

RSA® Credential Manager

Web-based solution for the rapid deployment and lifecycle management of RSA SecurID® authenticators

At a Glance

- Self services end-users for most commonly requested token activities
- Streamlines credential deployments and reduces ongoing administrative costs
- Fully integrated into RSA® Authentication Manager 7.1 management console
- Rapidly speeds the binding of users to their credentials

Identity assurance is the set of capabilities and methodologies that minimize business risk associated with identity impersonation and inappropriate account use. Credential management is a core capability of an identity assurance strategy which brings confidence to organizations by allowing trusted identities to freely and securely interact with systems and access information, opening the door for new ways to generate revenue, satisfy customers and control costs.

The RSA Identity Assurance portfolio extends user authentication from a single security measure to a continual trust model that is the basis of how an identity is used and what it can do. Trusted identities managed by RSA bring confidence to everyday transactions and support new business models by providing secure access for employees, customers and partners while striking the right balance between risk, cost and convenience. RSA Identity Assurance solutions apply appropriate access controls that mitigate risk according to the value and criticality of the data, application, identity or transaction.

RSA Credential Manager is a core component of the RSA Identity Assurance portfolio that provides full lifecycle management of RSA SecurID® credentials. Credential Manager contains tools that both speed the setup and automation of workflows, and enable users to self manage many aspects of their day-to-day token usage. With RSA Credential Manager the entire deployment process – including populating the database and issuing of token codes – is fully automated.

Built-in Self Service to Empower End-users

Users stay productive with the self-service features found in RSA Credential Manager. Utilizing the Self-Service Console hosted off RSA® Authentication Manager's built-in web server, users can select from a variety of options:

- **Report a temporarily lost or unavailable token.** If a user has left his hardware token at home while traveling, for example, an on-demand token code, or set of one-time token codes, is issued to authenticate him temporarily to the network.
- **Report a permanently lost or damaged token.** This is similar to the above, except that an extra workflow can be initiated to disable the user's lost/damaged token and, if necessary, issue a new token to the user.
- **Forgotten PIN.** A token code can be issued to the user to authenticate before a PIN reset is initiated as an extra security precaution.
- **Grant Emergency Access.** In the event a user forgets both login and PIN, emergency access can be granted by asking the user 'life questions' pre-populated from the database.
- **Request a replacement token.**
- **Test a token.**

Placing tools in the hands of users greatly reduces the number of calls and trouble tickets into the help desk, and can keep end users productive and satisfied. Self-service features are included in both the Base and Enterprise Server licenses.





On-demand Authenticators = Flexible Options

The RSA SecurID On-demand Authenticator is the innovation behind many of the self-service features found in RSA Credential Manager. By enabling delivery of user-requested (or On-demand) token codes to mobile cell phones or registered e-mail addresses, the overall flexibility of the solution grows. This opens up deployment scenarios, such as supporting user requests 24x7x365, so that after-hours employees can on-board without human intervention, e.g., during a business disruption or an emergency which necessitates that large numbers of users gain remote access to the network quickly. End users can even troubleshoot problems, such as PIN/password resets, or request emergency access using registered life questions in the database. Contractors and vendors can securely access the network without being pre-issued hardware or software tokens. Best of all, when combined with the self-service features of RSA Credential Manager, On-demand Authenticators create an automated system that makes both users and administrators more productive. The utilization of On-demand Authenticators meets both of the requirements of two-factor authentication: something you know (login/PIN) and something you have (pre-registered mobile device or e-mail address).

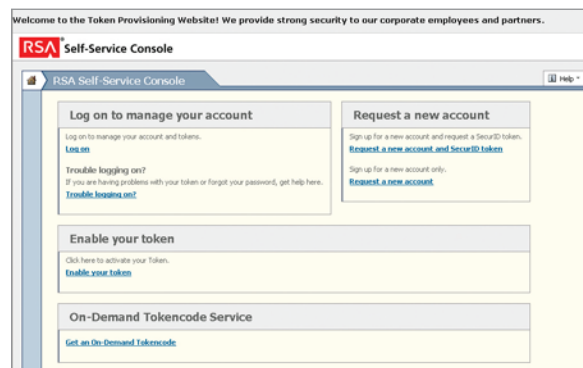
Building Automation with Workflow Provisioning

Workflow provisioning allows for the creation of productivity-saving processes that speed deployment scenarios and ease the work load of IT staff. For example, an administrator can setup workflows so that registration requests from new users within a particular security domain, or ones that fit a certain profile, are routed to a pre-defined approver. That approver can be the head of a department with direct reports in that location or a business manager with a fiscal line of responsibility to that office. With delegated capabilities, approvers familiar with the work situation at a particular location are empowered to make the decision.

A two-step approval process is supported. For example, after a department head approves a user request, that request can then be reviewed by a security admin to further assure the identity of the user. The approval workflow process makes it possible for users who are not already populated in the database to register, be approved and receive a token code via SMS/e-mail – all within a matter of minutes – resulting in access to network resources in a timely manner while enforcing enterprise-wide security policies for strong authentication. Several workflow templates are included with RSA Credential Manager. Workflow provisioning is included in the Enterprise Server license.

Flexible, Integrated and Customizable

RSA Credential Manager is browser-based and menu-driven, and installs along with the RSA Authentication Manager software; there is no desktop software to install separately. Administrators simply launch a browser from any PC and proceed. And, along with tight integration into the RSA Authentication Manager console, Credential Manager is scalable, fitting the needs of small and large organizations alike. Customizable e-mail templates and workflows allow policies to be built around business processes that help keep the organization safe and in compliance. Self-service screens can be tailored with a company logo and selectable fields to present a unified front to the end user.



With the Self-Service Console users manage token lifecycles – from enabling new credentials to enabling tokens to initiating On-demand Authentication.

RSA Credential Manager includes Self Service in the Base Edition License, and Self Service and Workflow Provisioning in the Enterprise Edition License



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

©2008 RSA Security Inc. All Rights Reserved.
RSA, SecurID and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

RCM DS 0208