FCC ID: OC8SA108

First Access Enterprise

Reference Manual

About this Manual

The Reference Manual is intended for the system administrator, as a guide for implementing the First Access security solution. It assumes a working knowledge of Windows NT Server and Workstation.

Chapter 1 introduces the **First Access System**. It puts the role of First Access Enterprise into perspective by providing a background sketch of enterprise security and the role played by the end-user in the security of any organization.

A brief overview of the **System Architecture** in **Chapter 2** is followed by a description of the installation procedure in **Chapter 3 - First Access Enterprise**. The procedure is preceded by a section on several considerations that are to be noted before starting the installation.

Chapter 4 describes how the First Access system has been integrated with the User Manager for Domains utility of Windows NT.

Chapter 5 provides a deployment guide in the form of a sample case study where the system administrator is guided through the fundamental steps needed to put the First Access system into operation.

An in-depth description of **Vicinity Authentication** is provided in **Chapter 6** followed by step-by-step instructions on how to configure a First Access user's authentication and authorization profile. End-user authentication is described in **Chapter 7**.

Typographic Conventions

Notes are written in *italics* and are used to draw attention to important points .

Tips remind the reader of points that are pertinent to the topic under discussion.

Bold italics This style is used to indicate items that appear on interfaces such as menu options.

Vicinity Authentication™ This style is used for trademarks of First Access Ltd.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

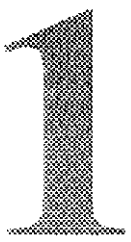
Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Table of Contents

Table of Contents

Table of Contents

CHAPTER



Introducing First Access

Enterprise Security

With the shift from massive mainframes to the more flexible client/server network technology, with today's world of internet connections, intranets and extranets, few, if any computing environments work in isolation anymore.

The Internet has revolutionized our lives in more ways than one. Not only has it brought new technologies into existence, it has changed the fundamental concept of networking and business Two key features of this new environment are 'communication' and 'mobility'. The phenomenal degree of mobility brings into prominence a wide array of threats to information technology from illegitimate users. Securing your product and proprietary information has become **the** vital concern of corporate environments.

Vendors have not been far behind to jump on the security bandwagon and supply companies with the ideal solution. Today there is a bewildering array of security products to counter every type of security threat imaginable.

There are authentication systems to assist in the all-important user identification and access control systems to control data access based on the identity of the user. Active content security servers/clients and anti-virus programs are employed to guard against external/internal software attacks. Cryptography protects the integrity of your data when in transit and firewalls restrict traffic between the LAN and other external networks.

Enterprise Security and the end user

It is fairly obvious that the cornerstone of any security policy must start with the identification of the legitimate users of the system. These users may be employees, system administrators, customers and the like. All of these users however do not have access to the same data and also differ in what they are allowed or should be allowed to do with the data. Thus the root of enterprise security is in controlling which user can view, modify and delete which data.

User identification or authentication is a critical component of the security policy of any organization. The impact that a simple user can have on the security of a system is only now beginning to be understood by IT managers and system administrators.

Recent studies show that most computer frauds originate from within the organization. Internal penetration and break-ins have contributed more than their fair share to leaks in proprietary information and financial losses.

Existing End User Authentication Technologies

A quick overview of the technologies currently being employed show that the end user authentication arena is still dominated by password-based authentication mechanisms. Two other technologies that are gaining ground are biometric and smart card based authentication techniques.

Passwords

The oldest method employed in end user authentication is the password. Today most commercial operating systems continue to use passwords as the means of authentication.

Passwords have however come a long way since their inception when they were entered in clear text, for all the world to see. Most systems employ strict password policies in terms of the length and type of characters that make up the password etc.

The inherent flaws of password based authentication are too well known to need illustration.

Biometrics

Biometrics identification is a technique of identifying a person by a physical characteristic. Not too long ago biometrics was applied for identification and securing access at top secret systems and highly secure facilities. The use of biometrics for network log-in authentication is a fairly new trend that has rapidly gained a market niche for itself.

Two factors come up for consideration: the cost and psychological aspect of employing such a solution for authentication. The cost of implementation depends directly on the level of security desired by the organization. The need for specialized hardware drives up the cost of what is even otherwise a fairly expensive solution, especially in widespread corporate networks.

Social acceptance has also not been forthcoming because it is intrusive and psychologically disturbing to many employees.

Smart Cards

Smart Cards appear to be the prevailing answer to successful end user authentication and are being deployed at many organizations.

Many network operating systems, especially Microsoft are shipped today with smart card enabled technology.

Smart cards are superior to their credit card counterparts whom they closely resemble in physical appearance. On the software side, smart cards are progammable; they have storage and processing capabilities. The built-in processor enhances software only solutions based on client authentication, logon support and secure e-mail. On the hardware side they are portable, relatively tamper proof and cost-effective.

Today's smart cards are contact smart cards. That is, the smart card can communicate with a computer only after it is passed through a smart card reader. The reader has to be connected to the computer.

Drawbacks of Existing Technologies

The most obvious feature of all these technologies is that they are all user-dependent, some more so than others. They are also time consuming and fairly complicated for the end user to follow on a day-to-day basis.

It is difficult to ensure user compliance when users have to log off every time they leave their computers, even for coffee-breaks. With contact smart cards for example, users have to pass the card through the reader to log off. The tendency to ignore this altogether notwithstanding, it is also possible that users will leave the cards within the reader, defeating the very purpose of the exercise.

The First Access Concept

First Access based its concept of internal user authentication on the premise that for the end user authentication process to be really secure, user intervention has to be kept to a bare minimum. First Access has introduced a new paradigm in the world of computer security - **Vicinity Authentication™**.

Vicinity Authentication™ negates the need for passwords, because the process by which the user's identity is established is based on Sensor/Card communication. It is completely automated and does not require any action on the part of the user. It is only after a positive identification that user action is required, probably in the form of a PIN, if so configured.

Minimum user intervention being required, chances of security breaches are correspondingly reduced. It is practical, because it involves no changes in the individual's work habits. The authentiaction process process takes only a few minutes. And perhaps most important is the fact that even after authentication, the user is logged off automatically when he/she walks away, precluding idle browsing and illegal data access.

The First Access Product

The First Access product has been designed specifically for the corporate environment. It is optimized to work in small to medium to densely populated PC/NC office environments.

The First Access product package, **First Access Enterprise™** aims at providing a complete solution for internal network authentication through the:

- **First Access Sensor™**
- **First Access Card™**
- **First Access Server™**
- **First Access Client™**

The **First Access Sensor™** and the **First Access Card™** comprise the hardware kit and are integral units of the product.

The **First Access Server™** manages the server-based elements of the software. The **First Access Server™** provides the interface to register First Access users and create their authentication profiles and generally manage First Access user security. The information on each registered First Access user is stored in the First Access database which also physically resides on the server.

The **First Access Client™** manages the client-based elements of the software. It is installed on the workstation of each client. Interactive logon, identification and authentication are performed through the Graphical and Identification interface on the client's workstation.

Features

Integration with Existing Authentication Systems

The First Access system uses industry standard authentication systems. As such it integrates completely with existing authentication systems like Kerberos and RADIUS.

System Scalability

System scalability as related to **First Access Enterprise™** refers to the fact that the solution can be deployed within any network organization, regardless of the size of the network.

The number of First Access protected workstations can be increased at any time by simply connecting additional sensors, distributing additional cards and installing the client elements of the software.

Flexibility

Installing the First Access security solution does not make it imperative that all network users have to be First Access users. You can decide who to include in the First Access user list by means of a simple mouse-click, by which you enable the **First Access Card™**.

Additionally, once you have defined First Access users, the system provides the option of accepting the default security settings (already configured) for a user or customizing the settings according to the security level of the user. You can set up the First Access system according to the level of security you require.

Ease of Use

The First Access solution is characterized by its ease of use, both for the network administrator who has to implement the security system, and on the other end of the scale, for the end user who has to conform to the policies.

For the administrator, centralized security management makes it easy to configure and maintain user authentication profiles. For the end user, since it does not require any change in the individual's work habits, it is easy to follow. Moreover, built-in automated features like **AutoDetect™** and **AutoLock™** ensure effortless user compliance.

CHAPTER

First Access-System Architecture

Overview

An understanding of the First Access system and how it works must begin with an overview of the system architecture and how the different parts work to make a smooth whole.

This chapter describes:

- Main features of the system design
- System components

Main Design Features

Client/server Architecture

A client/server architecture is mostly employed in a network environment where the client and server machines work together to accomplish the processing of the application being used.

First Access Enterprise also employs a client/server structure in its software to accomplish its goals. The **First Access Server™** software which is installed on a Windows NT server provides the capability for centralized administration of its security policy - in terms of implementation and user management. The **First Access Client™** , installed on client workstations is typically optimized for user interaction and provides the interface for user identification and authentication.

Domain Model Integration

The First Access system is fully integrated with the domain model network in Windows NT. **First Access Enterprise™** is integrated with the NT Servers, both the primary domain controller (PDC) and the backup domain controller (BDC) in terms of user management and database synchronization.

Centralized Security Management

Considering the pivotal role of the User Manager in the world of user security, the First Access Server has been fully and seamlessly integrated with the User Manager for Domains. All aspects of First Access user security are defined and administered through the First Access Card Manager interface which appears as an extension of the User Manager.

RADIUS/Kerberos Compliance

The **First Access Server™** is fully compliant with existing network authentication protocols such as RADIUS and Kerberos.

System Components

The table below briefly describes the various components, hardware and software, that interact to accomplish Vicinity Authentication.

Table 2.1 First Access - System Components

Component	First Access Enterprise		Description
	First Access Server	First Access Client	
First Access Sensor	✓	✓	Hardware unit connected to server and client's workstation via serial port. For more information, refer to the section - "First Access Sensor" on page 14.
First Access Card		✓	Hardware unit carried by users; interacts with Sensor to securely establish user's identity. For more information, refer to the section - "First Access Card" on page 15.
First Access Card Manager	✓		GUI installed as extension of User Manager for Domains on NT Server (Primary Domain Controllers and Backup Domain Controllers). Used to configure security profile of First Access user. For more information, refer to the section - "First Access Card Manager" on page 16.

Table 2.1 First Access - System Components (continued)

Component	First Access Enterprise		Description
	First Access Server	First Access Client	
FA GINA Authentication Module		✓	GUI installed on First Access Client's workstation. End-user authentication interface. For more information, refer to the section - "First Access Graphical and Identification Authentication Interface" on page 20
First Access Configuration Manager		✓	GUI installed as independent application. Used to set Sensor's detection range. Can be accessed from the Control Panel and GINA. For more information, refer to the section - "First Access Configuration Manager" on page 17.
First Access Database	✓		Installed on the First Access Server (PDCs and BDCs). Repository and storage of all First Access user information. For more information, refer to the section - "First Access Database" on page 17.

Functional Description of System Components

The First Access hardware kit is comprised of :

- First Access Sensor
- First Access Card

The administrative elements of the software are executed by the First Access Server through the:

- First Access Card Manager
- First Access Database

Interactive identification and authentication is executed by the First Access Client through the:

- First Access Graphical and Identification Interface (GINA)
- First Access Configuration Manager

First Access Sensor

The Sensor is First Access's equivalent of the standard smart card reader. The Sensor is connected via a serial port (RS232, USB or keyboard) to the server as well as the client's workstation.

The **First Access Sensor™** is capable of:

- Vicinity detection
- Multiple-card identification
- Card initialization

Vicinity Detection

Utilizing wireless technology, the Sensor is able to detect the presence of a **First Access Card™** over a distance of several meters. It is thus capable of vicinity detection as opposed to proximity detection.

The vicinity detection process is continuous, that is, the Sensor monitors the area for the presence of cards and the authenticated user.

When the workstation is left unattended, the Sensor does not detect the Card and the system activates the **AutoLock™** mode, whereby the desktop is locked and unauthenticated access is denied.

Multiple Card Identification

The **First Access Sensor™** can identify the presence of multiple cards within the vicinity and consequently the presence of multiple users. These Cards are advertised in the Logon Information window. Access is however restricted to a single user.

Initialization

An important function of the **First Access Sensor™** is to initialize the **First Access Card™** that is distributed to a First Access user. The procedure initializes the Card with identifying information through infra-red technology and makes it receptive to Sensor communication and identification.

First Access Card

The **First Access Card™** is the size of a credit card, slightly thicker. It can be carried anywhere on the user's person, including pockets, or, can be worn as a badge.

When the **First Access Sensor™** detects a **First Access Card™**, it is immediately advertised on the screen. The appearance of the on-screen card is determined by a number of attributes that can be assigned to the card. The Card ID appears on all on-screen cards.

The **First Access Card™**:

- Vicinity smart card
- Establish user identity

Vicinity Smart Card

If the **First Access Card™** is on the user's person, it communicates with the **First Access Sensor™** from a distance of several meters. The **First Access Card™** is a vicinity smart card, as opposed to contact smart cards. That is, it does not require contact with the reader (the Sensor) to execute its function.

Externally, the appearance of the card is left to the company's discretion and may include company logos, employee numbers etc.

Establish User Identity

The First Access Card through the communication with the Sensor securely establishes user identity. The user performs authentication only after the initial identification is positive. If the details are inconsistent, user access is denied at a very early juncture in the interactive logon process.

First Access Card Manager

In Windows NT, almost all aspects of user security are controlled through the functions and menu options accessible from the ***User Manager***. Keeping this in mind, the ***First Access Card Manager***, which is the interface used to establish the authentication and authorization profile of First Access users has been installed as an extension of the ***User Manager***.

The ***Card Manager*** is used to configure the security profile of a First Access user. The settings are user-related and are stored in the First Access database. User authentication is performed on the basis of these settings.

The First Access Card Manager can be accessed from the ***User Properties*** panel by clicking on the ***1st-Access*** button.

The following settings can be configured through the Card Manager:

- Card ID
- On-screen Card's display settings
- PIN Code verification settings

- Logon settings
- Peripheral authorization settings

For information on configuring a First Access user's security profile, refer to **Chapter 7 - First Access User / Card Administration**. A description of First Access's principle of user authentication is provided in **Chapter 6 - First Access Vicinity Authentication**.

First Access Database

The repository of all First Access users' security settings; it exists as a distinct entity, but is synchronized with the databases of the PDC and the BDCs.

First Access Configuration Manager

The distance at which the First Access Sensor is able to identify the card is not arbitrary but can be set from every workstation which has a Sensor connected to it.

Such flexibility is essential because the Sensor's range is directly influenced by the conditions in the working environment. The structure of the area, density of workstations and the degree of RF interference are all factors influencing the optimal distance. The distance itself can be as close a meter from the workstation, extending to several meters.

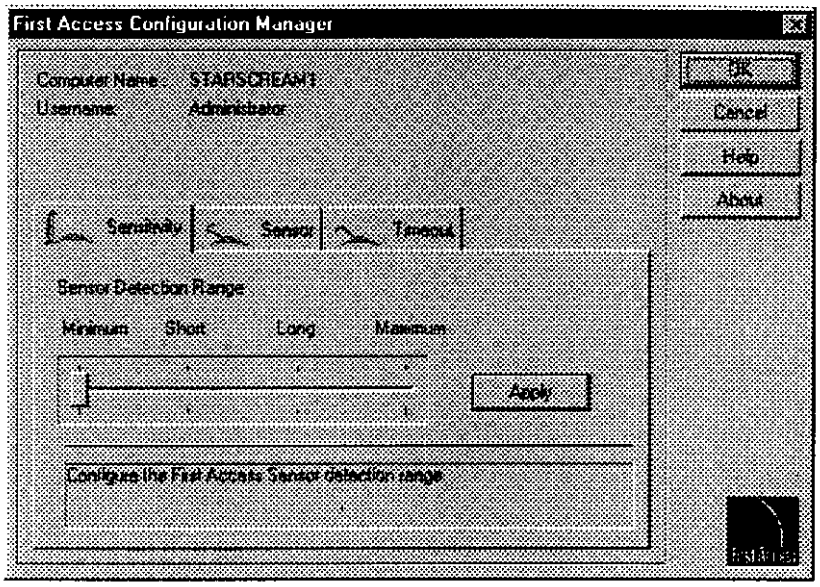
The ***Configuration Manager*** can be accessed on the server and Windows 95/98 systems through the ***Control Panel*** where it appears as independent applet.

For troubleshooting purposes, the end user can change the distance through the Sensor Settings button on the **Autolock ™** *and* ***Logon Information*** *and the* ***NT Security*** *windows.*

The ***Configuration Manager*** is used to:

- Set Sensor's receptivity
- Define a timeout prior to activating AutoLock

Figure 2.1 First Access Configuration Manager



Sensor Detection Range

Sensor sensitivity refers to the distance at which or from which the Sensor can detect a First Access Card. This distance is variable and can be adjusted per computer.

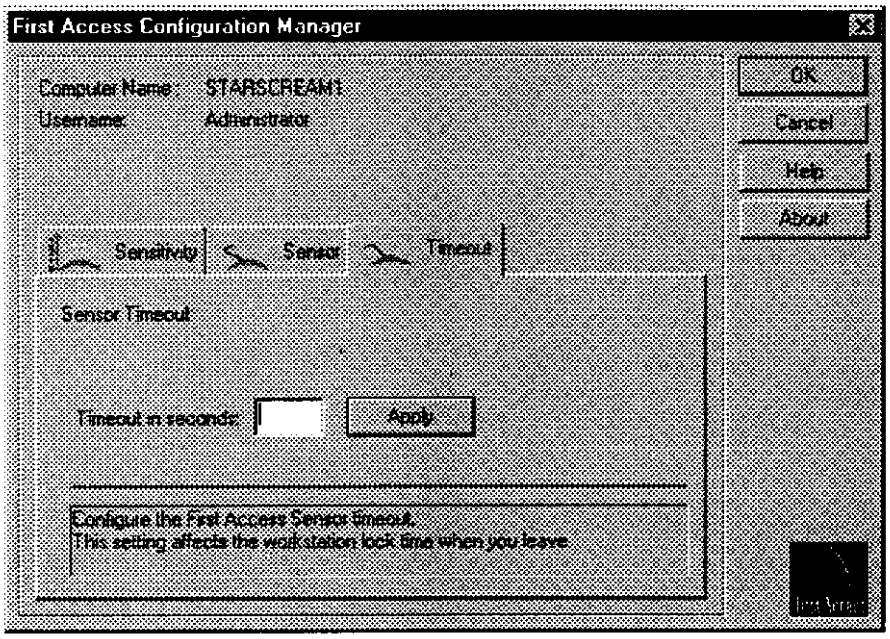
The ***Sensitivity*** panel (Figure 2.1) in the ***Configuration Manager*** displays the available settings for the Sensor. Once you have established the maximum distance at which the Sensor can communicate with the Card, you can fine tune the distance through the tab options in the Configuration interface.

Define a Timeout

Typically the Sensor continuously monitors the area within the range assigned and automatically locks the workstation when it does not detect the Card. Such a situation can occur even if you happen to turn away from the computer and block the Sensor's receptivity.

To circumvent such situations, the ***Timeout*** option has been included. When you specify a timeout (in seconds), you can in effect delay the automatic locking of the computer until the defined number of seconds have elapsed.

Figure 2.2 The Timeout panel of the Configuration Manager



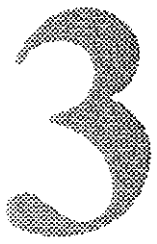
First Access Graphical and Identification Authentication Interface

The First Access authentication mechanism consists of a three-step procedure, involving identification, validation and verification. These requirements are user-specific. Any changes made through the Card Manager are immediately effective and reflected in the GINA.

Identification is automated and is user transparent; user action may be required in the validation and verification phases. Validation may be ***automatic*** which is usually assigned to users logging on at a defined workstation, whereby the user is authenticated on identification. ***Click-card validation*** is a valid authentication method for both workstation and domain logons and requires the user to identify the Card image. Authentication is also associated with PIN Code verification.

Furthermore, the **AutoLock™** feature which comes into play when an authenticated user moves beyond the vicinity of the Sensor, ensures continuous authentication. In this case, to regain access, the user has to perform re-authentication.

CHAPTER



Installing First Access

Overview

This chapter is divided into two parts:

SECTION I - Before Installation

This part covers useful topics and features that you have to be aware of before starting the actual installation procedures. The following topics are discussed:

- General considerations
- Notes on Enterprise Installation
- First Access Kit - Checklist
- System Requirements

SECTION II - Installing First Access Enterprise

This part describes the actual installation process for First Access Enterprise. You are guided through the installation procedure in detail, with notes and tips added wherever appropriate.

Section I - Before Installation

Considerations

Backup

As with the installation of any new application, it is always recommended to update or create a backup of the system disk with all pertinent information.

Emergency Repair Disk

Your Emergency Repair Disk should be updated immediately before you install First Access Enterprise. In the event that the server becomes corrupt or unstable after installation, you can use the ERD with the Setup program to re-install Windows NT Server.

Product Serial Number

The Product Serial Number appears on a label that is pasted on the package. It reflects the configuration that you ordered.

The First Access CD-ROM includes two packages:

- First Access Enterprise
- Demo

First Access Enterprise is the complete networking solution comprising of the First Access Server and the First Access Client to be installed on the network servers and client workstations respectively. An order for this package is also inclusive of the number of client licenses.

The Demo is an evaluation version with all the functionality of the working version, but without network connections. It is possible to install the Demo version on the Primary Domain Controller, and on workstations.

Encryption Key

During the course of installation, you are prompted for an encryption key. First Access enables you to use an encryption key to protect security related data. You are given the option of generating a key, typing one from your keyboard or loading an existing key.

For maximum safety, it is recommended that you allow Setup to automatically generate your encryption key.

Notes for Enterprise Installation

- First Access Server should be installed first on the NT server that has been designated as the primary domain controller (PDC). The master First Access database physically resides on the PDC.
- It is recommended to install First Access Server also on the backup domain controllers (BDC).

  This action ensures that the BDCs are at all times synchronized with the First Access database in the PDC. Thus changes to the PDC are correspondingly replicated in the BDCs as well and vice-versa.
- First Access Client should then be installed on each individual work station.
- It is possible to install both First Access Server and Client software on the servers, PDC and/or BDC by selecting both options from the Installation Type dialog during Setup.
- It is possible to install First Access Server on the BDCs and First Access Clients on workstations **only** through the network share **(netsetup.exe)** created after installation on the PDC.

  If you attempt to install on the BDC or on a client workstation form the CD, an error message appears.

System Requirements

Platforms

- First Access Server NT 4 Server
- First Access Client Windows 95/98, Windows NT 4 workstation
- Serial port

Memory requirements

- At least 50 MB free

First Access Kit - CheckList

Hardware

- ❑ First Access Sensor
- ❑ First Access Cards

Software

- ❑ First Access CD-ROM (Enterprise)

Documentation

- ❑ Reference Manual (this book)
- ❑ CD-ROM Install Quick Reference
- ❑ User's Quick Reference
- ❑ Registration form

Part II - Installation Procedure

The installation procedure for First Access Server and First Access Client are almost identical. Where applicable, differences are explicitly stated.

The First Access InstallShield Wizard

All installations are carried out through the InstallShield Wizard which is activated on starting Setup. The InstallShield Wizard is similar to any standard wizard.

You are guided through a series of screens. Each screen performs a specific task during installation.

Activating Setup

Setup can be executed directly from the CD and through netsetup.

Navigating through Setup

- You can access the succeeding screen by clicking **NEXT**.

  You can backtrack to a previous screen by clicking **BACK**.

The License Agreement

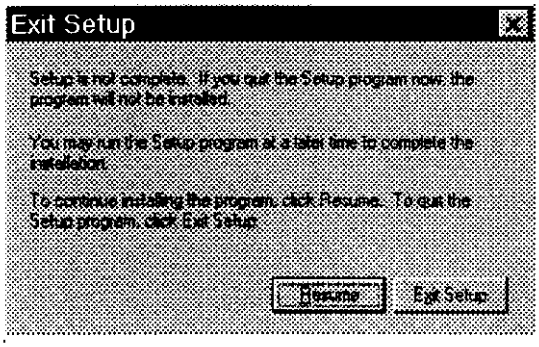
The License Agreement appears at the beginning of this document. If you have started the installation procedure, the License Agreement is the second screen to appear. It is essential that you read the agreement in its entirety.

- Clicking the **NEXT** button is tantamount to accepting the agreement.
- To cancel installation, click **NO**. In this case, Setup will abort. Return the package to the place of purchase for a full refund.

Exiting Setup

- You can exit Setup by clicking the **CANCEL** or **EXIT** buttons, depending on what is displayed on the current panel.

  This action brings up a dialog that prompts you to exit Setup or resume the procedure.



Installation

Where are you?

Step 1 - Activating Setup

From CD

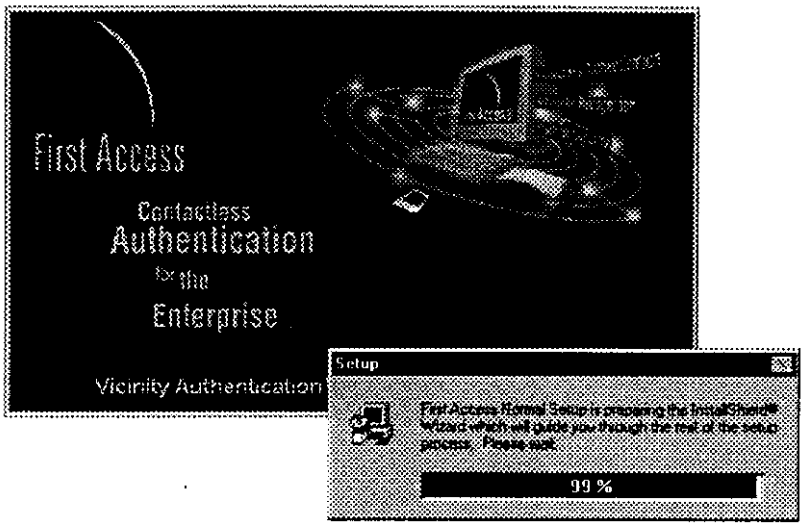
- Insert the First Access CD into the CD-ROM drive.

  The CD is Auto Run and activates the Setup Wizard.

OR

- From the ***Start*** menu, select the ***Run*** command: type d:\install.exe (where d: is the CD-ROM drive letter and click **OK**).

The InstallShield Wizard is activated. The Wizard will walk you through the install process.

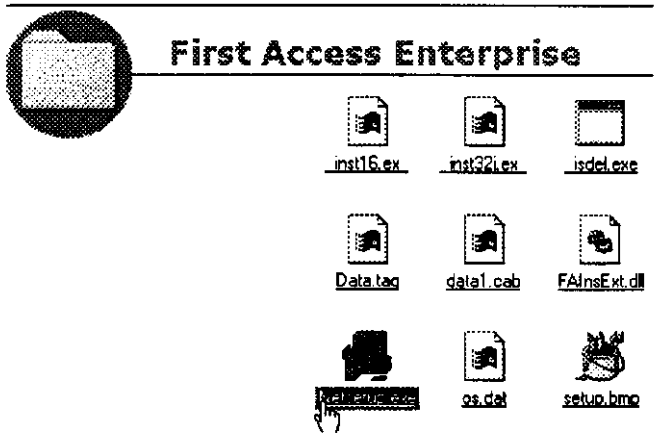


Through Netsetup

First Access Client

1 From the Client's workstation, access the program folder where First Access Enterprise has been installed.

2 Scroll through to find the *Netsetup.exe* file and double-click on it to activate Setup.



First Access Server

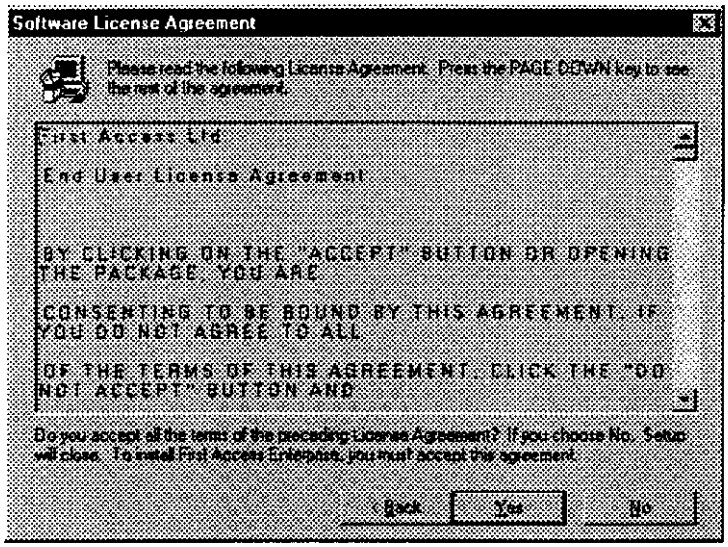
1 From the Backup Domain Controller, access the program folder in the Primary Domain Controller where First Access Server has been installed.

2 Scroll through to find the *Netsetup.exe* file and double-click on it to activate Setup.

Where are you?

Steps 2 & 3 - The Welcome Dialog and License Agreement

These form the introductory phase of the Setup process. You have to accept the License Agreement before you can proceed with the installation.



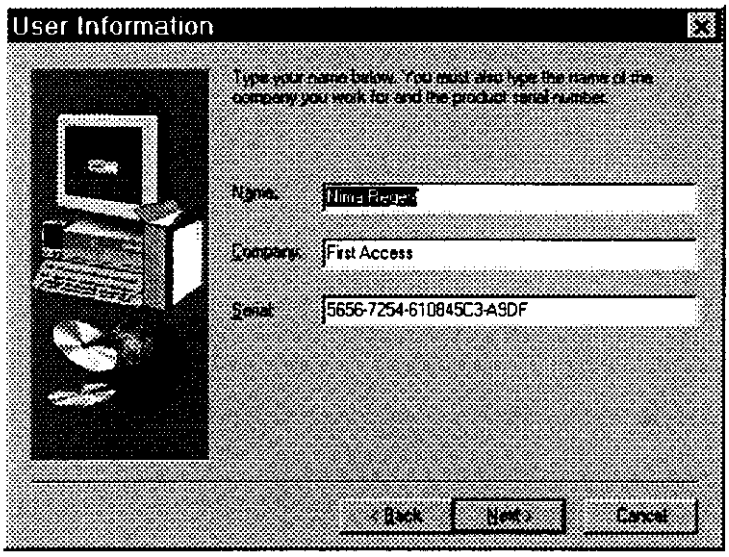
Where are you?

Step 4 - Entering User Information

The User Information screen prompts you to enter the:

- User name
- Company name
- Serial number of the product

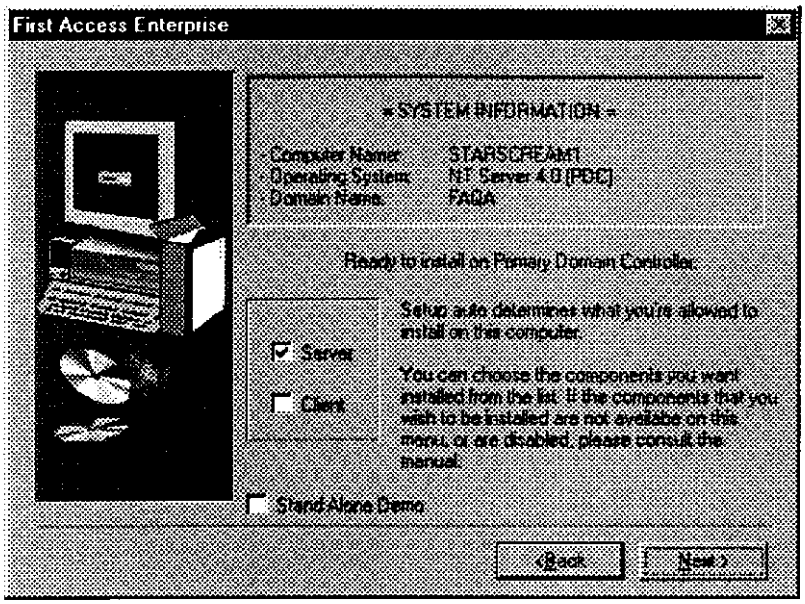
When the Client and Server software are installed through netsetup, the product serial number appears automatically.



Where are you?

Step 5 - Selecting the Installation Type

The Setup program identifies the computer on which you are performing the install as the PDC, BDC or workstation and displays this information along with the computer name and the platform.



You can install the Server and the Client software.

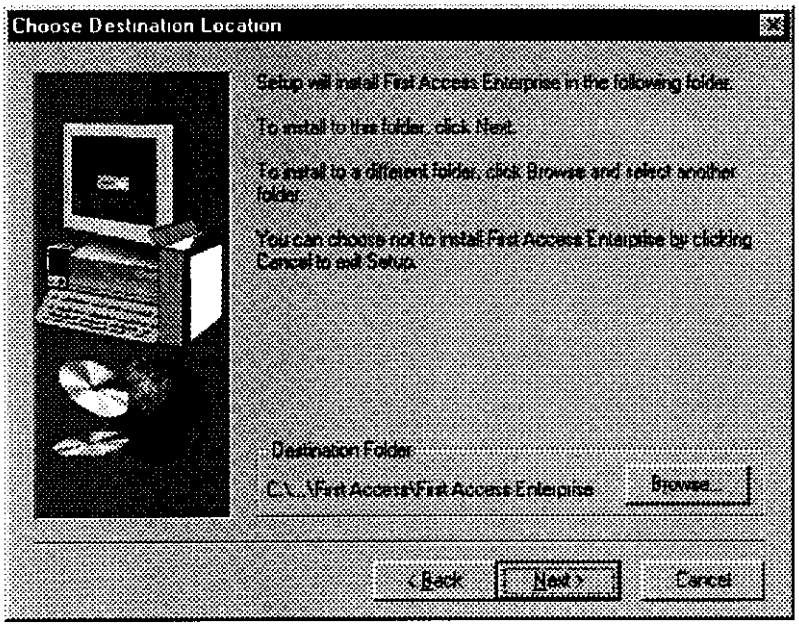
The Demo option is enabled only if you have ordered this version.

The following combinations are possible:

SYSTEM	SERVER ONLY	SERVER & CLIENT	CLIENT ONLY	DEMO
PDC	☑	☑ (optional)	☑(optional)	☑
BDC	☑	☑(optional)	☑(optional)	☒
Client	☒	☒	☑	☑

Where are you?

Step 6 - Selecting the Destination Location



You can choose one of two options:

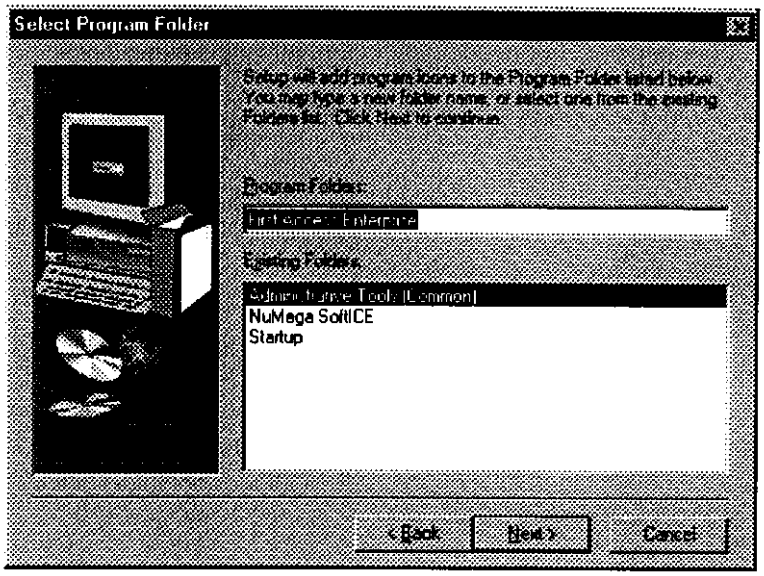
- Accept the default target drive and folder displayed under Destination Folder.

OR

- Click **BROWSE** and select a different location.

Where are you?

Step 7 - Selecting the Program Folder



You can choose one of two options:

- Accept the default Program folder displayed in the Program Folders box.

OR

- Select a different folder from the list of existing folders.

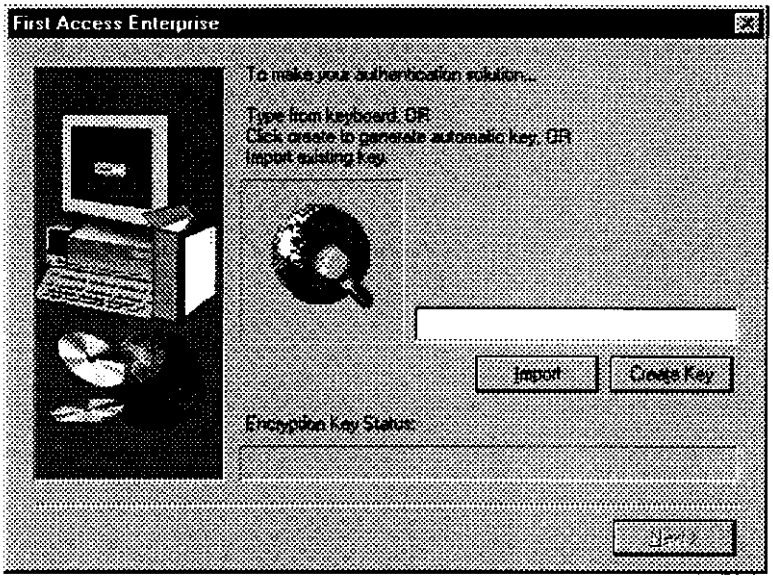
*If you select a different **Program Folder**, make a note of the folder's name (and path). You will be required to access this folder when you install the Client and Server software through the network share.*

Where are you?

Step 8 - Creating an Encryption Key

***Not applicable to First Access Client.**

Setup prompts you to create the Encryption key.



The Encryption key can be created in one of three ways:

- Typing a random key from the keyboard

OR

- Clicking **CREATE KEY** to automatically generate an encryption key (the text box will display 'Randomly created key')

OR

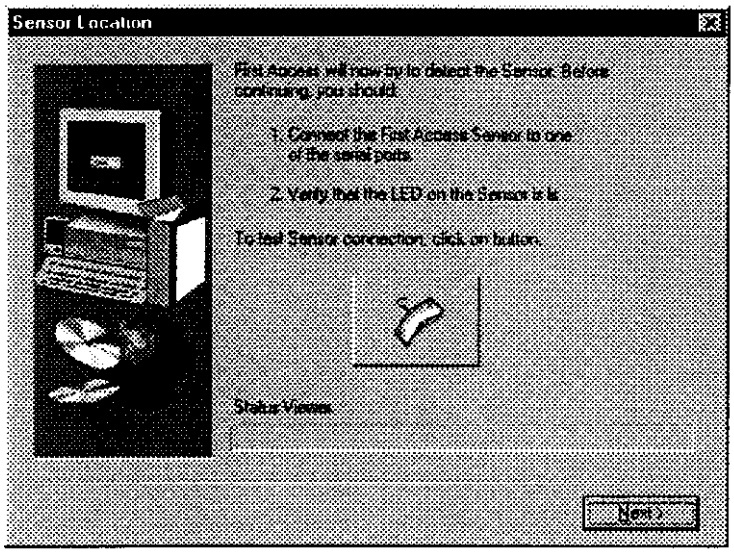
- Clicking **IMPORT** to load an existing key

If you type in a key or create one, Setup generates a symmetric encryption key which is stored in the First Access database.

Where are you?

Step 9 - Connecting the Sensor

Assuming that the Sensor has not been connected, follow the instructions as stated on the panel.

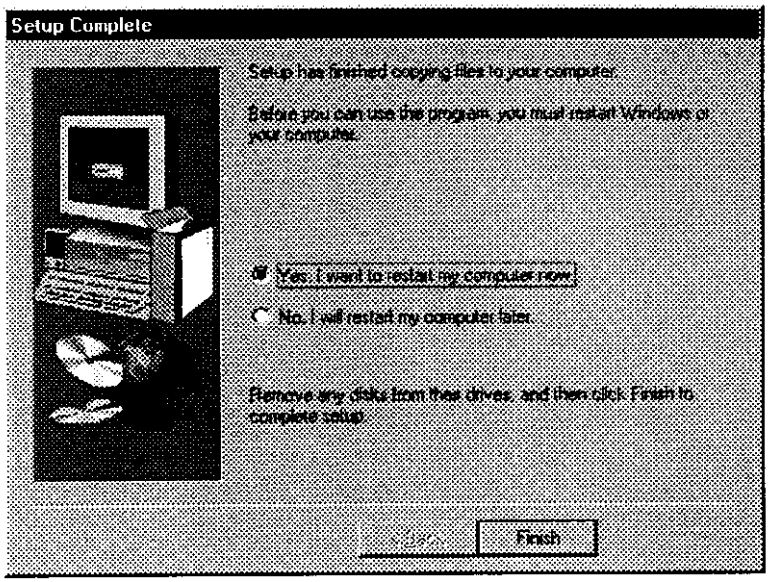


After connecting the Sensor and the LED lights up, click on the Sensor button to test the connection.

Where are you?

Step 10 - Completing Installation

Setup informs you that it has finished copying files to your computer.



You can take one of two actions:

- Choose the Restart immediately option and click **FINISH**.

OR

- Choose the Restart later option and click **FINISH**.

It is recommended to restart your computer immediately so that you can start First Access and check that everything works as it should.

Verifying Installation

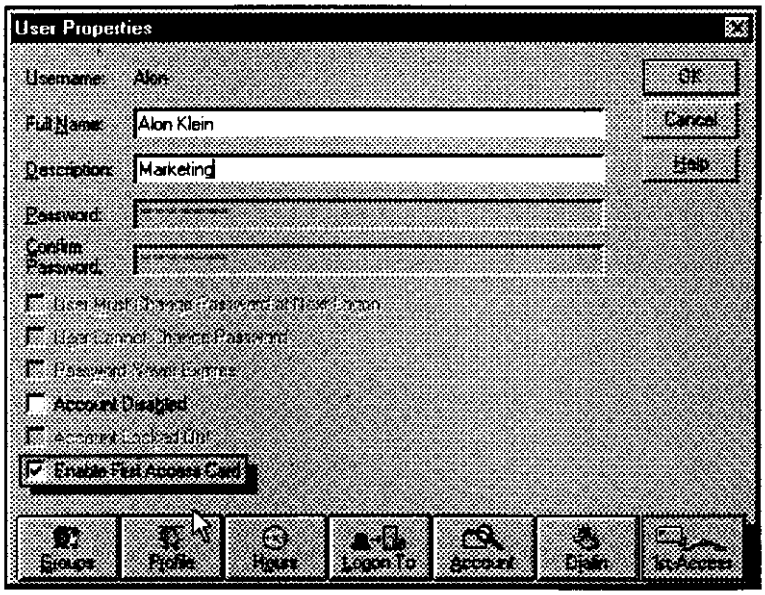
Now that you have installed the required Editions, to use the First Access program, you will have to exit all applications and restart your computer. It is also a good idea to verify the installation procedure.

1 Click *Start*; from the list of *Administrative Tools*, select *User Manager for Domains*.

2 Select any user to call up his/her *User Properties*.

3 Check if the following appear:

- ***Enable First Access Card*** check-box option
- The *1st-Access* button



Uninstalling First Access

You can uninstall First Access software through the Control Panel. The only pre-requisite is that you should have administrative rights to perform uninstall.

1 Access ***Settings***, ***Control Panel***:

2 Double-click on the ***Add-remove Programs*** icon to bring up the dialog box.

3 Click on the ***Install/Uninstall*** tab. Select ***First Access Enterprise*** from the list.

4 Click on the **ADD/REMOVE** button and click **YES** to confirm.

CHAPTER

4

First Access Integration with User Manager

Overview

One of the main tasks of a system administrator is to supervise the users of the system. This task typically starts with establishing user accounts and then defining user environment settings, profiles, security policies etc. Almost all these tasks in Windows NT are accomplished through the User Manager.

Seamless integration with the User Manager is one of the key features both in design and operation of the First Access system. Functions and options have been added to key interfaces to facilitate easy implementation of First Access' **Vicinity Authentication™** mechanism.

This chapter provides a brief description of the User Manager and those functions that you would typically use to administer user accounts. First Access extensions to the User Manager's interfaces are discussed in detail.

User Manager Window

The User Manager appears as the ***User Manager for Domains*** and is accessed from the ***Administrative Tools***.

In addition to the user management functions, the User Manager window displays the list of users and groups. Registered First Access users can be visually identified through the card icon that appears alongside the user name.

The window can be used as an on-line status indicator of First Access users. The appearance of the icon changes to reflect the current status of the user. Quick on-the-fly updates are always available.

The table below shows the representative icons and their status indication, with references to sources of detailed information regarding each status.

Table 4.1 Representation of First Access users in the User Manager Window

STATUS INDICATION	DESCRIPTION
Registered First Access user	First Access user with valid Card
First Access Card disabled	A First Access user for whom the Enable First Access card option has been cleared. User's card will not be usable for authentication.
Workstation 'locked'	Authenticated First Access, user not in Sensor's vicinity. Access to workstation access is disabled.
First Access Card Lockout	First Access user's card has been locked out on account of three consecutive PIN errors.

Selecting Multiple Users

The NT functionality of multiple user selection is supported. The extent of the user management functions available depends on the type of users selected. Your selection can include only First Access users or Microsoft users, or, a combination of the two.

If the list includes a combination of regular and First Access users, **only standard functions** (excluding, password related functions) are enabled. That is, you can disable/enable the use of the selected accounts and modify the ***Group*** memberships, ***Logon*** functions and the like.

The security attributes of First Access users cannot be collectively defined or modified.

Creating & Managing User Accounts

The ***User*** menu options are used to create and control user accounts for the domain. These are achieved through the following functions:

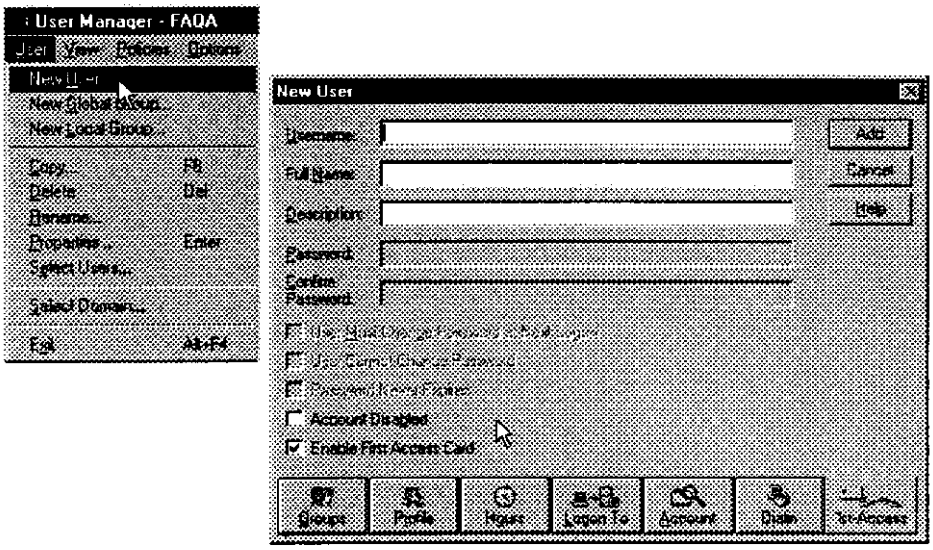
Creating New Users

Brings up the ***New User*** dialog box for a new user where you provide information necessary to create a new user, such as:

- Username
- Password
- Group memberships
- Logon restrictions

If the First Access system has been installed, a new user will be registered initially as a First Access user since by default, the ***Enable First Access Card*** option is selected(Figure 4.1.).

Figure 4.1 New User dialog box with the Enable First Access Card option selected by default



Copying, Renaming and Deleting Users

The *Copy* function allows you to select a user account by highlighting it on the User Manager window and then create a new user by copying characteristics from the existing user account.

When the *Copy* function is applied on an existing First Access user, all settings are copied, except of course the Card ID. Clicking on the **ADD** button brings up the ***Card Initialization*** dialog.

The ***Delete*** function can be used to remove the user account from the domain.

The ***Rename*** menu function allows you to select a user account and change the user name.

Creating New Groups

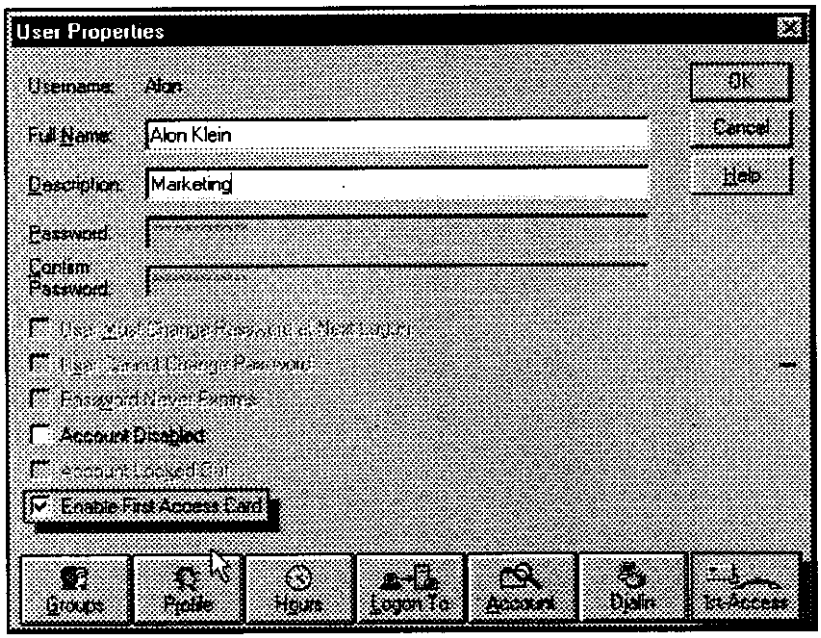
Using the ***New Local*** and/or ***Global*** group functions, you can create new groups if the built-in groups are not sufficient and then use the ***User Rights*** menu function to manage user rights.

The User Properties Panel

The features in the ***User Properties*** panel are used to administer user accounts. The options available in this panel are similar to that of the ***New User*** dialog box, except that you use the ***User Properties*** panel generally to modify the properties of an existing user account.

When the First Access system is installed, two new controls appear in the ***User Properties*** panel, in the form of a check box option and an additional function button.

Figure 4.2 User Properties Panel with First Access Controls



The ***Enable First Access Card*** option if selected, makes the First Access authentication settings operative and disables non-relevant settings, such as all the password settings.

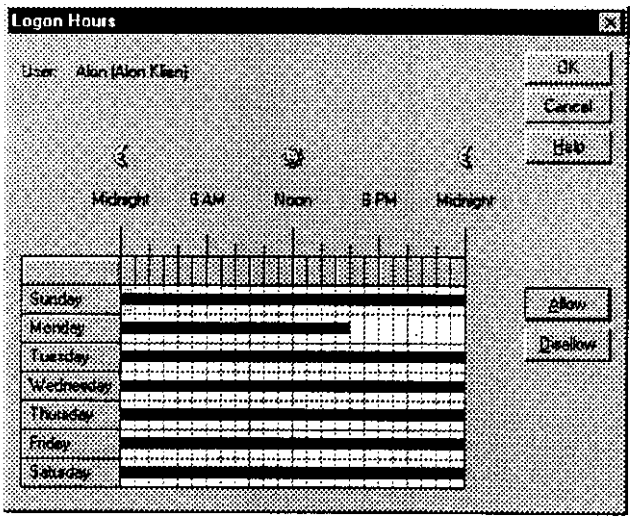
The ***1st-Access*** button accesses the interface which allows you to configure the authentication/authorization profile of a First Access user.

The other standard function buttons at the bottom of the panel enable you to set several environmental parameters for the user's account.

- The ***Group*** memberships dialog box sets the group affiliations of the user. The two lists show the groups to which the user belongs and those to which he/she does not belong. The Add/Remove buttons can be used to move a group form one list to the other.
- The ***Profile*** button enables you to specify a logon script that runs every time the user logs on to the domain or the system.
- The ***Logon Hours*** button can be used to set the hours of operation for the user.

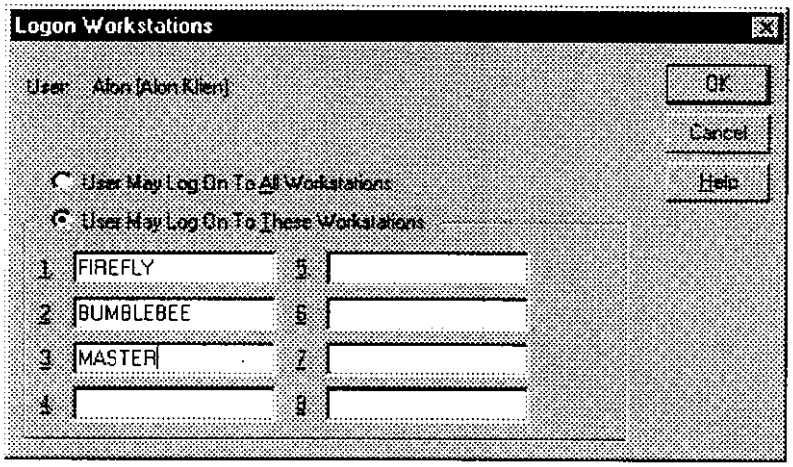
  The operational hours set by this function apply also to First Access users. If a First Access user attempts authentication after the permitted operational hours, the advertised Card displays an icon intimating that access is denied.

Figure 4.3 Logon Hours panel



- An extremely useful feature is the capability to delineate workstations which the user is allowed to access. These workstations can be defined through ***Logon to*** button. Optionally the user can access all workstations.

Figure 4.4 The Logon Workstations panel with accessible workstations defined



A First Access user will be unable to authenticate himself/herself at a restricted workstation, though the Card will be advertised in the ***Logon Information*** window. An icon appears on the advertised Card indicating why access is denied.

For example, if First Access user Alon Klein, attempts authentication at workstations other than those listed in Figure 4.4 above, his First Access Card will be advertised (capture of card)

- Account expiration policies can be accessed and set through the ***Accounts*** button on the ***User Properties*** panel.
- The ***Dialin*** button on the ***User Properties*** panel, enables you to define dial-in permissions for a user. A First Access user cannot avail of Remote Access Services (RAS) as long as he/she is assigned Card authentication.

Setting Policy Options

You use the menu options under ***Policy*** to set global policies for your domain or server as a whole, as opposed to the properties that you set for individual users.

Three types of policies can be defined, each encompassing several options:

- Account Policy
- User Rights policy
- Audit policy

Accounts Policy

The ***Accounts*** policy is a powerful feature in Windows NT to control various facets of the user operating environment.

The account policy controls the way passwords are used by all user accounts, such as minimum and maximum password age, minimum password length, password uniqueness, forcible disconnection beyond logon hours and account lockout.

Since by definition, the First Access authentication mechanism is based on vicinity identification and authentication, password policies are no longer relevant. Consequently enabling First Access, automatically nullifies existing passwords and invalidates account policy controls related to passwords, including ***Account Lockout***.

All settings relating to the user's account policy are automatically restored whenever the First Access Card option is disabled, with one exception. The user's previous password is non-existent; he/she is automatically prompted for a new password.

User Rights Policy

The ***User Rights*** policy defines the mode and extent of user access to the resources within the entire system. These can be enforced in the usual manner and range from allowing computer access from network, adding workstations to domain, to shutting down the system.

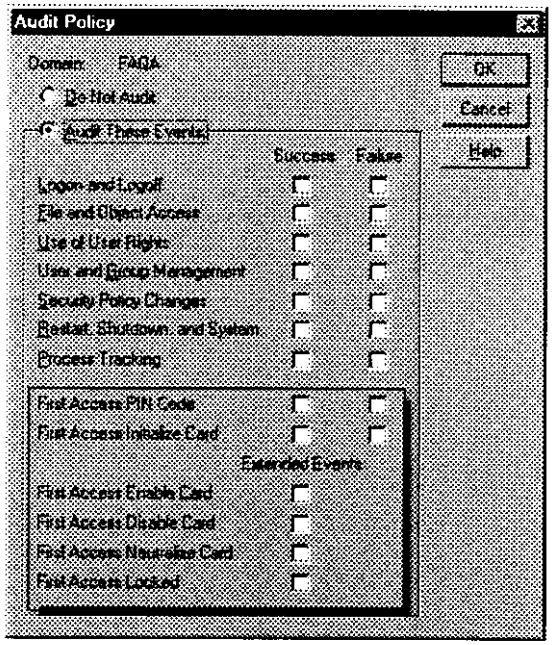
Audit Policy

The ***Audit*** feature is used to select the system, security and applications events to be audited. This is a powerful function that shows which user accesses which objects, the type of access attempted and whether the events were successful or not.

Once you have selected the events to be audited in each category, the ***Event Viewer*** can be used to view those events that are stored in the ***System***, ***Application*** and ***Security logs***.

Auditing functionality has been enhanced to include several First Access security events. Accordingly, First Access related events are recorded in the ***Security Log*** of the ***Event Viewer***.

Figure 4.5 User Manager's Audit Policy)



- ***First Access PIN Code entry***

  Monitors the number of successful and/or unsuccessful PIN Code entry attempts of users.

- ***First Access Initialize***

  Monitors the number of successful and/or unsuccessful initialization attempts of First Access Cards. For more information on the procedure, refer to **Chapter 7 - First Access User / Card Administration, "Initializing First Access Cards" on page 85**.

In addition, there are several events termed extended events. These events are single-state events:

- ***First Access Enable Card***

  Monitor all occurrences when the ***Enable First Access Card*** checkbox option in the User Properties Panel is **selected**. For more information, refer to **Chapter 7 - First Access User / Card Administration, "Enabling a First Access User" on page 83**.

- ***First Access Disable Card***

  Monitor all occurrences when the ***Enable First Access Card*** checkbox option in the User Properties Panel is **cleared**, thus disabling First Access security controls for the user. For more information, refer to **Chapter 7 - First Access User / Card Administration, "Enabling a First Access User" on page 83**.

- ***First Access Card Lockout***

  Monitor all occurrences when the a First Access Card has been 'locked out' because of consecutive errors in PIN Code entry. Usually, a maximum of three attempts are allowed. For information on PIN policies, refer to **Chapter 6 - First Access Vicinity Authentication, "PIN Code Verification" on page 76**. The configuration procedure is explained in **Chapter 7 - First Access User / Card Administration**.

- ***First Access Locked Card***

  Monitor all occurrences when the **AutoLock™** function is activated and workstation access is disabled. The computer 'waits' for the authenticated user to 'unlock' by re-authenticating himself or herself. For more information, refer to **Chapter 6 - First Access Vicinity Authentication, "AutoLock & Unlock" on page 73**.

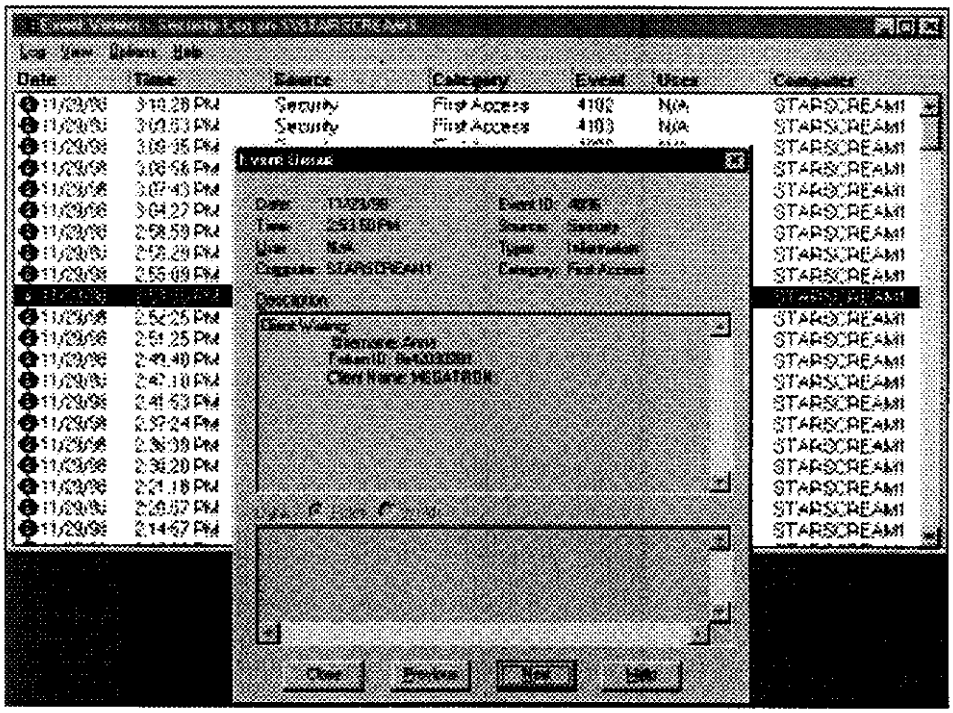
Using Event Viewer to view Audited Events

The *Security Log* of the *Event Viewer* records occurrences of all First Access events that are audited. A First Access event can be identified by the classification First Access which appears under *Category*.

To view details of a First Access Event:

- Find and highlight the required First Access event.
- Double-click the event to display the description of that event.

Figure 4.6 Details of the highlighted event selected from the Event Viewer



View Options

The ***Options*** menu remain unchanged.

Setting Trust Relationships

The final function that you can perform through the User Manager is define trust relationships. The ***Trust Relationships*** dialog box enables you to add domains that are trusted by your domain, and those domains that are permitted to trust you.

The First Access system supports domain trust relationships. A First Access user once authenticated can access resources in trusted domains.

User Manager Window

CHAPTER

First Access - Deployment Guide

Installing First Access Enterprise

The Scenario

You are about to install First Access Enterprise on your domain. The domain comprises of:

- PDC
- BDCs - two in number
- Clients: three Windows NT, two Windows 95/98.

B

Before you start, check if the following are at hand:

- ❑ CD-ROM
- ❑ CD - Install Quick Reference
- ❑ First Access Sensor and required number of First Access Cards.

At any point, you can refer to the following chapters in this manual for information:

- *Chapter 3 - Installing First Access*
- *Chapter 4 - First Access Integration with User Manager*
- *Chapter 7 - First Access User/Card Administration*

The Procedure

- Installing First Access Server on the PDC
- Installing the First Access Server on the BDCs
- Configuring the authentication profile of users
  - Accessing the User Manager for Domains
  - Configuring for existing users
  - Configuring for new users

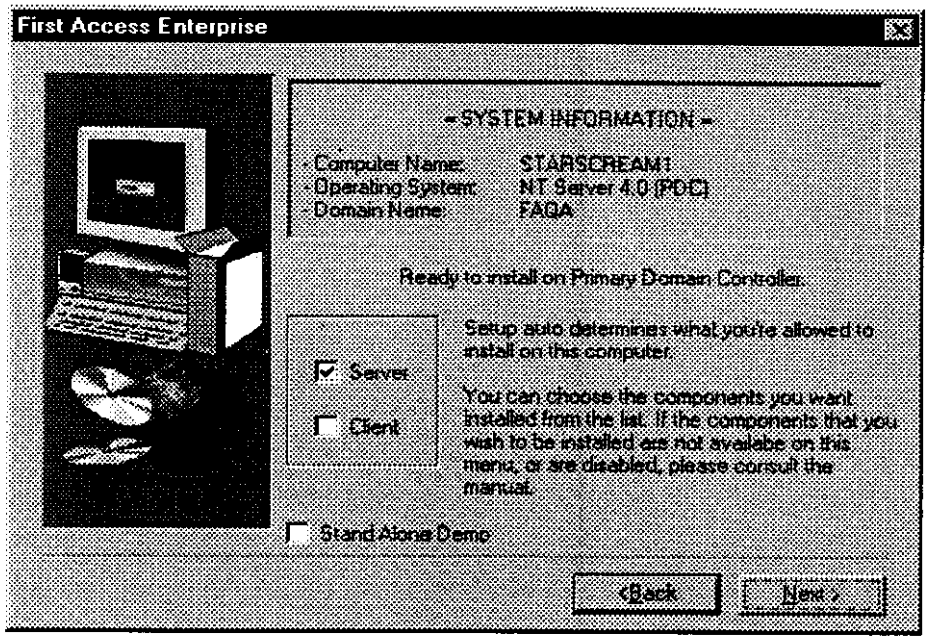
Installing First Access Server on PDC

1 Insert the CD into the CD-ROM drive. The CD is automatically run and should activate Setup.

2 In the ***User Information*** screen, enter the ***Product Serial Number*** and other details.

3 In the ***Installation Type*** screen that follows, you have the option of installing both the Server and Client software. In this case, you will select the Server option.

Figure 5.1



4 Make a special note of the ***Program Folder*** if you select one different from the default provided. You will need this information when you install First Access Client through netsetup.

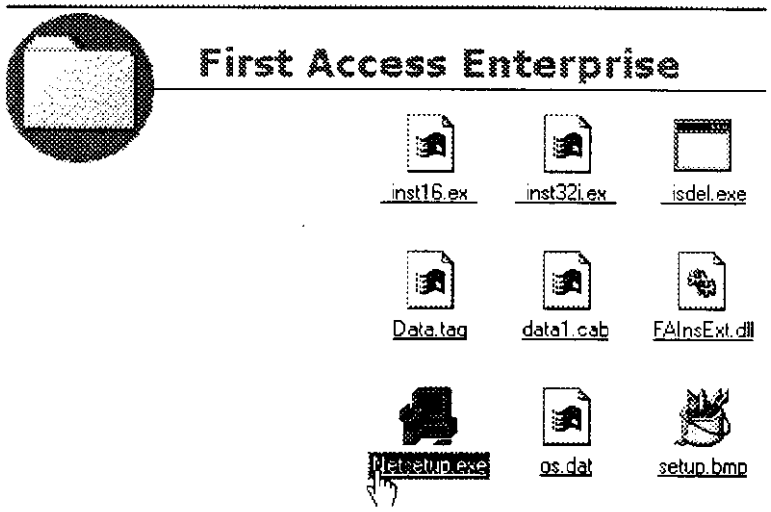
5 Follow instructions until Setup is complete.

Installing First Access Server on BDC

Now you will install the First Access Server on all your Backup Domain Controllers to ensure synchronization. The installation can be done only through netsetup.

1 Access the ***netsetup.exe*** file from the ***Program Folder*** of First Access Enterprise on the PDC.

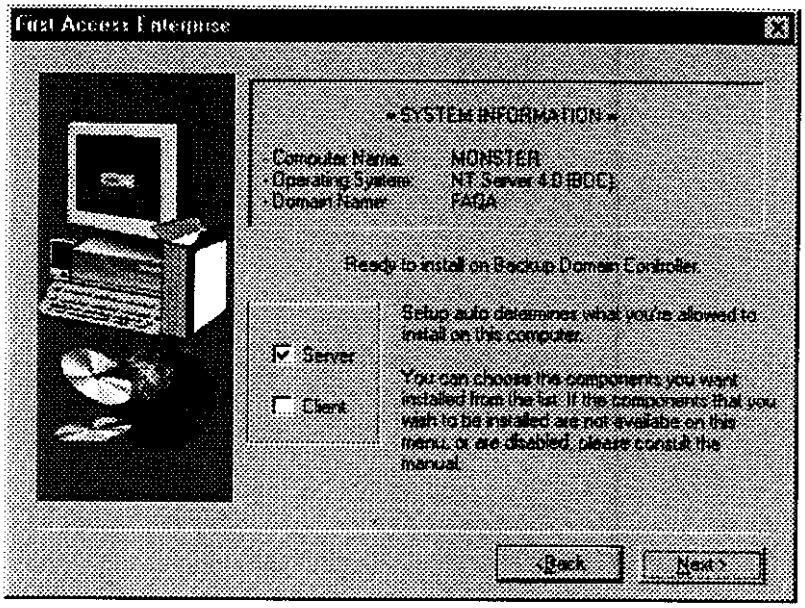
Figure 5.2 Installing First Access Server on the BDC through netsetup.exe



2 Double-click on the file to start ***Setup***.

3 In the ***Installation Type*** screen, the system information displays that you are installing on the BDC. Select the ***Server*** option.

Figure 5.3 Selecting the Installation Type on the BDC



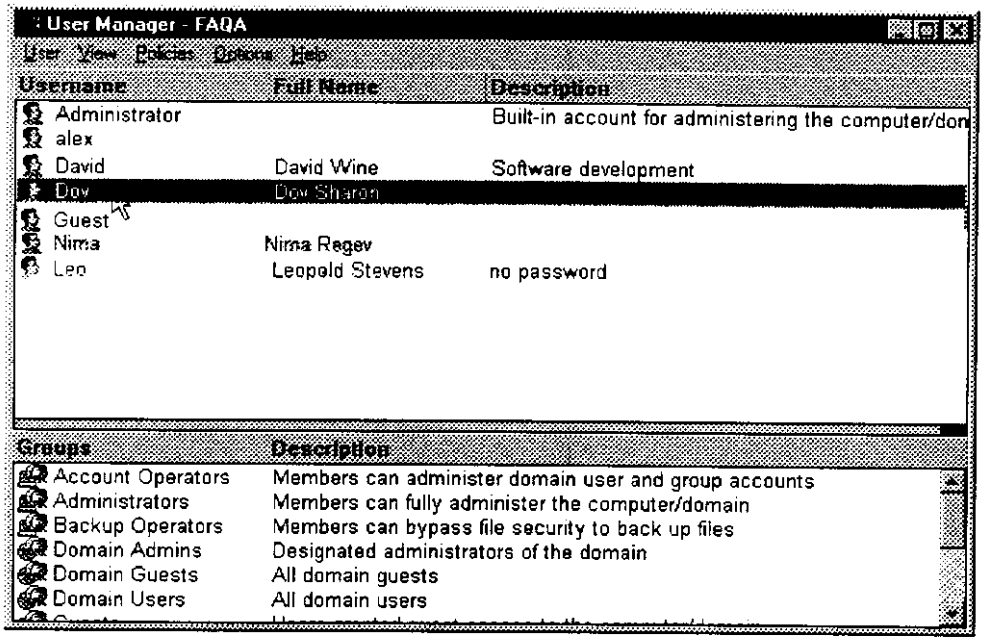
The remainder of the procedure is identical to that of the PDC. After completing the installation, follow the same procedure to install on the other BDCs in the domain.

Accessing User Manager for Domains

You will now configure the authentication and authorization profile for existing and new users through the ***User Manager for Domains***.

Figure 5.4 shows a sample of the current User Manager window. Note that there are no First Access users at present.

Figure 5.4 The User Manager window before defining First Access users



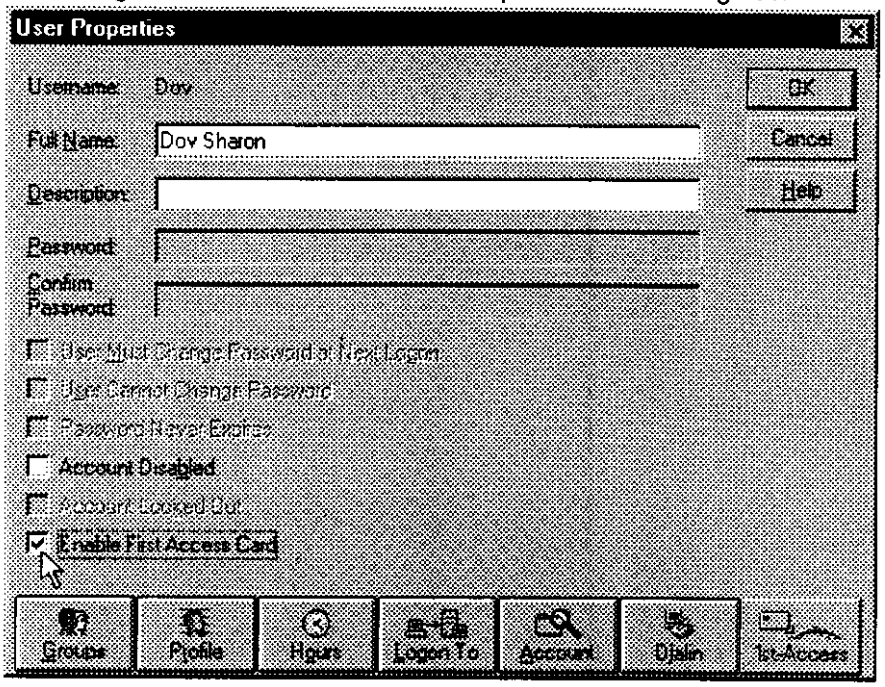
- You will enable the First Access Card for two existing users, in this case, Dov and Nima.
- You will create two new users and configure their security profiles.

Configuring the Authentication Profile for Existing Users

1 From the ***User Manager*** window, select an existing user, (Dov in our example) and double-click to bring up the ***User Properties*** panel.

2 Select the ***Enable First Access Card*** option.

Figure 5.5 Selecting the Enable First Access Card option for an existing user

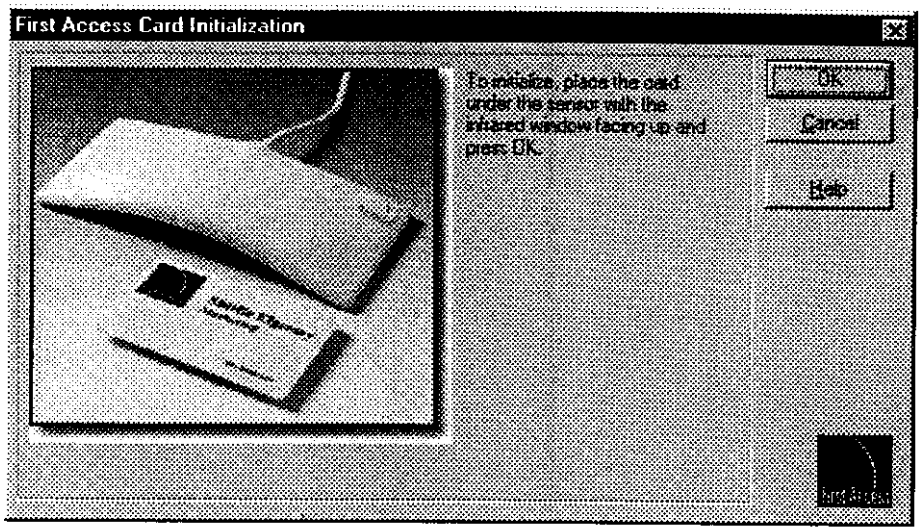


- Password settings are rendered invalid.
- Default First Access authentication settings are activated. You will accept the default settings for now.

3 Initialize the Card that will be given to the user as follows:

- Click ***OK*** on the ***User Properties*** panel. The Card Initialization dialog box appears:

Figure 5.6 The Card Initialization Panel



- Position the Card so that the IR window faces the Sensor.
- Click ***OK***. The procedure generates a unique Card ID.

4 Repeat steps **1** through **3** for another user (Nima in our example).

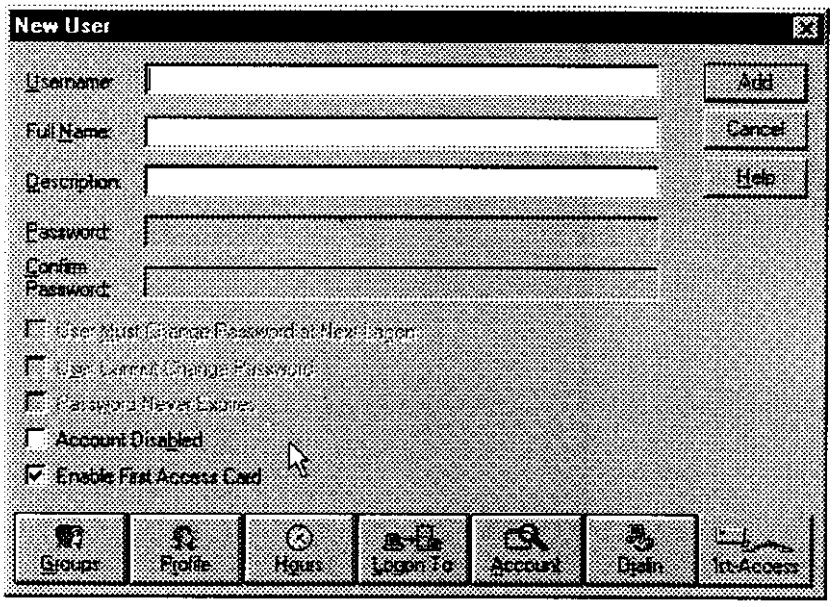
Configuring the Authentication Profile for New Users

1 From the ***User Manager*** window, select the *New User* option.

Note that since the First Access Server is already installed, the ***Enable First Access Card*** option is already selected.

In the *New User* dialog box, enter relevant details such as the username. In this case, the user name will be Jonathan Stone.

Figure 5.7 New User Dialog with the First Access Card option enabled by default



2 Click on the ***1st-Access*** button to bring up the ***First Access Card Manager***. Change the default authentication/authorization settings, as required.

3 Initialize the card as follows:

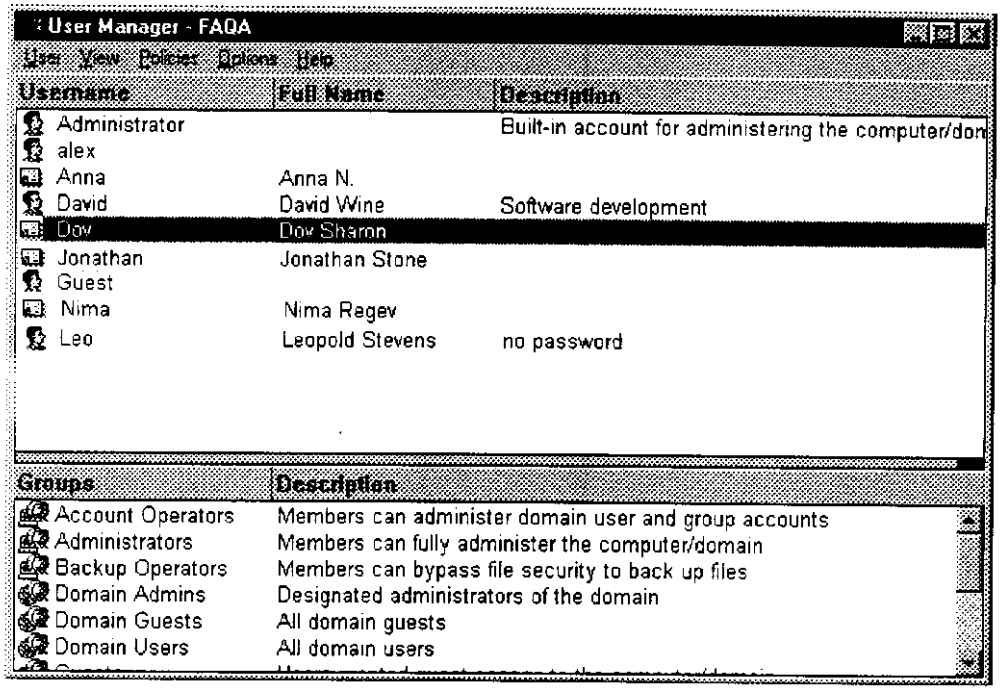
- Click ***OK*** on the ***User Properties*** panel. The Card Initialization dialog box appears. Refer to Figure 5.6.
- Position the Card so that the IR window faces the Sensor.

4 Click ***OK***. The procedure generates a unique Card ID.

5 Repeat steps **1** through **4** for another new user, for instance Anna.

After completing the procedure, a look at the User Manager window will now show four users identifiable as First Access users.

Figure 5.8 User Manager window displaying newly defined First Access Users

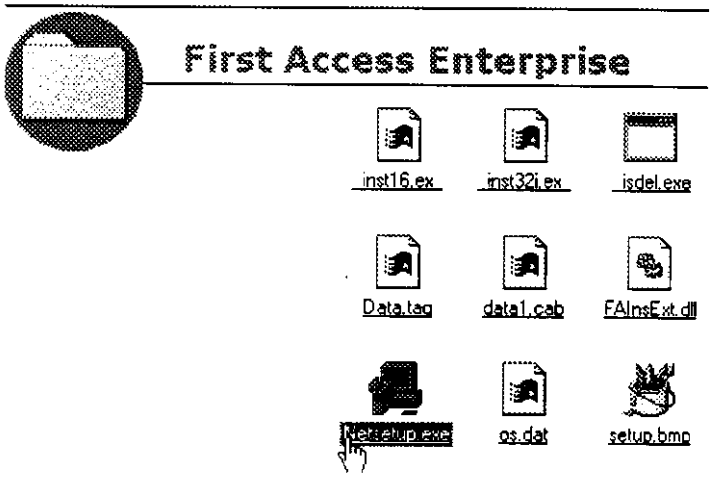


Installing First Access Client

Now you will install the First Access Client software on the designated workstations, Windows NT and/or 95/98.

1 From one of the client workstations, access the network server, in this case, the PDC which has the First Access Server installed.

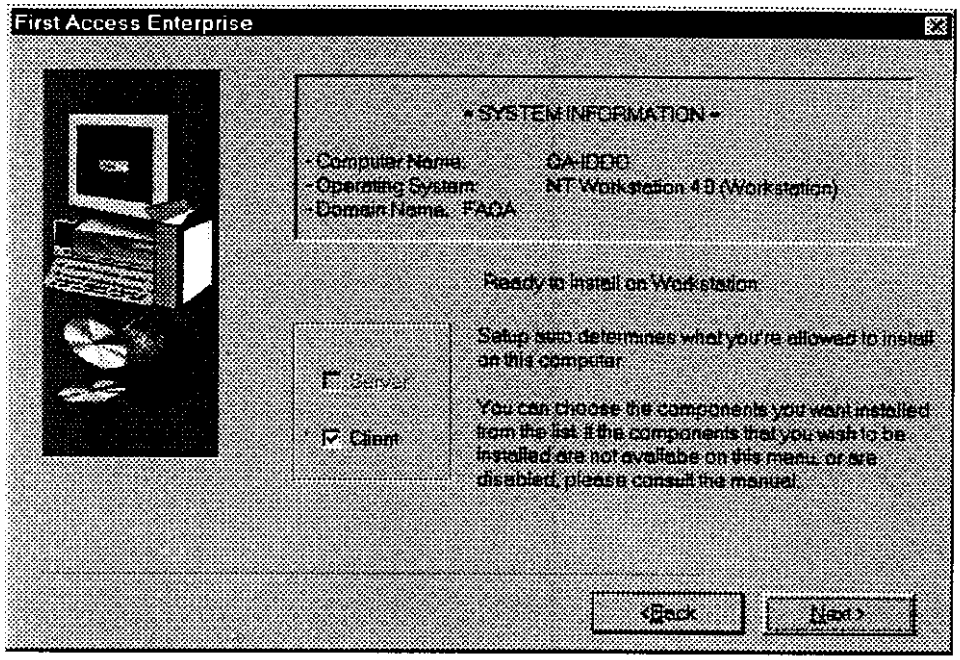
Figure 5.9 Activating Client Setup through Netsetup



2 Double-click on the **netsetup.exe** file to run the Setup program for First Access Client.

3 In the ***Installation Type*** panel, the Client check box is enabled by default (Server option is disabled).

Figure 5.10 Installation Type panel for Client with Server option disabled by default



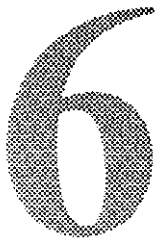
4 Continue until the Setup procedure is complete.

5 Repeat steps 1 through 4 on the other client workstations.

Distributing the First Access Cards

The final step is to distribute the initialized cards to the relevant users.

CHAPTER



First Access - Vicinity Authentication

Overview

Before you get down to the nuts and bolts of actually configuring the authentication and authorization profile of a First Access user, it is important to understand the concept of **Vicinity Authentication™**.

This chapter addresses the following topics:

- Characteristics of **Vicinity Authentication™**
- How it works
- Levels and methods of authentication

Characteristics of Vicinity Authentication™

In an arena heavily dominated by password-based authetnication, the immediate and obvious difference is that passwords are no longer required for authentication.

- **Distance based contactless authentication**

  Identification of a First Access user occurs at a distance of several meters from the workstation. This factor at once separates it from authentication models based on proximity, which require the smart card to be placed if not actually within the reader, at least extremely close to it, in order to securely identify the user.

  The **First Access Card™** communicates with the **First Access Sensor™** without coming into contact with it at any time.

- **Automated authentication mechanism**

  First Access's authentication mechanism is largely automated. All that is required is the presence of the **First Access Card™** on the user's person and the **First Access Sensor™** to be connected to a serial port on the client workstation.

  The Card communicates with the Sensor performing identification; the entire process is user transparent and takes place without user intervention.

  After successful identification, depending on the system's configuration, the user might be required to merely approach the computer or identify his/her Card, and input a PIN.

  The automation continues even after authentication through the **AutoLock™** feature which 'locks' the workstation if and when it is left unattended for a certain time.

- **Secured communication**

  Sophisticated algorithms ensure completely secured transmission between Card and Sensor and then between server and client.

- **Three-factor authentication policy**

  In contrast to a single factor authentication policy which is restricted to password control, **Vicinity Authentication™** is based on multilateral authentication. Automatic identification is coupled with validation based on pre-defined security attributes, and optionally verification through PIN entry, for successful authentication.

  Thus merely possessing the Card or guessing the PIN do not in themselves guarantee authentication or penetration.

- **Continuous authentication**

  Conventional authentication systems check the identity of the Card at the start of the session and ultimately require the user to remember to logoff if he/she has to leave the workstation. Moreover, the action of logging off requires the card to be placed within the reader. There is a tendency to leave it in the reader thus nullifying the very purpose of the exercise.

  With **Vicinity Authentication™**, the Sensor polls continuously for the presence of the Card and automatically disables access to the workstation when it does not detect the Card. The **AutoLock™** function as this is termed, ensures that data integrity and network security are not compromised throughout the working session of an authenticated user. This is especially significant in the context of Windows 95 systems since it provides the only means of real-time desktop protection.

  Only the authenticated user or an administrator can 'unlock' the system, the former by reauthentication and the latter through manual logon using the administrator account and forcibly logging off the user.

- **Single sign-on support**

  Today's distributed computing environments make single sign-on support an integral part of any authentication mechanism. Single sign-on requires a method of identification and authorization that can be administered across the enterprise in a consistent manner and permits the user to access in a single transparent manner all information systems to which he or she is authorized.

Through **Vicinity Authentication™**, the end-user is identified and authenticated without the need to remember multiple IDs or passwords. This identity can be used to access resources in trusted domains.

How it Works

The two main aspects of interactive logon consists of the initial logon followed by the identification and authentication process.

Windows NT provides a secure way for users to logon initially through the secure attention sequence (SAS) thus preventing access through Trojan horse programs. This is followed by the actual identification and authentication implemented through the Graphical Identification and Authentication DLL, referred to as the GINA.

First Access retains the standard secure attention sequence (SAS) used by Windows NT. This is the ***CTRL+ALT+DEL*** key combination.

The standard GINA has been replaced by the First Access GINA which implements **Vicinity Authentication™**. **Vicinity Authentication™** can be visualized as being executed in three phases each of which dovetail into the other, such that one begins where the other leaves off.

- **AutoDetect™**ion and identification
- User validation and verification
- **AutoLock™** and unlock

AutoDetection & Identification

The first phase of any authentication protocol begins with user identification. In **Vicinity Authentication™** , the process of user identification is completely automated and user-transparent.

It is based on Sensor /Card communication through an RF channel. The resulting transmission is secured through sophisticated algorithms. Moreover since the identification occurs at an extremely early juncture, specifically just after the **CTRL+ALT+DEL** sequence (for Windows NT) if the user is logging on for the first time, or, on approach if the

workstation has already been in use, fraudulent access is actively prevented at a preliminary phase in the authentication process.

What essentially happens here is that the user's credentials are read from the Card, checked with the database and approved, thus granting access to the next stage of the authentication process.

This process is activated as soon a user equipped with the **First Access Card™** approaches the workarea. The Sensor 'detects' the presence of the Card, identifies the presence of a First Access user and checks the Card ID with that existing in the **First Access Database™**.

Validation

Validation is the second stage and forms the crux of the authentication process. In this stage of the process, the **First Access Client™** works with the **First Access Server™** to implement the authentication profile that has been set for the particular user.

Depending on the system configuration settings, this phase focuses on a pre-defined action the particular user has to perform.

It might require something as simple as merely approaching the workstation, or identifying the user's First Access Card advertised on the screen. Depending on the security level of the particular user, two types of validation can be implemented - automatic or click-card. For detailed information, refer to the section on "Methods of Authentication" on page 75.

Validation can be supplemented by verification which requires personal, secret information known only to the user, in the form of a PIN (personal identification number).

AutoLock & Unlock

When the authentication is complete and successful, the user initiates a work session, Sensor/Card communication comes into play again.

The **First Access Sensor** continuously monitors the area for the presence of the authorized user's Card (and hence the user). The moment the Sensor does not detect a Card, the system goes into AutoLock™ mode.

To put it simply, the user's system is 'locked', automatically, without any action on the user's part. From this point access is disabled and remains disabled until the authenticated user returns and performs re-authentication. No other user, not even one with a valid First Access card can access the computer. Behind the screen, everything goes on as usual, so background activity proceeds undisturbed and processing time is not wasted.

Once the authenticated user has 'unlocked' the computer, he/she simply picks up from where he/she left off with the knowledge that not only are files secure but that network access has been denied in the meantime.

Levels of Authentication

If your network is implemented on the domain model, (even the simplest one) domain users will logically have to perform functions from different workstations at different times, or, access network resources across the domain from the local computer.

First Access provides the capability of implementing validation and verification controls - for a single user - on two parallel levels:

- Workstation
- Domain

Workstation Logon

Defines user-validation with regard to a specific device - the user's own permanent computer.

Domain Logon

Defines the same user's authentication policy with regard to other workstations in the domain of which the user is a member.

Access to workstations within the domain can be further restricted through the ***User Manager's Logon to*** function. Here, you can delineate the specific workstations to which you as the administrator would want to grant access. For more information, refer to **Chapter 4 - First Access Integration with User Manager, "Creating & Managing User Accounts" on page 42**.

Methods of Authentication

The entire authentication procedure occurs at the client's workstation and is carried out through the Graphical Identification and Authentication (GINA) interface.

The initial identification is automated and the rest of the procedure can comprise of two stages - validation and verification. The mandatory part of the process is validation - which can be of two types:

- Automatic

OR

- Click-card

PIN entry verification can be enforced to reduce the likelihood of authentication fraud.

Automatic Validation

The user comes within a pre-defined distance at which the sensor communicates with the card. If the details check out, the computer automatically performs the authentication, bypassing the usual authentication window.

(figure showing user approach with magnified view of monitor showing a typical desktop)

PIN Code verification can be set as a requisite, in which case the user will have to enter the PIN Code.

Automatic validation is a valid option only for ***Workstation logon*** for obvious reasons. Otherwise, if it was a valid option for ***Domain logon***, other authorized users sharing the same workspace could be inadvertently logged-on.

Click-card Validation

The ***Click-card*** mode of validation requires the user to identify his/her card among those advertised in the Authentication Window and click on it to make the authentication.

(figure)

This is the only type of validation applicable for ***Domain logon***. Here also, PIN Code verification can be set as a requisite.

PIN Code Verification

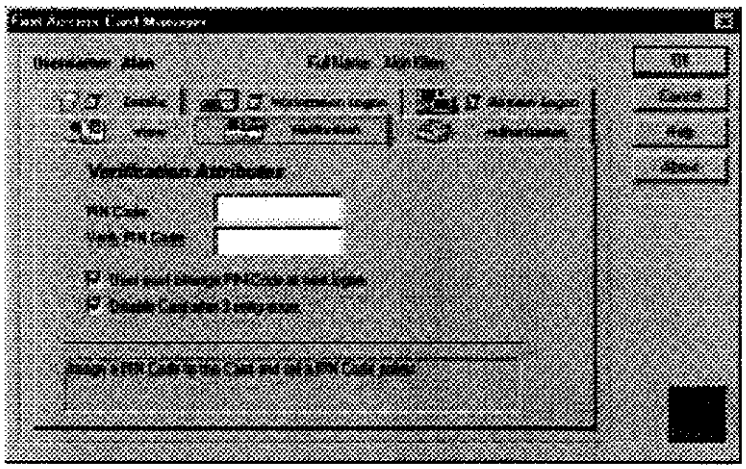
Over and above all the validation-modes, First Access provides you with the option of PIN Code verification as a secondary requirement for authentication.

Verification through PIN Code further secures the authentication process and is a useful and practical means to strengthen security. The combination of the validation and PIN provides for superior authentication.

You can define system-wide PIN Code policies and then enforce them selectively on a user-by-user basis.

System-wide PIN policies are automatically effective for any First Access user who requires PIN entry as a means to authentication.

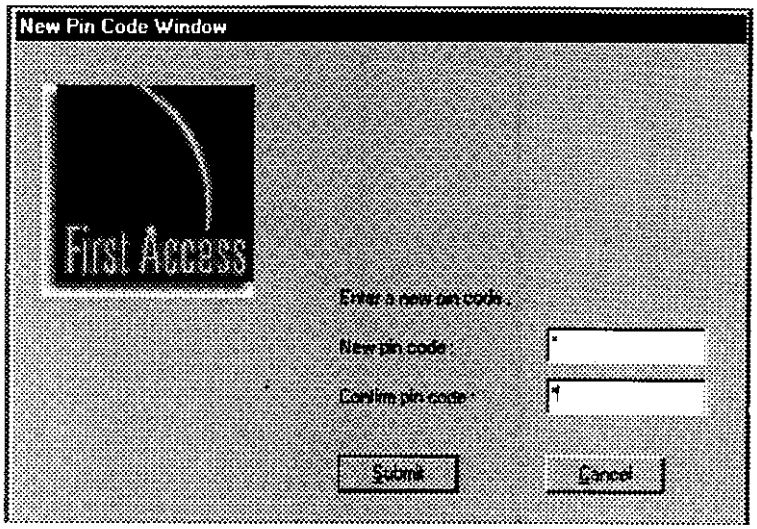
Figure 6.1 The Verification Panel to define PIN policies for First Access users



- **Mandatory PIN entry for first time user**

  You can make it mandatory for any user performing logon for the first time on a First Access system to enter a unique PIN Code.

Figure 6.2 The New PIN Code Screen



Forcing a new First Access user to enter the PIN Code during first time log-on is also a practical and easy way to reinforce and maintain security in the event of a user leaving or being replaced.

- **Implementing Card Lockout**

  You can also set a lockout policy by which three consecutive PIN Code errors automatically neutralizes a First Access Card. This corresponds to the ***Account Lockout*** feature in Windows NT, which is of course invalid for First Access users.

  The card will no longer be usable for authentication until you as the system administrator re-activates it.

PIN verification can be controlled on a **user-by-user** basis. This is done by controlling when the user is prompted to verify the PIN Code. Thus you can require:

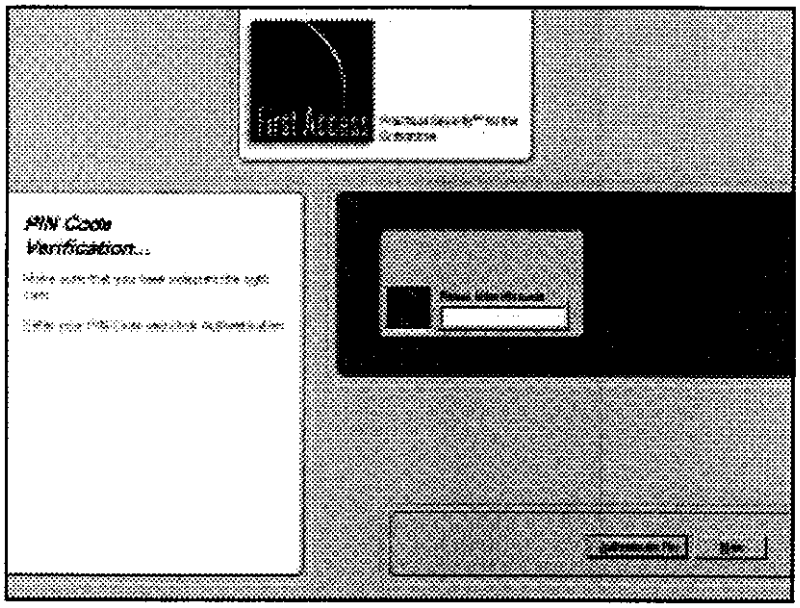
- **PIN entry only on initial logon**

  Prompts the user for PIN Code only once, that is, the first time the user performs system logon. (This is different from the PIN Code screen that prompts a new first time user to enter the PIN Code).

- **PIN entry at all times**

  Forces the user to enter the PIN Code not only during the initial workday logon, but also everytime that the same user performs re-authentication.

Figure 6.3 The PIN Verification Window



First Access User/Card Administration

The First Access administration program is simple to implement and easy to maintain. A First Access user's authentication profile is created through a single interface - the First Access Card Manager. For maximum convenience, it is installed as an extension of the User Manager and can be easily accessed from the User Properties panel.

User/card administration involves:

- Registering First Access users
- Configuring a First Access User's authentication profile
- Auditing First Access security events

Registering First Access users

To implement the First Access security system, you have to enable the First Access User Card option and initialize the Card.

Enabling the First Access Card makes the advertised Card receptive to commands and actions.

Initializing a card, encrypts it with the necessary data to facilitate communication with the Sensor.

Configuring a First Access User's profile

User profiles are configured through the ***First Access Card Manager***. This utility is accessed by clicking the ***1st-Access*** button. The relevant procedures are explained in detail in Chapter 7- First Access User /Card Administration.

A very useful smart feature is that default settings are already configured and are automatically operative after the First Access Card is enabled and initialized. Thus the First Access system is immediately operative and you can set about customizing the same user's profile later according to specific needs.

When new users are added with First Access installed, the ***Enable First Access Card*** is already selected by default.

Auditing First Access Events

Auditing events contributes immeasurably to internal and external security. First Access events are included in the Windows NT Audit list. They can be selected using the ***Audit Policy*** of the ***User Manager***. The category of events encompass all those influencing authentication and are explained in Chapter 4 - First Access Integration with User Manager.

On-the-fly auditing is also possible through the User Manager Window, which visually updates the status of all registered First Access users, through representative icons indicative of the following states:

- First Access Card enabled
- First Access Card disabled
- First Access Card neutralized
- First Access user logged on
- First Access user's workstation 'locked'

CHAPTER

7

First Access - User/Card Administration

Overview

Installing the First Access Server and the First Access Client on the servers and the required workstations, connecting the First Access Sensor is only part of the job of putting the First Access security system into operation.

To actually implement the Vicinity Authentication, you have to establish the authentication profile of First Access users. The procedure requires the following:

- Enabling First Access Cards
- Initializing the First Access Cards
- Configuring the authentication and authorization profile

This chapter describes the various facets involved in establishing the authentication and authorization profile of a First Access user.

Enabling a First Access User

Enabling the **First Access Card™** is one of two actions required to record a user in the **First Access Database™** .

It is done by the simple action of enabling a check-box option in the ***User Properties*** panel.

Enabling a First Access User Card

1 From the User Manager window, double-click on the required user's name.

The ***User Properties*** panel appears.

*For a new user, the **Enable First Access Card** option is selected by default.*

2 Select the ***Enable First Access Card*** option. This action has two effects:

   a Renders standard security settings, specifically password settings, invalid, as shown in the figure below. Only the ***Account Disabled*** option remains active.

   b Makes effective the default First Access security attributes.

Disabling a First Access User Card

At any time, you can clear the ***Enable First Access Card*** check box to disable the **First Access Card™** for a particular user.

Disabling the option for a registered First Access user:

- Renders First Access security settings invalid for the particular user. The particular user cannot perform authentication and therefore gain access through his/her First Access Card.
- Restores previously configured account policy settings. The user is prompted to enter a new password the next time he/she logs on.

*A disabled First Access card (as long as the specific user has not been deleted through the **User Manager**) can be re-enabled at any time.*

In this case, all previously configured authentication and authorization settings are restored.

1 From the ***User Manager***, double-click on the required user's name to call up the ***User Properties*** panel.

2 Clear the ***Enable First Access Card*** checkbox to disable the First Access card and restore standard password policies.

Enable and Disable Card *occurrences are among the* ***Extended Events*** *that can be audited and reviewed through the* ***Security Log*** *of the* ***Event Viewer****. For more information, refer to* **Chapter 4 - First Access Integration with User Manager, "Setting Policy Options" on page 47**.

Initializing First Access Cards

In order to provide the highest level of security to the network and organization, First Access Cards are supplied with no identifying elements. They have to be embedded with the necessary data to facilitate automatic identification by the Sensor; this process is termed initialization. The Sensor 'detects' the presence of a user through the Card and 'identifies' the user through the Card ID.

- First Access Cards can be initialized only by the administrator.
- Data is embedded using IR technology thus maintaining the highest security.
- Initialization generates a unique Card ID; since the ID is automatically generated, it is unique, preventing the possibility of duplication.
- The Card ID is relayed to the on-screen image of the Card when advertised. The ID, variously referred to as the Card ID and Token ID serves as the unique identifier of a First Access user.
- Cards can be initialized from the ***User Properties*** panel or from the ***Card Manager***. Both of these utilities are accessed from the ***User Manager***.

If you have selected ***First Access Card Initialize*** *among the events to be audited, you can track the successful and/or failed occurrences of card initialization for a particular user through the* ***Event Viewer****. For more information, refer to* **Chapter 4 - First Access Integration with User Manager, "Setting Policy Options" on page 47**.

Before initialization, insert the supplied batteries in the slots.

From User Properties

This is a quick way of initialization and can be chosen for instance to initialize First Access Cards after installation.

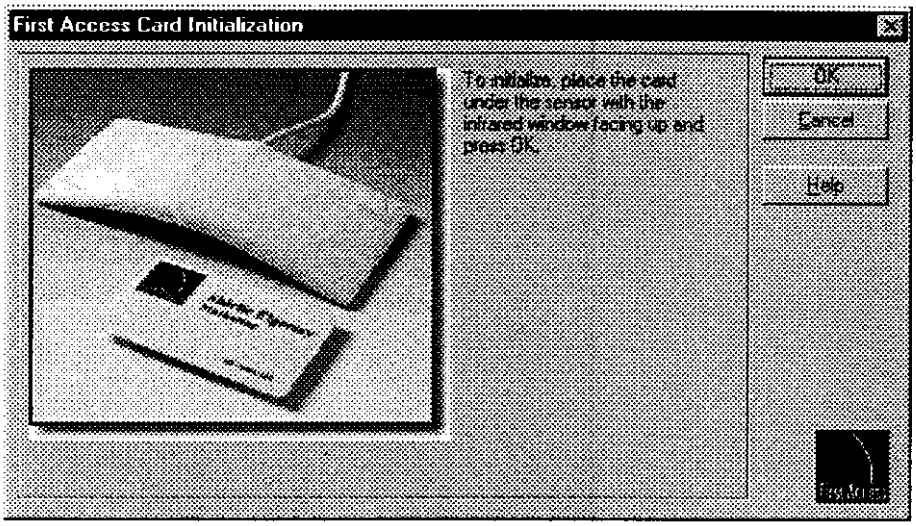
1 From the User Manager, select an existing user to call the ***User Properties*** panel.

2 From the ***User Properties*** panel, select the ***Enable First Access User Card*** option.

3 Click ***OK***.

The ***Card Initialization Manager*** prompts you to insert the First Access Card beneath the Sensor.

Figure 7.1 First Access Card Initialization Interface



4 Position the card as directed and click ***OK***. A screen appears indicating successful initialization.

If you click ***Cancel****, a warning is issued that the particular user has not been recorded in the First Access database. He/she is recorded as a regular user.*

From Card Manager

1 From the ***User Properties*** panel, click on the ***1st-Access*** button to access the ***First Access Card Manager***.

2 If the ***Enable First Access User Card*** option has not been selected, select the option.

3 Click on the ***Details*** tab in the Card Manager. The Card ID field displays an ID of 0, indicating that card has not been initialized.

4 Click ***Initialize***.

The ***Card Initialization Manager*** prompts you to insert the First Access Card beneath the Sensor. See Figure 7.1.

5 Position the card as directed and click ***OK***. A screen appears indicating successful initialization.

Configuring Security Attributes

The security attributes of a First Access user relates to configuring various settings that influence the behavior of the First Access Card™. The ***First Access Card Manager*** is the principal tool to configure the security profile of a First Access user.

The Card Manager provides you, the administrator with a centralized point from which to build and maintain security attributes. The user's security attributes are stored in the First Access database.

Through the Card Manager, you can:

- Initialize/re-initialize First Access Cards
- Configure security attributes of First Access users, relating to authentication, verification and authorization.

The First Access Client™ reacts with the First Access Server™ to authenticate the users based on the settings defined through the ***Card Manager*** and stored in the database.

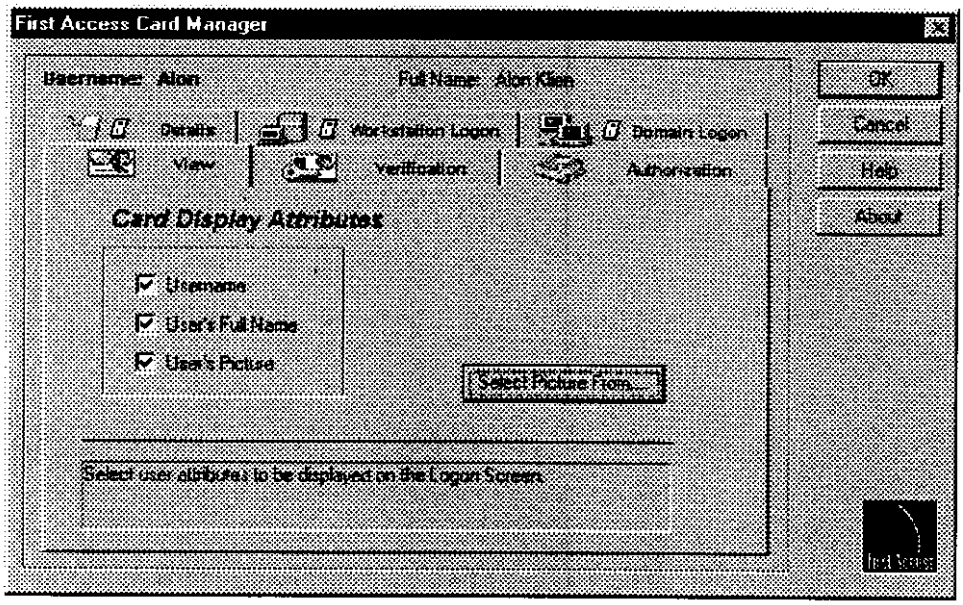
Any changes made to a First Access user's authentication profile are effective in real time. This feature is unlike Windows NT, where changes to user rights are made effective only after OS log-off and re-logon. You can continually assess the work situation and implement the necessary changes immediately.

Accessing the Card Manager

1 In the ***User Properties*** panel of a user, verify that the ***Enable First Access Card*** check-box is selected.

2 Click on the *1st-Access* button. The ***First Access Card Manager*** appears.

Figure 7.2 One of the panels of the First Access Card Manager



The ***First Access Card Manager*** has a tabbed interface, common in windows-based applications.

The ***User name*** and ***full name*** (if defined) displayed on top, identifies the user whose security settings are being configured.

The categories of security attributes are classified under relevant tab headings. Each tab corresponds to a specific attribute and has a dialog panel that you will have to work with to define requirements.

You can access the required panel by clicking on the corresponding tab.

The options in each panel are provided as check boxes or radio buttons which have to be selected/deselected, as appropriate.

The Status line below, provides a brief description of the current panel.

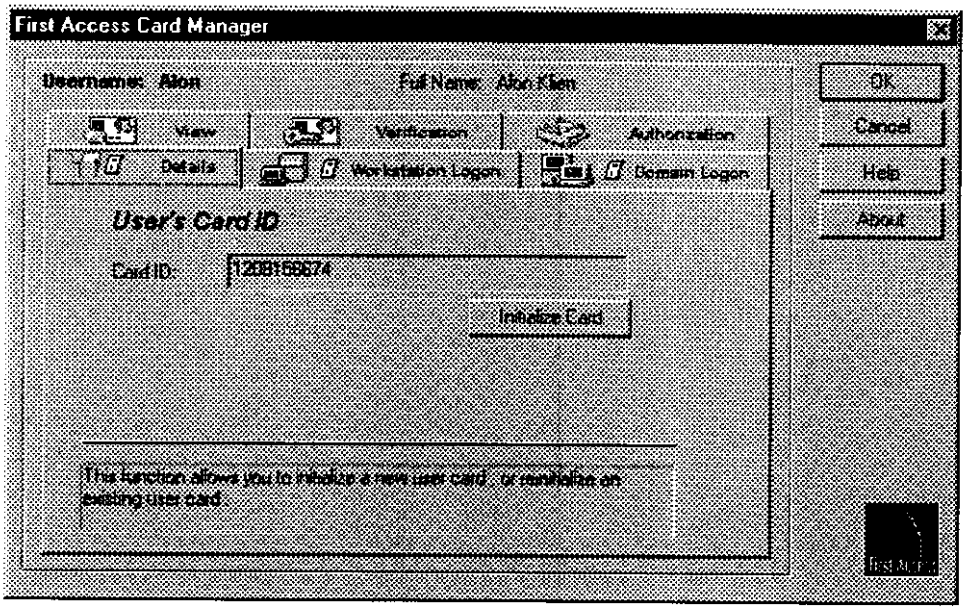
In addition, common to all panels are the standard functional buttons:

- ***OK*** – confirm and enforce all settings
- ***Cancel*** – cancel all current changes and return to original settings
- ***Help*** – access on-line help
- ***About*** – details on the First Access product/interface such as version number, etc.

Viewing /Changing Card ID

- Click on the ***Details*** tab. The Card ID panel is displayed.

Figure 7.3 Initializing the Card ID by changing the Card ID



Selecting Card's Display Attributes

Display attributes affect the appearance of a user's card on the logon screen. These attributes are presented as check-box options.

The Card ID automatically appears on every First Access Card.

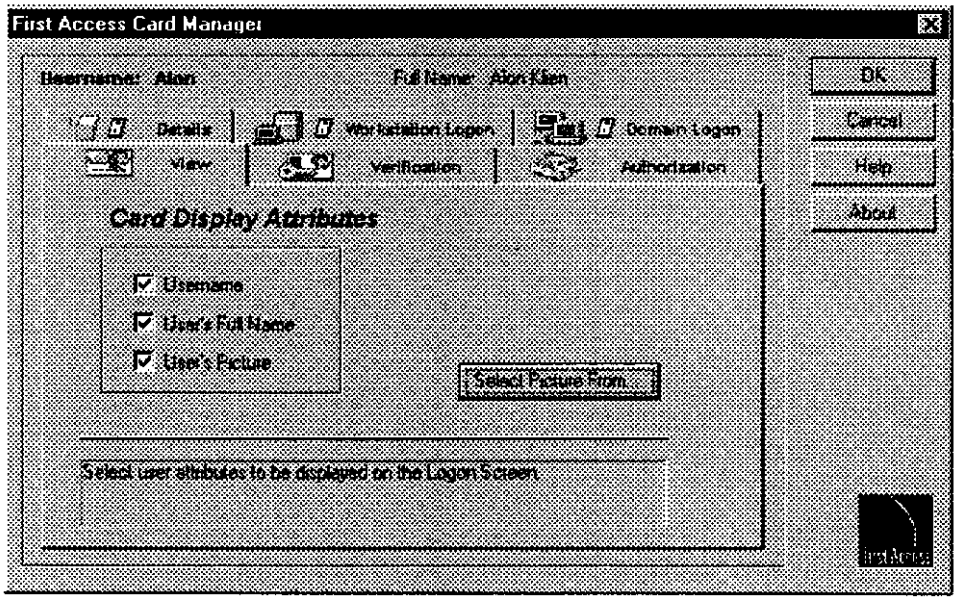
You can select a:

- Single attribute
- Combination of them
- None of them

By default, all attributes are selected.

1 Click on the *View* tab to access the view panel.

Figure 7.4 Setting the attributes for the user's Card Image



The following details can appear on an advertised First Access Card:

- ***Username*** – Name of user as assigned in ***User Properties***; usually the first name
- ***User's Full Name*** – Full Name as assigned in the ***User Properties***
- ***User's Picture*** –user's picture

The ***Select Picture From*** button allows you to browse and select the appropriate picture. The accepted picture format is ***bmp*** – a standard graphics format and the picture size cannot be more than 50 KB.

Click ***Open*** to confirm; the selected picture appears on the panel.

The picture has been loaded into the database and remains until you specifically change it.

If you decide not to use the picture, simply deselect the check box. This action ensures that the picture is not displayed on the user card.

2 Select required attributes.

Enforcing PIN Code Verification

First Access provides the option of PIN entry verification as a secondary requirement for authentication. You can enforce this over and above specific authentication modes, as an additional security measure.

The PIN can be an alphanumeric string of up to a maximum of fourteen characters.

You can define PIN policies on two levels:

- System-wide policies
- User specific policies

System wide policies concern the general implementation and management of PIN policies for all First Access users and are set through the ***Verification*** panel.

Since PIN entry is not mandatory for all users, you can control how user specific PIN requirements are implemented. These requirements are defined through the two ***Logon*** panels.

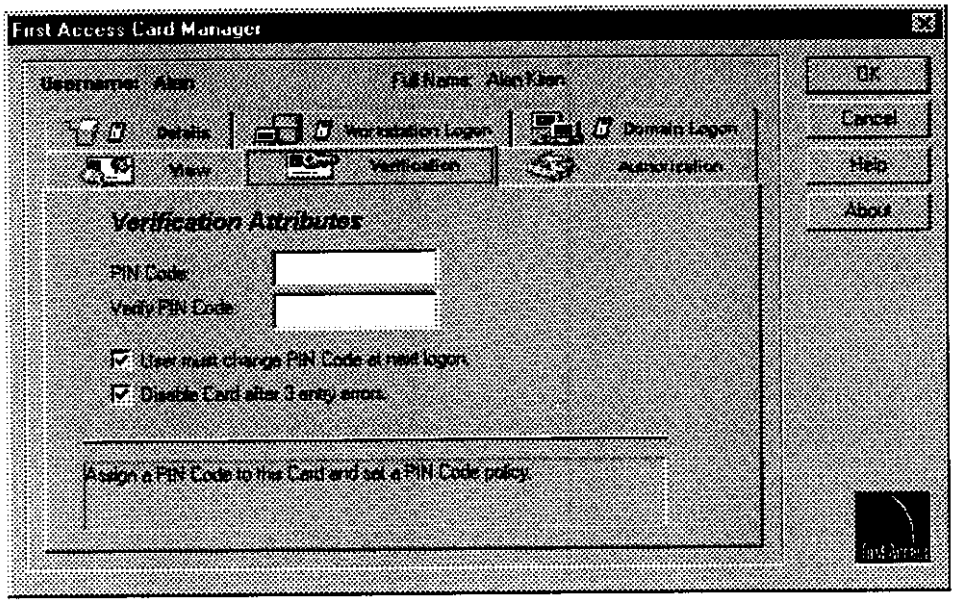
You can track the successful and/or failed occurrences of PIN Code entries for a particular user through the ***Event Viewer****.*

Setting System-wide PIN Policies

These policies are automatically effective if and when you activate PIN Code verification as an authentication requisite for a particular user.

1 Click on the ***Verification*** tab to access the panel:

Figure 7.5 Defining system-wide PIN Policies



2 If desired, in the PIN code text box, enter a null or neutral PIN Code for the user.

3 To force the user to enter a new PIN Code at the ensuing logon, select the check box for ***User must change PIN Code at next logon***.

Once the user enters a new PIN Code, this option is automatically deselected in the ***Card Manager****.*

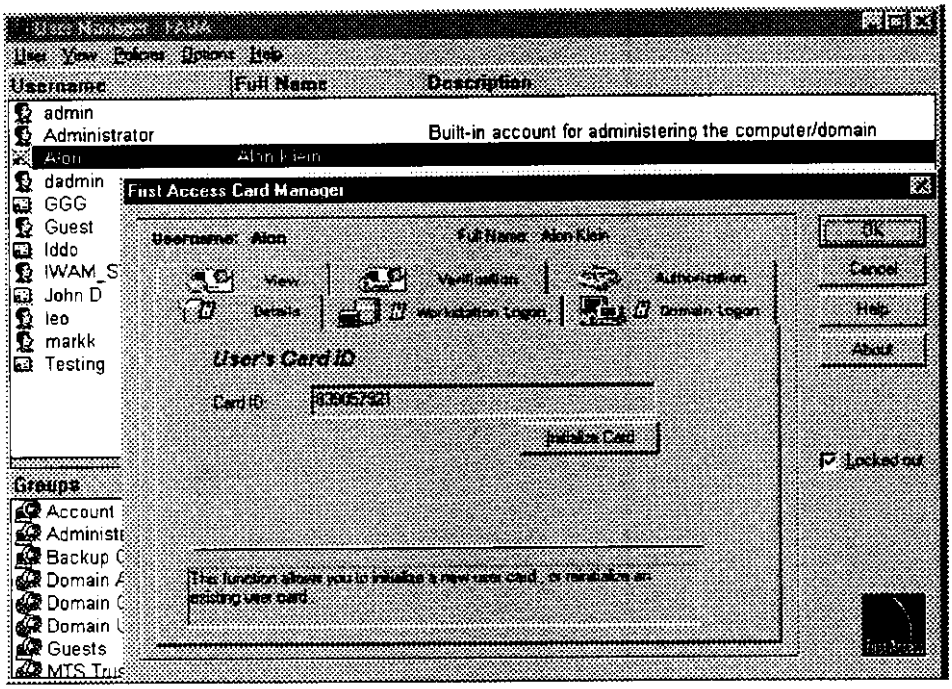
To force a change of PIN Code for the same user again, you have to reselect the option.

4 In order to automatically enforce Card lockout after three consecutive errors in PIN entries, select ***Disable Card after three entry errors.***

A locked out Card is flagged simultaneously:

- In the ***Logon Information window***; the label on the advertised card reads 'locked out'.
- In the ***Card Manager***; a locked-out card is indicated by the ***Locked Out*** check box (appears below the standard function buttons). See Figure 7.6.
- In the ***User Manager*** window; where the card icon appears with a red cross over it. See Figure 7.6.

Figure 7.6 Card Lockout status signalled simultaneously in User Manager Window & Card Manager



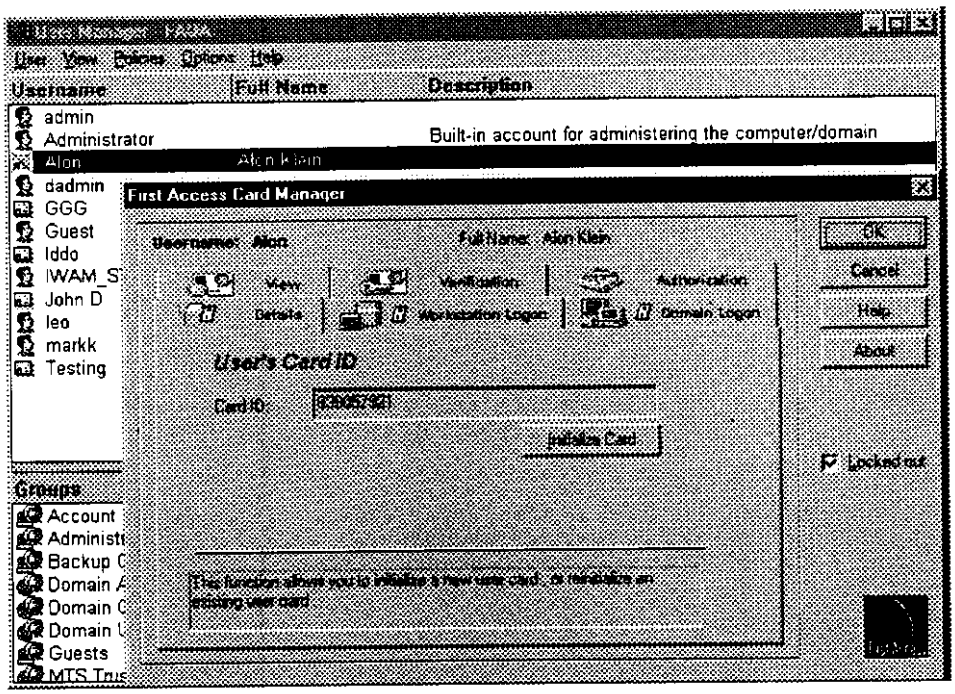
A locked out card can be reactivated only through the Card Manager by clearing the ***Locked Out*** check box.

4 In order to automatically enforce Card lockout after three consecutive errors in PIN entries, select ***Disable Card after three entry errors***.

A locked out Card is flagged simultaneously:

- In the ***Logon Information window***; the label on the advertised card reads 'locked out'.
- In the ***Card Manager***; a locked-out card is indicated by the ***Locked Out*** check box (appears below the standard function buttons). See Figure 7.6.
- In the ***User Manager*** window; where the card icon appears with a red cross over it. See Figure 7.6.

Figure 7.6 Card Lockout status signalled simultaneously in User Manager Window & Card Manager



A locked out card can be reactivated only through the Card Manager by clearing the ***Locked Out*** check box.

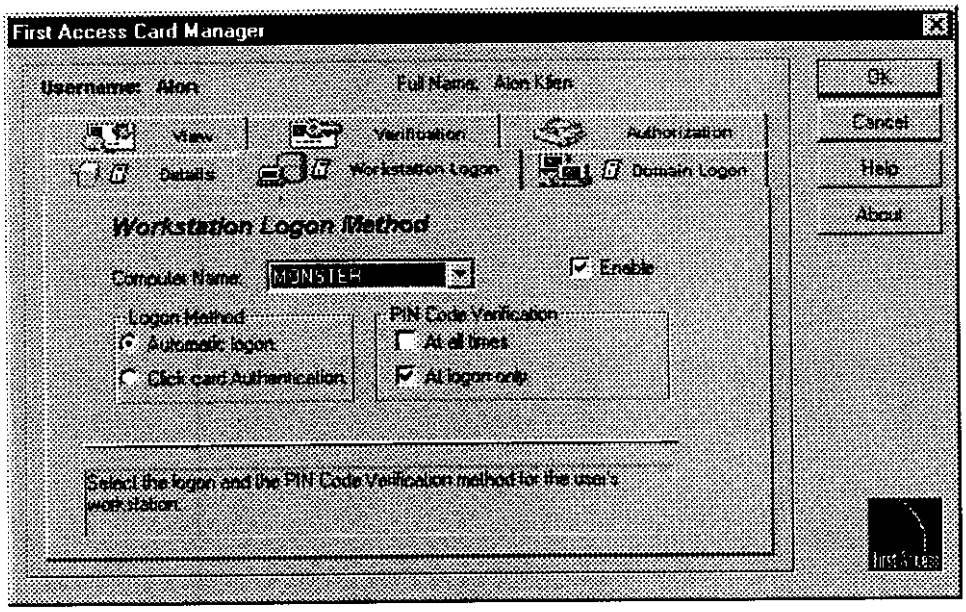
Specifying Authentication Settings

If your network is implemented on the domain model, you will have to define authentication settings for the same user on two parallel levels.

Workstation Authentication Settings

1 Click on the ***Workstation Logon*** tab to access the corresponding settings.

Figure 7.7 Defining Validation & PIN Code Verification for Workstation



2 Specify the validation-mode by clicking on the appropriate radio-button:

- If the user is to be validated on approach after passing identification, select ***Automatic validation***. This is the default.
- To validate the user only on correct identification of advertised card, select ***Click-card validation***.

3 Optionally, enforce PIN Code verification by selecting either or both options:

- To force user to enter the PIN Code during initial workday logon and on re-authentication, select the ***At all times*** option.
- To prompt for a PIN entry only during initial workday logon, select the ***At logon only*** option.

Domain Authentication Settings

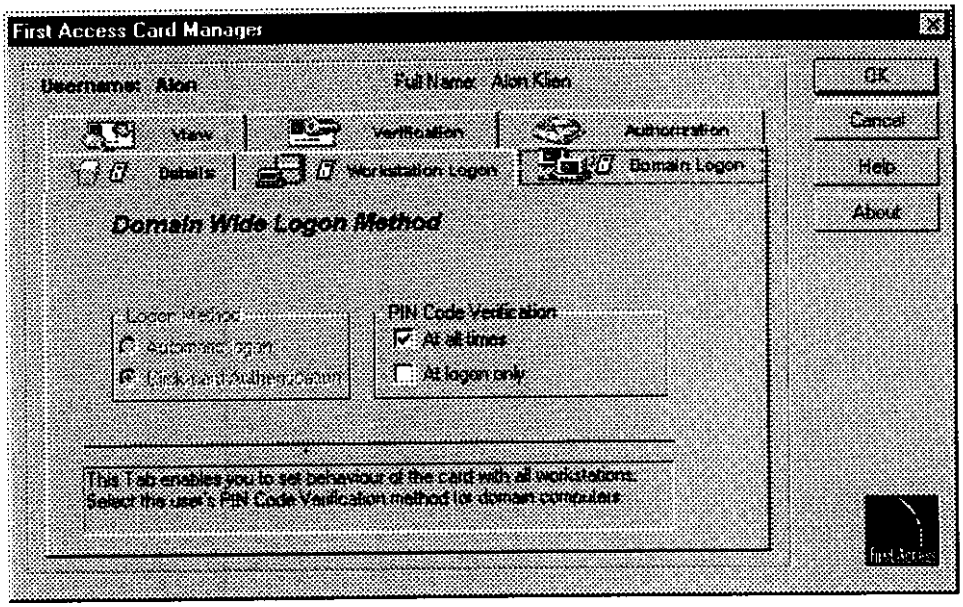
Each user account has optional list of workstations to which the domain user can logon. ***Click-card validation*** is the default and the only viable method for domain wide logon.

*User access to workstations in the domain can also be restricted to those defined in the **Logon Workstation** dialog (accessed through the **Logon To** function button). For more information refer to Chapter 4- First Access Integration with User Manager.*

A First Access user attempting authentication at a restricted workstation will be denied access. The advertised card will display a label intimating the relevant information.

1 Click on the ***Domain Logon*** tab to access the settings.

Figure 7.8 Defining Validation & PIN Code Verification for Domain



2 Optionally, enforce PIN Code verification by selecting either or both options:

- To force user to enter the PIN Code during initial workday logon and on re-authentication, select the ***At all times*** option.
- To prompt for a PIN entry only during initial workday logon, select the ***At logon only*** option.

Defining Peripheral Authorization

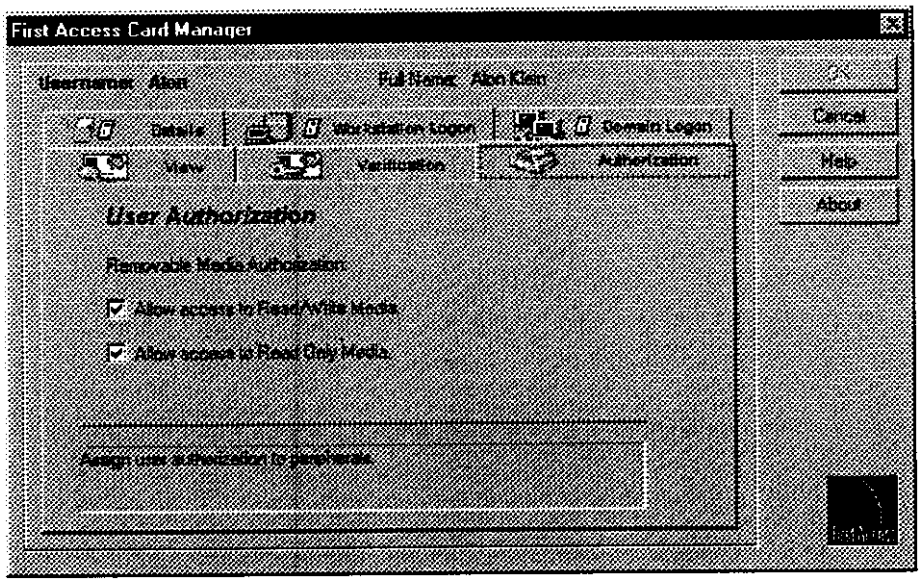
CD-ROM drives and floppy drives are standard peripheral equipment of most computers. Control over removable media is a vital and desirable feature of any security policy and offers several benefits.

The most obvious advantage of disabling the CD-ROM and the floppy drives is that it will prevent the user from booting through these devices and compromising the system. Chances of viruses entering the system are also greatly reduced. Finally, you can also effectively block potential exit points for proprietary information.

You can apply these controls on an individual user basis, and either disable access to both types of media or selectively impose the required restrictions.

1 Click on ***Authorization*** to access the panel.

Figure 7.9 Defining the Authorization Policy

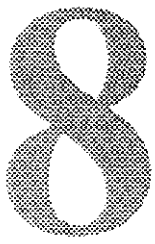


2 Proceed as follows:

*If changes are made to the **Authorization** settings of a user when he/she has already initiated a work session, the changes are effective only after logoff and relogon.*

- To restrict access to read-only media, select ***Allow access to Read Only Media***.
- To restrict access to read/write media, select ***Allow access to Read/ Write Media***.
- To disable access to both types of removable media, select both check box options.

CHAPTER



First Access - End User Authentication

Initial Logon

The mode of logon depends to an extent on the type of system that the client workstation is running. First Access Enterprise currently supports WIndows NT workstations and Windows 95/98 systems as clients.

Windows 95 Clients

Since Winlogon is not a feature of Windows 95 systems, booting or rebooting the computer brings up the First Access Logon Information Window instead of the traditional dialog box requiring the username and password.

Booting in Safe Mode

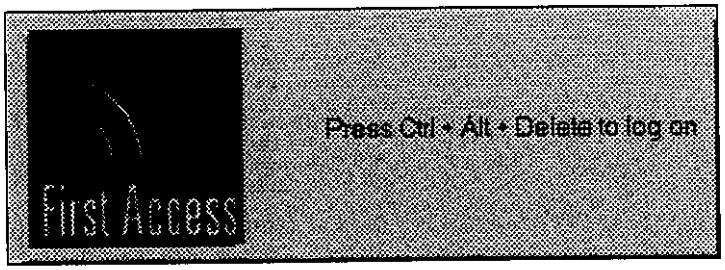
Installing the First Access system does not prevent booting in Safe mode with/without network support.

First Access users can manually access the resources on the local computer since blank passwords are permitted. Network access, however, is completely disabled.

Windows NT Clients

Windows NT clients start with a secure logon process, the secure attention sequence. The standard SAS in Windows NT is the *CTRL+ALT+DEL* key combination. The First Access system has chosen to retain this SAS; the First Access logo that appears indicates that the client workstation is First Access protected.

Figure 8.1 The SAS with the First Access Logo



The First Access Logon Information Window

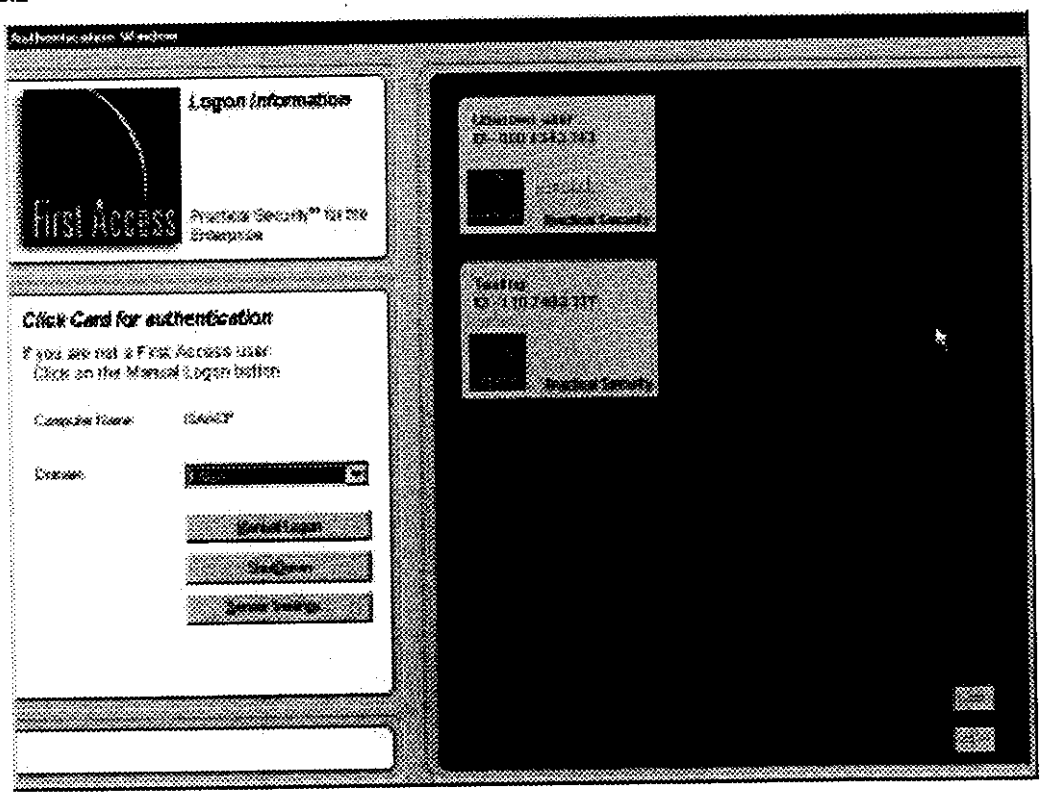
User identification and authentication through the Graphical Identification and Authentication module or the GINA forms the second component of the logon process.

The authentication interface is identical for both Windows 95/98 and Windows NT client systems.

The ***Logon Information*** window has two panels:

- The panel on the left displays general information on required actions and interactive tools in the form of buttons and the Domain combo-box.
- The panel on the right displays all the First Access Cards in the vicinity as detected by the First Access Sensor.

Figure 8.2



Navigational Aids

- Use the tab key to move from field to field

Selecting the Domain

The Domain combo-box displays the available domains. The following domains are generally displayed:

- Primary domain
- Trusted domains
- Local domain

Windows 95/98 systems display only the primary domain.

The system remembers the last domain logged into which is displayed in the drop down text box. If necessary the user attempting to perform authentication can select the correct domain from among the list of available ones.

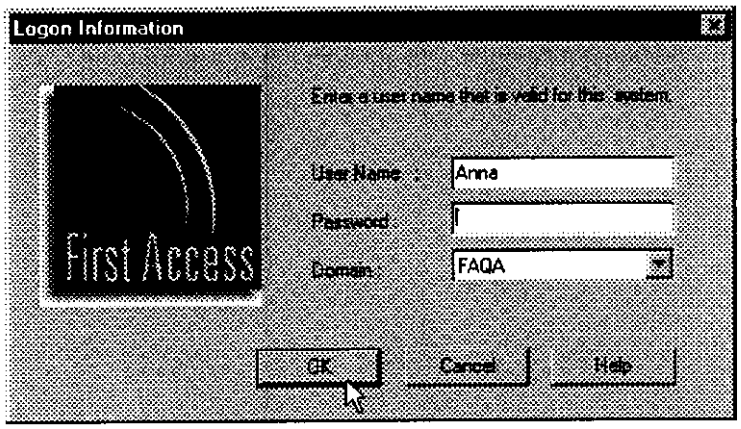
If the user does not have an account in the current domain, his/her First Access Card appears as 'invalid'.

Performing Manual Logon

The Manual logon option facilitates log on for those users not registered as First Access users. If a First Access user has problems performing authentication, the Manual logon button can be used for troubleshooting by users with administrative rights.

Clicking on the ***Manual Logon*** button accesses the ***Logon Information*** screen where the user is required to supply the username and password.

Figure 8.3 The Manual Logon Screen



Here again, the NT functionality of retaining the user name and domain of the last logon is maintained and these details are displayed in the relevant text boxes. The only input required from the user is the password. If necessary, a different domain can be chosen.

A checkbox option allows the user to avail of RAS, if so configured.

Performing Shutdown

The ***Shutdown*** button can be used to perform system shutdown before logging on. Clicking on the ***Shutdown*** button prompts a confirmation from the user to exit or restart the system.

Browsing and Selecting Cards

First Access cards are advertised on the right panel. They are displayed in columns and arranged in ascending order of appearance.

- To view cards that may not be visible on the screen, click the left/right scroll arrows on the bottom right of the window.
- You can select a card only when the focus is on the Card. To move focus to a particular card:
  - Press the tab key repeatedly until the focus is on the required card.

  OR

  - Press ALT + the correct numeric key to move the focus to the required card.
- To select the card, press ***ENTER*** or click on card.

Quick Troubleshooting

The Logon Information window provides continuous status updates to the user.

Card Display

The First Access Sensor being capable of multi-card identification, several First Access Cards may be advertised in the Logon Information Window at any one time. The label on each card displays the status of the card user.

- Disabled - appears if the ***Enable First Access Card*** option has been deselected.
- Invalid - appears if the advertised card does not have a user account in the current domain.
- Denied - this label appears in the following situations:
  - Access attempted when account is disabled
  - Access attempted after allowed logon hours
  - Access attempted from a restricted workstation
  - Access attempted after account expiry

- Locked out- appears as a result of three consecutive errors in PIN Code. The ***LOCKED OUT*** button appears in the Card Manager indicating this status. The administrator has to click on the button to re-activate the card.

Hardware

- Sensor Connection - if the Sensor at the workstation is not connected, an icon appears

Client/Server Communication

- If the PDC is offline, an icon appears indicating that the database cannot be updated.

Authentication

The authentication procedure is affected by several factors:

- The First Access Card: A First Access User has to have the First Access Card on his/her person.
- User's authentication profile: Primarily, authentication depends on the user's authentication profile defined in the Card Manager.
- Logon restrictions: Other factors influencing First Access user authentication would be restrictions imposed by the logon functions relating to operating hours and workstation access. Refer to **Chapter 4 - First Access Integration with User Manager**.
- Server/client communication: a breakdown in the PDC or BDC. If there are problems with the PDC, the user can still authenticate himself/ herself against the BDC. Changes in data such as new PIN codes are not updated.
- Sensor connection: if the Sensor is not properly connected, authentication will not be possible.

Authentication involves passing identification, validation and optionally verification controls.

Automatic Validation

If ***Automatic validation*** has been assigned, the user bypasses the logon information window. This happens when the user attempts logon to the workstation assigned to him/her.

Automatic validation will not be performed in the following instances:

- If two users assigned the same workstation, both of whom are assigned ***automatic validation*** approach the computer at the same time, automatic validation is not valid; instead both cards are advertised; either user will have to click on his/her card to perform validation.
- If two users, one assigned automatic validation and the other with click-card validation approach the computer; both cards are advertised; either user will have to click on his/her card to perform validation.

Click-card Validation

With ***Click-card validation***, the user has to identify and select the correct card from the cards advertised.

PIN Code Verification

PIN requirements can be different for workstation and domain logon respectively through the two Logon panels in the First Access Card Manager.

If so configured, a First Access user attempting logon for the first time is prompted to enter a new PIN Code.

Thereafter, also depending on the configuration, the user might have to verify his/her PIN Code on initial logon or at all times (after **AutoLock™** etc.).

The Card Lockout option is another powerful option, which if selected can neutralize a user's Card after three consecutive errors in PIN entry.

If the user enters the wrong PIN code twice and returns to the Logon Information screen by clicking the **MAIN** button a fresh entry attempt is initiated.

Illegitimate Card Lockouts can also occur. Consider the following scenario. (users have to be alerted of inadvertent ***card lockout***):

- User A has already logged on to his workstation. User C approaches another workstation. All the First Access Cards in the vicinity are advertised in the Logon Information window, including that of User A.
- If User C clicks on the Card of User A and is prompted for a PIN Code which he/she does not know, three errors causes Card Lockout.
- As long as User A continues working, nothing changes. But in the event of having activated **AutoLock™** or logoff and relogon, authentication will not be possible.

After Authentication

User Environment Profiles

Clients logging on to Windows 95/98 systems in the domain will access the preferences and desktop settings associated with the particular PC. 'Roaming profiles' are supported only on Windows NT workstations.

Screen Savers & Password Protection

Since, dual categories of passwords are a feature of Windows 95/98 systems, First Access users can activate the password protected screen saver feature.

For Windows NT workstations, since the screen saver password is the same as the system password, this option is disabled for First Access users.

User Access to Removable Media

Once the First Access user has been successfully authenticated, he/she is logged on and can generally perform work as usual.

For the duration of the work session, all activity proceeds according to the user rights and privileges as established by the user's account. Apart from the access restrictions that can be imposed on the user, a First Access user is assigned an authorization profile. The authorization settings control user access to removable media such as floppy diskettes and CDs.

User access can be restricted to:

- Read only media such as CD-ROMs
- Read/write media such as floppy diskettes

Workstation AutoLock™

The **AutoLock™** function is an integral feature of **Vicinity Authentication™**. It provides real-time desktop protection by automatically disabling access to a user's computer, when left unattended for a certain amount of time.

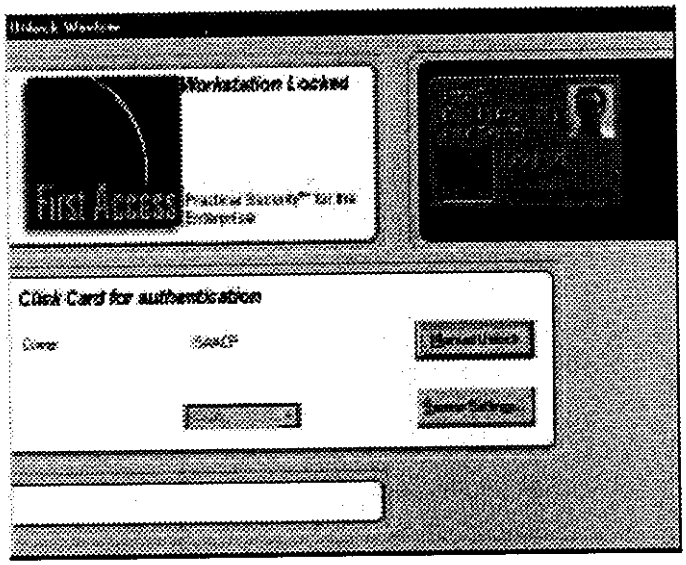
It is especially significant in the context of operating systems like Windows 95/98 which lack the logged on security functions (those in the NT Security Window) that are available to NT users.

The effectiveness of **AutoLock™** is that regardless of the client system, it is a completely automated, stable and secure mechanism providing continuous protection while eliminating user intervention.

On Windows 95/98 client systems, if the Close Window is on the screen, **AutoLock™** *is not activated until it is closed.*

This function is facilitated through the **First Access Sensor™** which continuously polls the area within its range for the Card and automatically disables access when it does not detect the Card.

Figure 8.4 The Unlock Window

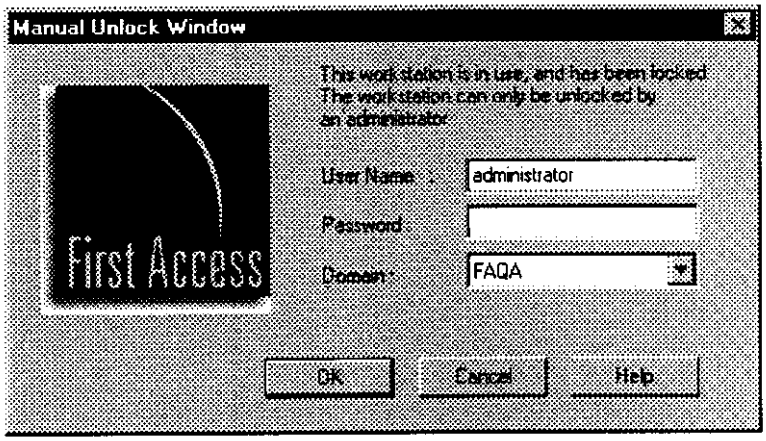


The Unlock Window Indicates that an authenticated First Access user has initiated a work session. Desktop access is therefore automatically denied to all other users.

- The color of the Card serves as a pointer to the user's current location, that is, within the Sensor's detection range or beyond, as shown in the following figures.

The workstation can be unlocked only by the logged on user by performing re-authentication. Alternatively, a user with administrative rights (for Windows NT clients only) can forcibly log off the current user and unlock the workstation.

Figure 8.5 Forced Administrative Logoff through the Unlock Window



You can remotely identify a 'locked' workstation from the User Manager for Domains window, through the crossed-out Card icon that appears alongside the username. For more information, refer to **Chapter 4 - First Access Integration with User Manager, "User Manager Window" on page 41.**

Sensor Configuration

The distance at which the Sensor can detect and identify the First Access e Card is variable and can be set per workstation. Since Sensor/Card communication is carried out through RF, the distance cannot be arbitrary. The optimum distance is influenced most obviously by the density of workstations in the work environment.

Sensor settings can be modified by end users directly from the ***Logon Information***, ***Unlock*** *windows. For Windows NT users, this button also appears in the* ***Security Window***.

To access the Configuration Manager:

- From the ***Logon Information Window***, click on the ***Sensor Settings*** button.

OR

- From the ***Unlock Window***, click on the ***Sensor Settings*** button.

OR

- From the ***Security Window***, click on the ***Sensor Settings*** button.
-

To set the Sensor's sensitivity:

Sensor Sensitivity refers to the distance at which or from which the Sensor can detect a First Access Card.

- Click on the ***Sensitivity*** tab.
- Click on the range desired.

To set the timeout:

- Click on the ***Timeout*** tab.
- Type in required time (calculated in seconds)

Logged on Security Functions

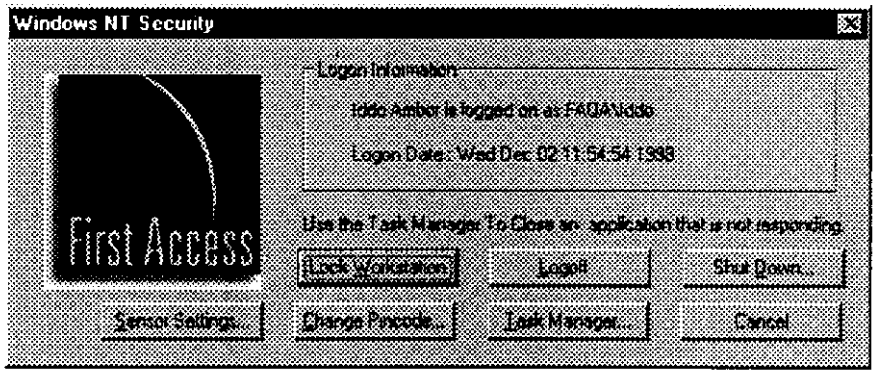
Users of Windows NT can access a number of standard security functions from the NT Security Window. As with any of the functions thus activated, only the logged on user who initiated the action or a domain user with administrative rights can counter the action.

*On client computers running Windows 95/98, pressing CTRL+ALT+DEL brings up the **Close Window**. For the duration that this window remains on screen, no action, including **AutoLock** is possible.*

Invoking the Windows NT Security Screen

- Press *CTRL+ALT+DEL*.

Figure 8.6 The Security Window



- Click on required button to activate function

Lock Workstation

Locks an in-use workstation, disabling access to all users. The workstation can be unlocked by the logged on user or by a user with administrative rights.

If the function was activated by a First Access user, then that user has to perform re-authentication.

- If a regular user presses *CTRL+ALT+DEL*, the ***Unlock Window*** appears displaying the authorized user's Card.

- If the workstation remains locked indefinitely, the administrator or a domain user with administrative rights can perform unlock through the ***Manual Logon*** button.

Logoff

End user's current working session.

System prompts to confirm.

- After complete log-off, any other authorized user can gain access.
- In the event of an incomplete log-off (prompt is unconfirmed), access remains denied to all other users.
- Only a domain-member user with administrative rights can circumvent this situation by clicking the ***Manual Unlock*** button and logging-off the current user. A prompt appears to this effect with the warning that any unsaved work will be lost.

Shutdown

Shutdown and switch-off computer.

- In the event of an incomplete shutdown, (prompt is unconfirmed), access remains denied to all other users.
- Only a domain-member user with administrative rights can circumvent this situation by clicking the ***Manual Unlock*** button and logging-off the current user. A prompt appears to this effect accompanied by a warning that any unsaved work will be lost.

Task Manager

Access the ***Windows Task Manager*** to close an application that is not responding.

Change PIN Code

Can be used to manually change a PIN Code. Clicking on this brings up the *New PIN Code* screen.

If the user changes his/her PIN when the PDC is off-line, the change is not updated.