RSA SECURID® ACCESS
Implementation Guide

LogonBox Limited
LogonBox
Version 2.1

Peter Waranowski, RSA Partner Engineering
Last Modified: October 17th, 2017

RSA READY

Solution Summary

LogonBox brings the most important parts of identity management under one cloud-hosted solution, providing you with a flexible, affordable, solution, without the installation headache, so you can start benefiting right away; password self service, single sign-on, password manager, remote access.

LogonBox supports a wide variety of User Databases and authentication methods, including authenticating to RSA SecurID servers via the RADIUS protocol to allow customers to integrate with their pre-existing RSA infrastructure.

RSA SecurID Access Features	
LogonBox 2.1	
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	-
FIDO Token	-
SSO	
SAML SSO	-
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	-

Supported Authentication Methods by Integration Point

This section indicates which authentication methods are supported by integration point. The next section (Configuration Summary) contains links to the appropriate configuration sections for each integration point.

LogonBox integration with RSA Cloud Authentication Service

Authentication Methods	IDR SAML	Cloud SAML	HFED	REST	RADIUS
RSA SecurID	-	-	-	-	n/t
LDAP Password	-	-	-	-	n/t
Authenticate Approve	-	-	-	-	n/t
Authenticate Eyeprint ID	-	-	-	-	n/t
Authenticate Fingerprint	-	-	-	-	n/t
Authenticate Tokencode	-	-	-	-	n/t
FIDO Token	-	-	-		

LogonBox integration with RSA Authentication Manager

Authentication Methods	UDP Agent	TCP Agent	REST	RADIUS
RSA SecurID	-	-	-	✓
AM RBA	-			-

✓ Supported
\- Not supported
n/t Not tested

Configuration Summary

All of the supported use cases of RSA SecurID Access with LogonBox require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Authentication Manager – LogonBox can be integrated with RSA Authentication Manager in the following way:

RADIUS Client

Authentication Manager RADIUS Configuration
LogonBox RADIUS Configuration

RSA SecurID Access Server Side Configuration

RSA Authentication Manager Configuration

RADIUS

To configure your RSA Authentication Manager for use with a RADIUS Agent, you must configure a RADIUS client and a corresponding agent host record in the Authentication Manager Security Console.

The relationship of agent host record to RADIUS client in the Authentication Manager can 1 to 1, 1 to many or 1 to all (global).

RSA Authentication Manager RADIUS server listens on ports UDP 1645 and UDP 1812.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the LogonBox with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

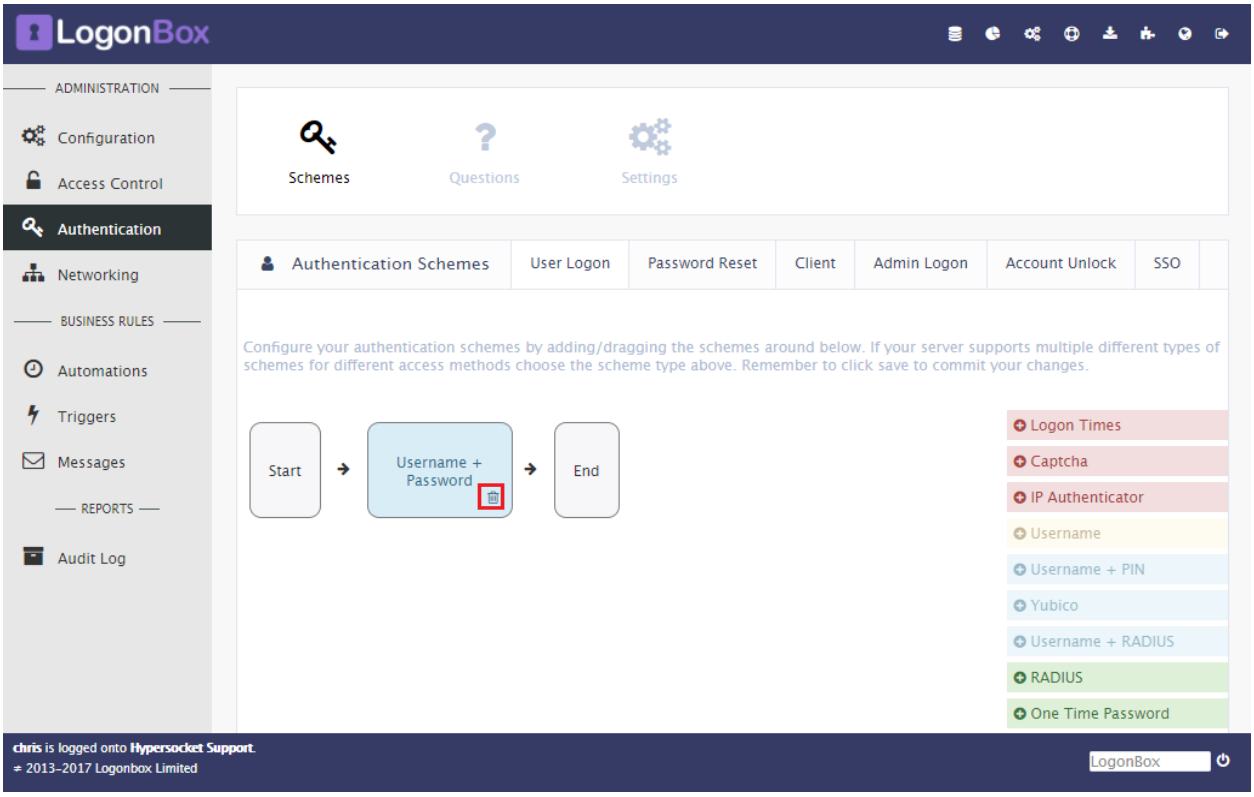
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

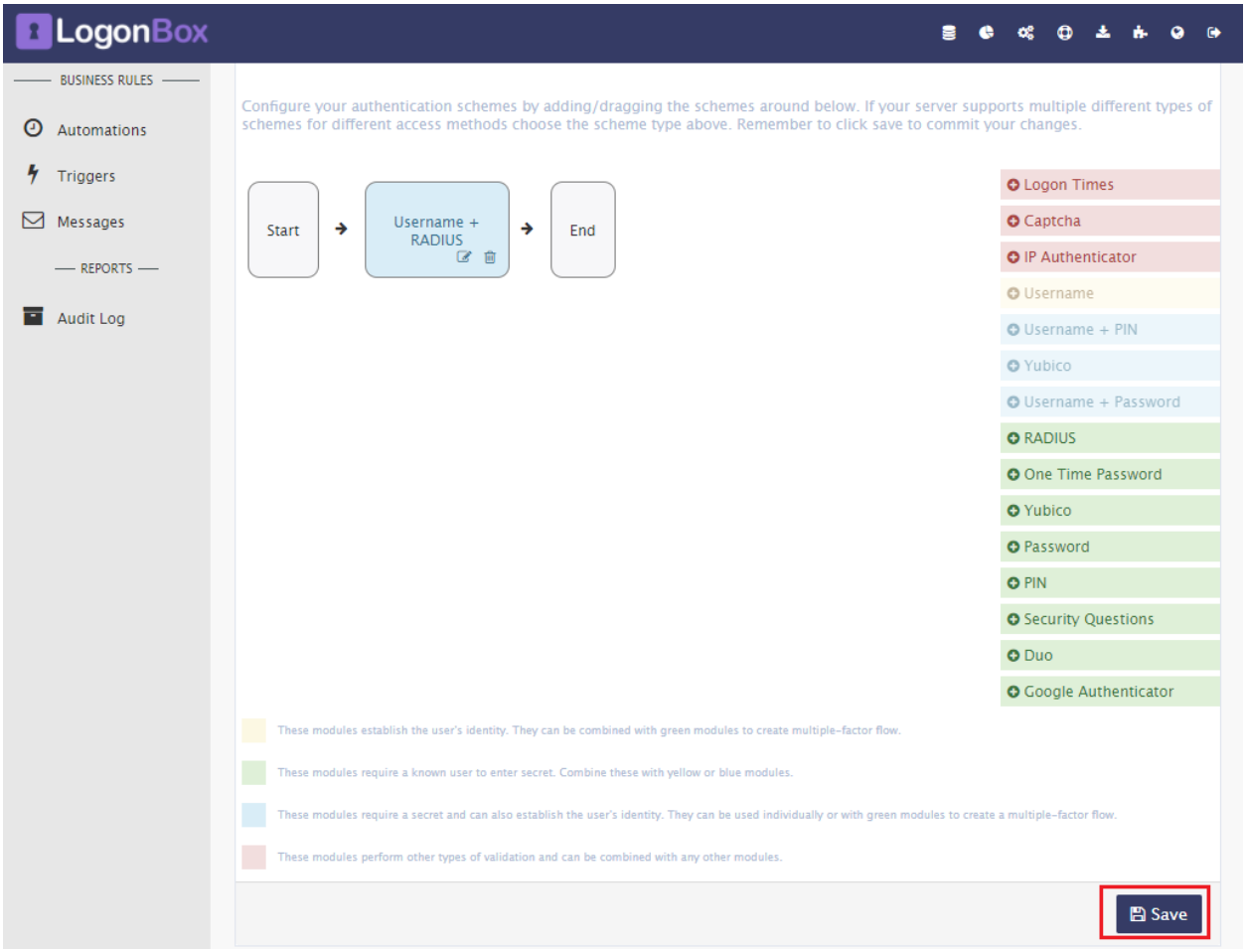
LogonBox RADIUS Client Configuration

Complete the steps in this section to integrate LogonBox with RSA SecurID Access using RADIUS authentication protocol.

1. Log on to your LogonBox realm and click on **Authentication** in the left hand navigation menu. Select the User Logon tab if it's not already selected and click the delete action on the existing **Username + Password** scheme to remove it.

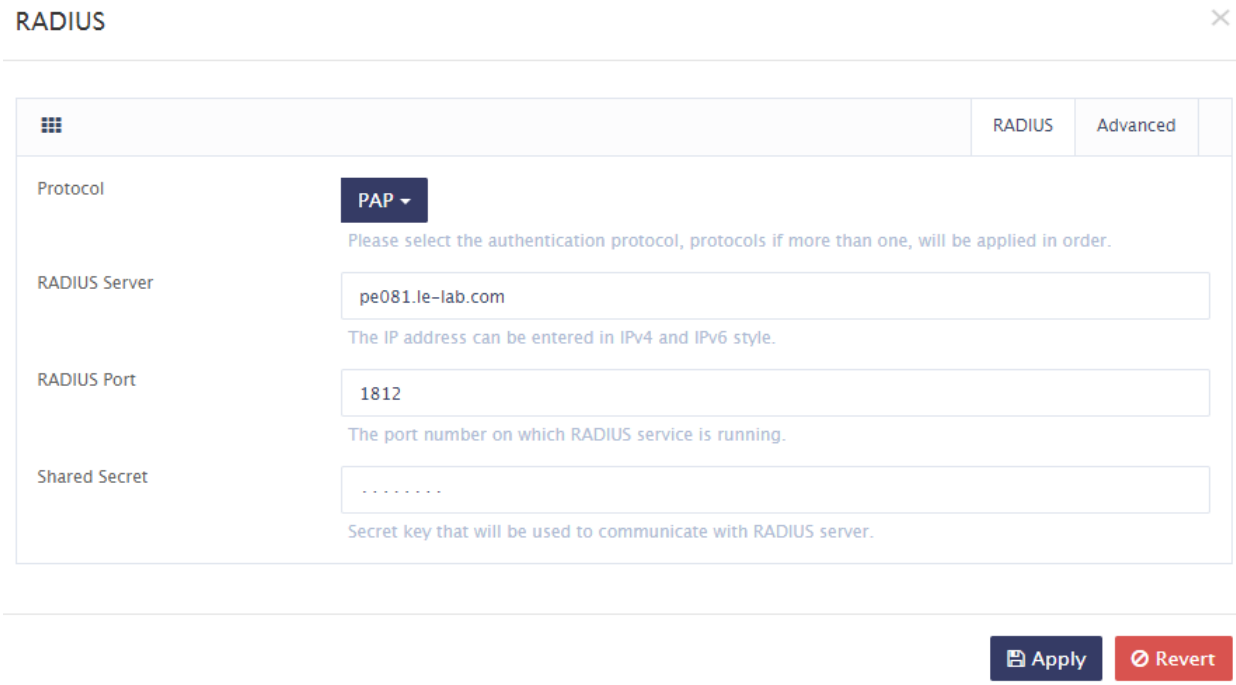


2. On the right hand side, click the "**+**" icon next to **Username + RADIUS** to add this to the scheme and click **Save** at the bottom of the page.



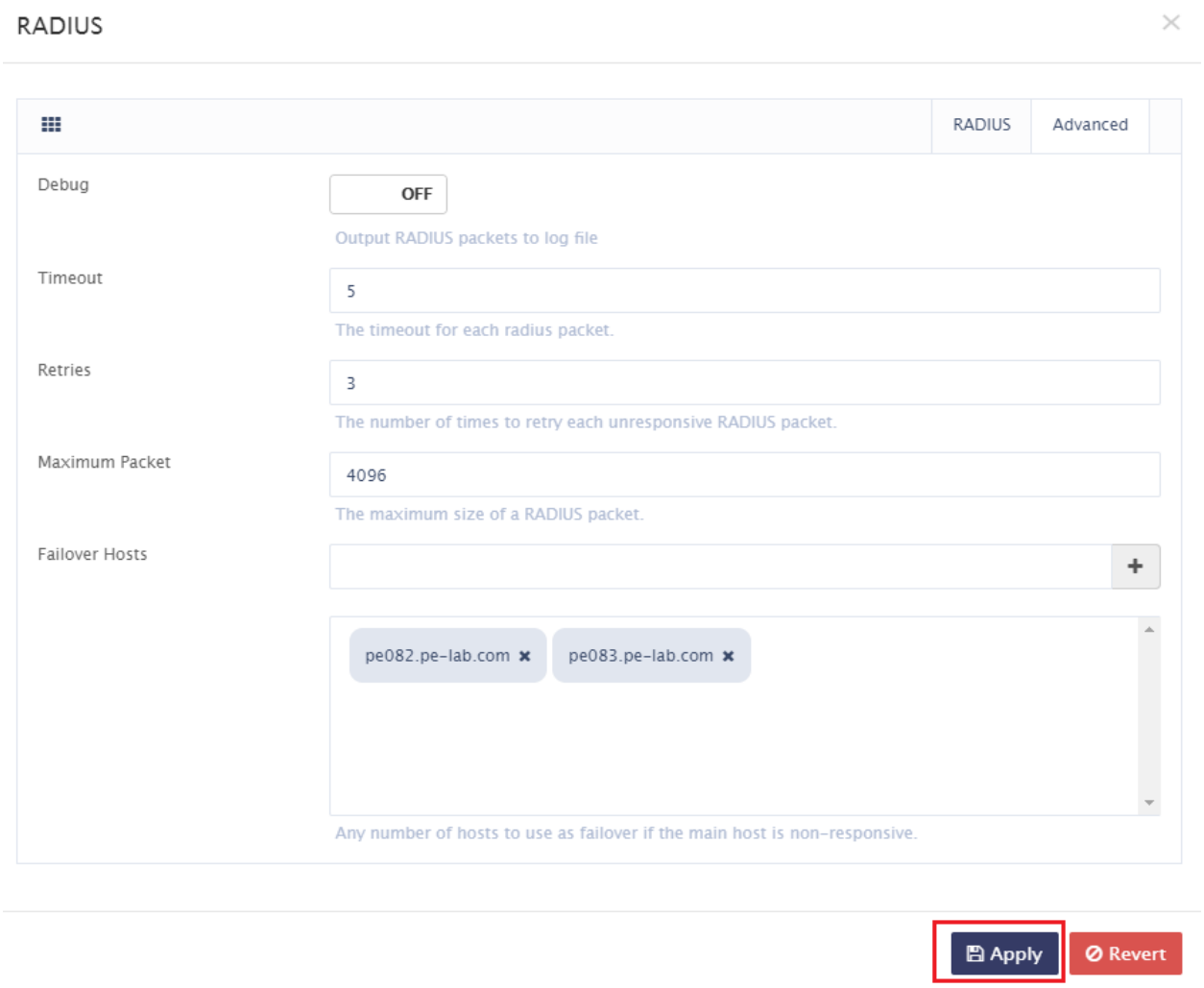
3. Click the edit icon in the **Username + RADIUS** module.

4. Configure the RADIUS server settings and click **Apply**.



- Select **PAP** from the Protocol drop-down menu.
- Enter the IP address or hostname of your RSA Authentication Manager server.
- Enter the RADIUS port of your RSA Authentication Manager. RSA Authentication Manager listens on both UDP 1812 and UDP 1645 by default.
- Enter the Shared Secret to match the shared secret as configured for this client in the RSA Authentication Manager server.

5. (Optional) Click on the **Advanced** tab. Here you can alter settings such as timeout periods and retry attempts as well as add any failover servers you want to use. Click **Apply** to complete the configuration.



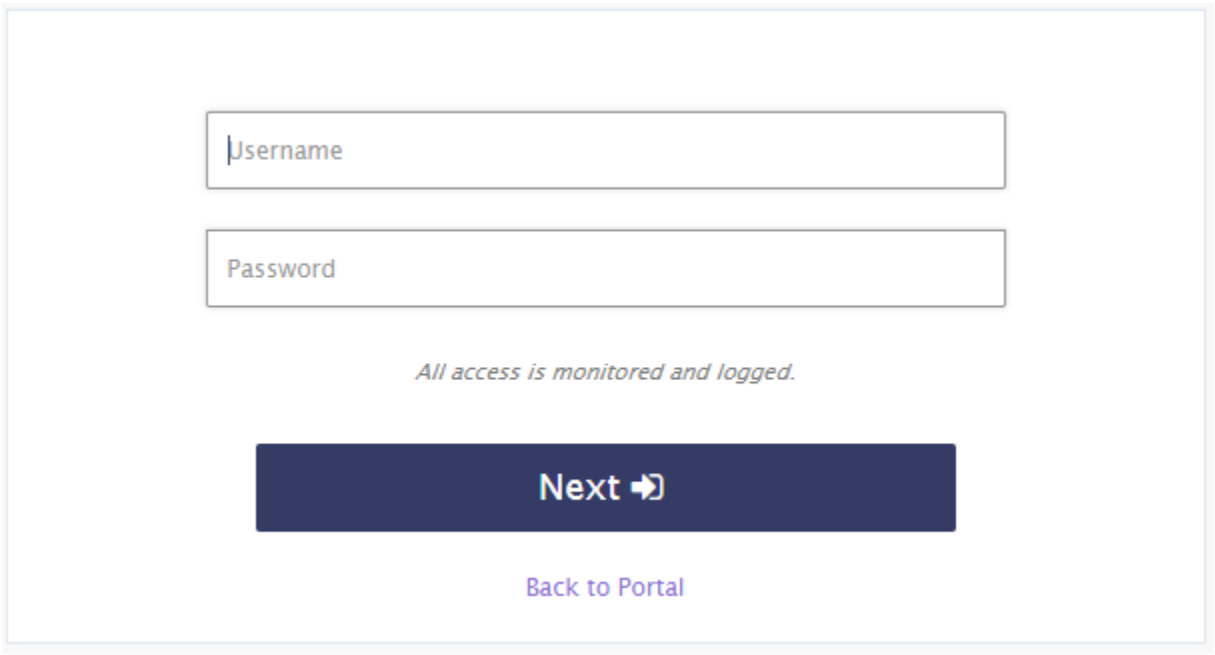
Your LogonBox realm is now configured for RSA SecurID Authentication.

! Important: LogonBox connects to a User Database so it can cache user objects so that users can be assigned to various resources. As it's not possible to list and cache users from a RADIUS server, this means that you will generally be using a third party user database, such as Active Directory.

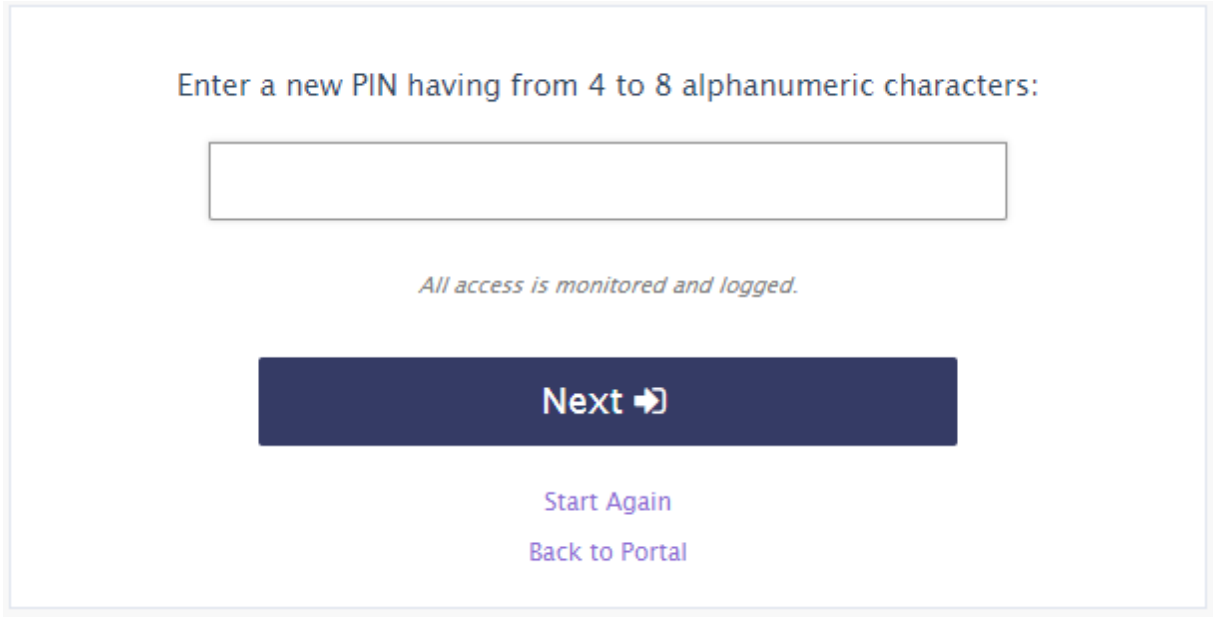
LogonBox requires that your usernames on your User Database match the usernames that you will be using to authenticate to RSA SecurID.

Login Screenshots

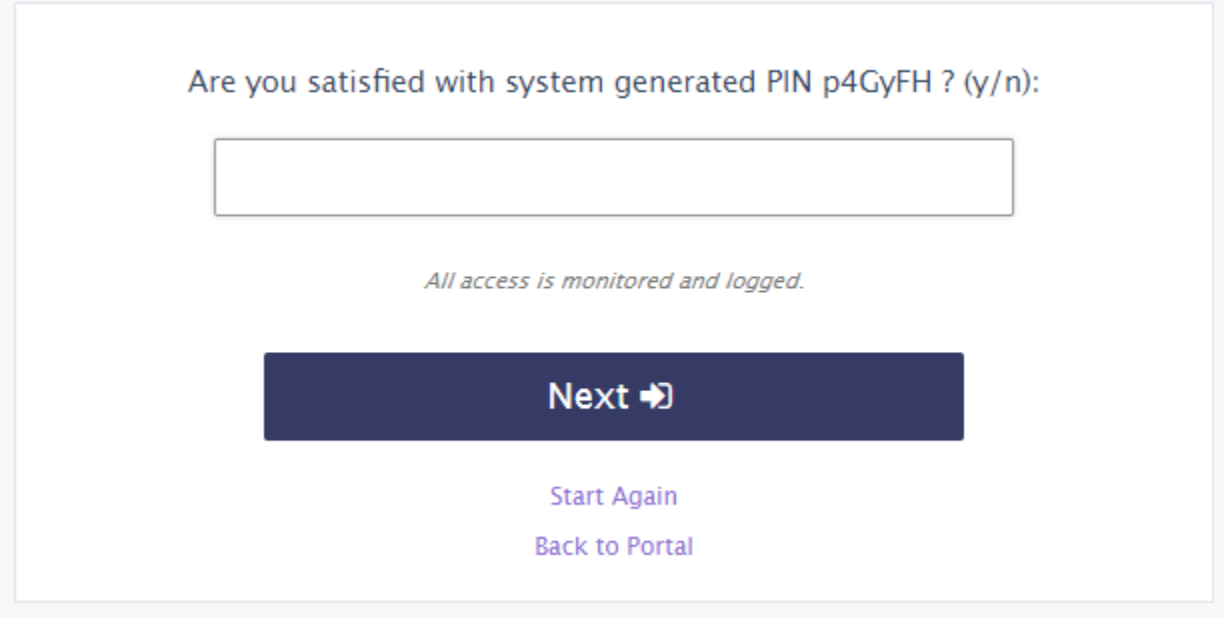
Login screen:



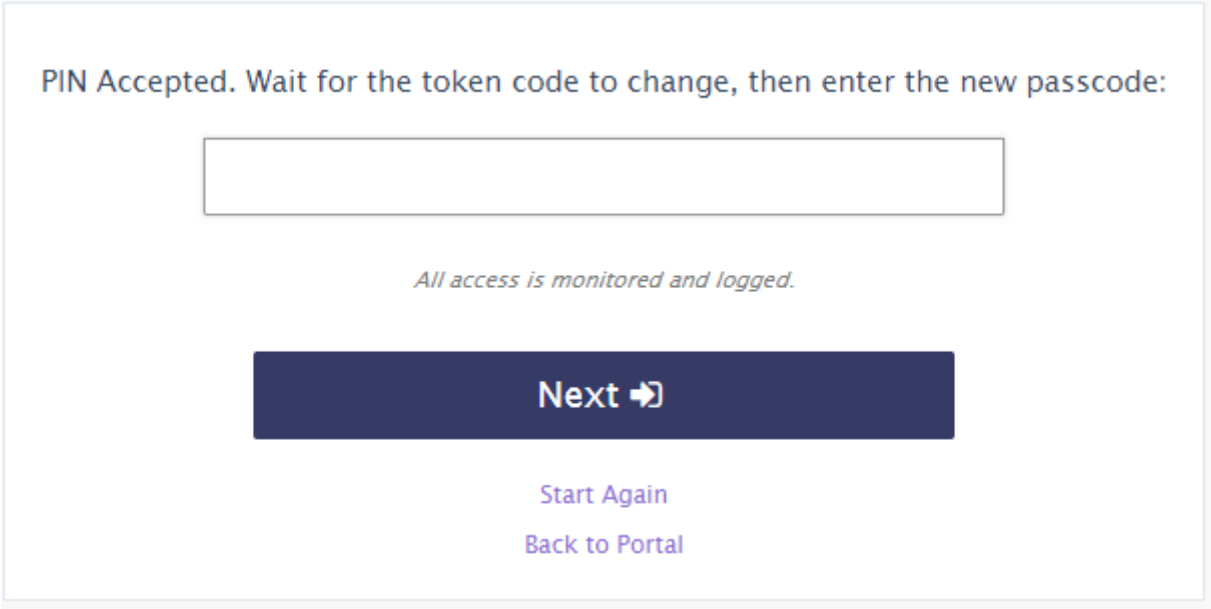
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA SecurID Access

Certification Environment Details:

RSA Authentication Manager 8.2 SP1, Virtual Appliance

LogonBox 2.1.0, Virtual Appliance

RSA Authentication Manager

Date Tested: August 11th, 2017

Authentication Method	REST Client	UDP Agent	TCP Agent	RADIUS Client
RSA SecurID	-	-	-	✓
RSA SecurID Software Token Automation	-	-	-	-
On Demand Authentication	-	-	-	✓
Risk-Based Authentication		-		-

✓ = Passed, **X** = Failed, **-** = N/A