ACE/Client for Windows NT
Local Authentication
with a Standard SecurID Card or Key Fob

You have been assigned a standard SecurID® Card or Key Fob to use when logging in. These security tokens generate and display unpredictable codes that change at a specified time interval (typically every 60 seconds).

To gain access to the protected system, you must enter a valid SecurID PASSCODE™, which is made up of two factors:

- your secret, memorized personal identification number (PIN)
- and the code currently displayed in your SecurID Card or Key Fob

With a conventional security system it is easy for someone to learn your password and log in under your identity. Requiring two factors ensures reliable identification and authentication.

Because this system creates an audit trail that cannot be repudiated, you may be held accountable for activities recorded identifying you as the perpetrator. Avoid the unauthorized use of your identity and privileges by protecting the secrecy of your PIN and the possession of your token. Read “User responsibilities” on page 5 to learn about your obligations as a tokenholder.

Before you begin

Have the administrator fill in the following information before you attempt to log in for the first time.

If you have any questions contact your security administrator, ________________________, at extension _____________.

□ The system will assign a PIN to you; you cannot create your own.
Read “Receiving a system-generated PIN.”

□ You will be allowed to use a PIN that you make up yourself.
Read “Creating your own PIN.”

□ Your PIN may contain letters as well as digits.

□ All PINs on the system must be the same length: ____ characters.

□ Your PIN may contain from ____ through ____ characters.

□ You will have a duress PIN.

Receiving a system-generated PIN

1. Initiate a login session. After you respond to the usual prompt for your login, the system will prompt you to enter a PASSCODE.

*For security reasons, responses to the **Enter PASSCODE** prompt are not displayed.*

2. If you have never received a PIN before, at the **Enter PASSCODE** prompt, type the code that is currently displaying in your SecurID token.

   If your token previously had a PIN and the administrator did not clear it when setting it into New PIN mode, enter the old PIN followed by the code that is currently displaying in your SecurID token.

3. Click **OK**. (If the system displays **Access Denied**, try again.)

   Once you have entered a valid tokencode, the New PIN dialog box will display.

4. Click **OK**.

1. You will be asked if you are ready to receive your new PIN. Make sure that no one can see your screen, then click **Yes**.

A system-generated PIN is displayed for 10 seconds or until you click **OK**. Memorize the PIN; DO NOT WRITE IT DOWN.

1. Wait for the tokencode on the card to change, and then follow the instructions in “SecurID authentication” on page 3.

Creating your own PIN

1. If you are going to create your own PIN, first give some thought to what it will be. Do not pick an obvious number like a birthday or phone number.

2. Initiate a login session. After you respond to the usual prompt for your login, the system will ask you to enter a PASSCODE.

   If you have never received a PIN before, at the **Enter PASSCODE** prompt type the code that is currently displaying in your SecurID token.

   If your token previously had a PIN and the administrator did not clear it when setting New PIN mode, enter the old PIN followed by the code that is currently displaying in your SecurID token.

3. Click **OK**. (If the system displays **Access Denied**, try again.)

4. Once you have entered a valid tokencode, the new PIN dialog box will display.

   There are two possibilities for New PIN creation:

   - You will create your own PIN
   - You will have the system generate a PIN for you

   If you want the system to generate a PIN for you, select the **Receive a system-generated PIN** radio button, then follow steps 4-6 in “Receiving a system-generated PIN.”

Make up a PIN that cannot be guessed easily.

If you want to create your own PIN, click the **I will create PIN** radio button. Enter your PIN, and press TAB. Enter your PIN again to confirm.

1. Click **OK**.

   If your PIN is acceptable, the system will prompt you to wait for the code on your token to change, and then you can log on.

   If any of the following messages displays, correct the error and try again:

   PIN and confirmation do not match.
   PIN must be 4-8 digits.
   New PIN rejected.

   If you are still denied access, contact your security administrator.

2. Once your PIN is accepted, wait for the next tokencode, and then follow the instructions in the next section "SecurID authentication."

SecurID authentication

The procedure in this section is the one you will follow whenever you need to be authenticated.

1. At the **Enter PASSCODE** prompt, type your PIN followed by the tokencode currently displaying in your card or key fob.

2. Click **OK**.

   If you have entered a valid PASSCODE, your Windows NT desktop will be displayed.

   Once accepted, a SecurID PASSCODE cannot be used again. To log in again, you must wait for a new tokencode to appear. The stack of countdown indicators on the left side of the LCD lets you know how soon the code will be changing.

   If the system displays **Access denied**, you may have typed in your PASSCODE incorrectly. Try again.

   If you are repeatedly denied access even though you are typing your PASSCODE correctly, contact your security administrator.

The “Next Tokencode” prompt

On occasion, even after you have typed your PASSCODE correctly, the system will ask you to enter the next tokencode that appears in order to confirm your possession of the SecurID token.

Wait until the tokencode changes, and carefully type the new one. Click **OK**.

If you are not granted access after correctly entering the next tokencode, contact your security administrator.

Duress PINs

If your system has the duress PIN option installed, you have two PINs: a regular PIN and a duress PIN. Use your regular PIN for normal logins. Use the duress PIN if you are ever forced to log in by an unauthorized person attempting to gain system access.

If you use your duress PIN, you will be granted access and see no difference in operation. However, the next time the ACE/Server administration program is run, the administrator will be notified that you have been forced by an intruder to log in.

Your duress PIN is your regular PIN with 1 added to it but with no carrying. For example:

If your regular PIN is	Then your duress PIN is
243890	243891
243899	243890
ABCDEF	ABCDEG
ABCDEZ	ABCDEA

User responsibilities

You are responsible for protecting the authentication factors entrusted to you. Keep your PIN secret and protect your SecurID token against loss and theft.

If an unauthorized person learns your PIN and obtains your SecurID token, this person can assume your identity. Any action taken by this intruder will be attributed to you in the system’s security log.

For your own protection and that of the system, always take the following precautions:

þ Never reveal your PIN to anyone. Do not write it down.

þ If you think someone has learned your PIN, notify the security administrator, who will clear the PIN immediately. At your next login you will have to receive or create a new PIN to use.

þ Exercise care not to lose your SecurID token or to allow it to be stolen. If your token is missing, tell an administrator immediately. The administrator will disable it so that it is useless to unauthorized users.

þ Do not let anyone access the system under your identity (i.e., log in with your PIN and a code from your SecurID token).

þ It is essential to site security that you follow your system’s standard logoff procedures. Failure to log off properly can create a route into the system that is completely unprotected.

þ Protect your token from physical abuse. Do not immerse it in liquids, do not expose it to extreme temperatures and do not put it under pressure or bend it. Each SecurID token comes with care instructions which you should read and follow.