Authenticating with an RSA SecurID Token

You have been assigned an RSA SecurID token to use when logging in.

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

- Your Personal Identification Number (PIN).
- The tokencode currently displaying on the front of your RSA SecurID token. The tokencode changes at a specified time interval, typically every 60 seconds.

Before You Begin

Your administrator will tell you:

- Whether you are to receive a system-generated PIN or create your own
- The required length of your PIN

Completing New PIN Mode

The first time you authenticate with an RSA SecurID token, you are in New PIN mode. This is because your token is not yet associated with a PIN, which is required for two-factor authentication.

To complete New PIN mode:

1. When you are prompted for your passcode, type the tokencode currently displaying on your RSA SecurID token.
2. Do one of the following:
   - Receive a system-generated PIN.

     When prompted, indicate that you want to receive a system-generated PIN. When the system-generated PIN displays, memorize it. *Do not write it down*.
   - Create your own PIN.
     - Indicate that you want to create your own PIN.
     - When prompted, enter a PIN.
     - When prompted again, confirm the PIN.
3. Wait for the next tokencode. Depending on the type of token you have, follow the instructions in “Performing RSA SecurID Authentication with a Standard Card or Key Fob” on page 2 or “Performing RSA SecurID Authentication with a PINPad” on page 2.

Performing RSA SecurID Authentication with a Standard Card or Key Fob

To authenticate with an RSA SecurID Standard Card or Key Fob:

1. When prompted for the passcode, enter your PIN followed by the tokencode currently displaying on your card or key fob. For example, if your PIN is 1234, and the current tokencode is 800261, enter **1234800261**.
2. If your administrator has enabled Windows password integration, you are prompted to enter your password the first time you authenticate. The next time you log on, you will only have to enter your RSA SecurID passcode. If Windows password integration is disabled, you will have to enter your password each time that you log on.

Note: Once they are accepted, RSA SecurID passcodes and tokencodes cannot be used again. To log on again, you must wait for a new tokencode to appear. The new tokencode appears after the last of the countdown indicators disappears from the left of your token's LCD.

Performing RSA SecurID Authentication with a PINPad

To authenticate with an RSA SecurID PINPad:

1. Enter your PIN into the PINPad, and press the diamond (♦) near the bottom of the PINPad. A new passcode appears on the token.
2. When prompted, enter your passcode.
3. As soon as your passcode has been accepted, press the **P** on your PINPad to clear the PIN from your card's memory.
4. If your administrator has enabled Windows password integration, you are prompted to enter your password the first time you authenticate. The next time you log on, you will only have to enter your RSA SecurID passcode. If Windows password integration is disabled, you will have to enter your password each time that you log on.

The Next Tokencode Prompt

Sometimes, even after you type your passcode or tokencode correctly, the system prompts you to enter the next tokencode that appears on your RSA SecurID token to confirm your possession of the token.

To authenticate in Next Tokencode mode with a standard card or key fob:

Wait until the tokencode changes, and then type the new one. Enter only the tokencode. Do not enter your PIN.

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

To authenticate in Next Tokencode mode with a PINPad:

1. Press the **P** on the PINPad to clear the PIN from your card's memory.
2. Wait until the tokencode changes, and then type the new one.
   Enter only the tokencode. Do not enter your PIN.

Authenticating When Offline

If your administrator has enabled offline authentication, you will need to perform RSA SecurID authentication when your computer is disconnected from the network. Before you can authenticate offline, however, you must authenticate while connected to the network. After you have authenticated once while connected, you can authenticate while offline, provided offline authentication is supported for your token type as specified by your administrator.

Authenticating When Locked Out of Your Computer

Several scenarios can prevent you from accessing your computer:

- You go for a period of time without logging in, and exceed the number of days of authentication allowed by your administrator
- You exceed the number of incorrectly-typed passcodes permitted by your administrator
- You forget your PIN
- You lose your token

If you encounter any of these scenarios, contact your RSA ACE/Server administrator, who can supply the correct type of emergency code for your situation.

Security Precautions

If an unauthorized person learns your PIN or obtains your RSA SecurID token, this person can assume your identity. Any action this intruder takes is attributed to you in the system security log.

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

- Never reveal your PIN to anyone.
- If you think someone has learned your PIN or your token is missing, notify the security administrator immediately.
- Follow your system’s standard logoff procedures. Failure to log off properly can create a route into the unprotected system.