

RSA Ready Implementation Guide for RSA | SecurID®

Drawbridge Networks PathProtect 1.0

Peter Waranowski, RSA Partner Engineering
Last Modified: March 9th, 2016

RSA
READY

Solution Summary

Multi-factor authentication is a strong security control that can thwart a number of threats, but integrating it with enterprise applications can be a challenge. Many legacy applications don't support two factor, and those that do still require effort to integrate.

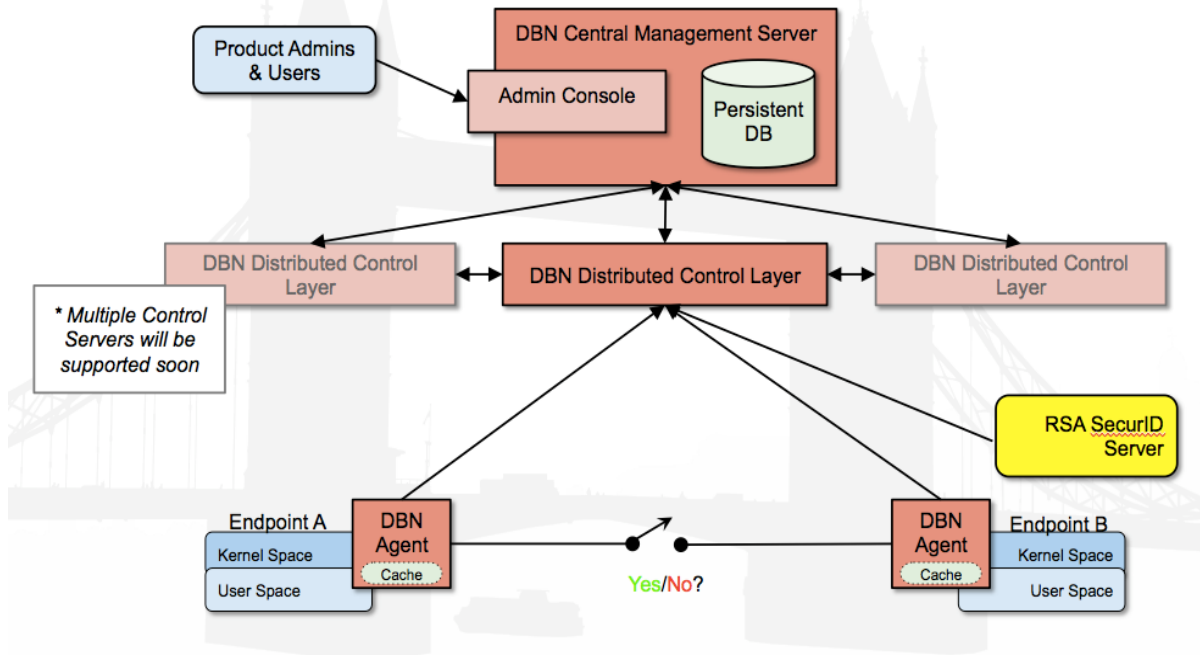
PathProtect makes it easy to enforce two-factor controls for access to any application in your enterprise without the need for direct application integration. PathProtect is an endpoint agent-based solution that orchestrates network policy for each endpoint via a central controller.

PathProtect can integrate with your enterprise two factor solution, such as RSA SecurID, and then challenge users for authentication before allowing access to key systems at the network layer.

Once PathProtect is integrated with RSA SecurID, enforcing new authentication requirements for applications in your enterprise is as simple as creating a firewall rule. PathProtect can demand two factor authentication from end users based on a number of policy options including Active Directory user groups as well as source IP address ranges. For example, PathProtect can be configured to deny remote desktop access to a web server unless the user requesting access is in the server administrator's group and has successfully two factor authenticated.

RSA Authentication Manager supported features	
PathProtect 1.0	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	No
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	No
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

DRAG-IBRIDGE NETWORKS



RSA Authentication Manager Configuration

Agent Host Configuration

To facilitate communication between the Drawbridge Networks PathProtect Server and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the Drawbridge Networks PathProtect Server and contains information about communication and encryption.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

! > Important: The UDP-based authentication agent's hostname must resolve to the IP address specified.

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with Drawbridge Networks PathProtect Server will occur.

Drawbridge Networks PathProtect Server will be communicating with RSA Authentication Manager via RADIUS, then a RADIUS client that corresponds to the agent host record must be created in the RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

! > Important: The RADIUS client's hostname must resolve to the IP address specified.

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Drawbridge Networks PathProtect Server with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Drawbridge Networks PathProtect Server components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Drawbridge PathProtect Configuration

1. Locate and edit the catapult.yml file.

Make the following edits under the section title "twoFactor":

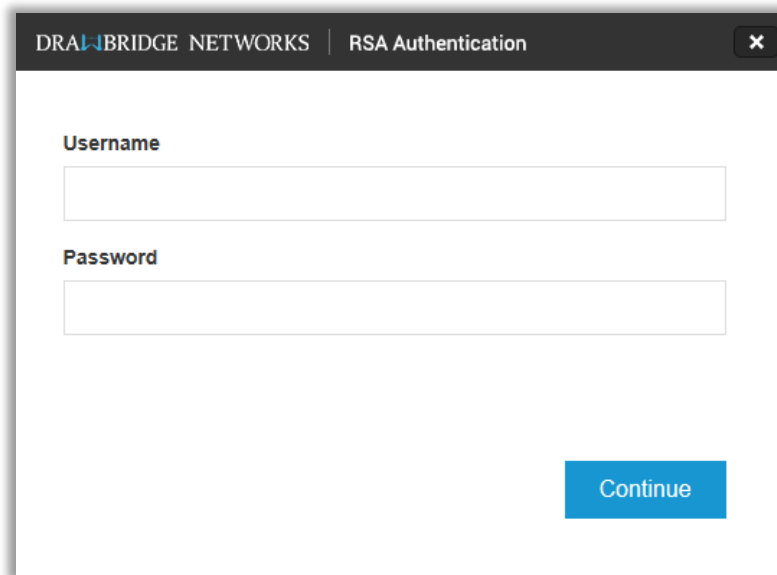
2. Set the type to RSA
 type: RSA
3. Set the shared secret
 ssec: "[shared secret]"
4. Set the IP or hostname of the RSA SecurID server(s)
 hosts:
 - [host]:[port]

Example:

```
type: RSA
ssec: "not so secret secret"
hosts:
  - 192.168.1.100:1812
  - 192.168.1.101:1645
  - 192.168.1.102:1812
```

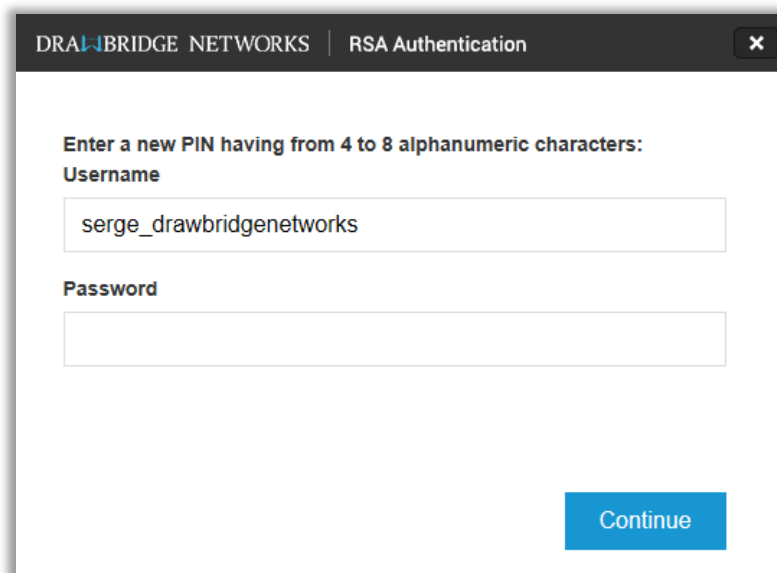
RSA SecurID Login Screens

Login screen:



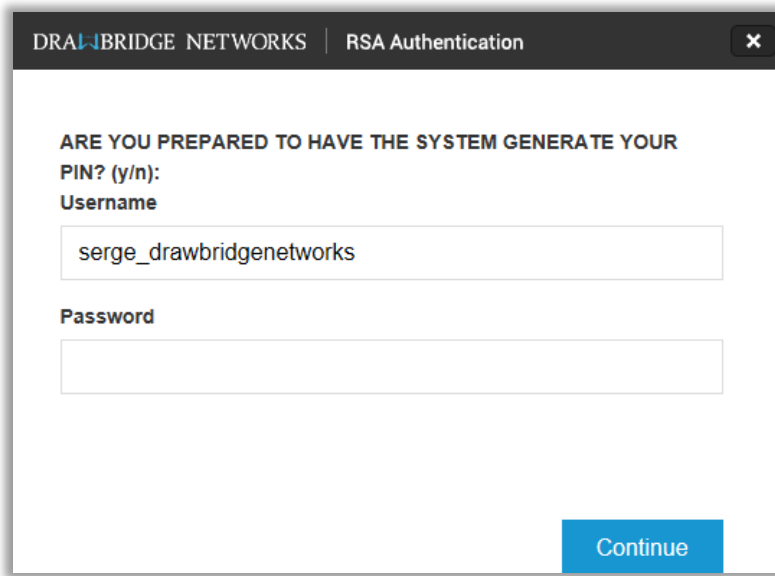
A screenshot of a web browser window titled "DRAL-IBRIDGE NETWORKS | RSA Authentication". The window contains a login form with two input fields: "Username" and "Password". Below the fields is a blue "Continue" button.

User-defined New PIN:



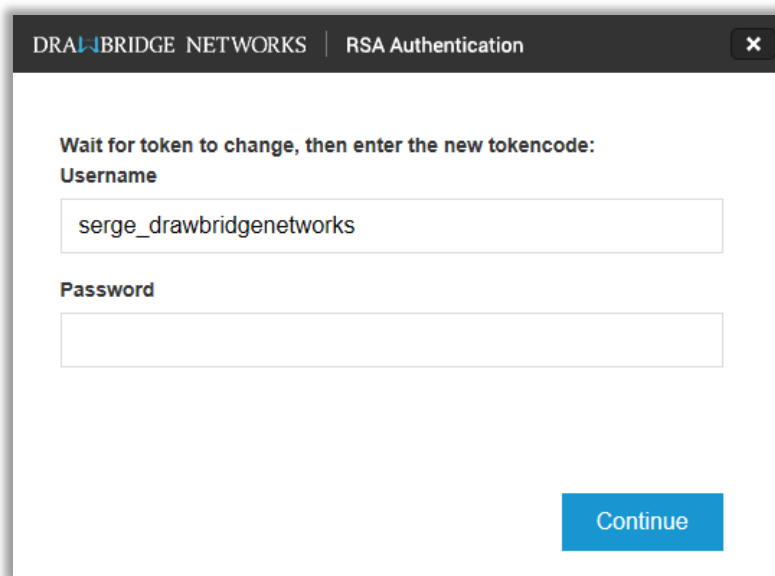
A screenshot of a web browser window titled "DRAL-IBRIDGE NETWORKS | RSA Authentication". The window displays the instruction "Enter a new PIN having from 4 to 8 alphanumeric characters:". Below this are two input fields: "Username" containing the text "serge_drawbridgenetworks" and an empty "Password" field. A blue "Continue" button is located at the bottom right.

System-generated New PIN:



A screenshot of a web browser window titled "DRAL-IBRIDGE NETWORKS | RSA Authentication". The main heading asks, "ARE YOU PREPARED TO HAVE THE SYSTEM GENERATE YOUR PIN? (y/n):". Below this, there are two input fields: "Username" with the text "serge_drawbridgenetworks" and "Password" which is currently empty. A blue "Continue" button is located at the bottom right of the dialog.

Next Tokencode:



A screenshot of a web browser window titled "DRAL-IBRIDGE NETWORKS | RSA Authentication". The main heading asks, "Wait for token to change, then enter the new tokencode:". Below this, there are two input fields: "Username" with the text "serge_drawbridgenetworks" and "Password" which is currently empty. A blue "Continue" button is located at the bottom right of the dialog.



Certification Checklist for RSA Authentication Manager

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	8.1 SP1	Virtual Appliance
DrawBridge Networks PathProtect	1.0	Linux

RSA SecurID Authentication

Date Tested: September 24th, 2015

Mandatory Functionality	Native UDP	Native TCP	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	N/A	N/A	✓
System Generated PIN	N/A	N/A	✓
User Defined (4-8 Alphanumeric)	N/A	N/A	✓
User Defined (5-7 Numeric)	N/A	N/A	✓
Deny 4 and 8 Digit PIN	N/A	N/A	✓
Deny Alphanumeric PIN	N/A	N/A	✓
Deny PIN Reuse	N/A	N/A	✓
Passcode			
16 Digit Passcode	N/A	N/A	✓
4 Digit Fixed Passcode	N/A	N/A	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	N/A	✓
On-Demand Authentication			
On-Demand Authentication	N/A	N/A	✓
On-Demand New PIN	N/A	N/A	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	N/A	✓
No RSA Authentication Manager	N/A	N/A	✓

✓ = Pass ✗ = Fail N/A = Non-Available Function