RSA SecurID Web Express 1.2
Planning Guide

Contact Information

See our Web sites for regional Customer Support telephone and fax numbers.

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

See our Web Site for regional Customer Service telephone and fax numbers.

Trademarks

License agreement

Third Party Licenses

This product may include software developed by parties other than RSA Security Inc. To view the text of the license agreements applicable to third-party software in this product, see Help > About in Web Express.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when exporting this product.

Distribution

Limit distribution of this document to trusted personnel.

The RC5™ Block Encryption Algorithm With Data-Dependent Rotations is protected by U.S. Patent #5,724,428 and #5,835,600.

First printing: May 2003

Contents

Preface

This guide provides information for planning your implementation of RSA SecurID Web Express. Use this guide before you install Web Express. This guide contains a general description of the Web Express product, guidelines for implementing Web Express, issues you may need to resolve, how the product interacts with RSA ACE/Server and other applications, and a set of common scenarios that you can use as a starting point for planning and maintaining your own Web Express server.

Getting Support and Service

RSA SecurCare® Online	**www.rsasecurity.com/support/securcare**
Customer Support Information	**www.rsasecurity.com/support**

Before You Call for Customer Support

Note: Customer support is not provided during the warranty period unless a valid Software Service Contract is in force.

Make sure you have direct access to the server running Web Express and the computer running RSA ACE/Server.

Please have the following information about Web Express available when you call:

- ❑ The name and version of the operating system on which the problem occurs.
- ❑ The name and version of the web server software running on your web server.
- ❑ Customization changes that you have made to Web Express.
- ❑ Any code you have developed that uses the Web Express API calls.

Please have the following information about the RSA ACE/Server available when you call:

- ❑ Your RSA Security Customer/License ID. You can find this number on the license distribution medium or by running the Configuration Management application on a Windows platform, or by typing ‘sdinfo’ on any UNIX platform.
- ❑ RSA ACE/Server software version number.
- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name and version of the operating system under which the problem occurs.

1 Introducing RSA SecurID Web Express

RSA SecurID Web Express is a workflow management application that automates and simplifies the process of assigning and distributing RSA SecurID hardware and software authentication devices (tokens) to users. Because it reduces the amount of time necessary to deploy tokens, Web Express significantly reduces administrative costs.

This guide is for managers and IT professionals who will plan the deployment of RSA SecurID tokens to end users. This guide does not discuss or recommend security policies. This chapter describes what Web Express does, the Web Express architecture, common administrative tasks and provides a sample token deployment workflow.

What RSA SecurID Web Express Does

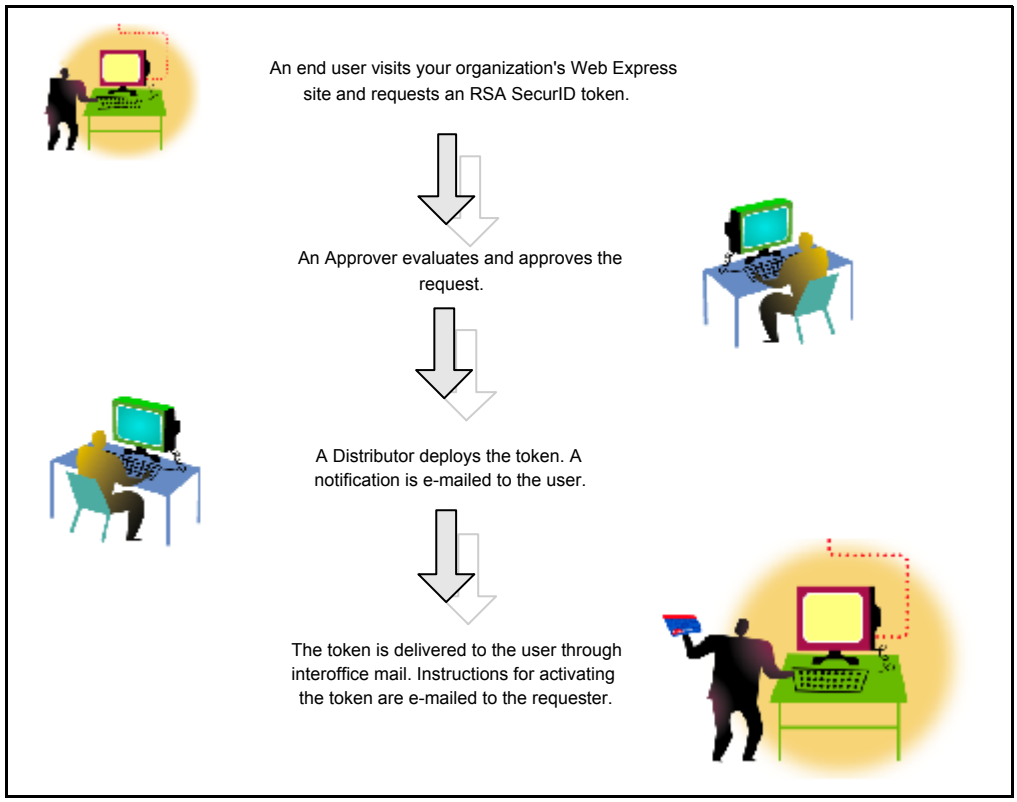
RSA SecurID Web Express simplifies and provides greater control over the process of deploying RSA SecurID tokens to end users. The product can automate many of the complicated and time-consuming tasks that administrators have traditionally performed when deploying RSA SecurID tokens, including

- Identifying users
- Populating user records in the RSA ACE/Server database
- Associating RSA SecurID token serial numbers with specific users
- Coordinating delivery of RSA SecurID tokens to end users
- Issuing software tokens
- Changing PINs, including the PINs of RSA SecurID tokens and PINs used with other applications
- Replacing expiring hardware tokens

With Web Express, end users can request and activate their own RSA SecurID tokens over a network while automatically updating your RSA ACE/Server database.

Sample Workflow

Because RSA SecurID Web Express can be customized in different ways, you can decide which processes to automate based on your company's security policies and needs. Here is a sample workflow for deploying a hardware token.



You can also pre-assign tokens to users prior to deployment, so that only the assigned user can activate and use the token. If you do not pre-assign tokens, and instead allow requesters to self-assign tokens, you can require requesters to enter an activation password, which provides an additional level of security for token activation. In any case, all tokens are distributed in an inactive state, and must be activated by the user through the Web Express Activate Token page.

Accommodates Your Business Environment

RSA SecurID Web Express can accommodate a wide range of environments and security needs. With Web Express you can deploy a large number of tokens to end users at one time or distribute tokens on an ongoing basis.

Web Express can be used as a standalone application, or it can be integrated with other software applications through a set of Application Programming Interfaces (APIs). The Web Express APIs offer entry points in the request process that you can use to verify user data, extract user data from other applications or data sources, or add user data to your organization's database or directory. Additionally, you can use the APIs to change user PINs and verify authentication data submitted as part of a Q & A authentication.

Provides Users with Flexible Web Access

Users can access Web Express services from any location, at any time. Because many of the deployment tasks are handled electronically over a network, Web Express greatly simplifies logistics in worldwide deployments. You can deploy tokens as quickly as necessary, to as many end users as required, wherever they are located.

Enables Users to Service Their Own Tokens

Through the Web Express Home Page, users can change their own PINs, request additional tokens, and activate tokens and replacements for expiring tokens. The Home Page increases efficiency by enabling users to service their own tokens from anywhere and at any time, while it decreases costs by reducing the number of calls to your Help Desk.

If you prefer to continue using your existing processes for servicing tokens, you can disable the Home Page options that you do not want to use.

Provides Administrators with Flexible Configuration Options

Here are some of the ways in which you can customize RSA SecurID Web Express to meet your company's needs.

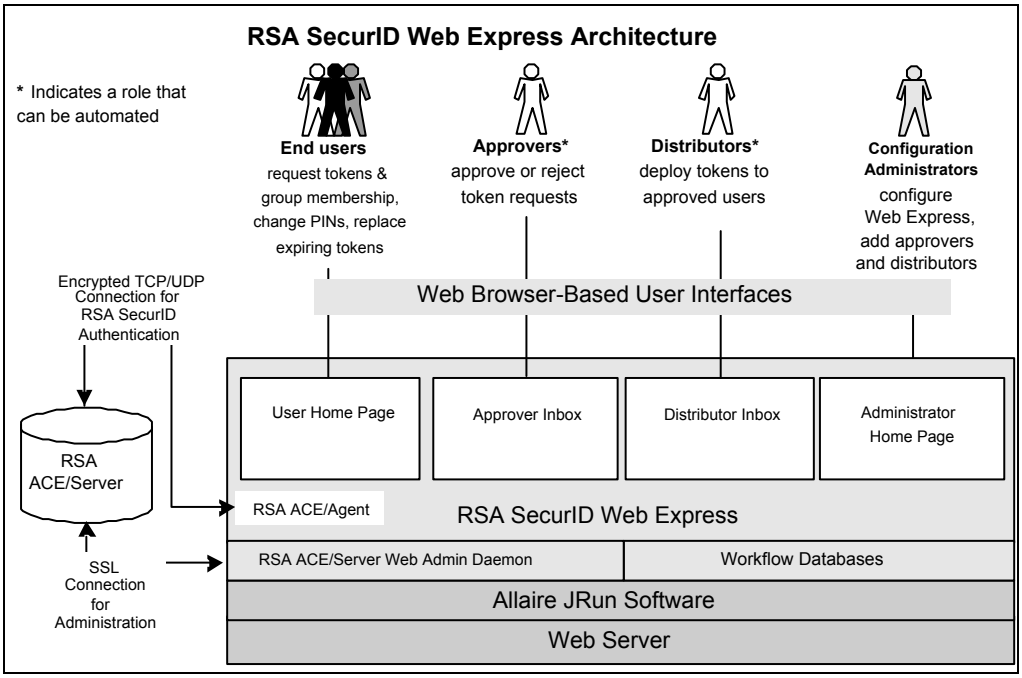
Options	Documentation
Approve token requests manually or automatically.	See the Help topic "Configure the Approver Role."
Assign and distribute tokens manually or automatically.	See "Planning Token Assignment"on page 17 and "Planning Token Distribution"on page 18, and the Help topic "Configure the Distributor Role."
Customize the end-user registration forms, ensuring that users are asked to enter only data that is relevant to your business.	See the chapter, "Customizing RSA SecurID Web Express" in the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*.
Extract or verify user data from company data repositories, or add new data to applications or data repositories using the Web Express Application Programming Interfaces (APIs).	See appendix A "Using the RSA SecurID Web Express APIs" in the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*.
Allow end users to change their own PINs.	See the Web Express System Settings page and the Help topic "Customize Web Express for Users."

RSA SecurID Web Express Architecture

RSA SecurID Web Express is a Java-based Web application that runs on Allaire Corporation's JRun application server software. The application consists of servlets that enable and manage the token request, processing, and distribution workflow within your organization. User token requests are stored and tracked in a database as they move through the process.

By default, Web Express uses Microsoft Access databases when installed on Windows platforms. For instructions on how to connect Web Express to a different database using the JDBC (Java Database Connectivity) driver, see the *RSA SecurID Web Express 1.2 for Windows Installation and Configuration Guide*.

The following diagram shows the Web Express architecture and the roles associated with it:



Administrative Task Summary

This section summarizes the primary administrative tasks associated with RSA SecurID Web Express. In some organizations, one person may have the expertise to perform all of the tasks; in others, the tasks may be divided among several people.

Person	Tasks
Configuration Administrator	• Installs and configures the web server. • Sets up the RSA SecurID Web Express software (includes Web Express servlet installation, as well as JRun application server installation and configuration) • Configures RSA SecurID Web Express settings • Customizes RSA SecurID Web Express • Adds Web Express administrators (Approvers, Distributors, and other administrators)
RSA ACE/Server Administrator	• Monitors event logs • Sets PIN and authentication parameters • Troubleshoots failed user authentication and RSA ACE/Server problems • Distributes **sdconf.rec** files to RSA ACE/Agent administrators • Adds users, Agent Hosts, groups, and tokens to the RSA ACE/Server database • Performs regularly scheduled database maintenance
Approver*	• Reviews token requests • Approves or rejects token requests
Distributor**	• Assigns tokens to approved users Does one of the following: • Distributes tokens to approved users. For hardware tokens, delivers tokens or tells users where to pick up tokens. For software tokens, delivers token on diskette or other media, e-mails tokens or tells users where to download tokens. • e-Mails details about approved users to token Distributor. The Distributor sends the tokens to the users.

* Not necessary if you configure Web Express to process requests automatically.

** Optional, depending on the method used to distribute tokens. For more information, see "Sample Deployment Scenarios" on page 25.

2 Planning Your Web Express Environment

Before you install RSA SecurID Web Express, some planning is necessary. You may decide to use the default configuration or you may decide to customize the product to fit your specific environment or business processes. In either case, read this chapter to ensure a smooth implementation.

For example, you need to decide:

- Whether you want to transfer end user information to and from corporate data repositories (for example, databases, LDAP directories, and so on)
- What data you want to store in your RSA ACE/Server database, and where the data will come from
- Which tasks in the token approval/deployment process you want to automate
- Whether you want to communicate with users primarily through e-mail or another means

This chapter walks you through each decision, laying out your choices. When you are ready to install and configure the product, use the *RSA SecurID Web Express 1.2 Installation and Configuration Guide* for your platform.

Planning What Data You Need to Capture in Web Express

RSA SecurID Web Express provides a range of options for entering, updating, and exporting user data. You decide which methods best suit your business.

Things to Consider

Think about what kinds of user data you will need to

- Identify users (for example, User IDs, names, and social security numbers)
- Notify users of request approvals or rejections (for example, e-mail addresses)
- Add to the RSA ACE/Server database after token requests are approved
- Deliver hardware tokens to users (for example, postal addresses or mail stops)
- Allow self-service PIN change (for example, questions users will need to answer in order to prove their identity when attempting to change the PIN)

Discussion

RSA SecurID Web Express provides a default user token request page that you can use without any additional customizing. The page includes the following fields:

- **User ID**
- **Last Name**

- **First Name**
- **E-mail Address**
- **Cost Center**
- **ACE/Server Group** (lists the available RSA ACE/Server groups)

If you choose to customize the form, you can

- Disable fields you do not plan to use
- Rename fields
- Designate certain fields as "required"
- Define up to 16 custom fields for additional token and user data, such as a social security number or date of birth, and stores the input in extension fields in the RSA ACE/Server database.

When customizing the form, consider how you will communicate with users when the tokens are actually deployed. If you plan to send tokens by postal mail, you might want users to enter their business or home addresses.

For instructions about customizing Web Express, see the chapter, "Customizing RSA SecurID Web Express," in the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*.

Using the Web Express APIs

At certain points in the workflow, Web Express provides entry points in its Application Programming Interfaces (APIs) for you to execute your own custom code. For example, you can write a Java method that enforces data integrity rules on the information in users' token requests. If the information is invalid or incorrect, appropriate action is taken (for example, the request is rejected automatically).

Note: To use the APIs, custom software must be written. If your organization lacks the skills or resources to write the software, RSA Security Professional Services can write it for you. For more information, visit the RSA Security web site or contact your RSA Security sales representative.

Things to Consider

- If you already have user information in other data repositories, will you import this data into Web Express?
- Will you export user data from Web Express to other data repositories?
- Will you use the Web Express APIs to verify the data in user requests and make corrections programmatically, or will you rely on Approvers to ensure that users have entered correct data?

Discussion

Web Express provides seven APIs that enable you to import data from and export data to other data repositories. For example, you can extract all new employees' e-mail addresses from a Human Resources database, import them into Web Express, and then export them to both the RSA ACE/Server database and to your company's accounting database.

Sharing data in this manner can minimize the amount of data that users need to enter when they request tokens, thus reducing errors.

The following table summarizes the purpose and benefits of each API.

Task	API	Benefits
Import data from an existing data repository into Web Express. Update request data from an existing data repository	**Data Import**	Keeps the RSA ACE/Server database consistent with other corporate data repositories (because Web Express sends the data to RSA/ACE Server after token requests are approved). Minimizes data entry, reduces errors.
Verify data entered during token request against data in an existing data repository.	**Validate Request**	Ensures that request data is accurate and consistent throughout the company. Validates data before approval. Strongly recommended if the token approval process is automated.
Extract approved user data from Web Express and populate other data repositories.	**External Data Distribution**	Permits data to be distributed to other applications. Promotes speed and accuracy when populating multiple data repositories.
Verify data entered during token activation against data in an existing data repository.	**Validate Activation**	Provides validation of additional fields during activation. Ensures that activation data is accurate and consistent throughout the company.
Collect a set of PIN requirements from the RSA ACE/Server or other application.	**Get PIN Parameters**	Gets PIN constraints from other applications and passes them to the ChangePIN API. This call works with RSA SecurID PINs, system PINs and PINs for other applications.
Change a user's PIN.	**Change PIN**	Enables users to use Web Express to set and change the PINs or passwords for other applications
Verify answers submitted as part of a Q & A authentication.	**Validate Q & A**	Matches answers submitted to information stored in customer-defined data source.

Planning RSA ACE/Server Group Assignments

In the RSA ACE/Server product, a group consists of an indefinite number of users associated in the database under a group name. Although users in a group often have common characteristics such as job type, location, or department, the principal reason for putting users in a group is to simplify the task of assigning access rights to large numbers of users.

Things to Consider

- Do you want to add new users to RSA ACE/Server groups through Web Express?
- Which groups do you want users to be able to select when requesting a token?
- How will you let users know which groups to select?

Discussion

If you decide to allow group designations in RSA SecurID Web Express, you must configure the Request Token page to display the drop-down list of groups. Each group that you define must have a corresponding group defined in the RSA ACE/Server database. When a user requests a token in Web Express, and selects a group from the drop-down list, the user is enrolled in that group in the RSA ACE/Server database.

For example, suppose that all department managers in London are restricted to accessing specific Agent Hosts. You might define a group in the RSA ACE/Server database called LONDONMGRS. Users who select this option when requesting a token through Web Express will be assigned to this group.

For detailed instructions, see the following documents:

Topic	Location
Creating groups in RSA ACE/Server	*RSA ACE/Server Administrator's Guide*
Mapping Web Express groups to RSA ACE/Server groups	"Specifying RSA ACE/Server Groups" in the chapter "Customizing RSA SecurID Web Express" in the *RSA SecurID Web Express 1.2 Installation and Configuration Guide* for your platform.

Planning the Token Approval Process

Things to Consider

- Who needs to approve each user's token request?
- For which departments or cost centers will each Approver be authorized to approve tokens?
- How should Approvers be notified when requests are waiting?
- Do you want to automate the approval process? If so, do you want to accept all requests or only requests from new users?

Discussion

If your company's security policy requires at least one person to approve each request, you can set up Web Express to route the requests to the appropriate inbox (for example, a department or cost center) to await approval. Authorized Approvers can then access their inboxes from the Web Express Admin Home page and view the requests before accepting or rejecting them.

If personal approval is not required, then Web Express can automate the entire process, ensuring rapid resolution for all requests. You can configure Web Express to automatically accept all token requests, or only those requests from users who are not already in the RSA ACE/Server database.

Important: If your approval process will be entirely automated, and you are extracting data from or importing it to another company database, RSA Security strongly recommends that you use the Validate Request API call to verify the data.

For more information, see the Help topic "Configure the Approver Role."

Planning Token Assignment

Token assignment binds the user to a specific token in the RSA ACE/Server database. Web Express provides multiple methods of token assignment, depending on the type of token requested.

For hardware token assignment:

- The Distributor assigns a token as part of token deployment.
- The requester self-assigns the token as part of token activation.

  Even when you have enabled the Distributor role, you can still configure user self-assignment. In either case, the token is not enabled until the requester activates it.

For software token assignment, there is only one option: software tokens are assigned automatically.

Things to Consider

- Are you deploying large numbers of tokens?
- Are you deploying hardware tokens, software tokens for desktop PCs, software tokens for other devices, or a mixture?
- How quickly do you need to deploy tokens?
- What are the constraints on your IT staff ?
- Does your company have a security policy that prohibits end users from receiving unassigned tokens? Does an authorized person need to assign a specific token number to each user?

Discussion

The fastest way to deploy large numbers of hardware tokens is to have users self-assign tokens. By this method, upon receiving their hardware tokens, approved users enter their token serial numbers on the Accept Token page. RSA ACE/Server then binds the token to the user and enables the token.

RSA Security recommends user self-assignment when you

- Want to reduce the burden of hardware token deployment and distribution on your IT staff
- Need to deploy large numbers of hardware tokens quickly or frequently

At some companies, the security policy might require tokens to be assigned by authorized staff. By this method:

1. An authorized person accesses the Distributor inbox from the Administrator Home page to view the queue of approved users and assign a token to each user.
2. Upon receiving approval notification, users enter their approval information on the Activate an Approved Token page for verification.

   Note: Users with hardware tokens must have their tokens in their possession to activate the tokens. Depending on the software token delivery method, users with software tokens may need to download the token *after* activating the token through the Activate Token page.

   The RSA ACE/Server enables the tokens.

For more information, see "The Activate Token Page" in the chapter "Customizing RSA SecurID Web Express" in the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*.

Planning Token Distribution

Token distribution is the method by which the requester receives the requested token. Web Express provides multiple methods of token distribution, depending on the type of token requested.

For hardware token distribution:

- The Distributor delivers an assigned or unassigned token to the requester.
- A third-party distribution house delivers the token to the requester.
- The requester picks up an unassigned token from a common area.

For software token distribution, there are three options:

- The requester downloads the token from the Download Token page.
- The requester receives the token in the approval e-mail.
- The Distributor physically delivers an assigned software token on a diskette.

Things to Consider

- How many tokens will you need to distribute on a daily basis? On a monthly basis?
- How many sites need to distribute tokens? Where are they located?
- Will you manage token distribution in-house or through a third party?
- How will you communicate token fulfillment plans and instructions to end users? To the party that is carrying out the distribution?
- For software tokens, will you need to configure a software token download page? Who installs the software token application, the users or IT personnel?

Discussion

Token distribution can be accomplished in in one of the following ways:

- Through a third-party organization or fulfillment house
- Through postal mail, express mail, or interoffice mail
- In person
- Through a web page configured to allow software token downloads

The method you use depends on how many tokens you need to deploy, the type of tokens you deploy, the availability of deployment personnel, and the particular needs of your company.

If you plan to use postal mail, be sure to do the following:

- Make sure that whoever will distribute the tokens is given the destination addresses.
- Decide whether you need to capture this information in Web Express.

You may be able to obtain this data from existing company databases, or from users when they submit token requests.

For details on communicating with end users, see the following section, “Planning User Communication for Token Registration.”

For details on configuring the Distributor role, see the Help topic “Configure the Distributor Role.”

Planning User Communication for Token Registration

Things to Consider

- How will you inform users that they need to register for tokens?
- What do users need to do when they receive and activate their tokens?
  - Do they need to provide the token serial number in order to self-assign the token?
  - Do they need to provide an activation password?
  - Do you want them to perform their first authentication and set a PIN?
  - Are they allowed to set their own PIN?
  - Do they need to set up Q & A authentication?

The answers to these questions depend on how you choose to configure and customize Web Express and the RSA ACE/Server. For more information on configuring Web Express, see the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*. For more information on the use of PINs in RSA ACE/Server, see the RSA ACE/Server Help and the *RSA ACE/Server Administrator's Guide*.

Discussion

The easiest way to inform users is through e-mail. Other methods to consider are postal mail, intranets, interoffice mail, and company newsletters.

RSA Security suggests that the e-mail contain

- A brief description of your new security policy
- How the user will receive the token
- What User ID the employee should use to register for the token
- The RSA SecurID Web Express URL
- What cost center and RSA ACE/Server group, if any, should the user specify when requesting a token?

For example, the following sample message includes the essential information:

```
From:     System Administrator
Sent:     Tuesday, May 5, 2003 3:35 PM
To:       Pat Wang
Subject:  New Security Policy

What is this e-mail about?
Our company is starting a new security policy requiring the use
of an RSA SecurID token to gain access to the network.

How will I receive my RSA SecurID token?
You will receive your RSA SecurID token through intra-office
mail a few days after you complete the registration form.
```

Which User ID should I use when I fill out the registration form?
Use the User ID with which you log in to your desktop.

To go to the first step of the request process, click:
http://www.intranet.ourcompany.com/RSASWE/WXUserHome.do

For details on configuring e-mail, see the chapter "Configuring RSA SecurID Web Express" in the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*.

Planning User Communication for Token Approval

Things to Consider

How will you inform users when their token requests have been approved or rejected?

Discussion

You can either tell the users in person, by mail or by e-mail. RSA SecurID Web Express can be configured to send the e-mail automatically. The message should contain

- The user's User ID and activation code
- Directions for completing the Activate Token page
- An active link containing the URL to the Activate Token page

For example:

```
From:     System Administrator
Sent:     Tuesday, May 5, 2003 3:47 PM
To:       Pat Wang
Subject:  You Are Registered

Congratulations! You have successfully registered with our
RSA Security system.

To continue the process, the RSA Security system will require
your User ID and activation code. This information should be
filled in for you. However, you may need to enter it manually.

Your User ID is: pwang
Your activation code is: 86759403

To go to the Activate Token page, click the following link:
http://www.intranet.ourcompany.com/RSASWE/WXUserActivateToken.d
o?tnApprovalCode=86759403&tnUserId=pwuan@ourcompany.com
```

Web Express provides sample e-mail messages that you can use as is, or edit to you particular needs. For more information, see "Customizing Approval and Rejection e-Mail Messages" in the chapter "Configuring RSA SecurID Web Express" in the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*.

Planning User Communication for Authentication Instructions

Things to Consider

How will users know how to authenticate?

Discussion

RSA Security provides the RSA SecurID Tour, which demonstrates how to authenticate using an RSA SecurID token. Users can launch the Tour from the User Home page. The tour includes information about authenticating with different types of RSA SecurID tokens, selecting PINs, New PIN mode, and Next Tokencode mode. The Tour provides all the information users need to start using their tokens.

For more information, see the *RSA ACE/Server Administrator's Guide* and the RSA ACE/Server Help.

Planning Multilingual Access

Things to Consider

- What languages do you need to use to communicate with end users who will request tokens?
- What languages do you need to use to communicate with Approvers who will accept or reject token requests, or with distribution personnel who will assign and deliver tokens?

Discussion

RSA SecurID Web Express makes it very easy to accommodate the needs of multilingual organizations. You can localize all parts of the Web Express user interface by editing the properties files and the Home page HTML files. Additionally, you may want to edit the e-mail templates and the Help.

For example, suppose that your Approvers in the United States speak English, while your end users in Europe and South America speak a variety of languages. You can display the Administration pages in English, and translate the Request Token page and other end user pages into as many languages as necessary.

For more information, see "Localizing Web Express" in the chapter "Customizing RSA SecurID Web Express" in the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*.

Planning the RSA/ACE Server Configuration

Things to Consider

- Which RSA ACE/Server host will be used?
- Which RSA/ACE Server port number do you want to use?
- How many connections to the RSA ACE/Server system will be allowed at one time?
- How often should Web Express check for connectivity with the RSA ACE/Server system?

Discussion

See your RSA ACE/Server Administrator to answer these questions.

Planning the JDBC Configuration

RSA SecurID Web Express requires a transaction database for holding active data, and an archive database for holding inactive data. Both databases must be JDBC-compliant. For Windows platforms, Web Express ships with the Microsoft Access database for these purposes. For UNIX platforms, you must have a third-party database.

Things to Consider

- Are there any reasons why you might want to use a database other than Microsoft Access?
- If you use a different database, what JDBC driver do you need?
- What is the maximum number of connections you want to allow for each database?

Discussion

For each database, you can set the minimum and maximum number of connections allowed. The default is 200.

You must use the JDBC-ODBC bridge driver to communicate with Access. This driver is automatically installed during Web Express setup. If you want to use a JDBC driver, you need to purchase one.

If you choose a database other than Microsoft Access, the vendor will most likely supply a JDBC driver.

For more information, see the chapters “Requirements and Preparations” and “Installing and Setting Up RSA SecurID Web Express” in the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*.

Planning Web Server Security

Because Web Express is a critical web application, RSA Security strongly recommends that you use the latest guidelines and best practices to secure the web server on which you will install the Web Express software.

For guidelines on securing

- Microsoft Internet Information Server (IIS), visit the Microsoft TechNet Security web site at **www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp**.
- JRun application server, visit the Macromedia Security Zone web site at **http://www.macromedia.com/v1/handlers/index.cfm?ID=23500**.
- Sun ONE Web Server, visit **http://docs.sun.com/db/prod/s1websrv**.

3 Sample Deployment Scenarios

This chapter describes four scenarios for deploying RSA SecurID Web Express. Each scenario presents typical business requirements and suggests how Web Express can help you fulfill them.

Scenario	Description	Page
"Scenario 1: Quick Start"	The "out-of-the-box" solution. Requires only basic Web Express configuration. This is the fastest way to get Web Express up and running.	26
"Scenario 2: Fully Automated Request Processing and Token Issuance"	The fastest way to deploy tokens. No human intervention is required to approve token requests and issue tokens to users.	28
"Scenario 3: New Employees"	Partial automation for token approval and deployment.	29
"Scenario 4: Full Approver Control"	When Approvers need to approve and issue tokens personally without a Distributor.	30

You can require all token request data to be entered by users, or you can configure Web Express to extract data from a combination of user input and external data sources.

Using the Web Express APIs

Use of the APIs provided with Web Express is always optional. You can use them if you decide to import data into Web Express from other corporate data repositories, export data from Web Express, or verify user input.

Important: You do not need to use the APIs to update or extract user data from the RSA ACE/Server database. Web Express automatically updates the RSA ACE/Server database after a token request is approved. Likewise, when a user requests a token, Web Express automatically checks whether the user is in the RSA ACE/Server database. If so, Web Express extracts the user's data and displays it when an Approver reviews a token request.

Creating Administrators

All Approvers and Distributors who use RSA SecurID Web Express must be administrators defined in Web Express. For instructions on creating adminisrators, see the Help topics "Configure the Approver Role" and "Configure the Distributor Role."

Scenario 1: Quick Start

RSA SecurID Web Express provides default settings that you can use immediately, "out of the box," with minimal additional configuration.

Additional configuration includes:

- Creating administrators, including Approvers and Distributors
- Creating cost centers, or editing the default cost centers
- Configuring e-mail connections and specifying default templates
- Configuring the connection to the RSA ACE/Server database

In this scenario, authorized Approvers review all token requests and a Distributor assigns and distributes hardware tokens to users. Web Express assigns software tokens and allows requesters to download tokens. The default settings are as follows:

Function	Web Express Configuration
Request approval	Configured for manual approval.
Token assignment and distribution	Configured for manual assignment and manual distribution of hardware tokens. Configured for automatic assignment and download delivery of software tokens.
APIs	Available but not used.

This is what happens:

Step	Actor	Action
1	User	• Requests a token through Web Express.
2	Approver	• Checks his or her inbox periodically to view new requests or, if notification is enabled, receives e-mail notification of the request. • Accepts or rejects the request.
3	Web Express software	• If the request is approved and a record for the approved user does not exist in the RSA ACE/Server database, the Web Express software creates one.

Step	Actor	Action
4	Distributor	• Checks his or her inbox periodically to view approved requests or, if notification is enabled, receives e-mail notification of the approval. • Deploys a specific, assigned token to the requester. • Arranges for user to receive his or hardware token (either by in-house means, postal mail or through a third-party fulfillment house). • Takes no action for software tokens when Web Express is configured for download delivery of software tokens.
5	Web Express software	• e-Mails an activation code and instructions to the user. • If needed, modifies the user's record in the RSA ACE/Server database to associate the user with the token serial number. If the token requires a PIN, puts the user's token in New PIN Mode. The token is disabled until the user activates it. • If configured to use a third-party fulfillment house, sends a notification e-mail to a contact person who arranges for a token to be delivered to the user.
6	User	When the requested token is a hardware token: • Receives the token and an e-mail containing an activation code and instructions. • Clicks the link containing the activation code to access Activate Token page and provides information to activate the token. • Performs the first authentication and creates a PIN for the token. When the requested token is a software token: • Receives an e-mail containing an activation code and instructions. • Clicks the link containing the activation code to access Activate Token page and provides information to activate the token. • Downloads the token. • Downloads the token application and installs it, if necessary. • Installs the token. • Authenticates for the first time and creates a PIN.

Scenario 2: Fully Automated Request Processing and Token Issuance

If your organization needs to deploy tokens rapidly, or needs to deploy large numbers of tokens, you probably want to take full advantage of the automation capabilities provided by RSA SecurID Web Express. This scenario also uses a third-party order fulfillment house to distribute tokens to users.

In this scenario, the settings are as follows:

Function	Web Express Configuration
Request approval	Configured for automated approval.
Token assignment and distribution	Configured for automated assignment and third-party distribution.
Data validation	The Web Express Validate Request API is used to verify data that users submit in their requests

Since the approval process is fully automated, the Validate Request API provides added error checking by verifying the data that the user enters against data in the organization's data repository (for example, an LDAP directory or Human Resources database). If the data is incorrect, the request may not be approved.

This is what happens:

Step	Actor	Action
1	User	• Requests a token through Web Express.
2	Your custom code (using the Web Express Validate Request API)	• Verifies the accuracy of user input by checking it against your data repository.
3	Web Express software	• Based on what your code returns from the Validate Request API, automatically approves or rejects the token request. • If the request is approved and a record for the approved user does not exist in the RSA ACE/Server database, Web Express creates one. • e-Mails an activation code and token activation instructions to the user. • Sends a notification e-mail to a third-party fulfillment house, who arranges for a token to be delivered to the user.

Step	Actor	Action
4	User	• Receives the token and the e-mail containing the activation code and activation instructions. • Clicks the link containing the activation code to access Activate Token page and provides information to activate the token. • Authenticates for the first time and creates a PIN.

Scenario 3: New Employees

In this scenario, a new hire is given a security token during employee orientation.

The settings for this scenario are as follows:

Function	Web Express Configuration
Request approval	Configured for automatic approval.
Token distribution	Configured for manual distribution.
Data validation	The Web Express Validate Request API can be used to validate user input, but it is not required.

This is what happens:

Step	Actor	Action
1	Approver, IT staffer, or administrative assistant	• Makes a token request on the user's behalf.
2	Web Express software	• Evaluates and approves or rejects the request automatically. • If a record for the approved user does not exist in the RSA ACE/Server database, the Web Express software creates one.
3	Distributor	• Checks his or her inbox to view the request or, if notification is enabled, receives e-mail notification of the request. • Deploys the token.
4	Web Express software	• e-Mails an activation code and token activation instructions to the user. • Has the option to modify the user's record in the RSA ACE/Server database to associate the user with the token serial number.

Step	Actor	Action
5	User	• Receives the token and e-mail notification. • Using a Web browser, enters the activation code and token serial number into Web Express to activate the token. • Authenticates for the first time and creates a PIN.

Scenario 4: Full Approver Control

This scenario shows how you might configure RSA SecurID Web Express when each Approver is required to personally deliver tokens to users in his or her group.

For example, you might use this scenario in any of the following situations:

- Approvers need complete control over token approval and deployment for their respective departments.
- Approvers or administrators must not only review token requests but also distribute the tokens.
- Your IT group wants to be solely responsible for approving and deploying tokens.

The settings for this scenario are as follows:

Function	Web Express Configuration
Request Approval	Configured for manual approval
Token assignment and distribution	Configured for automated assignment and distribution
APIs	Available but not used

This is what happens:

Step	Actor	Action
1	Approver	• Gives a token to the user (or sends it through postal mail).
2	User	• Requests a token through Web Express.
3	Approver	• Approves the user's request.
4	Web Express software	• If a record does not exist for the user in the RSA ACE/Server database, creates a record for the user. • Sends the user an activation code and activation instructions through e-mail. • Puts the user's token in New PIN Mode.

Step	Actor	Action
5	User	• Receives the token and e-mail notification. • Using a Web browser, enters the activation code and token serial number into Web Express to activate the token. • Authenticates for the first time and creates a PIN.

Next Steps

For instructions on setting up the RSA SecurID Web Express software, see the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*.