SecurID Token authentication

The reverse proxy token authentication process uses the RSA ACE/Agent client version 8.1.2.

RSA ACE/Servers authenticate several different tokens, including software tokens and hand-held microprocessor-controlled devices. RSA SecurID authenticators (tokens) are binary programs running on a workstation, installed on a smartcard, or running as a plug-in to a Web browser. RSA SecurID authenticators can run as an application. The application displays a window into which a user enters a Personal Identification Number (PIN), and the Software Token computes the passcode. The user can then authenticate to WebSEAL by entering the passcode into a login form.

The most typical form of RSA SecurID authenticator (token) is the hand-held device. The device is usually a key fob or slim card. The token can have a PIN pad, onto which a user enters a PIN, in order to generate a passcode. When the token has no PIN pad, the passcode is created by concatenating the user's PIN and tokencode. A tokencode is changing number displayed on the key fob. The tokencode is a number generated by the RSA SecurID authenticator at one minute intervals. A user then enters the PIN and tokencode to authenticate to the RSA ACE/Server.

WebSEAL supports both RSA token modes:

This mode is used when the user enters the correct PIN but an incorrect tokencode. Typically, the tokencode must be entered incorrectly three times in a row to send the tokencard into next tokencode mode. When the user enters the correct passcode, the tokencode is automatically changed. The user waits for the new tokencode, and then enters the passcode again.

- **New PIN mode**
  The token can be in New PIN mode when the old PIN is still assigned. The token is placed in this mode when the administrator wants to enforce a maximum password age policy. The token is also in New PIN mode when the PIN is cleared or has not been assigned. Newly assigned tokens might not yet have a PIN. A PIN can be cleared by an administrator when the user has forgotten it or suspects that it has been compromised.

RSA SecurID PINs can be created in different ways:

- User-defined
- System-generated
- User-selectable

PINs modes are defined by the method of creation, and by rules that specify parameters for password creation and device type.

WebSEAL supports the following types of user-defined PINs:

- 4-8 alphanumeric characters,non-PINPAD token
- 4-8 alphanumeric characters,password
- 5–7 numeric characters, non-PINPAD token
- 5-7 numeric characters, PINPAD token
- 5-7 numeric characters, Deny 4-digit PIN
- 5-7 numeric characters, Deny alphanumeric

WebSEAL does not support the following types of new PINs:

Related topics:

Token authentication module

Authentication process flow for tokens in new PIN mode

Do you want to...

Open a ticket and download fixes at the **IBM Support Portal**

Find a technical tutorial in **IBM Developer**

Find a best practice for integrating technologies in **IBM Redbooks**

Explore, learn and succeed with training on the **IBM Skills Gateway**