ACE/Client for Windows NT Remote Authentication with a SecurID PINPAD Card

You have been assigned a SecurID® PINPAD™ Card to use when logging in. This security token generates and displays 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 current tokencode generated by your SecurID card.

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 4 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."

☐ All PINs on the system must be the same length: ____ digits.
(The New PIN operation will take your card's LCD length into account and not generate or accept a PIN that is too long.)

☐ Your PIN may contain from _____ through _____ digits.
(If your card's display is smaller than this range, the New PIN operation will take this into account and not generate or accept a PIN that is too long.)

☐ You will have a duress PIN.

Receiving a system-generated PIN

1. Clear PIN entries from your card by pressing any number on the card, followed by the **P** on the lower right of the card. The display will clear and a new tokencode will show after the last of the countdown indicators has disappeared from the left of the LCD.
2. 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.*

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

   If your card previously had a PIN and the administrator did not clear it when setting New PIN mode, enter the old PIN into the card and press the diamond (◆) near the bottom of the card. At the **Enter PASSCODE** prompt, type the code that displays in the card.

4. Press RETURN. If you have entered the code incorrectly, the system will display **Access denied**. Try again. Once you have entered a valid tokencode, you will be prompted to perform the New PIN operation:

   Press <Return> to generate a new PIN and display it on screen
   or
   <Ctrl d> to cancel the New PIN procedure:

5. Press RETURN.

   A question is displayed:

   ARE YOU PREPARED TO HAVE THE SYSTEM GENERATE A PIN? (y or n) [n]

1. Make sure that no one can see your screen, and type **y**.

A system-generated PIN is displayed on your screen for 10 seconds.

1. Memorize your new PIN. Do not write it down.
2. Wait for the next tokencode, and then follow the instructions in “SecurID authentication” on page 3.

Creating your own PIN

Do not create a PIN that starts with a zero.

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. PINs for PINPAD cards may not begin with a zero.
2. Clear PIN entries from your card by pressing any number on the card, followed by the **P** on the lower right of the card. The display will clear and a new tokencode will show after the last of the countdown indicators has disappeared from the left of the LCD.
3. Initiate a login session. After you respond to the usual prompt for your login, the system will ask you to enter a PASSCODE.

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

4. If you have never received a PIN before, at the **Enter PASSCODE** prompt, type the code that is currently displaying in your card. If your card previously had a PIN and the administrator did not clear it when setting New PIN mode, enter the old PIN into the

card and press the diamond (◆) near the bottom of the card. At the **Enter PASSCODE** prompt, type the code that displays.

5. Press RETURN. If you have entered the code incorrectly, the system will display **Access denied**. Try again. Once you have entered a valid tokencode, you will be prompted by the New PIN operation.

   If the prompt reads:

   Enter your new PIN, containing 4 to 8 digits, or
   Press <Return> to generate a new PIN and display it on screen,
   or <Ctrl d> to cancel the New PIN procedure:

   complete this step and go to Step 7. Otherwise, go to Step 6 now.

   If you want the system to generate a PIN for you, follow steps 5-7 in "Receiving a system-generated PIN."

Make up a PIN that cannot be guessed easily.

   If you want to create your own PIN, type in the PIN you would like to use, and press RETURN.

6. If the prompt reads:

   Enter your new PIN, containing 4 to 8 characters,
   or <Ctrl d> to cancel the New PIN procedure:

   you cannot have the system generate a PIN for you. Enter the PIN you want to use. Press RETURN.

7. 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. Shield the LCD from view so that no one can see your PIN as you enter it. Enter your PIN into the card and press the diamond (◆) that appears near the bottom of the card.

Make sure no one can see the card's LCD as you enter your PIN.

   The card now generates and displays a PASSCODE with your PIN hidden in it. A small number (a "1" on most cards) on the right side of the LCD will flash off and on when there is data entered into it via the PINPAD.

2. At the **Enter PASSCODE** prompt, type the code currently displaying in your card, and press RETURN. If you have entered a valid PASSCODE, the system will display:

   PASSCODE accepted

   Once accepted, a SecurID PASSCODE cannot be used again. To log in again, you must wait for your card to change. 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 instead 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.

3. As soon as your PASSCODE has been accepted, press the **P** to clear the PIN from your card. After a PIN is entered, the next several codes generated are valid PASSCODEs. If someone were to obtain your card while the PIN is in it, that person could use your card to gain system access under your identity.

The “Next Code” prompt

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

Wait until the tokencode changes, then carefully type the new code followed by RETURN.

If you are not granted access after correctly entering the next code, 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
243860	243861
243869	243860

User responsibilities

You are responsible for protecting the authentication factors entrusted to you. Your PIN must be kept secret and your SecurID card must be protected against loss and theft.

If an unauthorized person learns your PIN and obtains your card, 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:

- Never reveal your PIN to anyone. Do not write it down.
- When entering your PIN into the card, shield it from view so that no one can see the LCD.
- Clear the PIN from your card by pressing the **P** key as soon as your PASSCODE has been accepted.
- 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.

- Exercise care not to lose your card or allow it to be stolen. If your card is missing, tell an administrator immediately. The administrator will disable your card so that it is useless to unauthorized users.
- Do not let anyone access the system under your identity (i.e., log in with your PIN and a code from your card).
- 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.
- Protect your card 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 card comes with care instructions which you should read and follow.