RSA SECURID® ACCESS
Implementation Guide

Intelligent Waves, LLC
Hypori Server 4.2

Peter Waranowski, RSA Partner Engineering
Last Modified: June 7th, 2018

RSA READY

Solution Summary

Hypori by Intelligent Waves (IW) is a proprietary virtual smartphone technology that represents a new and comprehensive approach to Enterprise Mobility Management (EMM) and Mobile Device Management (MDM). Hypori virtualizes the entire mobile experience - moving everything into a managed and secure environment.

While access to the Hypori service requires a mutually authenticated TLS connection, customers may wish to augment that authentication with additional forms of authentication – in particular, RSA SecurID tokens or mobile app enabled methods. When combining the Hypori X.509 authentication with RSA Authentication Manager or Cloud Authentication Service, administrators can be confident that the user connecting to the Hypori server is who they say they are and is connecting from their approved mobile device.

RSA SecurID Access Features	
Intelligent Waves Hypori Server 4.2	
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.

Intelligent Waves Hypori Server integration with RSA Cloud Authentication Service

Authentication Methods	REST	IDR SAML	Cloud SAML	HFED	RADIUS
RSA SecurID	-	-	-	-	✓
LDAP Password	-	-	-	-	✓
Authenticate Approve	-	-	-	-	✓
Authenticate Tokencode	-	-	-	-	✓
Device Biometrics	-	-	-	-	✓
SMS Tokencode	-	-	-	-	✓
Voice Tokencode	-	-	-	-	✓
FIDO Token		-	-	-	

Intelligent Waves Hypori Server integration with RSA Authentication Manager

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

✓ Supported
\- Not supported
n/t Not yet tested or documented, but may be possible

Configuration Summary

All of the supported use cases of RSA SecurID Access with Intelligent Waves Hypori Server 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 Cloud Authentication Service – Intelligent Waves Hypori Server can be integrated with RSA Cloud Authentication Service in the following way:

RADIUS Client

Cloud Authentication Service RADIUS Configuration
Intelligent Waves Hypori Server RADIUS Configuration

RSA Authentication Manager – Intelligent Waves Hypori Server can be integrated with RSA Authentication Manager in the following way:

RADIUS Client

Authentication Manager RADIUS Configuration
Intelligent Waves Hypori Server RADIUS Configuration

RSA SecurID Access Configuration

RSA Cloud Authentication Service Configuration

RADIUS

To configure RADIUS for Cloud Authentication Service for use with a RADIUS client, you must first configure a RADIUS client in the RSA SecurID Access Console.

Logon to the RSA SecurID Access console and browse to **Authentication Clients** > **RADIUS** > **Add RADIUS Client** and enter the **Name**, **IP Address** and **Shared Secret**. Click **Publish** to push your configuration change to the RADIUS server.

RSA Cloud Authentication RADIUS server listens on port UDP 1812.

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 be 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 Intelligent Waves Hypori Server with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

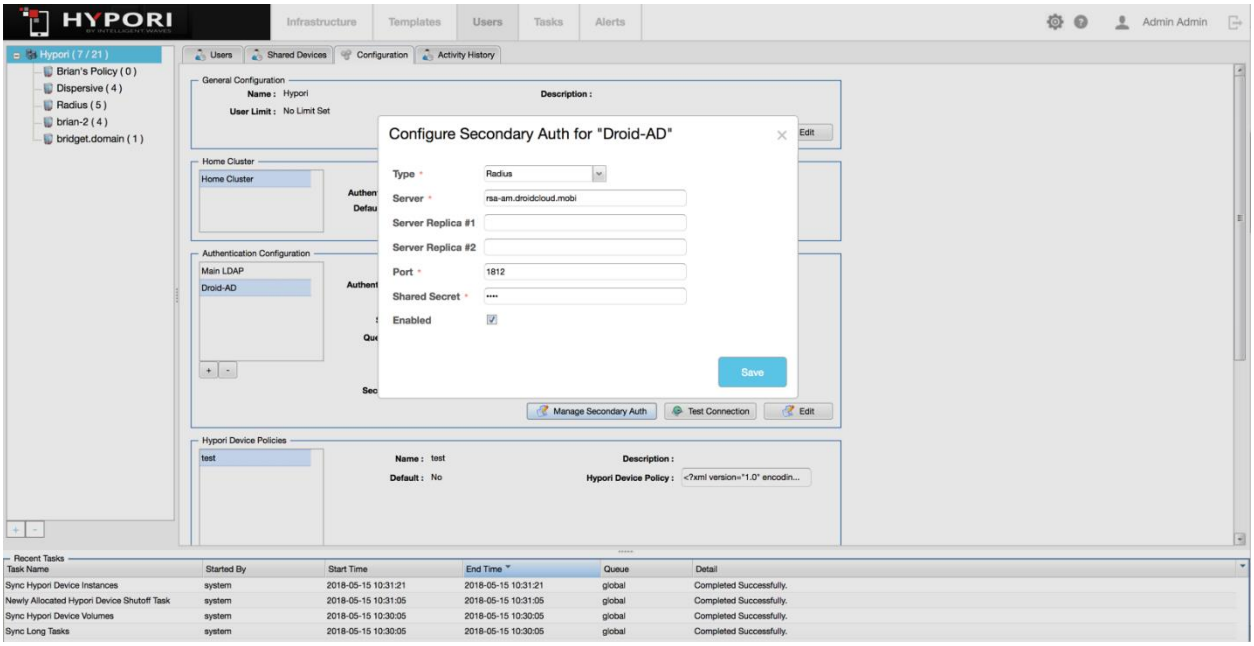
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

Intelligent Waves Hypori Server RADIUS Configuration

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

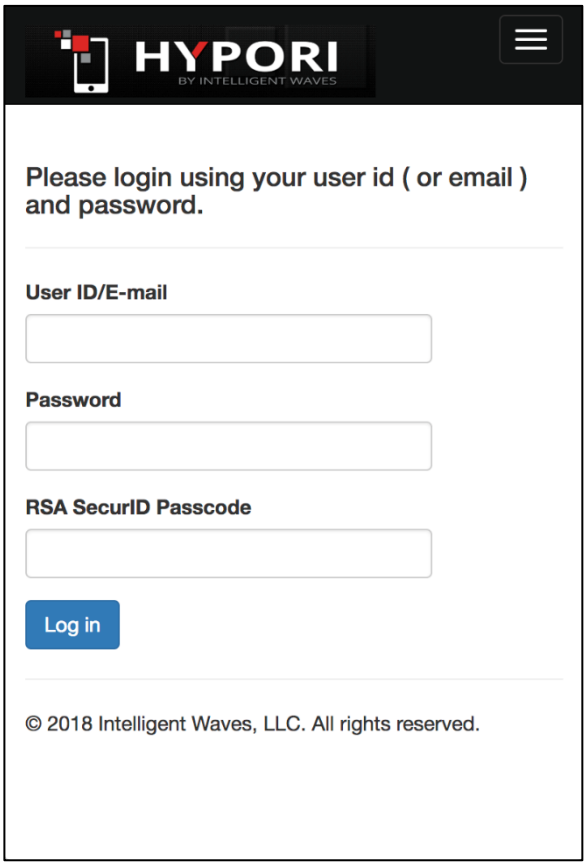
1. Logon to the Hypori admin console, open the **Users** tab and **Configuration** sub-tab.
2. Select the option to **Manage Secondary Auth**, configure the settings and click **Save**.



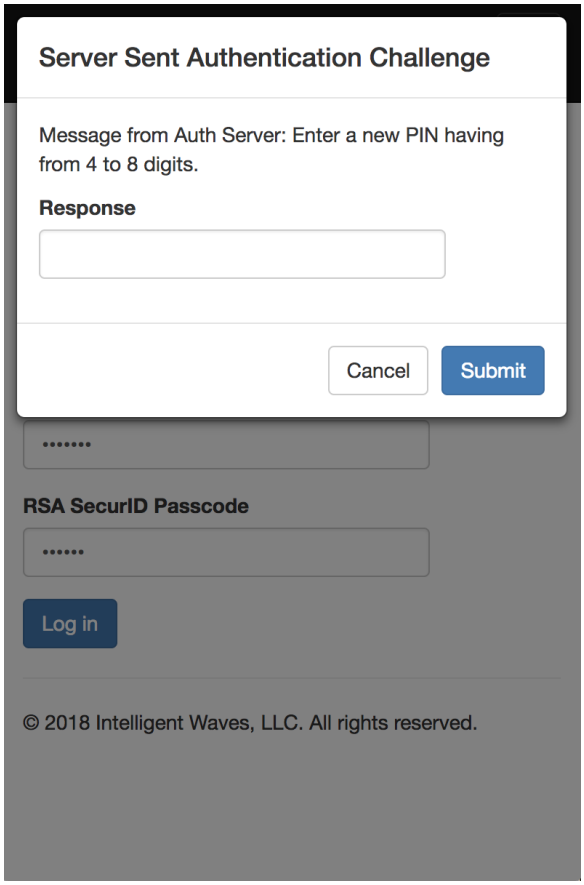
- **Type**: Select **Radius.**
- **Server**: Enter the hostname or IP address of the RSA RADIUS server.
- **Server Replica #1-2**: Enter the hostname or IP address of the RSA RADIUS replica server if any.
- **Port**: Enter **1812.**
- **Shared Secret:** Enter the same shared secret as configured in the RSA RADIUS server.
- **Enabled:** Mark the checkbox to enable the configuration.

Login Screenshots

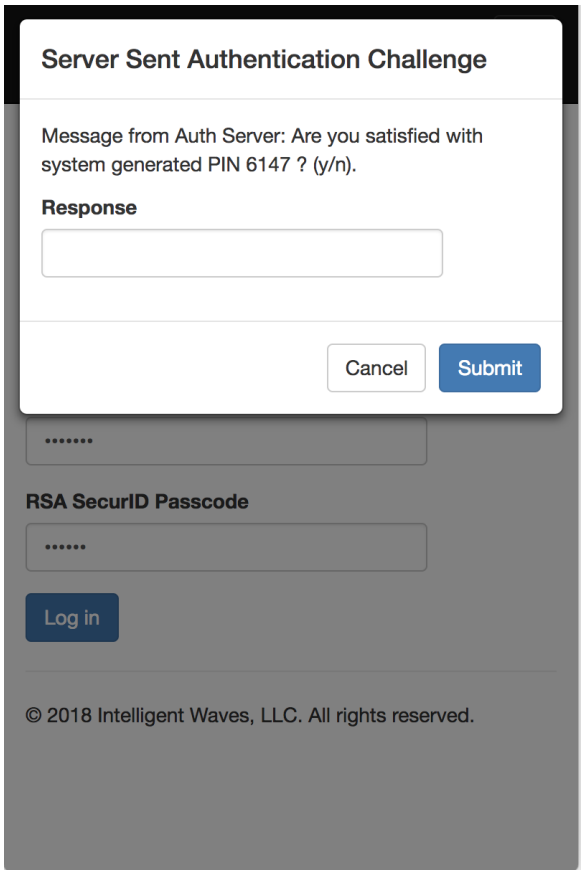
Login Screen:



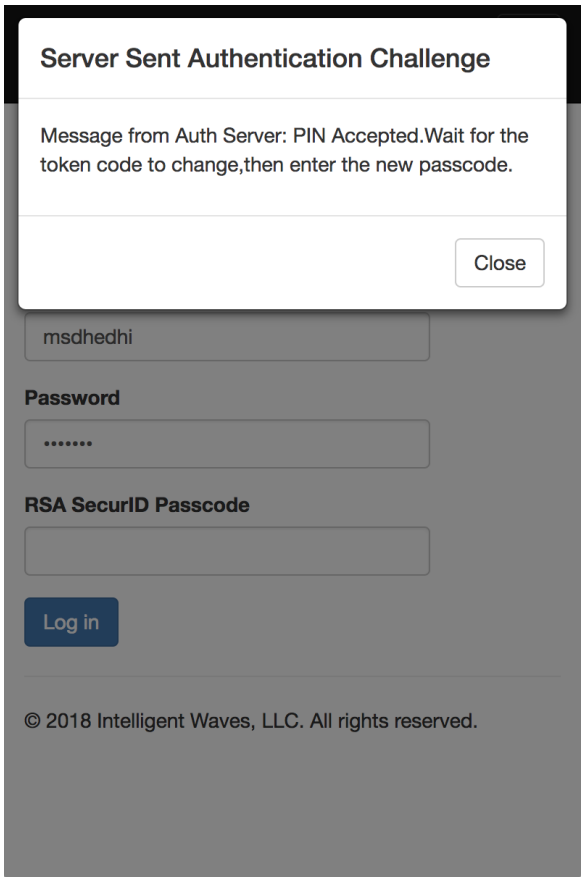
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA SecurID Access

Certification Environment Details:

RSA Authentication Manager 8.2, Virtual Appliance

Intelligent Waves Hypori Server 4.2

Intelligent Waves Hypori Client 4.1.3

RSA Cloud Authentication Service

Date Tested: May 7th, 2018

Authentication Method	REST Client	RADIUS Client
RSA SecurID	-	✓
LDAP Password	-	✓
Authenticate Approve	-	✓
Authenticate Tokencode	-	✓
Device Biometrics	-	✓
SMS Tokencode	-	✓
Voice Tokencode	-	✓
FIDO Token	-	

RSA Authentication Manager

Date Tested: May 1st, 2018

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