WebID®
Authentication with a SecurID PINPAD

You have been assigned a SecurID® PINPAD™ token to use when accessing WebID-protected URLs. This security token generates and displays unpredictable codes that change at a specified time interval (typically every 60 seconds).

To gain access to protected URLs, 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 token

With a conventional Web server security system, an intruder can easily learn your password and access sensitive data under your identity. Requiring two factors ensures reliable, highly secure identification and authentication.

Because the SecurID system creates an audit trail that cannot be repudiated, you may be held accountable for activities recorded identifying you as the user. Therefore, avoid the unauthorized use of your identity and privileges by protecting your SecurID token and the secrecy of your PIN. Read “User Responsibilities” on page 4 to learn about your obligations as a tokenholder.

Before You Begin

Contact your network administrator to obtain the following information before you attempt to log in for the first time.

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

Mark the applicable PIN conditions:

☐ The system will assign a PIN to you; you cannot create your own.
Read “Receiving a System-Generated PIN” on page 2.

☐ You will be allowed to use a PIN that you make up yourself.
Read “Creating Your Own PIN” on page 2.

☐ All PINs on the system must be ____ digits in length.
(The New PIN operation will take your token’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 token’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.

Browser Requirements

To authenticate through WebID, your browser must support HTML FORMs and Persistent Client State HTTP Cookies.

WebID supports Microsoft Internet Explorer versions 3.0 and later, and Netscape Navigator versions 1.1 and later browsers. Other browsers may work, but you should consult their manufacturers to make sure the programs support FORMs and Persistent Client State HTTP Cookies.

Receiving a System-Generated PIN

1. Clear any PIN entries from your token by pressing a number on the token followed by the **P** on the lower right corner of the token. The display will clear and a new tokencode will show after the last of the countdown indicators on the left of the LCD has disappeared.
2. Start your Web browser and initiate a login session on a protected URL. The system will prompt you to enter your username and a PASSCODE.
3. In the **USERNAME** field, enter the name you use to log in to the system.
4. If you have never received a PIN, type the code that is currently displaying on your token in the **Enter PASSCODE** field.

   If your token previously had a PIN and the administrator has not cleared it, enter the old PIN into the token and press the diamond (♦) near the bottom of the token. In the **PASSCODE** field, type the code that displays on the token.
5. Click **Send**.
   (If the system displays **Access Denied**, wait for the tokencode to change the LCD, then try again to log in.)
6. Once you have entered a valid tokencode, the "New PIN Request" page will display.
7. Make sure that no one can see your screen, and click **System Generated PIN**.
8. A system-generated PIN is displayed
9. Memorize your PIN. **Do not write it down.**
10. Wait for your token to generate the next tokencode, and then follow the instructions in "SecurID Authentication" on page 3.

Creating Your Own PIN

PINs for PINPAD tokens cannot begin with a zero.

1. If you are going to create your own PIN, give some thought to what it will be. Do not pick an obvious number like a birthday or phone number.
2. Clear all PIN entries from the token by pressing any number on the token followed by the **P** on the lower right of the token. The display will clear and a new tokencode will show after the last of the countdown indicators on the left of the LCD has disappeared.
3. Start your Web browser and initiate a login session on a WebID-protected URL. The WebID login page will appear, prompting you to enter your username and a SecurID PASSCODE.
4. In the **USERNAME** field, enter the name you use to log in to the system.
5. If you have never received a PIN, type the code that is currently displaying on your SecurID token in the **Enter PASSCODE** field.

   If your token previously had a PIN and the administrator did not clear it when setting New PIN mode, enter the old PIN into the token and press the diamond (♦) near the bottom of the token. In the **Enter PASSCODE** field, type the code that displays on the token.
6. Click **Send**. (If the system displays **Access Denied**, try again.)
7. Once you have entered a valid tokencode, the "New PIN Request" page will display, prompting you to create a PIN.

There are two possibilities for New PIN creation:

- **You will create your own PIN.**
  —Select the **I will create PIN** radio button, enter and verify your PIN in the fields, and then click **Send**.
- **You will have the system generate a PIN for you.**
  —Select the **System Generated PIN** radio button, and then click **Send**. When your new PIN appears, memorize it right away; **do not write it down**.

8. If your PIN is acceptable, wait for the next tokencode, and then follow the instructions in the next section, "SecurID Authentication."

   If any one 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.

SecurID Authentication

Follow this procedure whenever you are prompted to enter a PASSCODE:

1. In the **Username** field of the WebID login page, enter the name you use to log in to the system.

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

2. Shield the LCD of your token from view so that no one can see your PIN as you enter it. Enter your PIN into the token and press the diamond (♦) near the bottom of the token.
3. The token now generates and displays a PASSCODE with your PIN hidden in it. Enter this code in the **PASSCODE** field of the WebID login page.
4. Click **Send**.
5. If you have entered a valid PASSCODE, the protected URL will display in your browser. If the system displays **Access denied**, you may have typed your PASSCODE incorrectly. Wait for a new tokencode to appear in the LCD, then try again to log in.

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

6. Press the **P** on the lower right of your token to clear the PIN. After a PIN is entered, the next several codes generated are valid PASSCODEs. If someone were to obtain your token while the PIN is in it, that person could use your token to gain system access under your identity.

The "Next Tokencode" Prompt

On occasion, even after you have typed your PASSCODE correctly, the system will ask you to enter the next tokencode (sometimes called a "PRN") your token generates to confirm your possession of the token.

If you are prompted for a "Next Tokencode" or "Next PRN":

1. Wait until the tokencode changes, and carefully type the new one.
2. 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 enabled, 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 access to a WebID-protected URL.

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 an intruder has forced you 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 token must be protected against loss and theft.

If an unauthorized person learns your PIN and obtains your token, this person can assume your identity. Any action taken by this intruder will be attributed to you in the system's event 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 token, shield it from view so that no one can see the LCD.
- Clear the PIN from your token 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.
- Exercise care not to lose your token or allow it to be stolen. If your token is missing, tell an administrator immediately. The administrator will disable your token so that it is useless to unauthorized users.
- Do not let anyone access the system under your identity (i.e., log in with your username and a PASSCODE from your PINPAD).
- 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 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 that you should read and follow.