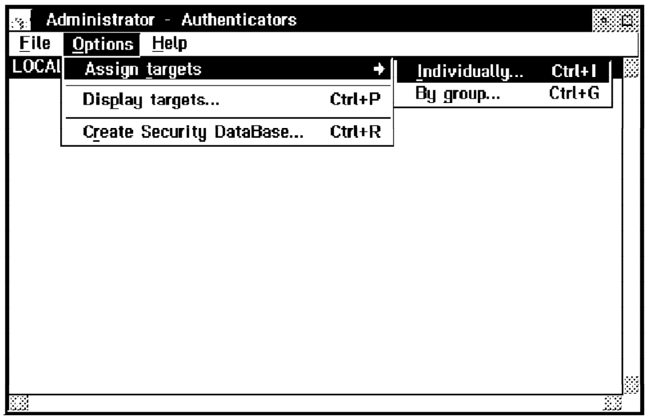
- One target at a time. Use this method if you are assigning only a few targets for each authenticator. For the exercise, use this method.
- By groups of targets. Use this method if you are assigning a large number of targets.

1.4.5.1 Assigning One Target at a Time to the Authenticator

If you are assigning just a few targets to the authenticator, you can assign them one at a time.

To assign one target at a time to the authenticator, perform the following steps:

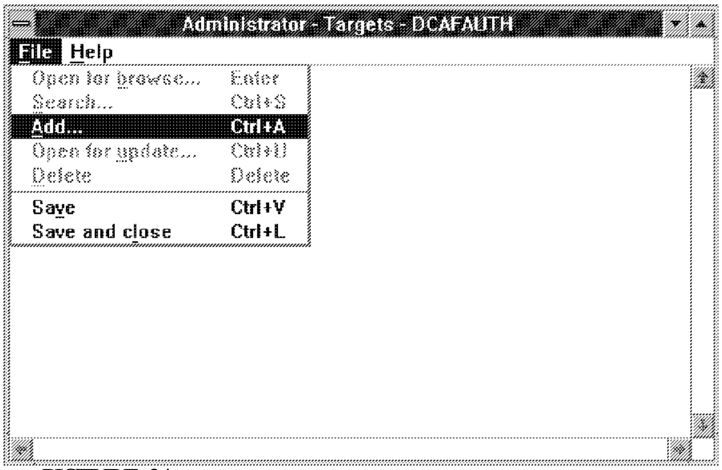
1. From the Administrator - Authenticators window, select the authenticator to which you are assigning the target and choose **Assign targets** from the Options pull-down menu (Figure 33).



| PICTURE 33

Figure 33. Authenticators with Options Pull-Down Menu

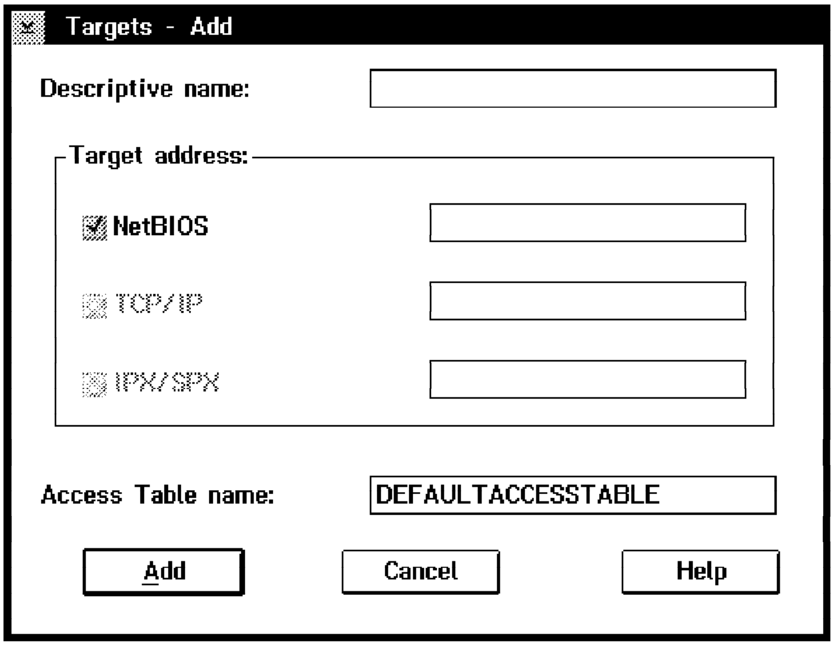
2. From **Assign targets**, select **Individually...**. The Administrator - Targets window (Figure 34) is displayed. The name of the authenticator you selected appears on the title bar.



PICTURE 34

Figure 34. Administrator - Targets Window with Pull-Down Menu

3. Choose **Add...** from the File pull-down menu. The Targets - Add window (Figure 35) appears.



PICTURE 35

Figure 35. Targets - Add

4. In the Descriptive name field, enter a name that helps identify the target. The descriptive name can be 1-60 characters in length, including:

   - Upper- or lowercase letters (A-Z, a-z).
   - Digits (0-9).
   - Special characters #, @, and $.

5. The Target address box contains entry fields for the LAN protocols, NetBIOS, and TCP/IP, which you enabled when you added the remote authenticator (see "Defining the Authenticators for the Administrator" in topic 1.4.4). Enter the target address for the enabled LAN protocols.

   NetBIOS
   Enter the LAN adapter address of the target workstation.

   Character guidelines:

   - Exactly 12 hexadecimal characters long
   - Upper- or lowercase letters (A-F, a-f)
   - Digits (0-9)
   - Blanks not allowed

   TCP/IP
   Enter the IP address of the target workstation. It is a string composed of four substrings of numbers, divided by a period (nnn.nnn.nnn.nnn.). The range for each substring is 0-255. You can find it in the configuration notebook in c:\tcpip\bin\tcpipcfg.

6. In the Access table name field, enter the table that you created for the target (see "Defining Access Levels for the Targets" in topic 1.4.2). If you enter a table that does not exist, the authenticator uses the default table.

7. Press the **Add** push button. Repeat the procedure to add any other

targets. Then choose **Save and close** from the File pull-down menu. The Administrator - Authenticators window is displayed.

8. Choose **Save and close** from the File pull-down menu to return to the Security Administrator window.

You have added the targets to the authenticator. Now you are ready to transfer the security information to the authenticator. Continue with the instructions in "Transferring Security Databases to the Authenticators" in topic 1.4.6.

1.4.5.2 Assigning a Group of Targets to the Authenticator

You can assign a large number of targets to an authenticator by creating a group of targets. You need to create a file that lists each target and its LAN addresses. This nickname list file enables the authenticator to locate and authenticate sessions with the target.

You can create your own nickname file, or use the example file
| EQNTGNIK.TXT located in the DCAF installation directory of your
| administrator workstation.

Figure 36 provides an example.

```
TargetParis 10005aae9167 9.8.7.555
TargetSidney - 9.8.7.556
TargetNairobi 10005aae9168 -
TargetMoscow 10005aae9169 - -
```

Figure 36. Example Nickname List File (EQNTGNIK.TXT)

Each entry begins on a new line and contains the target's descriptive name, NetBIOS address, and TCP/IP address. Each item is separated by a blank. If the target does not have an address for a particular protocol, enter a dash (-) in its place. Save the file in ASCII format.

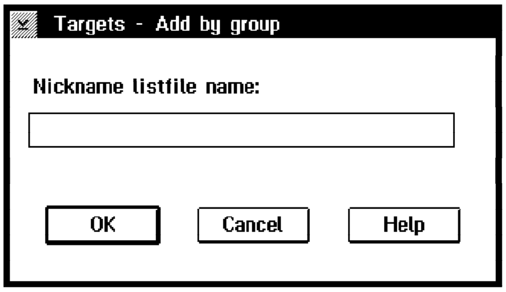
Recommendation

> It is recommended that you list a maximum of 50 targets in a single nickname file. Then you can perform the following steps for each nickname file you create.

Now you are ready to assign a group of targets to the authenticator. Complete the following steps:

1. From the Administrator - Authenticators window, select the authenticator to which you are assigning the group of targets and choose **Assign targets** from the Options pull-down menu (Figure 33 in topic 1.4.5.1).

2. From Assign targets, select **By group...**. The Targets - Add by Group window (Figure 37) is displayed.



PICTURE 36

Figure 37. Adding Targets by Group

Enter the path and name of the nickname list file that you created. The file must already exist on your workstation. Press the **OK** push button. The Administrator - Authenticators window is displayed.

3. Choose **Save and close** from the File pull-down menu to return to the Security Administrator window.

You have assigned a group of targets to the authenticator. Now you are ready to transfer the security information to the authenticator. Continue with the instructions in "Transferring Security Databases to the Authenticators" in topic 1.4.6.

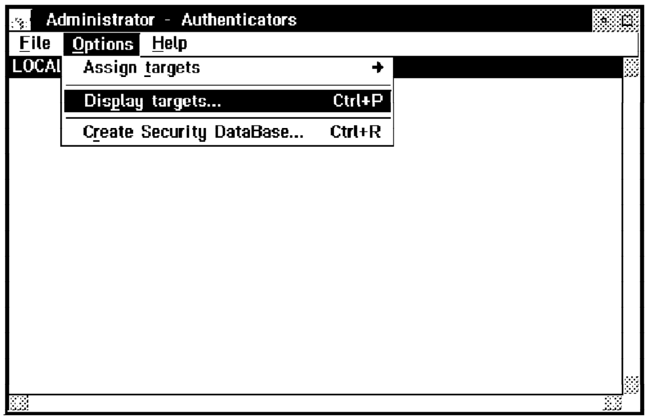
1.4.5.3 Displaying the Targets Assigned to an Authenticator

To check an authenticator's scope, you can display a list of its targets.

Complete the following steps:

1. From the DCAF Security Administrator window (Figure 25 in topic 1.4.2), choose **Authenticators**. The Administrator - Authenticators window (Figure 38) is displayed.

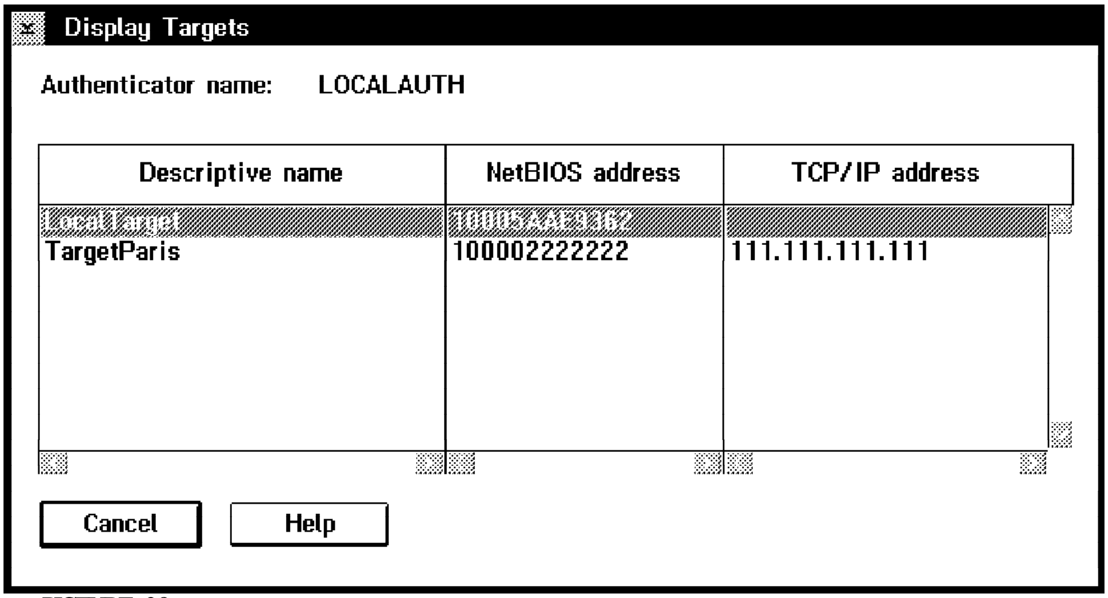
2. Select the authenticator for which you want to check the targets and choose **Display Targets...** from the Options pull-down menu.



| PICTURE 37

Figure 38. Authenticators with Options Pull-Down Menu

The Display Targets window (Figure 39) appears.



PICTURE 38

Figure 39. Display Targets

It lists all the targets assigned to the authenticator you selected and their LAN addresses. If the target is not enabled for a LAN protocol, the LAN address is blank.

3. Press the **Cancel** push button. The Administrator - Authenticators window is displayed.

4. Choose **Save and close** from the File pull-down menu to return to the Security Administrator window.

Now you are ready to transfer the security databases to the authenticator.

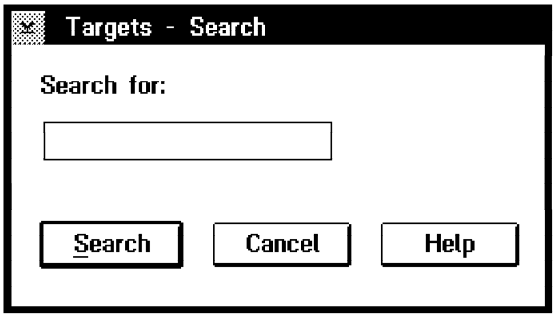
1.4.5.4 Locating Targets Assigned to the an Authenticator

After you assign targets to an authenticator, you can search for a specific target that is assigned to an authenticator. Perform the following steps:

1. From the Administrator - Authenticators window, select the authenticator to which you assigned the target and choose **Assign targets** from the Options pull-down menu (Figure 33 in topic 1.4.5.1).

2. From **Assign targets**, select **Individually...**. The Administrator - Targets window (Figure 34 in topic 1.4.5.1) is displayed. The name of the authenticator you selected appears on the title bar.

3. Choose **Search...** from the File pull-down menu. The Targets - Search window (Figure 40) appears.



PICTURE 39

Figure 40. Search Window

4. In the Search for field, enter the descriptive name of the target. The descriptive name can be 1-60 characters in length, including:

   - Upper- or lowercase letters (A-Z, a-z).
   - Digits (0-9).
   - Special characters #, @, and $.

5. Press the **Search** push button. The target appears highlighted in the Administrator - Authenticators window.

1.4.6 Transferring Security Databases to the Authenticators

After you finish creating the security databases, you need to transfer them to the authenticators.

For a Local Authenticator

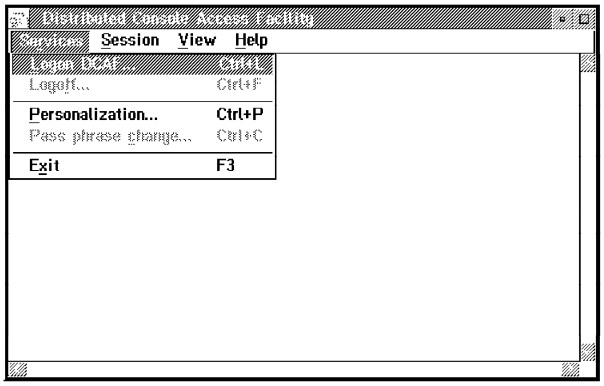
If the authenticator resides on the administrator workstation, ensure that the administrator is running and begin from step 8. If not, start here.

To transfer the security databases to the authenticators, complete the following steps:

1. Ensure that the LAN directory and gateway (where applicable) are running. On the administrator workstation, ensure that the administrator and controller are running. On the authenticator workstation, start the authenticator and the target:

   Choose the Distributed Console Access Facility icon from the desktop and then choose the **DCAF Authenticator** and **Target** icons.

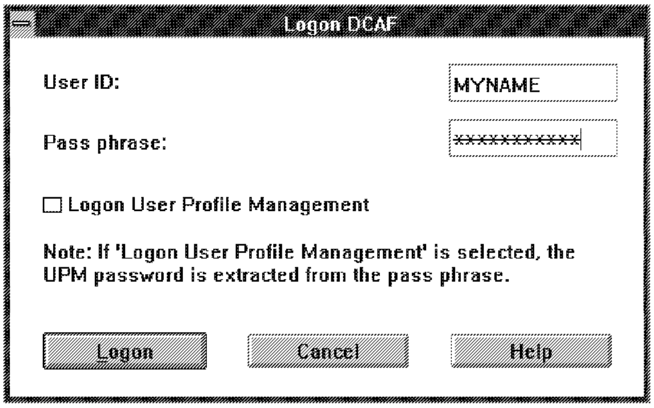
2. From the Services pull-down menu on the DCAF controller main window (Figure 41), select **Logon DCAF...**.



PICTURE 40

Figure 41. DCAF Controller with Services Pull-Down Menu

The Logon DCAF window (Figure 42) is displayed.



PICTURE 41

Figure 42. Logon DCAF

3. In the User ID field, enter the administrator user ID. When you transfer the initial security databases, you can use any user ID. After you transfer the initial security databases, only the security adminstrator, who is authorized with access level 0, can perform this transfer.

4. In the Pass phrase field, enter your pass phrase. As with the user ID, you can use any pass phrase for the initial transfer. For subsequent transfers, use the administrator's pass phrase.

5. To log on to the OS/2 User Profile Management when you log on to DCAF, select the Logon User Profile Management check box.

6. Press the **Logon** push button.

7. Switch to the Security Administrator main window (see Figure 23 in topic 1.4.1).

8. From the Options pull-down menu on the Security Administrator main window, choose **Transfer files**.

   A session window is displayed for each remote authenticator. The DCAF File Transfer Utility window displays the progress of the file transfer.

Otherwise, for a local authenticator, the files are copied to the security data path you specified for the authenticator. The EQNADMN.LOG file logs messages recorded during file transfers.

For subsequent updates, you can set up the administrator to transfer security database files automatically. "Transferring Security Databases Automatically" in topic 1.4.6.1 provides instructions.

You have completed setting up the security databases. Now you are ready to start a secure session. The Distributed Console Access Facility User's Guide explains how to start secure sessions.

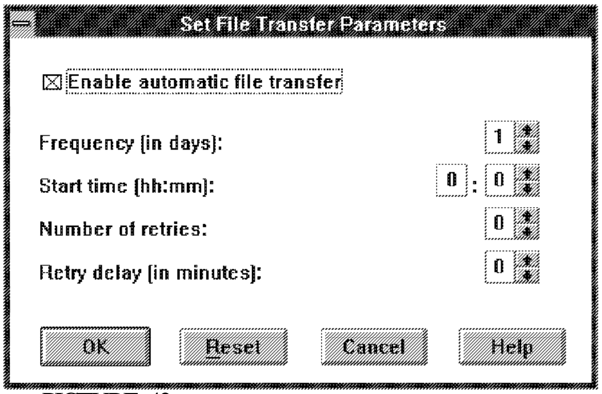
1.4.6.1 Transferring Security Databases Automatically

You can program the administrator to transfer security database files to the authenticators automatically at regular intervals. This is particularly useful if you update the security databases frequently or on a regular basis.

> **Suggestion**
>
> If you set up automatic transfers that could occur outside of work hours, it is recommended that you keep the administrator/controller and authenticator/target running. However, ensure that only authorized persons have physical access to the workstations.

Ensure that the administrator is running and that you have already created the security databases. If you have not, go back and create them before you begin here. To set up automatic file transfers, complete the following steps:

1. Select **Set parameters** from the Options pull-down menu on the Security Administrator window (Figure 23 in topic 1.4.1) and choose **Set file transfer parameters...** from the cascading menu. The Automatic File Transfer Parameters (Figure 43) is displayed.



PICTURE 42

Figure 43. Automatic File Transfer Parameters Window

2. Mark the **Enable automatic file transfer** check box.

3. In the Frequency (in days) field, enter how often the administrator

should send updated security information to the authenticators. The range is 1-30 days. The default value is 1.

4. In the Start time (hh:mm) field, enter the time at which the automatic file transfer should start. The range is 0-23 hours and 0-59 minutes. The default for both hours and minutes is 0. To start at midnight, enter **00:00**.

5. In the Number of retries field, enter the number of times the administrator should repeat the file transfer if it is not successful the first time. For no retries, enter **0**. The range is 0-5. The default is 0.

6. In the Retry delay (in minutes) field, enter the interval between retries. To retry immediately, enter **0**. The range is 0-60 minutes. The default is 0. Press the **OK** push button to confirm your choices.

7. To make your changes take effect, exit and restart the administrator.

If a file transfer is already in progress, the automatic file transfer is postponed until the next time that you specified.

1.5 Keeping DCAF Security Up to Date

During normal operations, you may need to update the security databases; for example, to add an access level to a table or change a controller′s access level.

Also, by periodically changing the security information, you make it more difficult for an intruder to break into a secure network. You can change the following elements:

- KEK
- Master key
- Random seed value
- Pass phrase

This chapter includes information about updating the security databases and changing the elements.