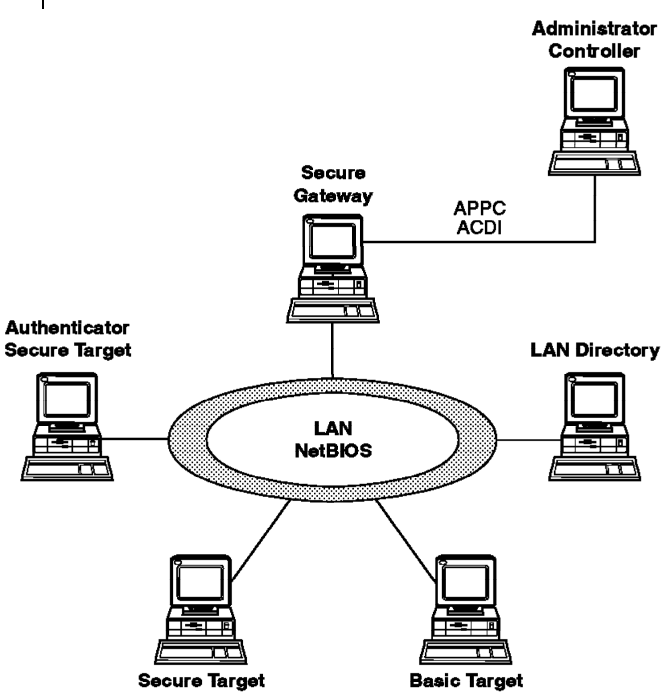
4.0 DCAF Security

4.1 Understanding DCAF Security

This chapter provides the following:

- A microcosm of a secure DCAF network. You can reproduce similar setups, according to your needs, across the network.
- The main tasks that you should perform to achieve and maintain it.
- A closer look at how the security data is passed around the network.



PICTURE 104

Figure 121. Example of DCAF Environment with DCAF Security

Figure 121 shows a LAN with both secure and basic DCAF targets. You can access any kind of target through a secure gateway.

The controller communicates directly (using APPC or asynchronous communication) with the secure DCAF gateway. All secure targets communicate with the secure DCAF gateway using NetBIOS communication. The secure DCAF gateway and at least one security authenticator are installed on each logical LAN (including bridged LANs) and secure OS/2 target on its own LAN (that is, there is one workstation on the LAN). If the secure OS/2 target is on its own LAN, then you must install the security authenticator, LAN directory, and secure DCAF gateway on the secure target. A security administrator is necessary to create, maintain, and distribute the security information.

4.1.1 About the Security Components

The security components are the security authenticator and the security administrator.

4.1.1.1 The Security Authenticator

The security authenticator controls the access of controllers to the secure targets. To guard against illegal access to the secure target, each secure target is assigned a primary and secondary security authenticator at installation. Only two security authenticators can authenticate sessions for a specific target. The second security authenticator is optional. The primary authenticates the session, and the secondary security authenticator serves as a backup.

4.1.1.2 The Security Administrator

The security administrator maintains a central database of security information and transfers it to the security authenticators in the network. The security information includes the access tables, the defined secure targets, the controllers, and the defined security authenticators in the network.

Whatever the number of secure LANs, there is always only one central security administrator for the whole network.

4.1.1.3 How the Security Components Are Distributed in the DCAF Environment

When the security administrator and the security authenticator are installed on different OS/2 workstations, then the security authenticator is being remotely administered by the security administrator. For the security administrator to transfer security information to remotely administered security authenticators, it must be installed on a controller. A remotely administered security authenticator must be installed on a secure OS/2 target.

When the security administrator and security authenticator are installed on the same OS/2 workstation, then the security authenticator is being locally administered by the security administrator. This means that the security information is transferred to the security authenticator locally without the need for a secure session. Typically, both are installed on a controller on the logical LAN. However, if there is only one security administrator and security authenticator in the network, they can both be installed on any OS/2 workstation on the LAN.

4.1.2 Using Cryptographic Services and Managing Cryptographic Keys

Data encryption and decryption are employed whenever necessary for the security information or communication that is sent across the network. An encrypted message is generated using the pass phrase that has been processed with cryptographic keys and random numeric values. It is this message that is sent to establish the secure session.

The security components rely on a subset of IBM's Common Cryptographic Architecture (CCA) cryptographic services. These services can be provided by either the IBM 4755 Cryptographic adapter card (if the card is installed on the workstation) or by the DCAF product's software implementation. The IBM 4755 Cryptographic adapter card can be installed and initialized on any workstation that requires the cryptographic services. The following require the cryptographic services:

- The security authenticator

- The security administrator

- The controller, when it wants to initialize a DCAF session with a secure DCAF gateway (to have a session with a secure target) or to change the pass phrase.

There are two cryptographic keys that are of importance to the user who is managing the security authenticator and the security administrator workstations:

- The master key
- The key-encrypting key (KEK)

The master key is used by the CCA services to encrypt and decrypt many data-encrypting keys and key-encrypting keys (KEK) that are stored in a key data set. It resides on the 4755 Cryptographic adapter card. The DCAF product also supplies a software implementation if you do not have the 4755 adapter installed. The key-encrypting key encrypts and decrypts all keys that are distributed in the network.

The user who is managing the security authenticator and the security administrators is asked to supply the format and input for the master key and the key-encrypting key (KEK) during installation and whenever it is desired to change the keys during normal operations. The security authenticator user must also supply the input for the random seed value (used to generate a random number). For more information, see "Installing the Security Administrator and Authenticator" in topic 2.1.1.4, "Changing the KEK, Master Key, and Random Seed Value" in topic 4.2.2.2, for the security authenticator, and "Changing the KEK and Master Key" in topic 4.2.1.8, for the security administrator. If the 4755 Cryptographic adapter card is installed, it contains the master key and random number generator information, but the user must supply the input for the KEK.

For an OS/2 workstation that has a 4755 Cryptographic adapter card, the KEK is stored in key storage. For the security administrator key-encrypting keys are stored under the following key labels:

- DCAFKEK.IMPORTER
- DCAFKEK.EXPORTER

The security authenticator's key-encrypting key is stored under the key label DCAFKEK.IMPORTER. For more information, see "Changing the KEK via 4755 Adapter" in topic 4.2.2.3.

Remember, it is important that the security administrator and security authenticators be physically protected. This means that the physical access to the workstations is restricted to the appropriate users.

4.1.3 Planning for Security

To establish a secure session, perform the following main tasks:

- Plan the DCAF network topology.
- Install and personalize the DCAF components.
- Configure the communications on the workstations.
- Define a database of users for secure gateways and targets.
- Distribute the security information to the security authenticator.
- Update the security information periodically.

The following explains each of the items in the list.

- Plan the DCAF network topology. How many secure targets do you need on a LAN? How many secure LANs do you need? Where can you install a secure gateway so that it is central for secure targets on the LAN? See "Levels of DCAF Security" in topic 1.1.2.3 for a brief introduction to DCAF security.

- Install and personalize, where necessary, the DCAF components. The following components are necessary for a secure setup. See "The DCAF Components" in topic 1.1.2.1 for a detailed description of the components.

  - Security Administrator
  - Security Authenticator
  - Controller
  - LAN Directory
  - Secure gateway (1)
  - Secure target (1)

  Table 23 shows the personalization parameters that are important to remember while you are installing a secure network. DCAF requires that you type consistent parameters at different stages in the installation and personalization in order for the workstations to communicate.

Table 23. Important Personalization Options during Installation

Component	**Security Authenticator Name**	**LAN Directory Name**	**Primary Address** (2) **Secondary Address**
Security Authenticator	X		
LAN Directory		X	
Secure Gateway	X	X	
Secure Target		X	X

  See "Installing and Personalizing the DCAF" in topic 2.0 for instructions.

- Configure the workstations. There are three subtasks in establishing and managing DCAF security. Each subtask requires a different configuration:

  - To distribute the security databases to the security authenticators See "Distributing the Security Databases to the

Security Authenticators" in topic 4.1.5 for a brief description. Choose a configuration between the controller and the gateway from "Configuring" in topic 3.0.

  - To start a secure session. See "Connecting to Secure Targets" in topic 4.1.6 for a brief description. Choose a configuration between the controller and the gateway from "Configuring" in topic 3.0 and complete the connection with "Gateway to a Target via NetBIOS on a Logical LAN" in topic 3.16.

  - To update the pass phrase of the controller on the security administrator See "Changing the Pass Phrase" in topic 4.1.7 for a brief description. See "Controller to the Security Administrator via APPC on a Token-Ring LAN" in topic 3.10 or " Controller to a Security Administrator via Asynchronous" in topic 3.12 for instructions.

- Define a database of controllers and their access to secure gateways and secure targets. See "Setting Up the Security Databases with the Security Administrator" in topic 4.2.1.2 for instructions.

- Distribute the security information to the security authenticator. See "Updating Security Data" in topic 4.2.1.7 for instructions.

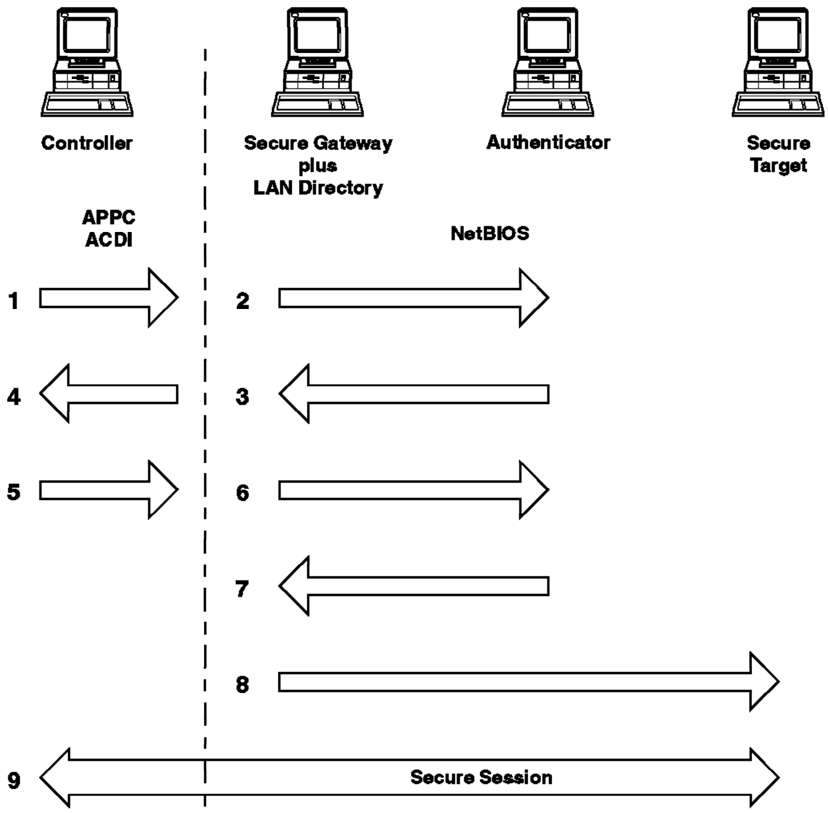
- Update the security information periodically. See "Updating Pass Phrase Change Requests" in topic 4.2.1.10 for instructions.

(1) To make it secure choose Personalize when you install it.

(2) Adapter addresses of the security authenticators, primary and secondary (optional), are requested during installation of a secure target.

4.1.4 How the Authentication Process Works

Figure 122 describes the data flow during the start of a secure session. The data flow is the same whether the components are installed on the workstations as shown or in a different combination. The steps below describe each segment in the figure.



PICTURE 105

Figure 122. The Data Flow when Starting a Secure Session

1. The controller tries to log on to a secure gateway.

2. The secure gateway checks with the security authenticator that the controller is authorized to access the secure gateway.

3. The security authenticator sends confirmation to the secure gateway.

4. The controller sees a list of the available targets, secure and basic, that are registered with the LAN directory associated with the secure gateway.

5. The controller tries to start a session with a secure target through the secure gateway.

6. The secure gateway checks with the security authenticator that the controller is authorized to access the secure target.

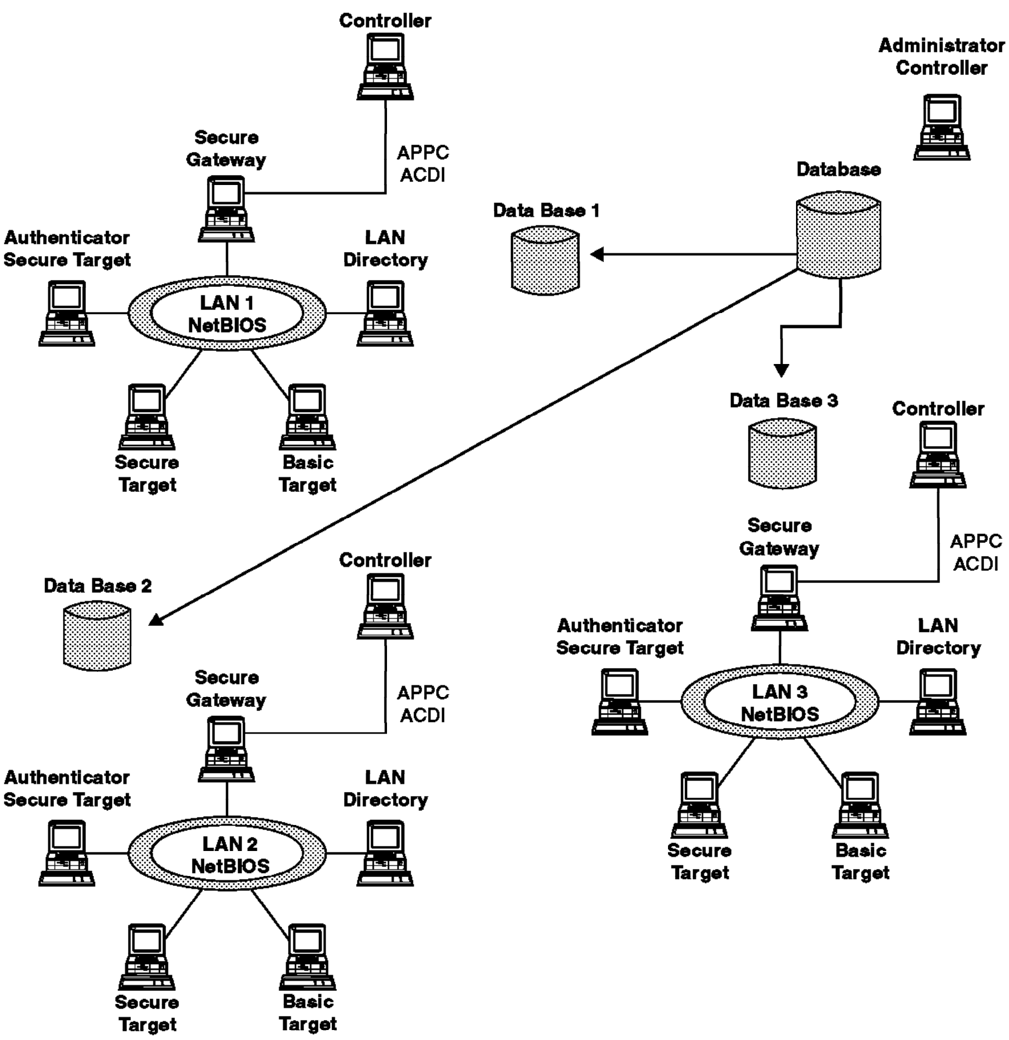
7. The security authenticator sends confirmation to the secure gateway.

8. The secure gateway checks that the secure target recognizes the security authenticator.

9. The secure session starts.

4.1.5 Distributing the Security Databases to the Security Authenticators

Figure 123 shows how DCAF distributes the new security information to the security authenticators on the network.



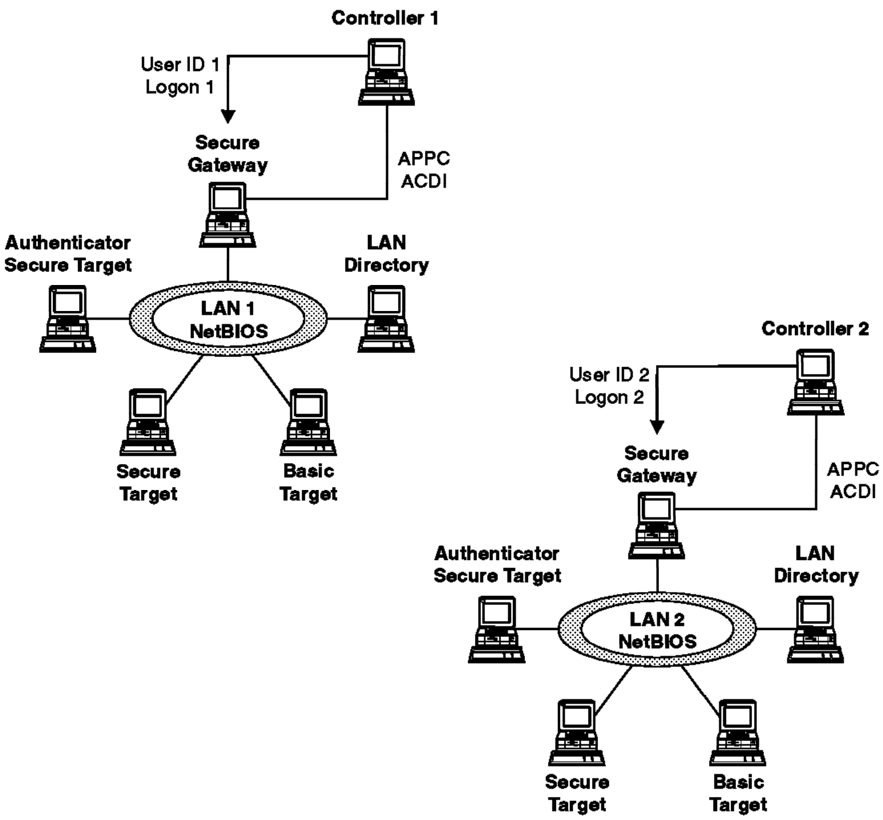
PICTURE 106

Figure 123. Updating the Databases of the Security Authenticator

DCAF distributes the security databases, and subsequent updates, to the security authenticators over a secure session. For this reason, the security administrator resides on a controller workstation and the security authenticator resides on a secure target.

4.1.6 Connecting to Secure Targets

Figure 124 shows how authorized controllers can connect to secure targets from any controller workstation in your network by using a user ID and a pass phrase that are recognized by the security authenticator.



PICTURE 107

Figure 124. Connecting to Secure Targets on a LAN

Authorized controllers can connect to secure targets that are on the same or a different LAN. The security administrator does not appear in the figure because it is not involved in the secure session.

To start a secure DCAF session, the controller chooses a secure DCAF gateway from the workstation directory. Next the user logs on to the DCAF product, and provides a user ID and pass phrase. The pass phrase is like a password except it can be from 4 to 80 characters long and contains embedded blanks. The pass phrase and the access to the DCAF gateway are authenticated or validated by the security authenticator. If successfully authenticated, the user chooses the secure target from the LAN Target Directory. The access for the controller to the secure target is authenticated by the security authenticator. If the access is successful, then the session will start, otherwise the attempt to start the session will fail. For a detailed description of the steps, see Distributed Console Access Facility User's Guide.

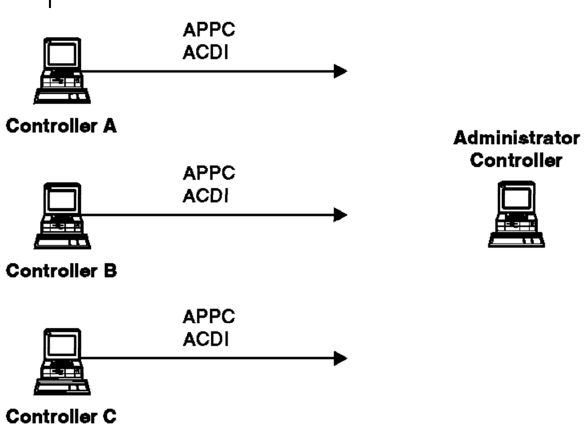
4.1.6.1 Understanding Access Levels

DCAF security uses access levels to filter the controller's access to secure targets. You create various access levels, which enable varying degrees of control over the secure targets. Then, you create access level tables that include or exclude privileges that the controller exercises over the targets. You associate an access level table with each secure target and an access level to each controller. The combination of the controller's access level and the target's access level table determines the access and actions that the controller can perform on the secure target.

A controller's level of access can vary from one target to another. For example, a controller with an access level of 5 can have full access to one target and limited access to another. The access level table of the first target enables all privileges for level 5. The access level table of the other target enables only one privilege for level 5.

4.1.7 Changing the Pass Phrase

Changing the pass phrase involves two steps. In Step 1 a controller (for example, controllers **A, B,** or **C** in Figure 125) changes the pass phrase and DCAF updates the controller's pass phrase in the security databases on the security administrator.



PICTURE 108

Figure 125. Changing the Pass Phrase

In Step 2 (as shown in Figure 123 in topic 4.1.5) the security administrator sends the updates to the security authenticators affected by the change.

With the new pass phrase, the controller can connect to the secure target from any controller workstation. The user ID and pass phrase, not the controller workstation, identify the controller to the security authenticator and the secure target.

4.2 Setting up Secure DCAF Sessions

For a brief overview of DCAF security, see "Levels of DCAF Security" in topic 1.1.2.3 and "For Secure DCAF" in topic 1.3.2.2.

4.2.1 Using the Security Administrator

The security administrator provides centralized maintenance for the security information databases and transfers the security information to the appropriate security authenticators. The security information is used by the security authenticator when a secure session is being authenticated. There is one security administrator in the network.

The security databases include target access tables, security authenticators, and the controllers.

For auditing purposes, the security administrator logs all sessions that pass through a secure gateway. The log tracks the session connections and the informational and error messages that occur. The message log file name is EQNADMIN.LOG. It is located in the directory where the DCAF product is installed.

The following tasks are described in this section.

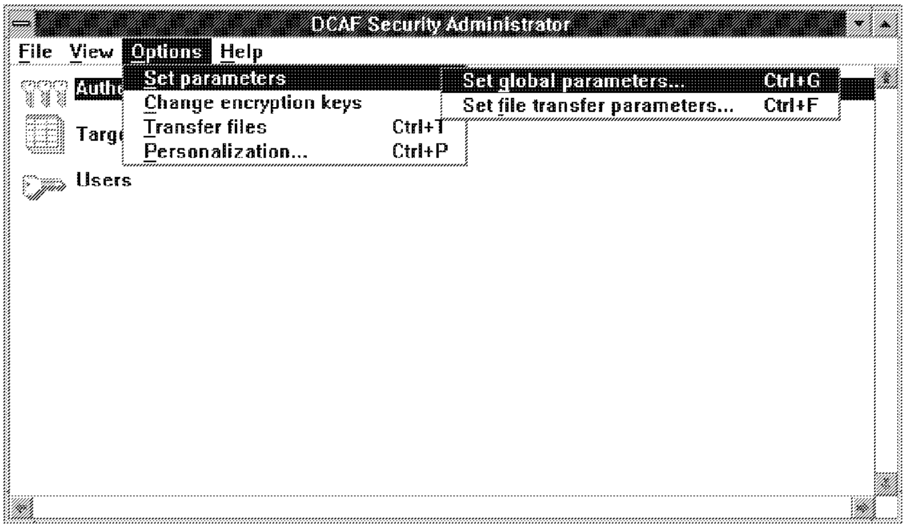
- Starting the Security Administrator
- Setting Up the Security Databases with the Security Administrator
- Creating the Target Access Tables Database
- Creating the Security Authenticator Database
- Creating the Controller Users Database
- Updating Security Data
- Updating the Authenticator KEK in the Administrator Database
- Changing the KEK and Master Key
- Updating Pass Phrase Change Requests
- Exiting from the Security Administrator

4.2.1.1 Starting the Security Administrator

To start the security administrator, first choose the DCAF work folder from the desktop, and then choose the **DCAF Security Administrator** icon.

4.2.1.2 Setting Up the Security Databases with the Security Administrator

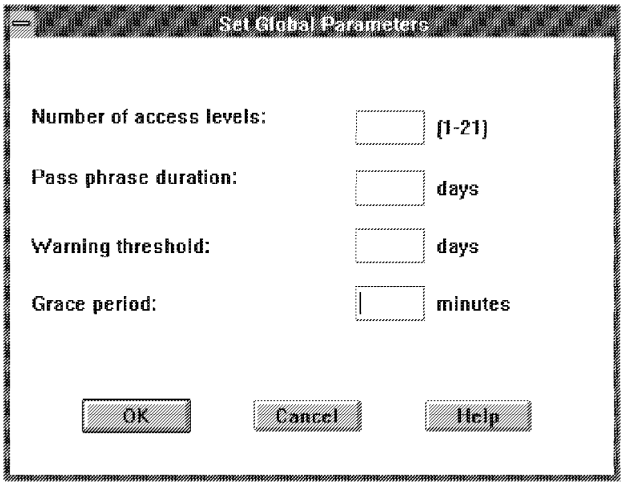
To set up the security databases on the security administrator, perform the following procedure: start the security administrator. The Security Administrator main window (Figure 126) appears.



PICTURE 109

Figure 126. Security Administrator Main Window with Options Pull-Down Menu

To set up authentication security for a network, first set the global parameters for the security information. From the **Options** pull-down menu, choose **Set parameters...** and then choose **Set global parameters...**.



PICTURE 110

Figure 127. Set Global Parameters

The Set Global Parameters window (Figure 127) appears. You must set each of the four parameters:

1. The number of access levels specifies how many user access levels that you want to define for your security system. The users are divided into classes called access levels. The user access level is a list of privileges associated with a particular target access table. You designate which privileges are allowed or disallowed during a secure session between a controller user and a target user. You can choose from 1-21 as the total number of access levels for the security information. The access levels themselves are numbered 0 to 20.

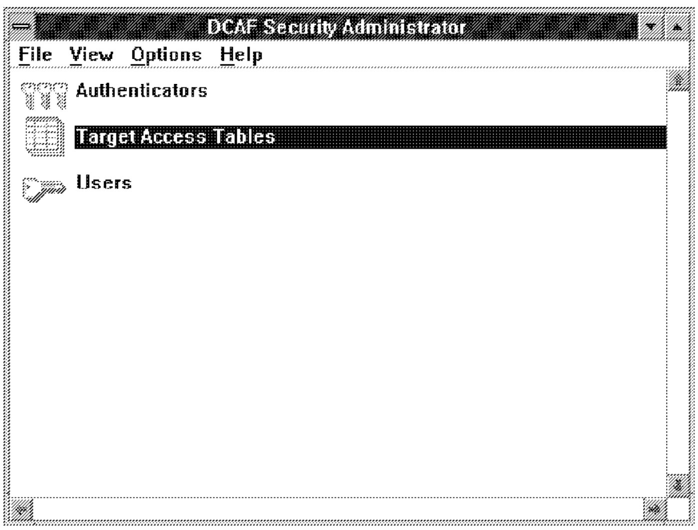
2. The pass phrase duration is the amount of time (in days) from its initial setting that a pass phrase is valid for any user. The range

is between 1 and 32 768 days.

3. The warning threshold is the amount of time (in days) that a user begins receiving daily messages that the pass phrase will soon expire. The range is between 1 and 32 767 days. The warning threshold must be less than the pass phrase duration.

4. The grace period is the amount of time (in minutes) that a user's pass phrase will remain valid after the expiration date. If the pass phrase is changed before or during the grace period, it will be accepted as valid by the security authenticator. After the grace period, controllers must contact the person that administers the security for the network. The range is between 1 and 32 768 minutes.

Press the **OK** push button when you have typed all of the information.



PICTURE 111

Figure 128. DCAF Security Administrator Main Window

After setting up the global parameters, create the centralized authentication databases (Figure 128) for the following:

- The security authenticators (**Authenticators**)
- The secure target access tables (**Target Access Tables**)
- The controllers (**Users**).

To choose a database, select the database, and then from **File** on the menu bar, choose **Open...** (or press **Enter**).

After completing the databases, the secure data is encrypted and transferred to the appropriate security authenticators. See "Updating Security Data" in topic 4.2.1.7.

4.2.1.3 How the Authentication Databases Work

The controller and secure target user are allowed certain privileges when accessing or communicating with each other during a secure session. The target access tables define the class of privileges (user access levels). There are seven different privileges that are allowed or disallowed when you are defining any user access level. The person administering the security for the system decides the definition for user access levels for each target access table in the database. Hence, the meaning of a particular user access level for one table may vary from the next table.

The range for the user access levels is numbered from 0-20. When you set up the global parameters for the security administrator (see Figure 127 in topic 4.2.1.2), choose (one time) the number of access levels (1-21) for all of the target access tables that you will create.

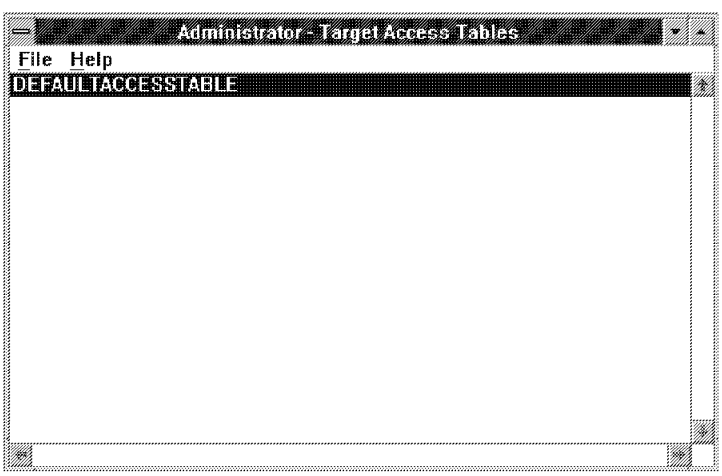
A primary security authenticator is in charge of authenticating the secure sessions for particular targets. For each security authenticator typed in the authenticators database, the targets that it is responsible for authenticating are assigned to it. Also, one target access table (known by its access table name) is assigned to each secure (OS/2 or DOS) target. Many targets can be associated with the same target access table.

Each secure target has a secondary security authenticator for a backup when the primary security authenticator is disabled. You can also choose the primary and secondary authenticators to be the same security authenticator. The primary and secondary authenticators are assigned when you are installing directly or creating an installation package for a secure target. You cannot personalize these options at a later time.

In the users database, each controller is assigned one user access level (0-20) that is an index into the target access table assigned to each secure target. The user is also assigned a user ID, a pass phrase, the authorized start and stop time for establishing sessions with secure targets, and permission start secure sessions on weekends.

You will want to set up the target access tables first because some of the information in the tables will be requested when you type information for the security authenticators database and the controllers database.

4.2.1.4 Creating the Target Access Tables Database

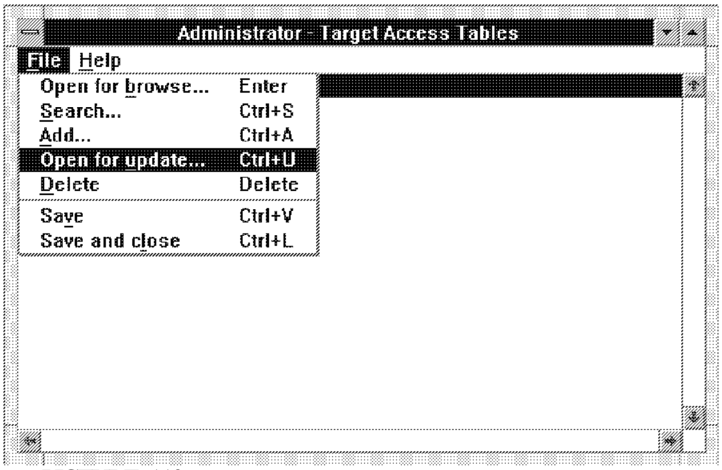


PICTURE 112

Figure 129. Target Access Tables

The target access tables are used by the security authenticator during the authentication process of a secure session between a controller and a target user. The table assigned to the target allows or withholds access level privileges for the controller and the target user.

When you choose the **Target Access Tables** from the Security Administrator main window (Figure 128 in topic 4.2.1.2), the Target Access Tables window (Figure 129) appears. It displays the list of the names of target access tables. The default access table is called **DEFAULTACCESSTABLE**. It is a predefined table that can be used as it is or can be modified. You cannot delete the default access table.



PICTURE 113

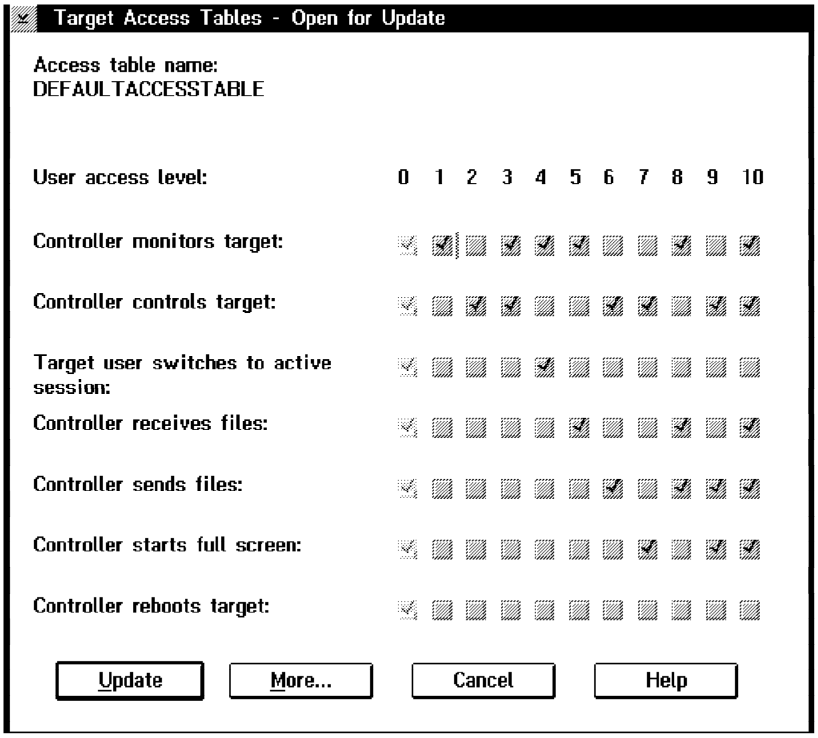
Figure 130. Target Access Tables with File Pull-Down Menu

The **File** pull-down menu provides a list of action choices for the target access tables database. You can:

- Browse (display only) an existing target access table
- Update (change) an existing target access table
- Add (create) a new target access table

Later, you may want to search for a particular target access table name in the list or to delete a table. You can save (Ctrl+V shortcut key) your information and changes at any time or save and close (Ctrl+L shortcut key) your database when you have completed your work. Saving your information means that all of your changes are written to the database files on the hard disk of your OS/2 workstation.

To update the default access table, select the **DEFAULTACCESSTABLE** and from the **File** pull-down menu, choose **Open for Update...** (or Ctrl+U shortcut key), as it appears in Figure 130.



PICTURE 114

Figure 131. Target Access Table - Open for Update (User Access Levels 0-10)

The Target Access Table - Open for Update window (Figure 131) appears. Within the target access table, there are seven different privileges (rows) for each user access level (shown as columns 0 to 10 at the top of the Figure 131). When an **X** appears in a box, then the privilege is allowed. A blank box means that the privilege is not allowed. To modify the table, mark or unmark the check box. You can press the **More...** push button to see user access levels 11 through 20 as shown in Figure 132.

When marked **X**, the following seven privileges are allowed:

1. The controller monitors the target. When in the monitoring state, the keyboard for the target remains unlocked.

2. The controller controls the target. When in the active state, the keyboard for the target is locked.

3. The target user can switch to an active session.

4. The controller receives files from the target. A file transfer is always initiated by the controller.

5. The controller sends files to the target.

6. The controller can start an OS/2 full-screen session on the OS/2 target.

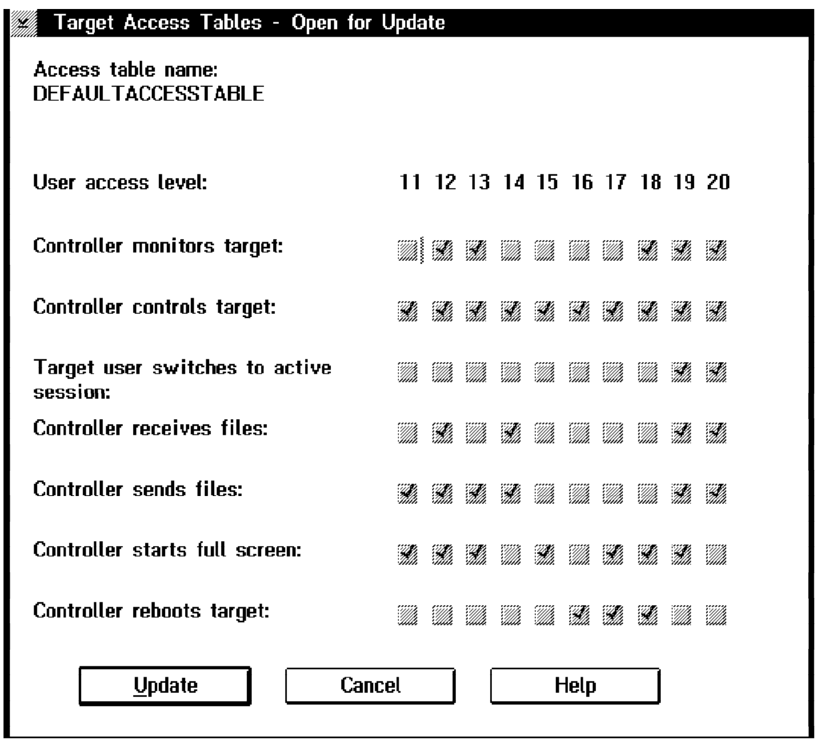
7. The controller can shut down and restart the target.

Note: Level 0 in this table allows all of the privileges (hence, is very powerful) and is reserved for the person that administers the security system. It is required that each target access table that is created have one user with a level zero access level. This level is not modifiable.

Certain privileges require that other privileges are also chosen (marked).

- For the controller to be able to start an OS/2 full-screen session or to restart the target, requires that the controller control the target.
- For the controller to be able to send or receive files requires that the controller either control the target or monitor the target (or both).
- For the target user to switch to an active session, requires that the controller either control the target or monitor the target (or both).

If none of the boxes is marked for a particular user access level in the target access table, then the controller assigned that user access level will not be allowed to start a session with a target. See return code 9 in the table Table 24 in topic 4.2.2.6.



PICTURE 115

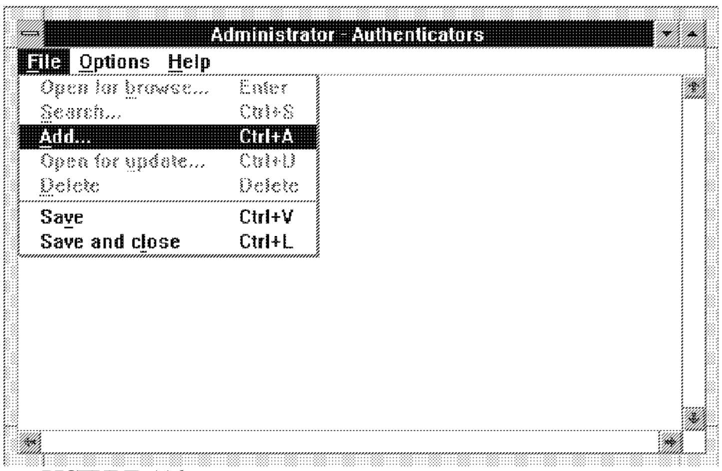
Figure 132. Target Access Table - Open for Update (User Levels 11-20)

When you press the **More...** push button in Figure 131, then the Target Access Table - Open for Update window appears. The user access levels for 11-20 are defined for the DEFAULTACCESSTABLE. You can use this default table or add (create) your own table. If you update the table and want to keep your changes, press the **Update** push button.

To create a target access table, choose **Add...** (or Ctrl+A shortcut key) from the **File** pull-down menu in Figure 130. After completing the target access table information, press the **Add** push button. After adding the target access tables, be sure to choose **Save** (or Ctrl+V shortcut key) from the **File** pull-down menu in Figure 130. The save action writes the information back to the database file on your OS/2 workstation.

4.2.1.5 Creating the Security Authenticator Database

The security authenticator database is used by the security administrator to know how to locate the security authenticators in the network when it is time to transfer the security information to them. The security authenticator uses the target information to know how to locate the targets that the security authenticator is to authenticate, and the names of the target access table associated with each target.



PICTURE 116

Figure 133. Authenticators with File Pull-Down Menu

When you choose the **Authenticators** from the Security Administrator main window (Figure 128 in topic 4.2.1.2), the Authenticators window (Figure 133) appears. It displays the list of the names of the security authenticators in the network. If this is the first time, the list is empty.

From the **File** pull-down menu, there is a list of action choices for the authenticators database. You can:

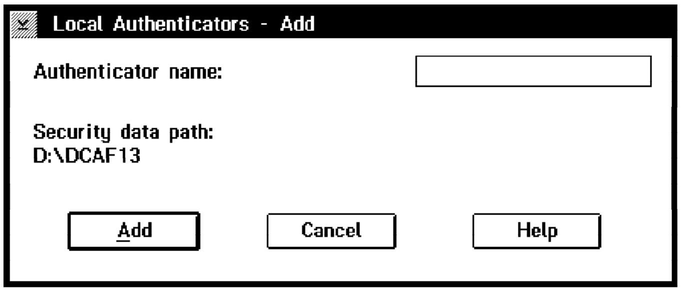
- Browse (display only) a defined security authenticator
- Update (change) a defined security authenticator
- Add (create) a new security authenticator

To add (define) a security authenticator, choose **Add...** (or Ctrl+A shortcut key) from the **File** pull-down menu. A message box appears asking, **Will this security authenticator be administered locally?**.

- Choose **Yes** if you are defining a security authenticator where the security authenticator and the security administrator are both installed on the same OS/2 workstation. There can be only one locally administered security authenticator in your network.

- Choose **No** if you are defining a security authenticator not installed on the same OS/2 workstation as the security administrator. The security authenticator is administered remotely by a security administrator located on a controller within the network.

Later, you may want to search for a particular security authenticator in the list or to delete one. You can save (Ctrl+V shortcut key) your information and changes at any time or save and close (Ctrl+L shortcut key) your database when you have completed your work. Saving your information means that all of your changes are written to the database files on your hard disk drive on your OS/2 workstation.



PICTURE 117

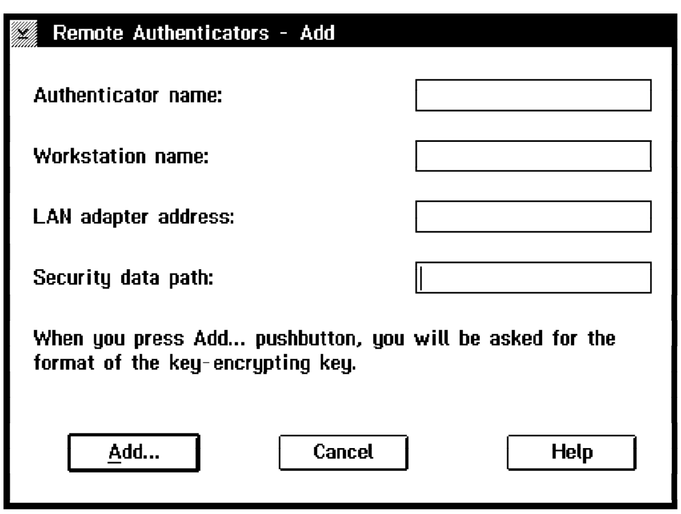
Figure 134. Local Authenticators - Add

If you choose **Yes** in the message box to locally administer the security administrator, then the Local Authenticator - Add window (Figure 134) appears.

Type the name of the local security authenticator. This unique name is used internally by the security administrator only. The security authenticator name is 1-12 characters in length. The path (for example, C:\DCAF13) where the data files will be stored on the security authenticator has already been defined during the installation of the security authenticator. The security administrator will send the files to this destination during the local file transfer of security information.

After typing the local security authenticator name, press the **Add** push button. After adding the security authenticators, be sure to choose **Save** (or Ctrl+V shortcut key) from the **File** pull-down menu in Figure 133. The save action writes the information back to the database file on your OS/2 workstation.

To change the name of the local security authenticator, you must first delete the existing security authenticator, and then add the security authenticator with the new name.



PICTURE 118

Figure 135. Remote Authenticators - Add

If you choose **No** in the message box to locally administer the security authenticator, then the Remote Authenticators - Add window (Figure 135) appears. There are four fields required for the remote security authenticator:

- The unique remote security authenticator name that is used internally by the security administrator only. The security authenticator name is 1-12 characters in length.

- The workstation name for the secure DCAF gateway that is installed on the same LAN as the security authenticator and is associated with the security authenticator. The security administrator must know through which DCAF gateway to send the security information files to the security authenticator.

  This is the workstation name recorded in the DCAF directory for the controller that is installed on the same workstation as the security administrator.

  - It can be 1-62 characters in length.

  - Blank spaces are not allowed between the characters.

- The LAN adapter address (hexadecimal address) of the target that is installed on the same workstation as the remote security authenticator. The security administrator must know the address of the target through which to send the security information files to the security authenticator. The LAN adapter address is the UAA and must be 12 characters in length, including:

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

- The drive and path (for example, C:\DCAF13) where the data files will be stored on the security authenticator. The security administrator sends the files to this destination during the (secure-session) file transfer of security information.

  - The path can be 50 characters bytes in length.
  - Blank spaces are not allowed between the characters.
  - No wildcard characters are allowed.

  Note: It is important that this data path match the data path that you typed during the installation of the security authenticator. See the description of the security data path in "Security Authenticator Installation" in topic 2.1.1.4.6.

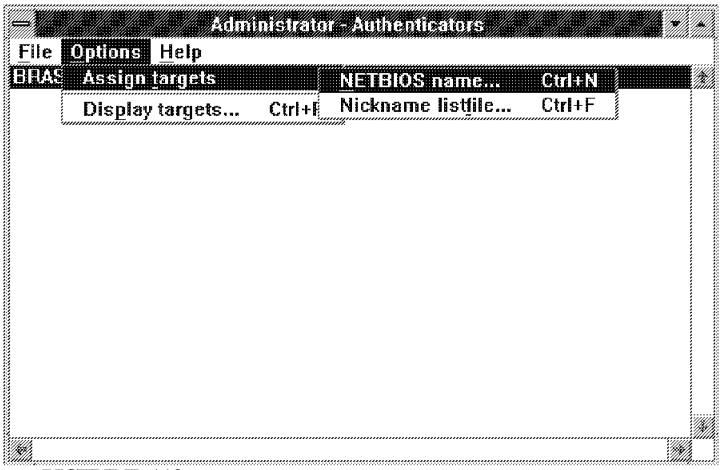
After typing the remote security authenticator information, press the **Add** push button. Then you will be asked for the authenticator key-encrypting key (KEK) and its format (hexadecimal or character). See "Supplying the Format for the Key-Encrypting Key" in topic 2.1.1.4.2 for more information.

Tip for Defining the KEK

The KEK **must** match the KEK that you typed during the installation of the remote security authenticator.

After adding the security authenticators, be sure to choose **Save** (or Ctrl+V shortcut key) from the **File** pull-down menu in Figure 133. The save action writes the information back to the database file on your OS/2 workstation.

To change the name of the remote security authenticator, you must first delete the existing security authenticator, and then add the security authenticator with the new name.



PICTURE 119

Figure 136. Authenticators with Options Pull-Down Menu

Each security authenticator is responsible for authenticating the secure sessions between the controller and targets.

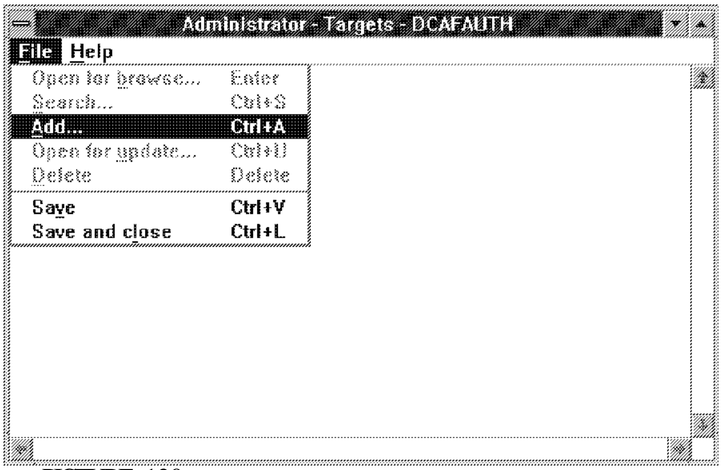
You can assign the target information either of two ways:

- The NetBIOS name enables you to assign an individual target one at a time.
- The Nickname listfile enables you to assign a group of targets as defined with the LAN directory nickname list file.

To assign the targets to the security authenticator, perform the following steps:

1. Select the security authenticator (Figure 136) and then, from the **Options** pull-down menu, choose **Assign targets**.
2. From the **Assign targets** menu, select either **NetBIOS name...** or **Nickname listfile...**.

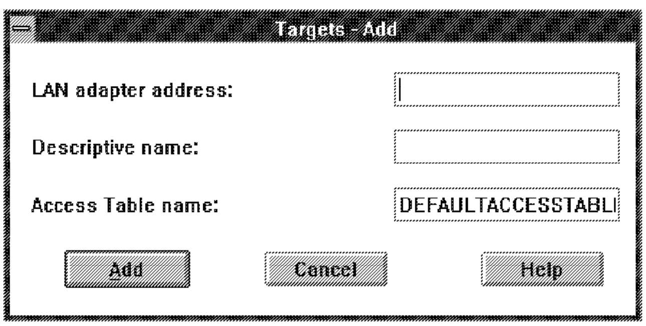
If you choose **NetBIOS name...**, then a list of the target names (Figure 137) appears.



PICTURE 120

Figure 137. Targets for Authenticator File Pull-Down Menu

If this is the first time, the list is empty. The name of the security authenticator to which you want to assign the target is displayed on the title bar. To assign a target, from the **File** pull-down menu, choose **Add...** (of Ctrl+A shortcut key).



PICTURE 121

Figure 138. Targets - Add

The Targets - Add window (Figure 138) appears. To add the target complete the following fields:

- The LAN adapter address (hexadecimal address) of the secure target workstation. The security authenticator must know the address of the target that it is authenticating. The LAN adapter address is the UAA and must be 12 characters in length, including:

  - Upper- or lowercase letters (A-F, a-f).
  - Digits (0-9).
  - Blank spaces are not allowed between the characters.

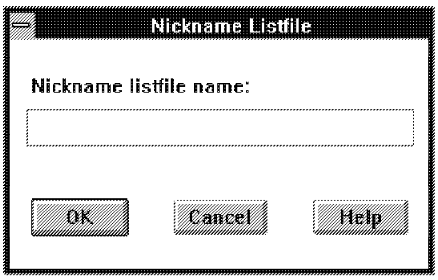
- The descriptive name for the target. The name has the same format as the nicknames in the LAN directory nickname list file. The descriptive name is 1-60 characters in length, including:

  - Upper- or lowercase letters (A-Z, a-z).
  - Digits (0-9).
  - special characters #, @, and $.
  - Blank spaces are not allowed between the characters.

- The access table name that defines the user's access level for the target workstation that is being added. If the target access table does not exist when the security administrator is transferring files to the security authenticators, then the DEFAULTACCESSTABLE will be assigned to the target. The access table name is 1-60 characters in length, including:

  - Upper- or lowercase letters (A-Z, a-z).
  - Digits (0-9).
  - Special characters #, @, and $.
  - Blank spaces are not allowed between the characters.

Press the **Add** push button after you have typed all of the information.

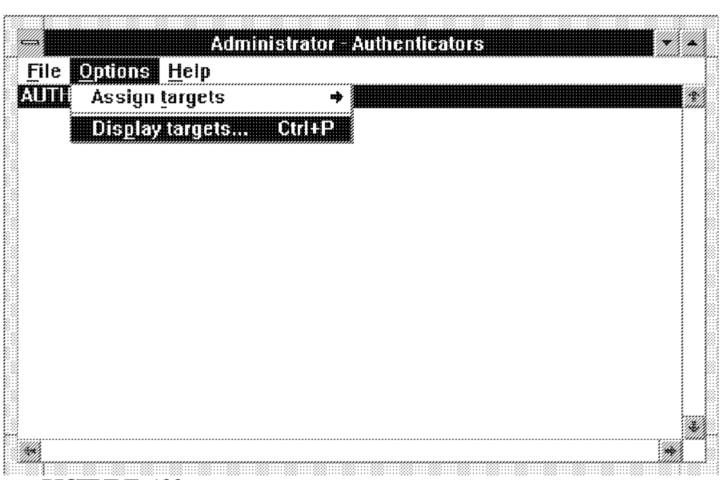


PICTURE 122

Figure 139. Nickname Listfile

If you choose **Nickname listfile...**, the Nickname Listfile window (Figure 139) appears. You can assign a group of targets to the security authenticator by typing the name of the LAN directory nickname list file. This is a user-defined file of nicknames for the target workstations. For more information on creating a nickname list file, see the <u>Distributed Console Access Facility User's Guide</u>

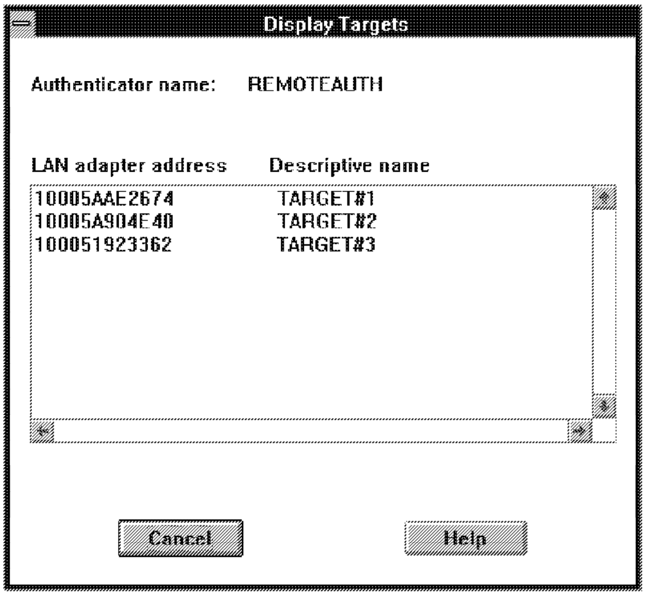
If you create the nickname list file, it will append the list of nicknames to the previously defined targets. The DEFAULTACCESSTABLE is used to assign the users access level. After typing the nickname list file name, press the **OK** push button.



PICTURE 123

Figure 140. Authenticators with Options Pull-Down Menu

After you have assigned the targets to the security authenticator, you can display the targets. First select the security authenticator, and then choose **Display Targets...** (or Ctrl+P shortcut key) from **Options** pull-down menu shown in Figure 140.

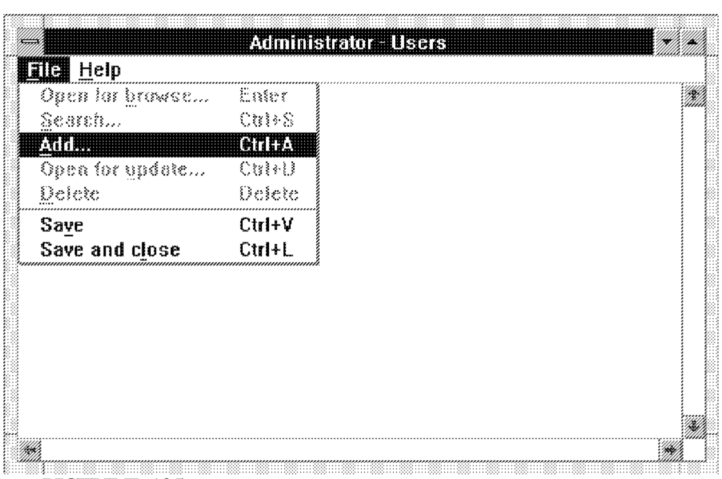


PICTURE 124

Figure 141. Display Targets

The Display Targets window (Figure 141) appears. The list of targets assigned to the specified security authenticator is displayed. For each target, the LAN adapter address and the descriptive name are listed.

4.2.1.6 Creating the Controller Users Database



PICTURE 125

Figure 142. Users

The controllers database is used by the security authenticator during the authentication process of a secure session between a controller and a target user. When a controller logs on, the security authenticator approves or rejects the user's user ID, pass phrase, starting and stopping session-initiation times, and whether the user can establish a secure session during the weekend.

The security authenticator also checks what privileges the controller is allowed by using with the controller′s access level as an index into the target access table associated with the secure target. If a privilege is allowed, then the choice for the privilege is made available. If a privilege is not allowed, then the choice is disabled. For example, if the controller has permission to send files but cannot receive files, then the Start the file transfer... choice is available from the Services pull-down menu on the controller session window. The Send push button on the File Transfer Utility window is available, but the Receive push button is disabled.

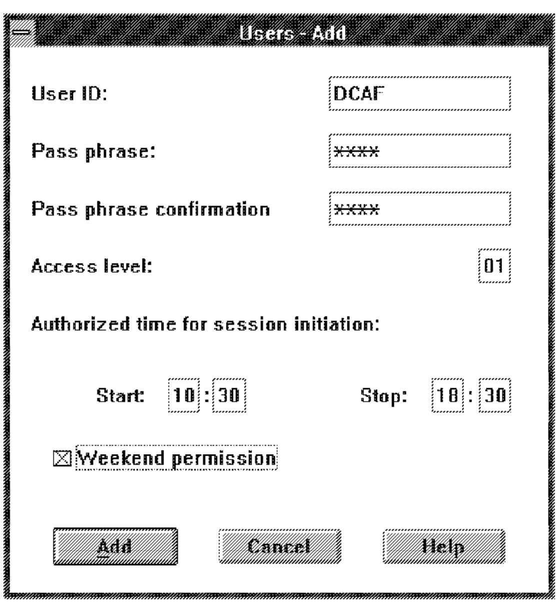
When you choose the **Users** from the Security Administrator main window (Figure 128 in topic 4.2.1.2), the Users window (Figure 142) appears. It displays the list of the controllers in the database. If this is the first time, the list is empty.

From the **File** pull-down menu, there is a list of action choices for the users database. You can:

- Browse (display only) a defined user
- Update (change) a defined user
- Add (create) a new user

Later, you may want to search for a particular controller in the list or to delete one. You can save (Ctrl+V shortcut key) your information and changes at any time or save and close (Ctrl+L shortcut key) your database when you have completed your work. Saving your information means that all of your changes are written to the database files on your hard disk drive on your OS/2 workstation.

To add a new controller, choose **Add...** (or Ctrl+A shortcut key) from the **File** pull-down menu.



PICTURE 126

Figure 143. Users - Add

The Users - Add window (Figure 143) appears. To add a new user to the user database, type and choose the data for the following six fields:

1. Type the user IDs by which the user is known in the DCAF security

system. Each user ID is unique in the system.

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

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

2. Type the initial pass phrase for each user. It can be changed by the controller at a later time.

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

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

3. Type the pass phrase confirmation must match exactly the data you typed in the pass phrase field.

4. Type the access level. It specifies the class to which the controller belongs and describes the privileges that the user is allowed for DCAF secure sessions. The access levels are defined when you create the target access tables. For more information, see "Creating the Target Access Tables Database" in topic 4.2.1.4.

   - Level 0 is reserved for the person with access privilege to the security administrator.

   - You have to add at least one user with the level 0 access level.

5. Type the start time and the stop time. It is the authorized time for session initiation with secure targets. You specify the start time and the stop time in hours:minutes. The valid ranges are:

   - Hours: 00 to 23
   - Minutes: 00 to 59.

   To give the user access 24 hours per day, type **00** in both the start and stop time fields. If the stop time is earlier than the start time, it means that the authorized time spans midnight.

6. Select the Weekend permission check box if you want to enable the controller to start secure sessions on Saturdays and Sundays. If the box is not marked, then the user can start secure sessions during the week days only.

7. After typing the user information, press the **Add** push button. After adding the controllers, be sure to choose **Save** (or Ctrl+V shortcut key) from the **File** pull-down menu in Figure 142. The save action writes the information back to the database file on your OS/2 workstation.

After completing the information for the three security databases, you are ready to transfer the information to the security authenticators.

4.2.1.7 Updating Security Data

When the security databases have been changed (updated), they need to be transferred to the appropriate security authenticators. If the security administrator is remotely administering the security authenticators, then you must transfer the files via the controller by establishing a secure session. If the security administrator is locally administering the security authenticator, then the files are transferred without a secure session.

To send the security files via the controller:

1. Start the controller. See the Distributed Console Access Facility User's Guide.

2. From the **Services** pull-down menu on the DCAF controller main window, choose **Logon DCAF...** When you type your user ID, it should be a user ID defined with access level zero so that you have all the access level privileges. Level zero is reserved for the person that administers the security system.

3. After successfully logging on, start the security administrator (if it is not already started). See "Starting the Security Administrator" in topic 4.2.1.1.

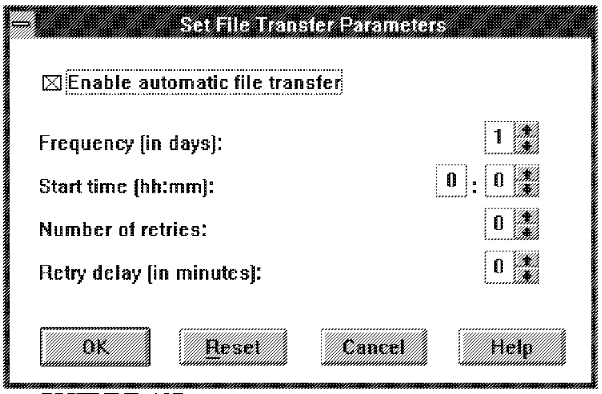
Before transferring files to the remote security authenticators, the security authenticator and target must be started (started and ready to establish a session with a controller). See the "Starting the Security Authenticator" in topic 4.2.2.1 and Distributed Console Access Facility Target User's Guide.

When you are ready to send the security files to the authenticator(s), choose **Transfer files** (or Ctrl+T shortcut key) from the **Options** pull-down menu on the Security Administrator main window (see Figure 126 in topic 4.2.1.2). The files are sent by the security administrator to the security authenticator(s).

During the file transfer, a session window is opened for each security authenticator. While the file transfer is in progress, the DCAF file transfer utility displays the percentage of the file that has been transferred.

You will receive a message if the file transfer was completely or partially successful. Another message lists the name of the file and the security authenticator if the transfer was unsuccessful. See the security administrator log file, EQNADMN.LOG, for messages about the file transfers.

You can optionally designate to have the files sent on a regular basis with the automatic file transfer. Choose **Set parameters** from the **Options** pull-down menu, and then choose **Set file transfer parameters...** from the cascading menu (see Figure 126 in topic 4.2.1.2).



PICTURE 127

Figure 144. Automatic File Transfer Parameters

The Automatic File Transfer Parameters (Figure 144) appears. There are five parameters to set up the automatic file transfer.

1. Mark the **Start automatic file transfer** to allow the file transfer to occur automatically.

   Note: If you are starting this choice for the first time, make sure that you already have some security information in the security databases.

2. Specify the frequency (how often) in number of days that you want the automatic file transfer to take place. The range is from 1-30 days. The default value is 1 day.

3. Specify the starting time in hours:minutes when the automatic file transfer should start. The range for the hours is from 0-23 hours. The range for the minutes is from 0-59 minutes. The default for both hours and minutes is 0. If you choose values of 00:00, the transfer will start at midnight.

4. Specify how many times you want to retry (number of retries) the file transfer if it does not complete successfully the first time. The security administrator will try to update only those security authenticators that did not receive the latest files. The retry range is from 0-5. The default is 0. If you specify 0, there are no retries if the transfer is not successful.

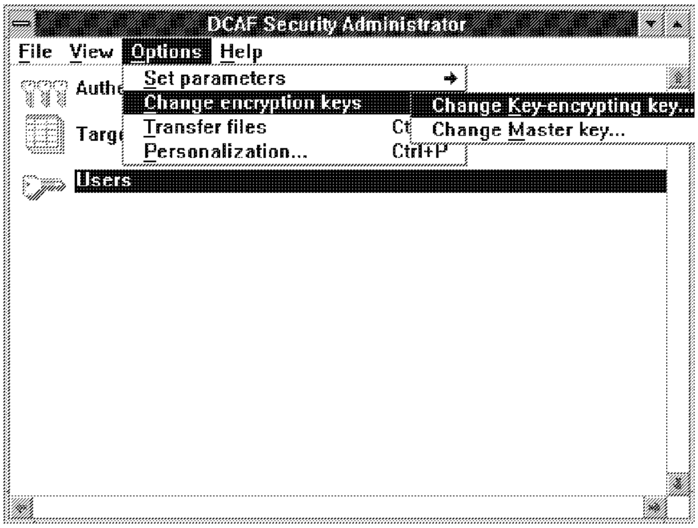
5. Specify the retry delay (interval between retries) in minutes. The range is from 0-60 minutes. The default is 0. If you specify 0, the retry begins immediately.

Press the **OK** push button to make your choices valid. To return to the previous entries, press the **Reset** push buttons and then the **OK** push button.

Note: To make your changes effective, exit the security administrator and then restart it.

If a file transfer is already in progress, the automatic file transfer of security information is postponed until the next designated time.

4.2.1.8 Changing the KEK and Master Key



PICTURE 128

Figure 145. Security Administrator Main Window with Options Pull-Down Menu

During normal operations, you may want to change the key-encrypting key and the master key. Each of the keys plays a part in validating a secure DCAF session through data and key encryption and decryption. By periodically changing the information, it makes it more difficult for an intruder to break into the security system.

From the **Options** pull-down menu (Figure 145), choose **Change encryption keys**. Then from the cascading menu, choose either **Change Key-encrypting key...** (or the Ctrl+K shortcut key) or **Change Master key...** (or the Ctrl+M shortcut key). For a description on how to update the KEK and the master key, see

- "Supplying the Format for the Key-Encrypting Key" in topic 2.1.1.4.2 for the KEK
- "Installing without the 4755 Cryptographic Adapter Card" in topic 2.1.1.4.1 for the master key

4.2.1.9 Updating the Authenticator KEK in the Administrator Database

DCAF provides a utility, EQNUTAD1.EXE, that enables you to update the authenticator KEKs in the administrator database. EQNUTAD1 reads a file that lists the authenticator names with their new KEKs and searches for the authenticator names in the authenticator database. If it finds the authenticator name, it updates the KEK associated with it.

Note: The new KEKs can be in hexadecimal format only.

To update the authenticator KEKs in the database, perform the following tasks:

- Prepare a text file that lists the authenticator names with the new KEKs. The default file name is EQNUTAD1.TXT. Do the following:

  1. Begin a new line for each authenticator. Starting from the column 1, type the authenticator name.

  2. Starting from the column 13, type the new KEK. It is exactly 32 hexadecimal characters in length. See "Supplying the Format for

the Key-Encrypting Key" in topic 2.1.1.4.2 for instructions on hexadecimal KEK character guidelines. Type a space between substrings.

If you specify a KEK that is longer, EQNUTAD1 truncates it to the first 32 characters. If you specify a KEK that is shorter, you receive an error message.

- Run EQNUTAD1:

  At the command prompt, type **EQNUTAD1** text file, where text file is the name of the file that contains the authenticator names and new KEKs.

4.2.1.10 Updating Pass Phrase Change Requests

The security administrator must be running (started) in order to process the pass phrase change requests sent from the controllers.

Whenever a valid pass phrase change request is processed on the security administrator (this is transparent to the user at the security administrator), a message is displayed on the screen asking whether a file transfer must be started to propagate the change to all of the security authenticators. Choose **Yes** to send the security information. Because another file transfer might be in process, the default choice is **No**. If you miss this message (your workstation is unattended when the message arrives), then periodically check the security administrator log file, EQNADMIN.LOG.

For APPC communication, you define Transaction Program Profile for each controller and the security administrator. See "Controller to the Security Administrator via APPC on a Token-Ring LAN" in topic 3.10, for instructions.

4.2.1.11 Exiting from the Security Administrator

To exit the security administrator, choose the **File** pull-down menu on the DCAF Security Administrator main window, and then choose **Exit** (or F3).

4.2.2 Using the Security Authenticator

The security authenticator provides the protection mechanism for secure DCAF sessions. The security authenticator is installed on an OS/2 workstation on each logical LAN in the network. If the controller requests a secure session with a target, the security authenticator validates the secure session via a secure DCAF gateway. The authentication process is transparent to the user, and the authentication activity is logged in the audit log file, EQNAUTH.LOG.

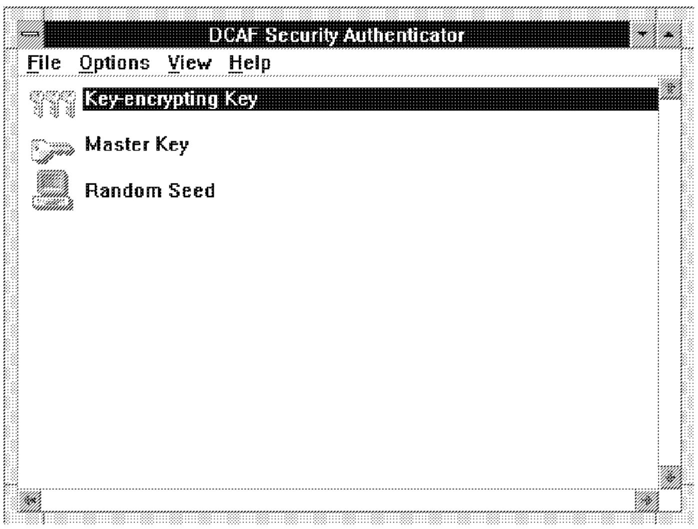
The following functions are described in this section:

- Starting the Security Authenticator
- Changing the KEK, Master Key, and Random Seed Value
- Changing the KEK via 4755 Adapter
- Updating the Key Label for Changed KEK from the Command Line
- Changing the Retry Limit for Invalid Pass Phrase
- Using the Security Authenticator Audit Log File
- Exiting from the Security Authenticator.

4.2.2.1 Starting the Security Authenticator

To start the when you are using OS/2 1.3, first choose the Distributed Console Access Facility group from the Desktop Manager window, and then choose the **Authenticator for the DCAF** program. To start the when you are using OS/2 1.3, first choose the DCAF work area folder from the desktop, and then choose the **Authenticator for the DCAF** icon.

4.2.2.2 Changing the KEK, Master Key, and Random Seed Value

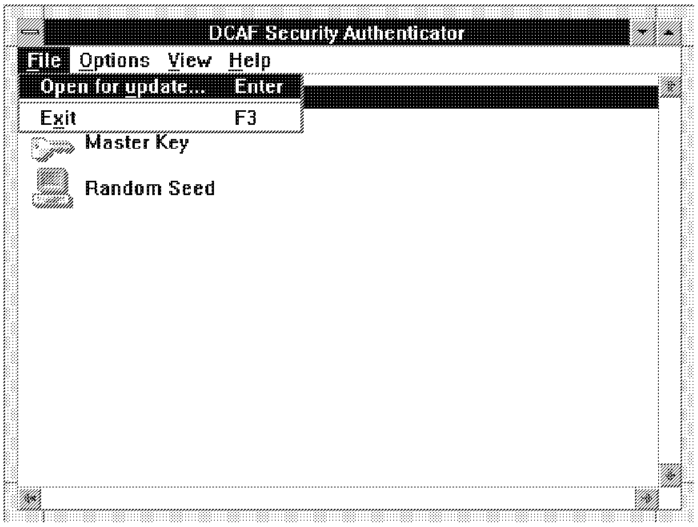


PICTURE 129

Figure 146. Security Authenticator Main Window

During normal operations, you may want to change the key-encrypting key, the master key, or the random seed value. Each of these keys and values plays a part in validating a secure DCAF session through data and key encryption and decryption. By periodically changing the information, it makes it more difficult for an intruder to break into the security system.

If you **do not** have the 4755 Cryptographic adapter card installed, you can update the master key and the random seed value (random number generator). The 4755 Cryptographic adapter card already contains the information for the master key and the random seed value. The key-encrypting key can always be updated. Select the item that you want to update from the DCAF Security Authenticator main window as shown in Figure 146.



PICTURE 130

Figure 147. Security Authenticator Main Window with File Pull-Down Menu

To update one of the items in the DCAF Security Authenticator window (Figure 147), select the item you want to update. Then choose **Open for Update...** from the **File** pull-down menu as shown in Figure 146.

- To update the KEK, select Key-encrypting Key. See "Supplying the Format for the Key-Encrypting Key" in topic 2.1.1.4.2 for further instructions.

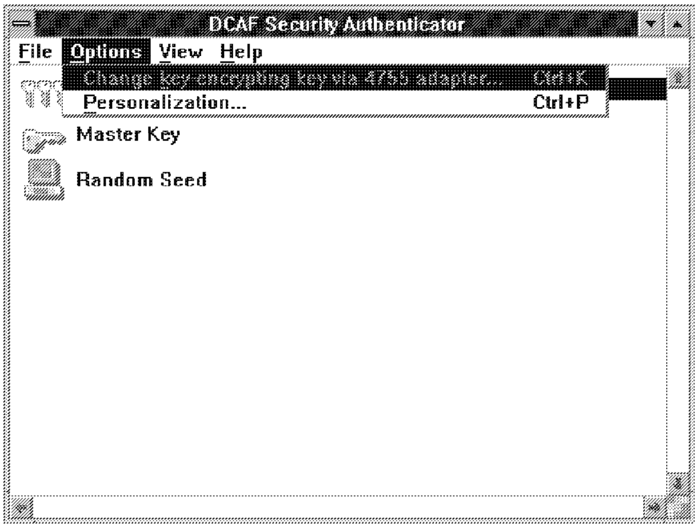
- To update the master key, select Master Key. See "Installing without the 4755 Cryptographic Adapter Card" in topic 2.1.1.4.1 for further instructions.

- To update the random seed value, select Random Seed. Then complete the following steps:

  1. Type eight or more characters in each of the input fields. The input for each field does not have to be the same. You must pause at least 1/2 second between keystrokes, or the keystrokes will not be registered.

  2. Press the **OK** push button when you have completed typing the information.

4.2.2.3 Changing the KEK via 4755 Adapter

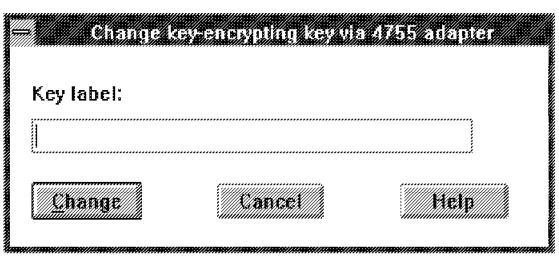


PICTURE 131

Figure 148. Security Authenticator Main Window with Options Pull-Down Menu

If the security authenticator has the 4755 Cryptographic adapter card installed, then the security authenticator KEK is changed via the Transaction Security System (TSS) software facilities.

After updating the KEK via the 4755 adapter, you must type the name of the key label that was used to store the new key-encrypting key. Choose the **Change key-encrypting key via 4755 adapter** from **Options** pull-down menu on the Security Authenticator main window as shown in Figure 148.



PICTURE 132

Figure 149. Change Key-Encrypting Key via 4755 Adapter

The Change Key-encrypting Key via 4755 Adapter window (Figure 149) appears.

1. Type the key label for the new KEK following the TSS guidelines. guidelines

   The key label must be 1-5 strings long, where each string is separated by a period.

   Each string is 1-8 characters in length, including:

   - Upper- or lowercase letters (A-Z, a-z)
   - Digits (0-9)

2. Press the **Change** push button. The security authenticator is immediately notified about the new KEK. If the key label that you typed does not exist, then a message will be displayed and you must

correct the input. It is assumed that the new KEK is already stored in key storage before you update the key label field.

Tip for the Key Label

Do not use DCAFKEK.IMPORTER as your key label when you change the KEK via the 4755 adapter. If you use the DCAFKEK.IMPORTER key label to store the new KEK, the old KEK will be overwritten and lost. The security authenticator must use the old KEK until the new encrypted data files are transferred from the security administrator to the security authenticator. The new data files are encrypted with the new KEK.

4.2.2.4 Updating the Key Label for Changed KEK from the Command Line

DCAF provides a utility, EQNUTAU1.EXE, that notifies the authenticator that the new KEK, changed via the 4755 adapter, is stored in key label DCAFKEK.NEW.

EQNUTAU1 does not update the KEK in the key label. See "Updating the Authenticator KEK in the Administrator Database" in topic 4.2.1.9 for information on updating the KEK. Ensure that the new KEK is in the DCAFKEK.NEW label.

To run EQNUTAU1, type **EQNUTAU1** at the command prompt on the authenticator workstation.

4.2.2.5 Changing the Retry Limit for Invalid Pass Phrase

DCAF provides a utility, EQNUTAU2, that enables you to change the limit of retries if a user types a nonvalid pass phrase. When the user reaches the limit of retries, DCAF revokes the user ID. The range for retries is 1-255. The default is 5.

To run EQNUTAU2, type **EQNUTAU2** retries at the command prompt, where retries is the new retries limit.

4.2.2.6 Using the Security Authenticator Audit Log File

The security authenticator keeps an audit log file, **EQNAUTH.LOG**. It is updated for each request for a secure DCAF session that is processed by the security authenticator. The file is located in the directory where the DCAF product is installed.

Whenever a controller wants to establish a session with a secure DCAF gateway or target, the security authenticator validates (accepts or rejects) the request. During the process, it logs the user ID of the controller, the adapter address of the DCAF gateway or target, and the result of the authentication process.

In case the attempt was unsuccessful, an error return code is also logged. The possible error return codes are listed in Table 24.

Table 24. Error Return Codes for the Security Authenticator Audit Log File

Return Code	Description
1	Your pass phrase has expired.
2	Your user ID has been revoked.
3	You typed your user ID incorrectly or the user ID has been removed by the person who administers the security for the network.
4	You typed your pass phrase incorrectly or the security authenticator has not received your new pass phrase.
5	You are restricted to initiating secure DCAF sessions during certain hours and the current time is not within those hours.
6	You are not allowed to initiate secure DCAF sessions during the weekend.
7	You are trying to access a remote workstation that does not exist or has not been defined for this network.
8	An error occurred on the security authenticator.
9	You do not have access privilege for the specified target.
10	The security authenticator has not been initialized yet. The security files have not been transferred from the security administrator.

4.2.2.7 Exiting from the Security Authenticator

To exit the security authenticator choose the **File** pull-down menu on the DCAF Security Authenticator main window, and then choose **Exit** (or F3). You will be asked to confirm to exit the security authenticator. If you choose to exit, then any current authentication requests that are being processed will stop, and the security authenticator will not be available to authenticate future requests.

APPENDIX1 Appendixes

APPENDIX1.1 Appendix A. Optimizing DCAF

This chapter provides some tips to help you get the best out of DCAF. In addition, you can find helpful suggestions on the DCAF forum through your IBM marketing representative or systems engineer.

APPENDIX1.1.1 Do's and Don'ts

Use these tips to improve DCAF performance.

- Do not use wallpaper and background patterns in the graphic environment on the target workstation during a session. It could interrupt the session.

- Do not do unnecessary mouse movements on the controller during connections on slow lines (such as asynchronous). They use up resources and slow down the connection.

- Before you start an MS-DOS prompt on the Windows target from the controller, do make sure that:

  - If you will be working in drive A (or physical drive B), the diskette is not write-protected and has been inserted in the drive on the target workstation.

  - If you will be using the printer, there is paper in the printer.

  Otherwise, the target workstation will switch to a DOS prompt and keystrokes from the controller will not work on the target. You must restart the target workstation on site.

APPENDIX1.1.2 Tuning Configuration to Improve Performance

You can improve DCAF performance by tuning some configuration parameters. Because the way communication resources are allocated and used varies from network to network, this section does not recommend exact values for tuning. It describes which parameters you should adjust to improve performance and suggests approximate values. Use trial and error to find the values that are right for your network. Remember that the lowest setting for parameters overrides higher settings elsewhere in your network.

APPENDIX1.1.2.1 Using LAPS to Connect a Gateway and Target on the Same Workstation

If you use LAPS 2.0, with refresh level WR07045, to communicate via NetBIOS between a target and gateway on the same workstation, performance slows down significantly. You can fix the problem either by using the LAPS interface or by editing the PROTOCOL.INI file. It is recommended that you use the LAPS interface and then edit the resulting PROTOCOL.INI file to check the values.

To use the LAPS interface, complete the following steps:

1. At an OS/2 prompt, type **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, in the Current Configuration list box, the IBM Token-Ring Network Adapter, and IBM IEEE 802.2 and IBM OS/2 NetBIOS protocols all appear.

5. 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.

6. Increase the value for the GDT selectors field. The default is 5. Suggested value: **15**.

7. Increase the value for the Loopback frame descriptors field. The default is 1. Suggested value: **8**.

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

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

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

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

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

13. Press the **Exit** push button.

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

To edit the PROTOCOL.INI file to adjust or check the values, complete the following steps:

1. At an OS/2 prompt, type **cd ibmcom**.

2. Edit the PROTOCOL.INI file.

3. In the [NETBEUI_nif] section, check or increase the values for LOOPPACKETS to a suggested value of **8** and for SELECTORS to a suggested value of **15**.

4. Save and close the PROTOCOL.INI file.

5. If you made any changes, stop all applications on the workstation and shut down the workstation.

APPENDIX1.1.2.2 Using APPC/APPN

To improve performance on APPC/APPN connections, you can tune some parameters in the configuration files on the connecting workstations. For Communications Manager/2, edit the .NDF files. To tune the .NDF files, complete the following tasks:

1. Edit the .NDF file on each connecting workstation.

2. In the DEFINE_MODE section, increase the value for MAX_RU_SIZE_UPPER_BOUND to a suggested value of **4000**. Increase the value for RECEIVE_PACING_WINDOW to a suggested value of **8**.

3. Save and close the .NDF file.

4. At the OS/2 prompt, type **cmverify** filename, where filename is the name of your configuration file, and press **Enter**. To update a currently active file dynamically, type cmverify filename /e.

In SNA environments, your tuning for DCAF may affect adversely the performance of other applications running in your network. Keeping in mind the requirements of the rest of your network, tune the following parameters.

For VTAM, tune the RU size and IOBUF parameters:

- RU size: Increase this value. VTAM supports a maximum of 64 KB.

- IOBUF: Increase to a suggested value of **4000**.

APPENDIX1.2 Appendix B. Startup Files

The DCAF program updates startup files when it is installed on the workstation. This section shows the entries that are added to the OS/2 CONFIG.SYS and the SYSTEM.INI files for OS/2 components, to the DCAFDOS.BAT file for the DOS target, and to the startup files for the Windows target.

Only entries relevant to the DCAF program are shown. Also, these entries show the DCAF program installed in the DCAF default drive and path. If a different drive or path is specified during DCAF installation, then the appropriate drive and path will be used.

APPENDIX1.2.1 Startup Files for OS/2 Components

The DCAF updates the CONFIG.SYS for the OS/2 components and, in addition, the SYSTEM.INI for the OS/2 target.

APPENDIX1.2.1.1 Changes to the CONFIG.SYS File

Table 25 shows the entries added to the CONFIG.SYS file for the various OS/2 DCAF components.

Table 25. Example CONFIG.SYS Entries for OS/2 DCAF Components

Component	**CONFIG.SYS Entries**
Controller	. . . LIBPATH=C:\DCAF13;.... SET PATH=C:\DCAF13;.... SET DPATH=C:\DCAF13;.... . . .
Target for OS/2	. . . DEVICE=C:\DCAF13\EQNRCSH.EXE CALL=C:\DCAF13\EQNRCLD.EXE DEVICE=C:\DCAF13\EQNVKBD.SYS . . . LIBPATH=C:\DCAF13;.... SET PATH=C:\DCAF13;.... SET DPATH=C:\DCAF13;.... . . .
DCAF Gateway	. .

	. LIBPATH=C:\DCAF13;.... SET PATH=C:\DCAF13;.... SET DPATH=C:\DCAF13;.... . . . DEVICE=C:\DCAF13\EQNGWDD.EXE /S . . .
DCAF LAN Directory	. . . LIBPATH=C:\DCAF13;.... SET PATH=C:\DCAF13;.... SET DPATH=C:\DCAF13;.... . . .
DCAF Gateway and LAN Directory	. . . LIBPATH=C:\DCAF13;.... SET PATH=C:\DCAF13;.... SET DPATH=C:\DCAF13;.... . . . DEVICE=C:\DCAF13\EQNGWDD.EXE /S . . .
Security Administrator	. . . LIBPATH=C:\DCAF13;.... SET PATH=C:\DCAF13;.... SET DPATH=C:\DCAF13;.... . . .
Security Authenticator	. . . LIBPATH=C:\DCAF13;.... SET PATH=C:\DCAF13;.... SET DPATH=C:\DCAF13;.... . . .

APPENDIX1.2.1.2 Changes to the SYSTEM.INI for the OS/2 Target

Figure 150 shows a sample entry of the statement that DCAF changes in the SYSTEM.INI file.

```
     .
     .
     .
  [boot]
  os2shield=C:\DCAF13\EQNSEADA.EXE
     .
     .
     .
```

Figure 150. Sample SYSTEM.INI for an OS/2 Target

APPENDIX1.2.2 DCAFDOS.BAT File for the DOS Target

When the DCAF is installed on the DOS workstation, a file containing the personalization options, DCAFDOS.BAT, is copied to the workstation. No DCAF entries are made to the CONFIG.SYS file on DOS workstations.

Figure 151 shows a sample DCAFDOS.BAT file.

```
 C:
 CD C:\DCAF13
 EQNDD.EXE /L C:\DCAF13\EQNDDERR.LOG /D DCAFLAN /O d4000s01633Fh07080250k0u0a0m0e111
```

Figure 151. Sample DCAFDOS.BAT for a DOS Target Workstation

APPENDIX1.2.3 Startup Files for the Windows Target

DCAF installation makes the following changes in the startup files on the Windows target workstation:

APPENDIX1.2.3.1 AUTOEXEC.BAT

Figure 152 shows a sample entry in the AUTOEXEC.BAT file.

```
     .
     .
     .
       PATH=c:\dcaf13;...
     .
     .
     .
```

Figure 152. Sample AUTOEXEC.BAT for a Windows Target Workstation

APPENDIX1.2.3.2 WIN.INI

The eqnwload.exe program includes the DCAF in the list of programs to be loaded when Windows starts up on the workstation. It starts the DCAF target as soon as Windows is started up if you have started the DCAF target in native DOS first. The version and installation path entries signal the presence of a version of DCAF on the workstation for when you install the DCAF in the future. Figure 153 shows sample entries in the WIN.INI file.

```
 .
 .
 .
  Load=c:\dcaf13\eqnwload.exe ...

 .
 .
 .
  [DCAF]
  Version=1.31
  Inst-Path=c:\dcaf13

 .
 .
 .
```

Figure 153. Sample WIN.INI for a Windows Target Workstation

APPENDIX1.2.3.3 SYSTEM.INI

These SYSTEM.INI entries replace the default drivers with the ones used by the DCAF. The DCAF includes the version of Windows that is installed on the workstation. Figure 154 shows sample entries in the SYSTEM.INI file.

```
 .
 .
 .
Mouse.drv=EQNMOUSE.DRV        (or EQNMOUS_.DRV)
Keyboard.drv=EQNKEYBD.DRV     (or EQNKEYB_.DRV)
Display.drv=EQNDI31.DRV       (or EQNDI_31.DRV)
Comm.drv=EQNCOMM.DRV          (or EQN_COMM.DRV)
 .
 .
 .
[386Enh]
Keyboard=EQNVKB31.386       (or EQNVK_31.386)
 .
 .
 .
```

Figure 154. Sample SYSTEM.INI for a Windows Target Workstation

APPENDIX1.2.3.4 PROGMAN.INI

The PROGMAN.INI entry includes a DCAF group in the workstation's Program Manager. Figure 155 shows sample entries in the PROGMAN.INI file.

```
  .
  .
  .
[Groups]
Group c:\WINDOWS\DCAF.GRP
  .
  .
  .
```

Figure 155. Sample PROGMAN.INI for a Windows Target Workstation

APPENDIX1.2.3.5 DCAFDOS.BAT

At the DCAF installation, the DCAFDOS.BAT file is copied onto the workstation. It contains personalization options for the DCAF target when the target is running in native DOS. Figure 156 shows a sample DCAFDOS.BAT file.

```
c:
cd c:\dcaf13
eqnstart <drive>:\<path>\dcaf.ini>dd_start.bat
call dd_start.bat
```

Figure 156. Sample DCAFDOS.BAT for a Windows Target Workstation

APPENDIX1.3 Appendix C. Response Files

This appendix contains examples of response files and a chart of valid parameters for each component. The examples contain installation keywords and all the possible personalization options for each component. The charts describe the personalization options and list the accepted values and the default, in bold, for each option.

APPENDIX1.3.1 Keywords for Installation

Each response file begins with the following keywords:

- Sourcedir: the drive and directory from which you are installing DCAF.

- Targetdir: the drive and directory to which you are installing DCAF on the remote workstation.

- Install: the component that you are installing.

- Rebootrequired: **Y** to restart the remote workstation when installation ends. This is useful for unattended workstations. **N** to not restart the workstation at the end of installation. **N** is the default.

APPENDIX1.3.2 Keywords for Personalization

Next to the personalization option, type the parameter. Erase any other option keywords for which you will use the default. Make sure that the personalization for each component begins and ends with the parentheses.

Keywords contain the following prefixes:

- Asy: asynchronous
- Basic: nonsecure target
- Dos: DOS target
- Ipx: IPX/SPX
- Nb: NetBIOS
- Tcp: TCP/IP
- Sec: secure target

APPENDIX1.3.3 OS/2 Target

An example response file for the OS/2 target follows.

```
# This is a comment
Sourcedir =Z:\CODE\SERVER\DCAF
Targetdir =D:\DCAF13
Install =OS2Tgt
Rebootrequired =Y/N

OS2Tgt =(
          NbAdapter =
          NbLanDirName =
          NbAutostart =
```

```
AsyComPortNum =
AsyConnectType =
AsyBaudRate =
AsyAutostart =
AsyBufAck =
StartMonitor =
RefreshRate =
SecureTgt =
SecPrimaryAuthAddress =
SecSecondaryAuthAddress =
BasicPassword =
BasicAllowReboot =
BasicAllowStartFS =
BasicAllowTargetSendFile =
BasicAllowTargetRcvFile =
BasicAllowTargetActive =
BasicAllowControllerActive =
BasicAllowControllerMonitor =
CanTerminate =
IndicatorRow =
IndicatorCol =
IndicatorColor =
BasicEnableHotKey =
BasicHotKey =
MessageDisplayTime =
LogFileName =
TcpLanDirAddress =
TcpLanDirPort =
TcpLocalPort =
TcpAutostart =
IpxLanDirNetworkAddr =
IpxLanDirNodeAddr =
IpxAutostart =
)
```

Table 26 shows the personalization parameters and accepted values for the OS/2 target.

Table 26. OS/2 Target Personalization Parameters

Keyword	Accepted Values	Description
NbAdapter	0 - 3 Default: **0**	The LAN adapter that the NetBIOS target uses.
NbLanDirName	The name of any valid LAN directory Default: **DCAFLAN**	The name of the LAN directory with which the NetBIOS target registers.
NbAutostart	Y or N Default: **N**	Enables the target to start NetBIOS automatically when the target starts.
AsyComPortNum	1 - 3 Default: **1**	The communication port that the target uses for asynchronous

		communication.
AsyConnectType	1 or 3 Default: **3**	Defines whether the target responds to a manual (1) or automatic data answering (3) connection with the controller.
AsyBaudRate	1200, 2400, 4800, 9600, 19200, 38400, 48000, 56000, 57800, or 64000. Default: **9600**	The modem transmission rate in bits per second.
AsyAutostart	Y or N Default: **N**	Enables the target to start asynchronous communications automatically when the target starts.
AsyBufAck	128 - 8192 Default: **1664**	The buffer acknowledge size enables the target to send a specific amount of data to the controller and wait for the controller′s acknowledgment before it sends new data.
StartMonitor	Y or N Default: **N**	Enables the target to start monitoring (Y) or active (N) state.
RefreshRate	100 - 4000 (in multiples of one hundred) Default: **100**	The interval, in milliseconds, between updates of the target screen that are sent to the controller display. If the connection with the controller is slow or has heavy traffic increase the value. If you enter a higher value, the screen updates are sent to the controller display less frequently.
SecureTgt	Y or N Default: **N**	Enables a secure target.
SecPrimaryAuthAddress	< 7FFFFFFFFFFF Default: None	The LAN adapter address of the primary authenticator of a secure target.
SecSecondaryAuthAddress	< 7FFFFFFFFFFF Default: None	The LAN adapter address of the secondary authenticator of a secure target.

BasicPassword	4 to 8 alphanumeric characters Default: None	The password for basic DCAF targets.
BasicAllowReboot	Y or N Default: **Y**	Enables the Controller to restart the target. (for basic DCAF targets only)
BasicAllowStartFS	Y or N Default: **Y**	Enables the controllerto start a full screen on the target (for basic DCAF Targets only)
BasicAllowTargetSendFile	Y or N Default: **Y**	Enables the controller to send files to this target (for basic DCAF targets only).
BasicAllowTargetRcvFile	Y or N Default: **Y**	Enables the target to receive files from the controller (for basic DCAF targets only).
BasicAllowTargetActive	Y or N Default: **Y**	Enables the target to switch to active mode during a session (for basic DCAF targets only).
BasicAllowControllerActive	Y or N Default: **Y**	Enables the controller to control the target (active mode) during a session (for basic DCAF targets only).
BasicAllowControllerMonitor	Y or N Default: **Y**	Enables the controller to monitor the target (monitoring mode) during a session (for basic DCAF targets only).
CanTerminate	Y or N Default: **Y**	Enables the target to terminate a session.
IndicatorRow	0 to 60 Default: **1**	Sets the row position of the status indicator on the target screen.
IndicatorCol	1 to 116 Default: **62**	Sets the column position of the status indicator on the target screen.
IndicatorColor	WONC (White on Cyan) CONW (Cyan on White) BONW (Black on	Sets the foreground and background colors of the status indicator.

	White) WONB (White on Black) Default: **WONC**	
BasicEnableHotKey	Y or N Default: **Y**	Enables the target hot key.
BasicHotKey	A to Z Default: **T**	The second part of the hot-key combination.
MessageDisplayTime	0 to 99 Default: **99**	Determines the length of time, in seconds, that a message is displayed on the screen.
LogFileName	1 to 8 characters in length with a 0-3 character extension Default: **EQNITG.LOG**	The name of the file that logs error messages for the target.
TcpLanDirAddress	nnn.nnn.nnn.nnn where nnn is any number from 0 - 255. Default: None	The address assigned to the target LAN directory during TCP/IP installation.
TcpLanDirPort	1024 to 65534 Default: **2500**	The port number assigned during the installation of the LAN directory for this target.
TcpLocalPort	1024 to 65534 Default: **2501**	The port number that the target uses for TCP/IP communication.
TcpAutostart	Y or N Default: **N**	Enables the target to start TCP/IP automatically when the target starts.
IpxLanDirNetworkAddr	00000000 to FFFFFFFE Default: None	A unique eight-digit hexadecimal number that identifies the LAN directory network to the target.
IpxLanDirNodeAddr	000000000000 to FFFFFFFFFFFF Default: None	The LAN adapter address of the IPX/SPX target.
IpxAutostart	Y or N Default: **N**	Enables the target to start IPX/SPX automatically when the target starts.

APPENDIX1.3.4 Controller

An example response file for the controller follows.

```
# This is a comment
Sourcedir =Z:\CODE\SERVER\DCAF
Targetdir =D:\DCAF13
Install =Controller
Rebootrequired =Y/N

Controller =(
            EnableMsgLog=
            MessageDisplayTime =
            LogFileName =
            HotKey =
            )
```

Table 27 shows the personalization parameters and accepted values for the controller.

Table 27. Controller Personalization Parameters

Keyword	**Accepted Values**	**Description**
EnableMsgLog	Y or N Default: **Y**	Enables a file that logs information and error messages for the controller
MessageDisplayTime	0 to 99 Default: **99**	Determines the length of time, in seconds, that a message is displayed on the screen.
LogFileName	1 to 8 characters in length with a 0-3 character extension Default: **EQNCONTL.LOG**	The name of the log file.
HotKey	A to Z Default: **T**	The second part of the hot-key combination.

APPENDIX1.3.5 LAN Directory

An example response file for the LAN directory follows.

```
# This is a comment
Sourcedir =Z:\CODE\SERVER\DCAF
Targetdir =D:\DCAF13
Install =LanDir
Rebootrequired =Y/N
```

```
LanDir      =(
              NbAdapter=
              NbLanDirName=
              NbListFileName=
              NbAutostart=
              NbNumOfGwAccess=
              LogFileName=
              TcpListFileName=
              TcpAutostart=
              TcpLocalPort=
              IpxListFileName=
              IpxAutostart=
              )
```

Table 28 shows the personalization parameters and accepted values for the LAN directory.

Table 28. LAN Directory Personalization Parameters

Keyword	Accepted Values	Description
NbAdapter	0 - 3 Default: **0**	The LAN adapter that the NetBIOS LAN directory uses.
NbLanDirName	The name of any valid LAN Directory Default: **DCAFLAN**	The name of the LAN directory with which the NetBIOS target registers.
NbListFileName	1 to 8 characters in length with a 0-3 character extension Default: **EQNLDNET.DAT**	Name of the file that lists NetBIOS targets by nickname.
NbAutostart	Y or N Default: **N**	Enables the LAN directory to start NetBIOS automatically when the target starts.
NbNumOfGwAccess	1 to 254 Default: **4**	The number of NetBIOS sessions that can be started simultaneously with the LAN directory through the same gateway.
LogFileName	1 to 8 characters in length with a 0-3 character extension Default: **EQNLDNET.LOG**	The name of the file that logs error messages for the LAN directory.
TcpListFileName	1 to 8	Name of the file that

	characters in length with a 0-3 character extension Default: **EQNLDTCP.DAT**	lists TCP/IP targets by nickname.
TcpLocalPort	1024 to 65534 Default: **2500**	The port number that the LAN directory uses for TCP/IP communication.
TcpAutostart	Y or N Default: **N**	Enables the target to start TCP/IP automatically when the target starts.
IpxListFileName	1 to 8 characters in length with a 0-3 character extension Default: **EQNLDIPX.DAT**	Name of the file that lists IPX/SPX targets by nickname.
IpxAutostart	Y or N Default: **N**	Enables the target to start IPX/SPX automatically when the target starts.

APPENDIX1.3.6 Gateway

An example response file for the gateway follows.

```
# This is a comment
Sourcedir =Z:\CODE\SERVER\DCAF
Targetdir =D:\DCAF13
Install =Gateway
Rebootrequired =Y/N

Gateway    =(
             NbAdapter=
             NbLanDirName=
             NbSessions=
             LogFileName=
             SecureGw=
             SecAuthName=
             BasicPassword=
             )
```

Table 29 shows the personalization parameters and accepted values for the gateway.

Table 29. Gateway Personalization Parameters

Keyword	Accepted Values	Description
NbAdapter	0 or 1 Default: **0**	The LAN adapter that the NetBIOS gateway uses.
NbLanDirName	The name of any valid LAN directory Default: **DCAFLAN**	The name of the LAN directory with which the NetBIOS gateway registers.
NbSessions	1 to 254 Default: **16**	The number of NetBIOS sessions that can be started simultaneously with the LAN directory through this gateway.
LogFileName	1 to 8 characters in length with a 0-3 character extension Default: **EQNGWAUD.LOG**	The name of the file that logs information and error messages for the gateway.
SecureGw	Y or N Default: **N**	Enables a secure gateway.
SecAuthName	• Must match the name assigned to the security authenticator. • The name is 1-12 characters in length. • Cannot be a single asterisk (*) or all blanks. Default: None	The unique name by which the authenticator associated with the gateway is recognized by the DCAF security environment.
BasicPassword	4 to 8 alphanumeric characters Default: None	The password for basic gateways.

APPENDIX1.3.7 Windows Target

An example response file for the Windows target follows.

```
# This is a comment
Sourcedir = Z:\CODE\SERVER\DCAF
```

```
Targetdir =C:\DCAF13
Install =WinTgt
Rebootrequired =Y/N

NbAdapter =
NbLanDirName =
TcpLanDirAddress =
TcpLanDirPort =
TcpLocalPort =
IpxLanDirNetworkAddr =
IpxLanDirNodeAddr =
AsyComPortNum =
AsyBaudRate =
AsyBufAck =
StartActive =
CanTerminate =
RefreshRate =
SecureTgt =
SecPrimaryAuthAddress =
SecSecondaryAuthAddress =
EnableHotKey =
HotKey =
LogFileName =
BasicPassword =
DosHotKey1 =
DosHotKey2 =
DosHotKeyPressedTime =
DosUnload =
DosScreenBuffSize =
DosRow =
DosCol =
DosColor =
DosChip8042Info =
```

Table 30 shows the personalization parameters and accepted values for the Windows target.

Table 30. Windows Target Personalization Parameters

Keyword	Accepted Values	Description
NbAdapter	0 or 1 Default: **0**	The LAN adapter that the NetBIOS target uses.
NbLanDirName	Any valid LAN Direcory name Default: **DCAFLAN**	The name of the LAN directory with which the NetBIOS target registers.
TcpLanDirAddress	nnn.nnn.nnn.nnn where nnn is any number from 0 - 255. Default: None	The address assigned to the target LAN directory during TCP/IP installation.
TcpLanDirPort	1024 to 65534 Default: **2500**	The port number assigned during the installation of the LAN directory for this target.

TcpLocalPort	1024 to 65534 Default: **2501**	The port number assigned during the installation of the LAN directory for this target.
IpxLanDirNetworkAddr	00000000 to FFFFFFFE Default: None	A unique eight-digit hexadecimal number that identifies the LAN directory network to the target.
IpxLanDirNodeAddr	000000000000 to FFFFFFFFFFFF Default: None	The LAN adapter address of the IPX/SPX target.
AsyComPortNum	1 - 3 Default: **1**	The communication port that the target uses for asynchronous communication.
AsyBaudRate	1200, 2400, 4800, 9600, 19200 38400, or 56000. Default: **9600**	The modem transmission rate in bits per second.
AsyBufAck	128 - 8192 Default: **1664**	The buffer acknowledge size enables the target to send a specific amount of data to the controller and wait for the controller′s acknowledgment before it sends new data.
StartActive	Y or N Default: **N**	Enables the target to start in active (Y) or monitoring (N) state.
CanTerminate	Y or N Default: **Y**	Enables the target to terminate a session.
RefreshRate	100 - 4000 (in multiples of one hundred) Default: **100**	The interval, in milliseconds, between updates of the target screen that are sent to the controller display. If the connection with the controller is slow or has heavy traffic increase the value. If you enter a higher value, the screen updates are sent to the controller display less frequently.
SecureTgt	Y or N Default: **N**	Enables a secure target.

SecPrimaryAuthAddress	< 7FFFFFFFFFFF Default: None	The LAN adapter address of the primary authenticator of a secure target.
SecSecondaryAuthAddress	< 7FFFFFFFFFFF Default: None	The LAN adapter address of the secondary authenticator of a secure target.
EnableHotKey	Y or N Default: **Y**	Enables the target hot key.
HotKey	A to Z Default: **T**	The second part of the Windows hot-key combination.
LogFileName	1 to 8 characters in length with a 0-3 character extension Default: **EQNTGLOG**	The name of the file that logs error messages for the target.
BasicPassword	4 to 8 alphanumeric characters Default: None	The password for basic DCAF targets.
DosHotKey1	1 to 10• Default: **Left Shift Key**	The first part of the DOS hot-key combination.
DosHotKey2	1 to 10• Default: **Right Shift Key**	The second part of the DOS hot-key combination.
DosHotKeyPressedTime	50 to 9999 Default: **250**	The number of milliseconds that the user must press the hot key to enable it to take effect on the target.
DosUnload	Y or N Default: **Y**	Enables the target to unload the DCAF DOS TSR from memory.
DosScreenBuffSize	2000, 3440, 4000, 6880 or 8000 Default: **4000**	The size of the memory buffer that the DCAF DOS TSR allocates to contain an image of the full-screen display.
DosRow	0 to 50 Default: **1**	Sets the row position of the status indicator on the screen.
DosCol	1 to 63 Default: **63**	Sets the column position of the status indicator on the screen.

DosColor	WONC (White on Cyan) CONW (Cyan on White) BONW (Black on White) WONB (White on Black) Default: **WONC**	Sets the foreground and background colors of the status indicator.
DosChip8042Info	Y, N, or U (unknown) Default: **U**	Determines the existence of the 8042 chip on the target.

- The following is the DOS hot key set:

```
 3 =Left Alt Key
 4 =Left Control Key
 7 =Left Shift Key          Default for Key1
 8 =Right Shift Key         Default for Key2
10 =Caps Lock Key
11 =Num Lock Key
12 =Scroll Lock Key
14 =System Request Key
15 =Right Alt Key
16 =Right Control Key
```

APPENDIX1.3.8 DOS Target

An example response file for the DOS target follows.

```
# This is a comment
Sourcedir =Z:\CODE\SERVER\DCAF
Targetdir =C:\DCAF13
Install =DosTgt
Rebootrequired =Y/N

NbAdapter =
NbLaaUaa  =
NbLanDirName =
StartMonitor =
CanTerminate =
Unload =
SecureTgt =
SecPrimaryAuthAddress =
SecSecondaryAuthAddress =
BasicPassword =
EnableHotKey =
HotKey1 =
HotKey2 =
HotKeyPressedTime =
ScreenBuffSize =
IndicatorRow =
IndicatorCol =
IndicatorColor =
LogFileName =
Chip8042Info =
```

Table 31 shows the personalization parameters and accepted values for the

DOS target.

Table 31. DOS Target Personalization Parameters		
Keyword	**Accepted Values**	**Description**
NbAdapter	0 or 1 Default: **0**	The LAN adapter that the NetBIOS target uses.
NbLaaUaa	LAA or UAA Default: **LAA**	The LAN adapter address type that the NetBIOS target uses.
NbLanDirName	Any valid LAN Direcory name Default: **DCAFLAN**	The name of the LAN directory with which the NetBIOS target registers.
StartMonitor	Y or N Default: **N**	Enables the target to start monitoring (Y) or active (N) state.
CanTerminate	Y or N Default: **Y**	Enables the target to terminate a session.
Unload	Y or N Default: **Y**	Enables the target to unload the DCAF DOS TSR from memory.
SecureTgt	Y or N Default: **N**	Enables a secure target.
SecPrimaryAuthAddress	< 7FFFFFFFFFFF Default: None	The LAN adapter address of the primary authenticator of a secure target.
SecSecondaryAuthAddress	< 7FFFFFFFFFFF Default: None	The LAN adapter address of the secondary authenticator of a secure target.
BasicPassword	4 to 8 alphanumeric characters Default: None	The password for basic DCAF targets.
EnableHotKey	Y or N Default: **Y**	Enables the target hot key.
HotKey1	1 to 10• Default: **Left Shift Key**	The first part of the DOS hot-key combination.
HotKey2	1 to 10• Default: **Right Shift Key**	The second part of the DOS hot-key combination.
HotKeyPressedTime	50 to 9999 Default: **250**	The number of milliseconds that the

		user must press the hot key to enable it to take effect on the target.
ScreenBuffSize	2000, 3440, 4000, 6880 or 8000 Default: **4000**	The size of the memory buffer that the DCAF DOS TSR allocates to contain an image of the full-screen display.
IndicatorRow	0 to 50 Default: **1**	Sets the row position of the status indicator on the target screen.
IndicatorCol	1 to 63 Default: **63**	Sets the column position of the status indicator on the target screen.
IndicatorColor	WONC (White on Cyan) CONW (Cyan on White) BONW (Black on White) WONB (White on Black) Default: **WONC**	Sets the foreground and background colors of the status indicator.
LogFileName	1 to 8 characters in length with a 0-3 character extension Default: **EQNDDERR.LOG**	The name of the file that logs error messages for the target.
DosChip8042Info	Y, N or U (unknown) Default: **U**	Determines the existence of the 8042 chip on the target.

• The following is the DOS Hot Keys set:

```
 3 ==Left Alt Key
 4 ==Left Control Key
 7 ==Left Shift Key          Default for Key1
 8 ==Right Shift Key         Default for Key2
10 ==Caps Lock Key
11 ==Num Lock Key
12 ==Scroll Lock Key
14 ==System Request Key
15 ==Right Alt Key
16 ==Right Control Key
```

APPENDIX1.3.9 Security Authenticator

An example response file for the security authenticator follows.

```
# This is a comment
```

```
Sourcedir  =Z:\CODE\SERVER\DCAF
Targetdir  =D:\DCAF13
Install  =Authenticator
Rebootrequired  =Y/N

Authenticator  =(
                  Use4755Adapter=
                  MasterKeyFormat=
                  MasterKey=
                  KekFormat=
                  Kek=
                  RandomSeed=
                  LocallyAdministered=
                  AuthName=
                  SecurityDataPath=
                  NbAdapter=
                )
```

Table 32 shows the personalization parameters and accepted values for the security authenticator.

Table 32. Security Authenticator Personalization Parameters

Keyword	Accepted Values	Description
Use4755Adapter	Y or N Default: **N**	Specifies whether or not the workstation uses the IBM 4755 cryptographic adapter card.
MasterKeyFormat	P or H Default: **P**	The format to use for the master key: Pass phrase (P) or Hexadecimal (H)
MasterKey	4 to 80 characters for Pass phrase format, 32 hexadecimal characters for hexadecimal format Default: None	Encrypts and deciphers other data-encrypting keys.
KEKFormat	P or H Default: **P**	The format to use for the KEK: Pass phrase (P) or Hexadecimal (H).
KEK	4 to 80 characters for Pass phrase format, 32 hexadecimal characters for hexadecimal format Default: None	Encrypts and deciphers security data.

RandomSeed	1 to 1000 Default: None	Used for random number generation.
LocallyAdministered	Y or N Default: **N**	Specifies whether or not the security administrator is installed on the same workstation as the security authenticator.
AuthName	1 to 12 characters. Case sensitive Default: None	The unique name by which the authenticator is recognized by the DCAF security environment.
SecurityDataPath	Any valid path name, up to 50 characters in length Default: DCAF path in which security administrator installed.	The directory where the security data files are stored.
NbAdapter	0 or 1 Default: **0**	The LAN adapter number used by the security authenticator.

APPENDIX1.3.10 Security Administrator

An example response file for the security administrator follows.

```
# This is a comment
Sourcedir =Z:\CODE\SERVER\DCAF
Targetdir =D:\DCAF13
Install =Administrator
Rebootrequired =Y/N

Administrator =(
                Use4755Adapter=
                MasterKeyFormat=
                MasterKey=
                KekFormat=
                Kek=
                EnableAcdi=
                AsyComPortNum =
                AsyBaudRate=
                SecurityDataPath=
               )
```

Table 33 shows the personalization parameters and accepted values for the security administrator.

Table 33. Security Administrator Personalization Parameters

Keyword	**Accepted Values**	**Description**

Use4755Adapter	Y or N Default: **N**	Specifies whether or not the workstation uses the IBM 4755 cryptographic adapter card.
MasterKeyFormat	P or H Default: **P**	The format to use for the master key: Pass phrase (P) or Hexadecimal (H)
MasterKey	4 to 80 characters for pass phrase format, 32 hexadecimal characters for hexadecimal format Default: None	Encrypts and deciphers other data-encrypting keys.
KEKFormat	P or H Default: **P**	The format to use for the KEK: Pass phrase (P) or Hexadecimal (H).
KEK	4 to 80 characters for Pass phrase format, 32 hexadecimal characters for hexadecimal format Default: None	Encrypts and deciphers security data.
EnableAcdi	Y or N Default: **N**	Enables ACDI pass phrase processing.
AsyComPortNum	1 - 3 Default: **1**	The communication port that the security administrator uses for asynchronous communication.
AsyBaudRate	1200, 2400, 4800, 9600, 19200, 38400, 48000, 56000, 57800, or 64000. Default: **9600**	The modem transmission rate in bits per second.
SecurityDataPath	Any valid path name, up to 50 characters in length Default: DCAF path in which security administrator installed.	The directory where the security data files are stored.

APPENDIX1.4 Appendix D. DOS Target Technical Information

The technical information included in this section discusses command line personalization parameters, NetBIOS resources, the use of terminate and stay resident applications, and code page changes while using the DCAF on the DOS target, whether it is a simple DOS target or a Windows target operating in native DOS.

APPENDIX1.4.1 Personalization and Command-Line Parameters

Important Information: It is **strongly recommended** that you personalize the DOS target component by using the DOS target personalization windows when you are creating a DOS target package for installation. See "Personalizing the DCAF Controller and Other Components" in topic 2.7. There is minimal error-checking for the data that is typed when the DOS command line personalization is used.

You can specify personalization options that will be used when you start the target-for-DOS component on the DOS workstation via command line personalization. Or you can use a text editor to update and to save the changes for these parameters in the DCAFDOS.BAT file.

The file, DCAFDOS.BAT, is automatically created by the DCAF during installation. This file contains the command to invoke the target for DOS component, EQNDD, with the parameters set to the values that you selected when you created the installation package. The **D** represents a decimal number. The **H** represents a hexadecimal number. The **C** represents a character. The command EQNDD is followed by the parameters that you want to use. The following figure shows the format of a sample DCAFDOS.BAT file.

```
EQNDD.EXE /O dDDDDsDDDDHHhDDDDDDDDkDuDaDmDeDDD
          /D CCCCCCCCCCCC
          /L fullpathfile
```

Figure 157. Format for Sample DCAFDOS.BAT File

You do not need to specify the parameters in any specific order, nor do you need to specify them all. If you do not specify a parameter, the default values for that parameter will be used. It is necessary to use the correct number of digits for the numeric fields by padding the field to the left with leading zeroes. The length of the parameters on the command line must not be greater than 128.

The parameters that are used by the DCAF in the DCAFDOS.BAT file are summarized in the following tables.

Table 34. Personalization and Command-Line Parameters for DOS

Parameter	Description
/D	The 1-12 character name of the LAN directory to be used by the DCAF DOS target component. The default name is DCAFLAN. This parameter is case sensitive.
/L	The 1-56 character fully qualified drive, path, and file name of the message log file for the DOS target component. For the DOS target workstation, the default is C:\DCAF13\EQNDDERR.LOG.
/R	Unload the target for DOS component from the workstation. This is a command-line option and is used in the following manner: EQNDD /R.
/O	The combination of 33 decimal numbers, hexadecimal numbers, and characters that define the DOS target workstation personalization options. **′d′ screen buffer size:** Four decimal digits specify the size of the display in total number of bytes (characters and attributes) that will be displayed on the controller screen. This number equals the number of rows multiplied by columns multiplied by two (to include the attributes) to obtain the total number of bytes for the display. For example, a display mode of 25 rows by 80 columns would be 4000 characters. The default is 4000. **′s′ status indicator:** Four decimal digits specify the position of the session status indicator. The first two decimal digits specify the row number (00-50). The default is 01. If you prefer not to display the status indicator, set the row number to 00. To keep the status indicator from scrolling up the screen, configure the status indicator to row 01. The next three decimal digits specify the column number (01-63). The default is 63. Two hexadecimal digits specify the attributes. (See Table 35 for the list of attributes.) The default,′3F,′ means that the background for the indicator is cyan, and the foreground text is white. **′h′ hot keys:** Eight decimal digits specify the two keys that must be pressed simultaneously to activate the DOS target user interface panel. The first two digits specify the first key. The default is 07, the left shift key. The next two digits specify the second key. The default is 08, the right shift key. The next four digits specify the amount of time that the user must press the keys. The default is 0250 milliseconds. A table that follows shows the list of key codes.

/O	**'k' keyboard processing:** One decimal digit specifies the type of keyboard processing. (0=software decision, 1=keyboard chip stuffing technique, and 2=BIOS keyboard write services (INT 16H)). The default is 0.
	'u' LAN adapter addressing: One decimal digit specifies the kind of LAN-administered addressing to be used; Locally Administered Address or Universally Administered Address, (0=LAA, 1=UAA). The default is 0, LAA.
	'a' LAN adapter number One decimal digit specifies the LAN adapter number to be used (0 or 1). The default is 0.
	'm' monitor mode start: One decimal digit specifies whether to start the session in active state (0) or monitoring state (1). The default is 0, active state.
	'e' security options: (0=disable, 1=enable). The default is 111 for the three choices of the security option. The first decimal digit specifies whether the target workstation operator can use the hot key to change the session state. The second decimal digit specifies whether the target workstation user is allowed to terminate a session. The third decimal digit specifies whether the target workstation user can shut down (unload from memory) the DOS target component.

Table 35. Status Indicator Attributes

Hexadecimal Value	**Background Color**	**Foreground Color**
78	White	Black
0F	Black	White
7B	White	Cyan
3F	Cyan	White

Table 36. Key Codes for the Hot Key Combination

Code	**Key**
03	Left Alt key
04	Left Control key
07	Left Shift key
08	Right Shift key

10	Caps lock key
11	Num lock key
12	Scroll lock key
14	System Request key
15	Right Alt key
16	Right Control key

APPENDIX1.4.2 Specifying NetBIOS Resources

For DOS target workstations, the parameters for names, sessions, and commands are specified following the LAN Support Program module, DXMT0MOD.SYS, in the CONFIG.SYS file. Following the LAN Support Program entry, DXMT0MOD.SYS, define the maximum number of sessions, commands, and names. You must add the minimum values for DCAF to the values that you already have for your NetBIOS environment. The following are the minimum values for the DCAF:

- Maximum number of sessions=1
- Commands=15
- Names=2

APPENDIX1.4.3 Using Terminate and Stay Resident Programs with the DCAF

Some Terminate and Stay Resident (TSR) utilities work only when loaded before the DOS target, and some work only when loaded after the component. If the DOS target does not work or the TSR utility does not work, try switching the order in which they are loaded. Also, the order in which the TSR programs are loaded will affect whether the DOS target can be unloaded (removed from memory). Normally, the last TSR to be loaded should be the first to be unloaded. This should ensure that the interrupt vectors are returned to the correct state as the TSR programs are terminated.

For example, if the DOS target is loaded before the DOSSHELL program is loaded, then the DOS target can only be unloaded (removed from memory) after the DOSSHELL is unloaded from memory. If the DOS target is loaded after the DOSSHELL is loaded, then it must be loaded from the DOSSHELL command line instead of being loaded from within the DOSSHELL. Because the DOS target is a TSR program, it must be unloaded before the user can return to the DOSSHELL. To ensure that the session with the controller is closed correctly, it is recommended that the DOS target be unloaded from memory by using the user-interface panel or the command EQNDD /R, instead of allowing the DOSSHELL to terminate and unload the component.

Although the DOS target is designed to be application independent, there may be situations where the DOS target and other DOS applications conflict in the use of system resources. For an example concerning keystroke handling, see ″DOS Target Keyboard Processing″ in topic APPENDIX1.4.4. If a DOS application takes a long time during the interrupt 8 intervals (the interval timer), then the DOS target may not be able to send a complete refresh of the display to the controller. The Personal Communications/3270 emulation program is an example of this type of DOS application, and this particular program is not supported by the DCAF.

APPENDIX1.4.4 DOS Target Keyboard Processing

Sometimes the DOS target cannot function properly when there is a conflict of resources with an application that writes directly to the 8042 keyboard chip. The Personal Communications/3270 emulation program is an example of this type of DOS application, and the DCAF does not support this program.

If keystroke errors occur when the DOS target is running and another application is also running on the DOS target workstation, then select a different type of keyboard processing for the DOS target component and try again. Selecting a different type of keyboard processing requires creating a new DOS target installation package and choosing a different keyboard processing option during personalization. If the problem continues, then the application running on the DOS target workstation may have a conflict of resources like the one described for the Personal Communications/3270 emulation program.

APPENDIX1.4.5 Changing the Keyboard Layout

If the DOS target user wants to change the keyboard layout with the KEYB command, then the KEYB command must be started before the DCAF in the chain of TSR programs. For convenience, add the command to the AUTOEXEC.BAT file.

It is important to make any keyboard changes before a session has been established by the controller with the DOS target workstation. If you change the keyboard layout after a session has been established, then the controller does not know that the keyboard layout has changed and will not map the keyboard-layout change.

When the controller first initiates a session with the DOS target workstation, the DOS target workstation gives the controller the keyboard layout code (the country code), but not the subtype code (the subcountry code). The controller uses a default subcountry code. If the default subcountry code matches the DOS target workstation's subcountry code, then the keyboard layouts will match precisely. If the subcountry codes do not match, then there will be a few discrepancies in the keyboard layouts.

APPENDIX1.4.6 Code-Page Changes while Using the DCAF

Sometimes starting a new application on the DOS target workstation can cause the code-page to change. During a session between a controller and a DOS target workstation, the code-page change notification cannot be sent to the controller when the DOS target workstation is in TSR mode.

To send the code-page change notification to the controller, the DOS target user must put the DOS target in the foreground. You can put the DOS target in the foreground by pressing the hot key combination and bringing up the DOS user interface panel. With the next display update to the controller, the code page change notification is sent.

APPENDIX1.5 Appendix E. Windows Target Technical Information

The technical information for the Windows target is divided into two parts: one for when the target operates in the Windows graphic environment and another for when it operates in the DOS full-screen environment. This appendix provides technical information about manual personalization and deinstallation of the Windows target. For technical information for the target workstation when it is operating in the native DOS environment (that is, outside of Windows), see Appendix D, ″DOS Target Technical Information″ in topic APPENDIX1.4.

APPENDIX1.5.1 Manual Personalization

You can personalize the Windows target in two ways:

- From the DCAF Target Personalization window

  For details, see ″In the Windows Environment″ in topic 2.8.2.1.

- In the DCAF.INI file

  When, during personalization in the Windows environment, you define an option other than the default value, the DCAF program creates a DCAF.INI file and lists any personalization options that you have defined. To personalize the target by hand, you can edit the DCAF.INI file.

To personalize the target by editing the DCAF.INI file, do the following:

1. At the DOS prompt, type the name of the directory where Windows is installed.

2. Open the DCAF.INI file to edit it. Each personalization parameter is defined by a keyword and the value you want to assign. In the DCAF.INI file, you will see definitions only for personalization parameters other than the default values.

   The following text is an example of the DCAF.INI file with keywords for all the DCAF personalization parameters and sample values. In your DCAF.INI, you will find keywords with definitions only for the parameters that you personalize. The label **[DCAF]** must be at the top of the file.

   ```
   [DCAF]
   StartActive=1
   CanTerminate=1
   Adapter=0
   LanDirectory=622LAN
   CommPortNum=2
   BaudRate=9600
   LogFileName=MESSAGE.LOG
   EnableHotKey=1
   HotKeyAsciiCode=Q
   HotKeyScanCode=16
   DOSHotKey1=0
   DOSHotKey2=2
   ```

```
HotKeyPressedTime=251
Unload=0
ScreenSize=3440
RowStatus=2
ColStatus=62
ColorStatus=123
Chip8042Info=2
```

3. After you finish editing the file, save and close it. See Table 6 in topic 2.8 for details on when the personalization changes will take effect.

When you personalize the Windows target manually, remember that:

- Only those parameters for which you assign a definition other than the default will be in the DCAF.INI file.
- If you delete a statement from the DCAF.INI file, the DCAF Windows target runs with the default value of the parameter that you delete.
- Manual personalization is especially convenient if you are working in the DOS full-screen environment and want to personalize the target.

APPENDIX1.5.2 Manual Deinstallation

To deinstall the DCAF Windows target from the workstation, you must undo the changes that were made in the Windows system files when you installed the DCAF. To make the changes by copying the backup system files that were created during installation, see "Deinstalling the Windows Target" in topic 2.3.4. The system files are WIN.INI, PROGMAN.INI, SYSTEM.INI in the Windows directory and AUTOEXEC.BAT in the root directory.

To deinstall the Windows target manually, do the following:

1. If you are working in Windows, exit from your Windows session by choosing Exit Windows from the File menu.

   A confirmation dialog box appears, prompting you to confirm that you want to end your Windows session.

2. Choose the **OK** button. The native DOS full-screen window appears.

3. At the DOS prompt, type

   del DCAF13 and press **Enter**, where DCAF13 is the directory where the DCAF program is installed on your workstation.

4. At the DOS prompt, change to the directory where Windows is installed on your workstation, by typing **cd** directory and pressing **Enter**.

5. Edit the WIN.INI file and delete the following statements:

   ```
   [DCAF]
   Version=1.31
   InstPath=c:\DCAF13
   ```

   Then delete c:\DCAF13\EQNWLOAD.EXE, from the following statement:

   ```
   Load=c:\DCAF13\EQNWLOAD.EXE
   ```

   Save and close the WIN.INI file.

6. In the SYSTEM.INI file, change the following statements:

From:

```
Mouse.drv=EQNMOUSE.DRV      (or EQNMOUS_.DRV)
Comm.drv=EQNCOMM.DRV        (or EQN_COMM.DRV)
   .
   .
   .
[386Enh]
Device=VDCFD.386            (or VDCF_.386)
Keyboard=EQNVKB31.386       (or EQNVK_31.386)
```

To:

```
Mouse.drv=MOUSE.DRV         (or filename of your mouse driver)
Comm.drv=COMM.DRV           (or filename of your communications driver)
   .
   .
   .
[386Enh]
Keyboard=*VKD
```

Save and close the SYSTEM.INI file.

7. In the PROGMAN.INI file, delete the following statements:

```
[Groups]
Group c:\WINDOWS\DCAF.GRP
```

Delete [Groups] only if DCAF is the only group listed.

Save and close the PROGMAN.INI file.

8. At the DOS prompt, type **del DCAF.INI** and press **Enter**.

9. In the AUTOEXEC.BAT file, delete c:\DCAF13, where c:\DCAF13 is the path where the DCAF program is installed on your workstation, from the following statement:

```
Path=c:\DCAF13
```

Save and close the AUTOEXEC.BAT file.

The next time you open Windows, you will not see the DCAF group and target icon included in the Program Manager.

10. At the DOS prompt, change to the Windows system subdirectory, by typing **cd system** and pressing **Enter**.

11. At the DOS prompt, type: **del eqn*.*** and press **Enter**.

12. Then type: **del vdcf*.386** and press **Enter**.

You have completed deinstallation.

APPENDIX1.6 Appendix F. Common Modem Device Initialization Strings

This appendix provides a collection of the most common modem device initialization strings for DCAF.

APPENDIX1.6.1 Initialization String Commands for DCAF

Because the initialization string that a modem uses to work with DCAF is unique for each model, only a general explanation of the meanings of each command in the string follows. Use trial and error to find the string that is right for your modem. The following provides each command in the string and an explanation of what it means.

Command	Description
&F	Resets to the factory default modem settings.
&C1	Carrier Detect Signal.
&D2	Data Set Ready signal. When the DTR goes off, the modem enters the command state.
&S0=0	Modem answers on the first ring.
&S7=60	Modem waits 60 seconds for a carrier.
&K0	Disables any kind of hardware- or software-flow control.
&Q0	Sets the communication mode to asynchronous.
&N<u>xx</u>	Where <u>xx</u> is a number. Sets the phone link rate for baud rates of 19200 bps. This command is not always available.
%C<u>xx</u>	Where <u>xx</u> is a number. Disables V.42bis and/or MNP** level 5 compression.

APPENDIX1.6.2 Common Modem Device Initialization Strings

The following section includes the initialization strings for some common modems.

For Settings Over 19200 bps: If you are using Communications Manager and a modem speed that is faster than 19200 bps, ensure that ASYNCDDC.SYS is defined in the Device statement of your CONFIG.SYS.

DCAF supports the following initialization strings for modems. Models are listed alphabetically.

Note: Depending on the type of terminal you are using, certain characters may not appear correctly online. Refer to the printed book for exact modem settings.

Table 37. Settings for Commonly Used Modems

Model	Modem Setting	Suggested DCAF Setting
ATI** 9600 ETC-E	AT&F&C1&D2S0=0S7=60&K0&Q0|	9600
Digicom 9624LE	AT&F&C1&D2&M0*E0*F0*H0*N3S0=1S7=60| AT&F&C1&D2&M0*E9*F3*H0*N6S0=1S7=60|	9600 19200
Digicom Eagle	AT&FS7=60&C1&D2S0=0*F0*Q2E0|	9600
Elsa 2440-TR	ATZ|AT\Q3\N0|	9600
Hayes** Accura 144 + FAX 144	AT&FS7=60&C1&D2S0=0&Q0&K0| AT&FS7=60&C1&D2S0=0&Q9&K3|	9600 19200
Hayes Optima 288 V.FC	AT&FN5S7=60S11=55S37=12&C1&D2S0=1&Q5&K1B81|	19200
Hayes Smartmodem Optima 9600	AT&FS7=60&C1&D2S0=0&Q0&T5&K0| AT&FS7=60&C1&D2S0=0&Q5&T5&K3|	9600 19200
Hayes Smartmodem Optima 14400	AT&FS7=60S11=55&C1&D2S0=0&Q5&K3|	19200
Hayes V_SERIES	AT&FS7=60&C1&D2S0=0&Q0&T5&K0| AT&FS7=60&C1&D2S0=0&Q5&T5&K3|	9600 19200
IBM 7851	AT&F˜˜˜E1V1X4&C1&D2%E1&K0	9600
IBM 7855	AT&FS7=60&C1&D2S0=0&Q0\Q0\R0| AT&F0&C1S0=0\Q2\N3&AP8\M14&I1\A3%C0|	9600 19200
IBM PS/2 Internal 14.4 DATA/FAX	AT&F&C1&D2S0=0&K0&Q0|	9600
Intel** Faxmodem 14.4	AT&F&C1&D2S0=0S7=60\N\Q%C"H| AT&F&C1&D2S0=0S7=60\N3\Q3"H3|	9600 19200

<table>
<tr><td>Intel SatisFAXtion** 400e</td><td>AT&F&C1&D2S7=60S0=0&T5\G0\N0\Q0%E1|</td><td>9600</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Motorola** UDS FastTalk** II</td><td>AT&FS7=60&C1&D2S0=1&M0%C\C0\G0\J1\N1\Q0\X0|</td><td>9600</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Motorola UDS FasTalk V.32/42b</td><td>AT&FS7=60&C1&D2&M%C%E\C\G\J1\M\N1\Q\X|</td><td>9600</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Practical Peripherals PM14400FXMT</td><td>AT&FS7=60&C1&D0S0=0N1&K0&Q0&B0|</td><td>9600</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Presticon 9600</td><td>AT&FE1V1X4S7=60&C1&D2S0=0\N6&S1\Q3%T0|</td><td>9600</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Prometheus Promodem 144E</td><td>AT&F&C1&D2&K0&M0\G0\N0%C0S0=1S7=60|
AT&F&C1&D2&K3&M0&Q5\N6S0=1S7=60|</td><td>9600
19200</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Siemens 9632-M</td><td>ATZ|AT*FL2|AT*SM1|</td><td>9600</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Telebit**</td><td>AT&F&C1&D2S58=0S7=60S68=0S69=0S180=0S190=0|</td><td>9600</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>ThinkPad* 700C high-speed datafax (internal)</td><td>AT&FS7=60&C1&D2S0=0Q5&T5&K3%C3|</td><td>19200</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>US Robotics 14400 Sportster</td><td>AT&F&C1&D2S0=0S7=60&H0&N6&K0&M0|
AT&FB0Q0X4&C1&D2&H1&K0&A3&N0&S1S0=1|</td><td>9600
19200</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>US-Robotics Courier High Speed•</td><td>ATZS7=60&C1&D2S0=0&H0&I0|
ATZS7=60&C1&D2S0=0&H1&I0&K3&M0|</td><td>9600
19200</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Zoom Faxmodem</td><td>AT&FE1Q0V1X4S7=60&C1&D2S0=0&T5|</td><td>9600</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Zyxel U-1496</td><td>AT&FS7=60&C1&D2S0=0&M0&H0|
AT&FS7=60&C1&D2S0=0&M0&N36&H3|</td><td>9600
19200</td></tr>
</table>

•Use the following switch setting:

1.Off	2.Off	3.On	4.Off

5.Off	6.Off	7.Off	8.On
9.Off	10.Off		

GLOSSARY Glossary of Terms and Abbreviations

This glossary defines important DCAF terms and abbreviations. It includes information from the IBM Dictionary of Computing, New York: McGraw-Hill, 1994. Definitions from the American National Dictionary for Information Processing are identified by an asterisk (*). Definitions from draft proposals and working papers under development by the International Standards Organization, Technical Committee 97, Subcommittee 1 are identified by the symbol **(TC97)**. Definitions from the CCITT Sixth Plenary Assembly Orange Book, Terms and Definitions and working documents published by the Consultative Committee on International Telegraph and Telephone of the International Telecommunication Union, Geneva, 1980 are preceded by the symbol **(CCITT/ITU)**. Definitions from published sections of the ISO Vocabulary of Data Processing, developed by the International Standards Organization, Technical Committee 97, Subcommittee 1 and from published sections of the ISO Vocabulary of Office Machines, developed by subcommittees of ISO Technical Committee 95, are preceded by the symbol **(ISO)**.

For abbreviations, the definition usually consists only of the words represented by the letters; for complete definitions, see the entries for the words.

Reference Words Used in the Entries

The following reference words are used in this glossary:

Contrast with. Refers to a term that has an opposed or substantively different meaning.

See. Refers to multiple-word terms that have the same last word.

See also. Refers to related terms that have similar (but not synonymous) meanings.

A

ACDI. Asynchronous Communications Device Interface.

active. In the DCAF program, the session state in which the controller has control of the target workstation. The target workstation keyboard is locked. That is, any keystrokes or mouse commands entered by the target workstation user will not be processed by applications running on the target workstation.

administrator. See security administrator.

Advanced Peer-to-Peer Networking (APPN). An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

advanced program-to-program communications (APPC).. An implementation of the SNA/SDLC LU 6.2 protocol that allows interconnected systems to communicate and share the processing of programs.

APPC. Advanced program-to-program communications.

application. A collection of software components that is used to perform specific types of work on a computer. For example, the DCAF program is a software application that is used to provide remote console services.

APPN. Advanced Peer-to-Peer Networking.

Asynchronous Communications Device Interface (ACDI). The programming interface that provides support for those who want to use the serial ports for asynchronous communications in a multitasking environment. ACDI interacts with the serial ports through the base operating system and ensures that interrupts are handled and data is buffered for applications as required.

authentication. (1) A process that is used to verify the integrity of transmitted data, especially a message. (2) In computer security, a process that is used to verify the user of an information system or protected resources. (3) A process that checks the integrity of an entity. (4) See also password.

authenticator. See security authenticator.

autostart. Some of the components of the DCAF can be configured to start up with little or no operator involvement. For example, the component might automatically initiate when the Communications Manager is started or when the AUTOEXEC.BAT file calls the program.

autotask. An unattended-operator-station task that does not require a workstation user. For example, the DCAF target workstation does not require an operator. The target workstation can be configured so that the DCAF is automatically enabled and the controller component establishes the session. Autotasks are typically used for automated console operations.

B

backbone. (1) In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges. A backbone may be configured as a bus or as a ring. (2) In a wide area network, a high-speed link to which nodes or data switching exchanges are connected. (3) In the DCAF, the SNA backbone connects the OS/2 controller workstation with the OS/2 target or DCAF gateway workstations by means of an LU 6.2.

backtab. To move the cursor to the beginning of the previous entry field or the previous selection field. Contrast with Tab.

backup copy. A copy of information or data that is kept in case the original is changed or destroyed.

busy. The DCAF session state when the target workstation user is changing session states, and the controller user must wait before attempting to change the session state.

button. (1) A mechanism on a pointing device, such as a mouse, that is used to request or initiate an action. See mouse button. (2) A graphical device that identifies a choice. See radio button and push button. (3) A graphical mechanism in a window that, when selected, results in an action. For example, a list button produces a list of choices. See list button, maximize button, minimize button, and restore button.

C

CCA. Common cryptographic architecture. Services supplied by either the IBM 4755 Cryptographic Adapter card or by the DCAF product's software implementation.

Cancel. An action that removes the active pop-up window without performing any changes and returns the user to the window that preceded it. See also Close. Contrast with Exit.

choice. Any item that a user can select.

click. To press and release a mouse button without moving the pointer off the choice. See double-click. See also drag select.

Close. A choice that removes a window and all its associated windows from the screen.

command. A request for system action.

command area. The area on the panel that contains the command entry field. See also command entry field.

command entry field. An entry field in which a user types commands. See also command area.

component. In the DCAF program, it is a specialized part of the program that can function independently of the other components. For example, a workstation operating on DOS may have only the target for DOS component installed. The DCAF components include the controller, OS/2 target, DOS target, DCAF gateway, LAN directory, Security Administrator, Security Authenticator, and the Packager.

configuration. (1) (TC97) The arrangement of a computer system or network as defined by the nature, number, and the chief characteristics of its functional units. The term may refer to a hardware or a software configuration. (2) The devices and programs that make up a system, subsystem, or network. (3) In the DCAF program, the arrangement of components and workstations in the network. Also, the collective set of item definitions that describe such a configuration. (4) See system configuration.

configuration file. (1) In Communications Manager, a file that describes the devices, optional features, communications parameters, and programs installed on a workstation. (2) For the base operating system, the

CONFIG.SYS file that describes the devices, system parameters, and resource options of a workstation.

connection type. When personalizing the asynchronous communications parameters for an OS/2 target, the connection type is represented by a number from 0 to 4. The default, type 3, is for automatic data answering.

controller. In the DCAF, the workstation that can monitor or take over and operate the keyboard and display of another workstation. Contrast with target workstation.

CP name. A network-qualified name of a control point (CP), consisting of a network ID qualifier identifying the network (or name space) to which the CP's node belongs, and a unique name within the scope of that network ID identifying the CP. Each APPN or LEN node has one CP name assigned to it at system-definition time.

D

DCAF. Distributed Console Access Facility.

DCAF gateway workstation. For the DCAF, a LAN-attached workstation that provides communication functions between a controller and a target workstation on a LAN. See also gateway and LAN gateway.

Disk Operating System (DOS). Software for the PC that controls the execution of programs. Its full name is the IBM Personal Computer Disk Operating System.

display. (1) To present information for viewing, usually on a terminal screen or a hardcopy device. (2) A device or medium on which information is presented, such as a terminal screen.

Distributed Console Access Facility (DCAF). (1) This program product provides a remote console function that allows a user at one programmable workstation to remotely control the keyboard input and monitor the display output of another programmable workstation. The DCAF program does not affect the application programs that are running on the workstation that is being controlled. (2) An icon that represents the Distributed Console Access Facility.

DOS. Disk Operating System.

double-click. To press and release a button on a pointing device twice within the time limit the user has defined for the operating environment, without moving the pointer off the choice. See click. See also drag select.

drag select. To press a mouse button and hold it down while moving the pointer so that the pointer travels to a different location on the screen. Dragging ends when the mouse button is released. All items between the button-down and button-up points are selected. See also click and double-click.

E

Enter. An action that submits information to the computer for processing. Enter tells the computer to perform actions on whatever has been selected.

enter. To submit all selected choices and entry-field information to the computer for processing; for example, to type information on a keyboard and press the Enter key.

entry. An input operation on a workstation.

entry field. An area in which a user types information. Its boundaries are usually indicated. See also selection field.

Exit. An action that ends the active application and removes, from the screen, all windows associated with the application.

F

field. An identifiable area on a screen. See entry field, command entry field, and selection field.

G

gateway. A functional unit that connects two computer networks of different network architectures.

Note: A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures.

See also DCAF gateway workstation and LAN gateway.

gateway workstation. See DCAF gateway workstation.

H

Help. A push button that provides information about the item the cursor is on or about the entire window.

help window. A window that contains information to assist a user.

hot key combination. A combination of two keys that, when pressed simultaneously for a period of time, can be used to cause a specific action. At the DCAF target workstation, the hot key combination can be used to manipulate the session status. During the installation or packaging of the target component, the hot key can be enabled or disabled and the key combination can be defined. At the controller, the hot key can be used to manipulate the keystroke mode. See also keystrokes local and keystrokes remote.

I

icon. A graphical representation of an object, consisting of an image, image background, and a label.

initiate. (1) In SNA, a request sent from a logical unit (LU) to a system services control point (SSCP) requesting that an LU-LU session be established. (2) In the DCAF, a target workstation's request to start a session. The target workstation must send a request to initiate a session to the controller before a session can be established. A target workstation can be initiated by the target workstation user or by an autostart command.

installation. The procedure of personalizing and copying the components of the DCAF product onto the workstations where they will be processed.

K

KEK. The DCAF key-encrypting key encrypts and decrypts all keys that are distributed in the network for the DCAF when this key is configured for secure DCAF sessions.

keystrokes local. A DCAF keystroke mode that occurs on the controller workstation when the keystrokes and mouse commands will be processed at the controller workstation. Contrast with keystrokes remote.

keystrokes remote. A DCAF keystroke mode that occurs on the controller workstation when the keystrokes and mouse commands will be transmitted to the target workstation and processed at the target workstation. Contrast with keystrokes local.

L

LAA. Locally administered address.

LAN. Local Area Network.

LAN directory. This DCAF component supplies the controller component with the names of the enabled DCAF target workstations, on the NetBIOS LAN, that are registered with the name of this LAN directory. Each NetBIOS LAN with DCAF has a specific DCAF LAN directory name. The name of the LAN directory is used by the DCAF components to make the logical connection between the DCAF components on the LAN.

LAN directory nickname list. For the DCAF, this file contains the list of user-defined nicknames and the associated UAA or LAA for the target workstations on the LAN. See LAN Target Directory.

LAN gateway. A functional unit that connects a local area network with another network using different protocols. See also gateway and DCAF gateway workstation.

LAN target. A DCAF term that is used when referring to a DCAF target workstation that is on a NetBIOS LAN. See LAN Target Directory.

LAN Target Directory. A DCAF window that can be displayed on the controller after the user has chosen a DCAF gateway or LAN directory from the DCAF directory. The window displays the LAN adapter addresses or the descriptive names for the target workstations that are registered with the same LAN directory as the chosen DCAF gateway.

link. In SNA, the combination of the link connection and the link stations that join network nodes. A link connection is the physical medium of transmission. A link, however, is both logical and physical.

list button. A button, labeled with a underscored down arrow, that produces a list of valid choices that can be selected for that field. See button.

local area network (LAN). (1) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. See also token ring. (2) A network in which communications are limited to a moderately sized geographic area such as a single office building, warehouse, or campus, and which do not generally extend across public rights-of-way. Contrast with wide area network.

locally administered. A DCAF security authenticator workstation is locally administered when it is installed on the same workstation as the DCAF security administrator component. When locally administered, the security data files can be transferred (locally) from the DCAF security administrator to the DCAF security authenticator without the need for a secure session to transfer the files. Contrast with remotely administered.

locally administered address (LAA). In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with universally administered address.

local node name. In a network, name of a point, accessed directly without use of a telecommunication line, at which one or more functional units connect channels or data circuits. (I)

locked. The state of a workstation when the keystrokes and mouse commands entered by the workstation user are not processed by the applications running on the workstation. For example, during an active DCAF session, the target workstation keyboard is locked.

M

master key. The master key is used by the CCA services to encrypt and decrypt many data-encrypting keys and key-encrypting keys that are stored in a key data set.

maximize button. A button on the rightmost corner of the title bar of a window that has not been maximized that, when selected, enlarges the window to its largest possible size. See button. Contrast with minimize button. See also restore button.

menu. A list of choices that gives users access to actions that can be applied to an object.

menu bar. The area near the top of a window, below the title bar and above the rest of the window, that contains choices that provide access to other menus.

message. Information not requested by a user but displayed or logged by an application in response to an expected or unexpected event.

minimize button. A button, located next to the rightmost button in a title bar, that, when selected, reduces the window to its smallest possible size. See button. Contrast with maximize button. See also restore button.

mode name. The name used by the initiator of a session to designate the characteristics desired for the session, such as traffic pacing values, message-length limits, sync point and cryptography options, and the class of service within the transport network.

monitoring. In the DCAF program, the session state in which the controller workstation user sees everything on the target workstation display, but the target workstation user controls the keyboard and mouse.

mouse. A device that a user moves on a flat surface to position a pointer on the screen. It allows a user to select a choice or function to be performed or to perform operations on the screen, such as dragging or drawing lines from one position to another.

mouse button. A mechanism on a mouse that a user presses to select choices or initiate actions.

N

NetBIOS. Network Basic Input/Output System. An operating system interface for application programs used on IBM programmable workstations that are attached to the IBM Token-Ring Network.

network. An arrangement of nodes and connecting branches.

network address. (1) An identifier for a node, station, or unit of equipment in a network. (2) In a subarea network, an address, consisting of subarea and element fields, that identifies a link, link station, physical unit, logical unit, or system services control point. Subarea nodes use network addresses; peripheral nodes use local addresses or local-form session identifiers (LFSIDs). The boundary function in the subarea node to which a peripheral node is attached transforms local addresses or LFSIDs to network addresses and vice versa.

node address. In a network, the unique code assigned to the point at which one or more functional units connect channels or data circuits. (I)

O

online. Stored in a computer and accessible from a workstation.

operator. A person who operates a machine. Contrast with autotask.

OS/2. An operating system that runs on a personal computer with an 80286 processor or larger (for example, an IBM Personal System/2 model 80).

P

packager. A DCAF component that creates installation packages from of the other DCAF components. These packages can later be installed on workstations. The components can be personalized during the creation of the package. The security authenticator and administrator components cannot be packaged.

panel. A particular arrangement of information that is presented in a window or pop-up. If some of the information is not visible because of the size of the panel, a user can scroll to see the information.

pass phrase. For a secure DCAF environment, each controller user has a pass phrase of 4 to 80 characters. The pass phrase may contain uppercase and lowercase letters, the digits 0 to 9, and the special characters #, @, $, and blanks.

password. A unique string of characters known to a computer system and to a user, who must specify the character string to gain access to a system and to the information stored within it.

password-only session. In the DCAF environment, a password-only session requires the controller user to type the correct password for the target or DCAF gateway workstation before a session is established. A nonsecure session is established when the user presses Enter without typing a password. Both these sessions do not require authentication. Contrast with secure session. See session.

personalization. Many of the features of the DCAF components are options that can be customized. During installation, the options for the DCAF components can be selected. Some of the options may be selected or changed, or both, after installation.

port number. In TCP/IP, a 16-bit number used to communicate between TCP and a higher-level protocol or application. Some protocols, such as the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP), use the same port number in all TCP/IP implementations.

PROGMAN.INI file. The Program Manager initialization file for Windows. See Program Manager.

programmable workstation. A workstation that has some degree of processing capability and that allows a user to change its functions.

Program Manager. An application that is central to the Windows operating system. It starts whenever you start Windows and continues to run as long as you are working with Windows. You can use Program Manager to start other applications and organize applications and files into groups that make sense to you. It is the default shell for Windows.

prompt. A symbol or action that requests an entry or selection from the user.

protocol. (1) (TC97) The set of semantic and syntactic rules governing the operation of functional units of a communication system that must be followed if communication is to be achieved. (2) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. (3) The DCAF program can use NetBIOS, SNA, and switched asynchronous protocols.

pull-down menu. A list of choices extending from a selected menu-bar choice that gives access to actions.

push button. A rectangle with text inside. Push buttons are used in windows for actions that occur immediately when the push button is selected.

R

radio button. A circle with text beside it. Radio buttons are combined to show a user a fixed set of choices from which only one can be selected. The circle is partially filled when a choice is selected.

Refresh. An action that updates the information that is being displayed.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunications line. (2) In Advanced Program-to-Program Communications (APPC), indicates that the partner logical unit (PLU) or transaction program is not at the local node.

remote console function. The function that allows one workstation to control another.

remotely administered. A DCAF security authenticator workstation is remotely administered when it is not installed on the same workstation as the DCAF security administrator component. When remotely administered, the security data files must be transferred via a secure DCAF session. It is necessary that a secure OS/2 target component be installed on the security authenticator workstation. Contrast with locally administered.

restore button. A button that appears in the rightmost corner of the title bar after a window has been maximized. When the restore button is selected, the window returns to the size it was before it was maximized. See button. See also maximize button and minimize button.

Restructured Extended Executor (REXX). A programming language. A REXX program can be used to call OS/2 or DOS commands.

REXX. Restructured Extended Executor.

S

screen. The physical surface of a display device upon which information is shown to a user. Contrast with panel.

scroll. To move a display image vertically or horizontally to view data that is not otherwise visible in a display screen or window.

search. The process of looking for a particular item.

secure session. In the DCAF environment, a secure session is a DCAF session that has been authenticated by the DCAF security authenticator. Contrast with password-only session. See session.

security administrator. The DCAF security administrator component centralizes the maintenance of the databases for the controller users, the target access tables, the secure target workstation information, and the security authenticators. This component updates the file EQNADMN.LOG with error and informational messages for the security file transfers.

security authenticator. The DCAF security authenticator verifies and authorizes the secure DCAF sessions between the controller and target components. The file EQNAUTH.LOG is used to log error and informational messages such as authentication requests. See also locally administered and remotely administered.

select. The process of explicitly identifying one or more objects to which a subsequent action will apply.

selection field. A set of related choices. See also entry field.

Send. (1) A choice in the Keystrokes pull-down menu that a user can select to send certain command key sequences to a target workstation. (2) A push button on the DCAF-File Transfer Utility window that causes a file to be sent to a target workstation.

server. On a local area network, a data station that provides facilities to other data stations; for example, a file server, a print server, a mail server, or an authentication server.

session. In the DCAF, the period of communications activity between DCAF components. See password-only session, secure session, and session state.

session state. The status of the DCAF session. The session state can be active, monitoring, busy, or suspended. Whether the controller or target workstations can change the session state depends on their configuration.

shortcut key. A key or combination of keys that a user can press to perform an action that is available from a menu; for example Alt+F4 = Close.

SNA. Systems Network Architecture.

SNA network. The part of a user-application network that conforms to the formats and protocols of Systems Network Architecture. It enables reliable transfer of data among end users and provides protocols for controller the resources of various network configurations.

status. The measure of the condition of a session. See session state.

suspended. In the DCAF program, the session state in which the controller does not control or monitor the target workstation. The controller does not receive display updates from the target, or in any way control the target workstation. Either the controller or the target workstation user can resume the session.

system configuration. A process that specifies the devices and programs that form a particular data processing system.

Systems Network Architecture. The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controller the configuration and operation of, networks.

Note: The layered structure of SNA allows the ultimate origins and destinations of information, that is, the end users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

tab. A typing action that moves the cursor to the beginning of the next entry field or the next selection field if no choice is selected. If the next selection field contains a selected choice, the cursor moves to that choice. Contrast with backtab.

target workstation. In the DCAF, the workstation whose keyboard and display will be monitored or taken over by the controller. Contrast with controller.

TCP. Transmission Control Protocol.

TCP/IP. Transmission Control Protocol/Internet Protocol. A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

title bar. The area at the top of each window that contains the window title and system-menu icon. When appropriate, it also contains the minimize, maximize, and restore icons.

token ring. A network with a ring topology that passes tokens from one attaching device to another. For example, the IBM Token-Ring Network.

U

UAA. Universally administered address.

universally administered address (UAA). In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique. Contrast with locally administered address.

unlocked. The state of a workstation when the keystrokes and mouse commands entered by the workstation user are processed by the applications running on the workstation. For example, when the DCAF session is in the monitoring state, the target workstation is unlocked.

user. Anyone who requires the services of a computing system.

user interface. The actions or items that allow a user to interact with and perform operations on a computer.

Using help. A help choice that gives a user information about how the help function works.

W

wide area network. A network that provides data communication capability in geographic areas larger than those serviced by local area networks. Wide area networks may extend across public rights-of-way. Contrast with local area network.

window. An area of the screen with visible boundaries within which information is displayed. A window can be smaller than or the same size as the screen. Windows can appear to overlap on the screen.

workstation. A programmable or nonprogrammable device that allows a user to do work. A workstation allows a user to transmit or receive information from a computer.

workstation definition. The description or profile of a workstation as defined in the DCAF directory on controllers. The definitions provide general and protocol descriptions of any workstation to which the controllers connect.

Index

Numerics

A

B

C

E

F

G

K

M

N

R

S

T

V

W

BACK_1 Communicating Your Comments to IBM

Distributed Console Access Facility
Installation and Configuration Guide
Version 1.31

Publication No. SH19-4068-01

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you prefer to send comments by mail, use the reader's comment form (RCF) at the back of this book. If you wish, you can give the RCF to the local branch office or IBM representative for postage-paid mailing.

If you prefer to send comments by FAX, use this number, which is in Italy:

39+6+596+62845

If you prefer to send comments electronically, use this network ID:

ROMERCF at VNET.IBM.COM

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies

COMMENTS Help us help you!

Distributed Console Access Facility
Installation and Configuration Guide
Version 1.31

Publication No. SH19-4068-01

We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	_	_

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	_	_
Complete	_	_
Easy to find	_	_
Easy to understand	_	_
Well organized	_	_
Applicable to your task	_	_

Specific Comments or Problems:

____

____

____

____

____

Please tell us how we can improve this book:

____

____

____

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

Please complete this form and mail it to:

DCAF End User Technologies
Rome Networking Software Laboratory
IBM SEMEA S.p.A.
P.le G. Pastore, 6
00144 Rome
Italy

or give it to your IBM representative.

Name . . . . ____
Company or Organization ____
Address . . . . ____
____
____
Phone No. . . . . ____

DSMBEG323I STARTING PASS 2 OF 2.
DSMPGL708E TEXT EXCEEDS RIGHT PAGE BOUNDARY ON PAGE 80.
DSMPGL708E TEXT EXCEEDS RIGHT PAGE BOUNDARY ON PAGE 81.