RSA SecurID Access Implementation Guide

WALLIX GROUP

Bastion 6.0

Peter Waranowski, RSA Partner Engineering

Last modified: March 29th, 2019

Table of Contents

Solution Summary

This section shows all of the ways that WALLIX Bastion can integrate with RSA SecurID Access. Use this information to determine which use case and integration type your deployment will employ.

Use Cases

User Sign-In - When integrated, users must authenticate with RSA SecurID Access in order to sign-in to the Wallix Bastion. User Sign-In can be integrated with RSA SecurID Access using RADIUS.

Integration Types

RADIUS integrations provide a text driven interface for RSA SecurID Access within the partner application. RADIUS provides support for most RSA SecurID Access authentication methods and flows.

Supported Features

This section shows all of the supported features by integration type and by RSA SecurID Access component. Use this information to determine which integration type and which RSA SecurID Access component your deployment will use. The next section in this guide contains the instruction steps for how to integrate RSA SecurID Access with WALLIXBastion using each integration type.

WALLIX Bastion integration with RSA Cloud Authentication Service

Authentication Methods	Authentication API	RADIUS	Relying Party	SSO Agent
RSA SecurID	-	✔	-	-
LDAP Password	-	✔	-	-
Authenticate Approve	-	✔	-	-
Authenticate Tokencode	-	✔	-	-
Device Biometrics	-	✔	-	-
SMS Tokencode	-	✔	-	-
Voice Tokencode	-	✔	-	-
FIDO Token	n/a	n/a	-	-

WALLIX Bastion integration with RSA Authentication Manager

Authentication Methods	Authentication API	RADIUS	Authentication Agent
RSA SecurID	-	✔	-
On Demand Authentication	-	✔	-
Risk-Based Authentication	n/a	-	-

✔ Supported

- Not supported

n/t Not yet tested or documented, but may be possible.

Configuration Summary

This section contains links to the sections that contain instruction steps that show how to integrate WALLIX Bastion with RSA SecurID Access using all of the integration types and also how to apply them to each supported use case. First configure the integration type (e.g. RADIUS) then configure the use case (e.g. User Sign-In).

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 RSA SecurID Access and WALLIX Bastion components must be installed and working prior to the integration.

Integration Configuration

RADIUS with AM

RADIUS with CAS

Use Case Configuration

User Sign-In

Certification Details

Date of testing: January, 2019

RSA Cloud Authentication Service

RSA Authentication Manager 8.3, Virtual Appliance

WALLIX Bastion 6.0

Known Issues

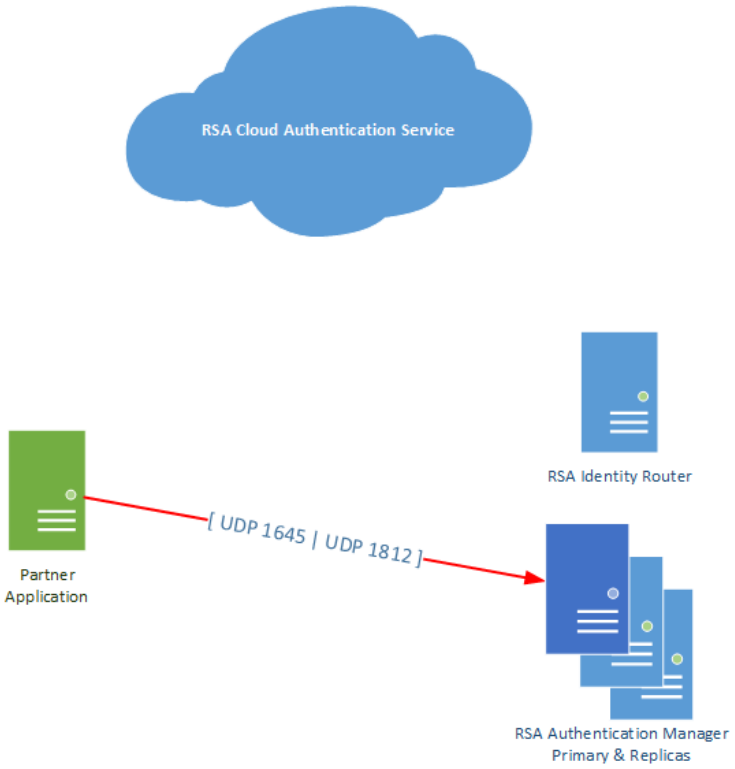
No known issues.

Integration Configuration

RADIUS with AM

This section contains instructions on how to integrate WALLIX Bastion with RSA Authentication Manager using RADIUS.

Architecture Diagram



RSA Authentication Manager

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 listens on ports UDP 1645 and UDP 1812.

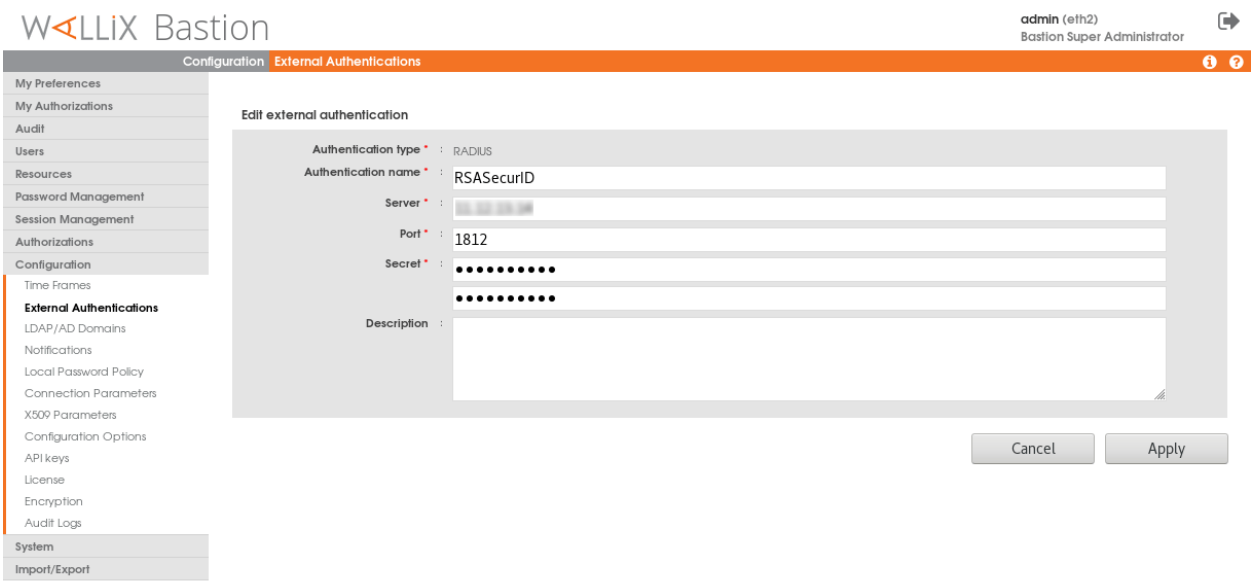
WALLIX Bastion

Follow the steps in this section to configure WALLIX Bastion as a RADIUS client to RSA Authentication Manager.

Procedure

1. Sign in to Wallix Bastion Administrative user interface and browse to **Configuration** > **External Authentication** and click to add a new **RADIUS** server.

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



- Authentication Name: Enter a descriptive name for the RSA Authentication Manager.
- Server: Enter the hostname or IP address of the primary RSA Authentication Manager server.
- Port: Enter 1812 or 1645.
- Secret: Enter the RADIUS shared secret to match as specified in the RSA AM Security Console.

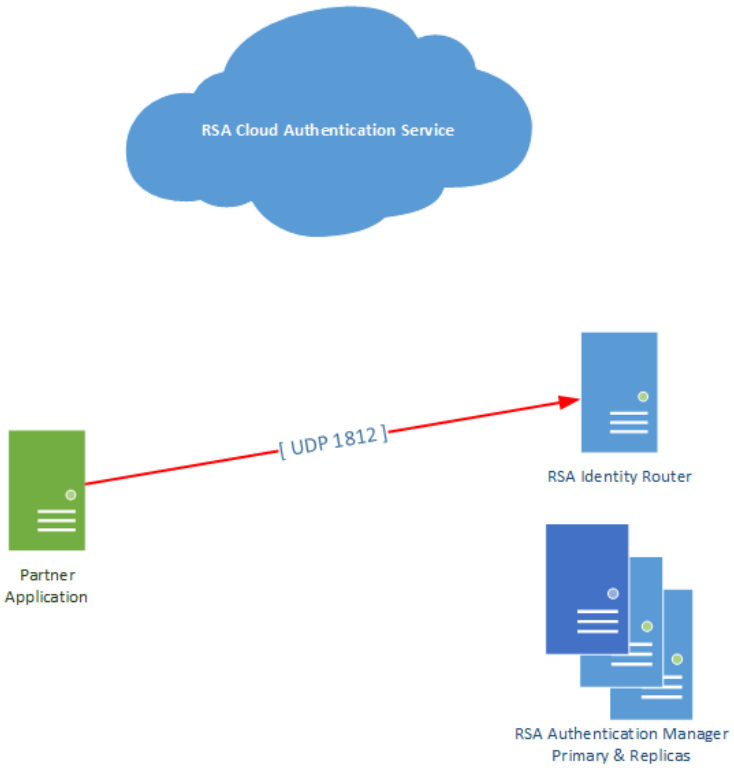
3. Repeat steps 1-2 for AM replica servers.

Next Step: Proceed to the Use Case section for information on how to apply the RADIUS configuration to the use case.

RADIUS with CAS

This section contains instructions on how to integrate WALLIXBastion with RSA Cloud Authentication Service using RADIUS.

Architecture Diagram



RSA Cloud Authentication Service

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 Cloud Administrative Console** and browse to **Authentication Clients** > **RADIUS** > **Add RADIUS Client** and enter the **Name**, **IP Address** and **Shared Secret**.

Click **Publish**.

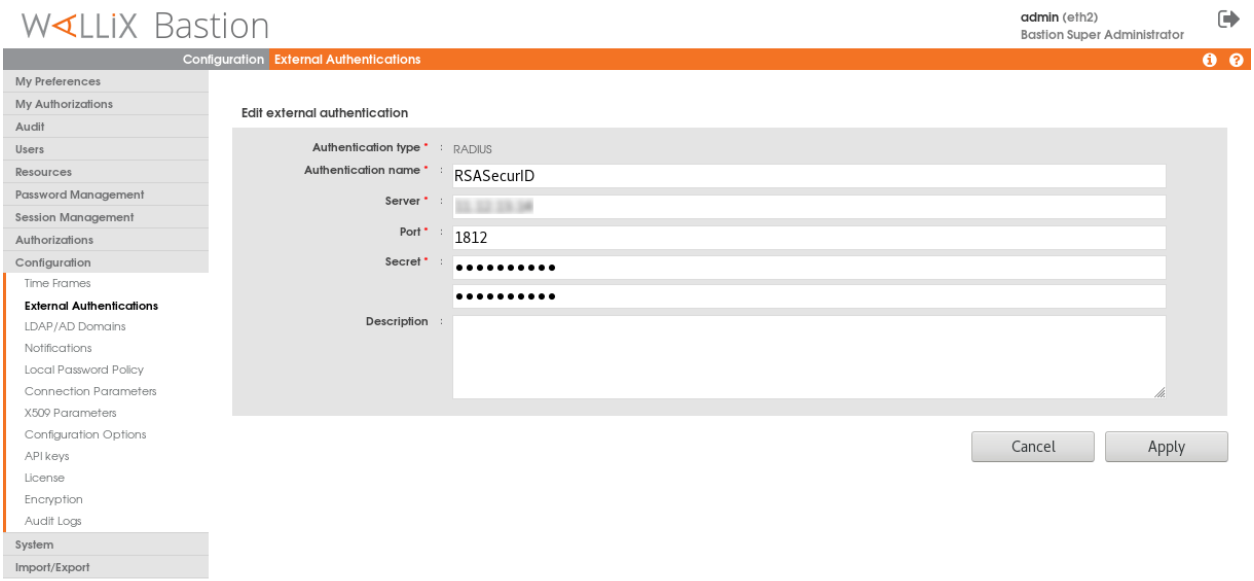
WALLIX Bastion

Follow the steps in this section to configure WALLIX Bastion as a RADIUS client to RSA Cloud Authentication Service.

Procedure

1. Sign in to Wallix Bastion Administrative user interface and browse to **Configuration** > **External Authentication** and click to add a new **RADIUS** server.

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



- Authentication Name: Enter a descriptive name for the RSA Identity Router.
- Server: Enter the hostname or IP address of the RSA Identity Router.
- Port: Enter 1812.
- Secret: Enter the RADIUS shared secret to match as specified in the RSA Cloud Administration Console.

3. Repeat steps 1-2 for replica RSA Identity Routers.

Next Step: Proceed to the Use Case section for information on how to apply the RADIUS configuration to the use case.

Use Case Configuration

User Sign-In

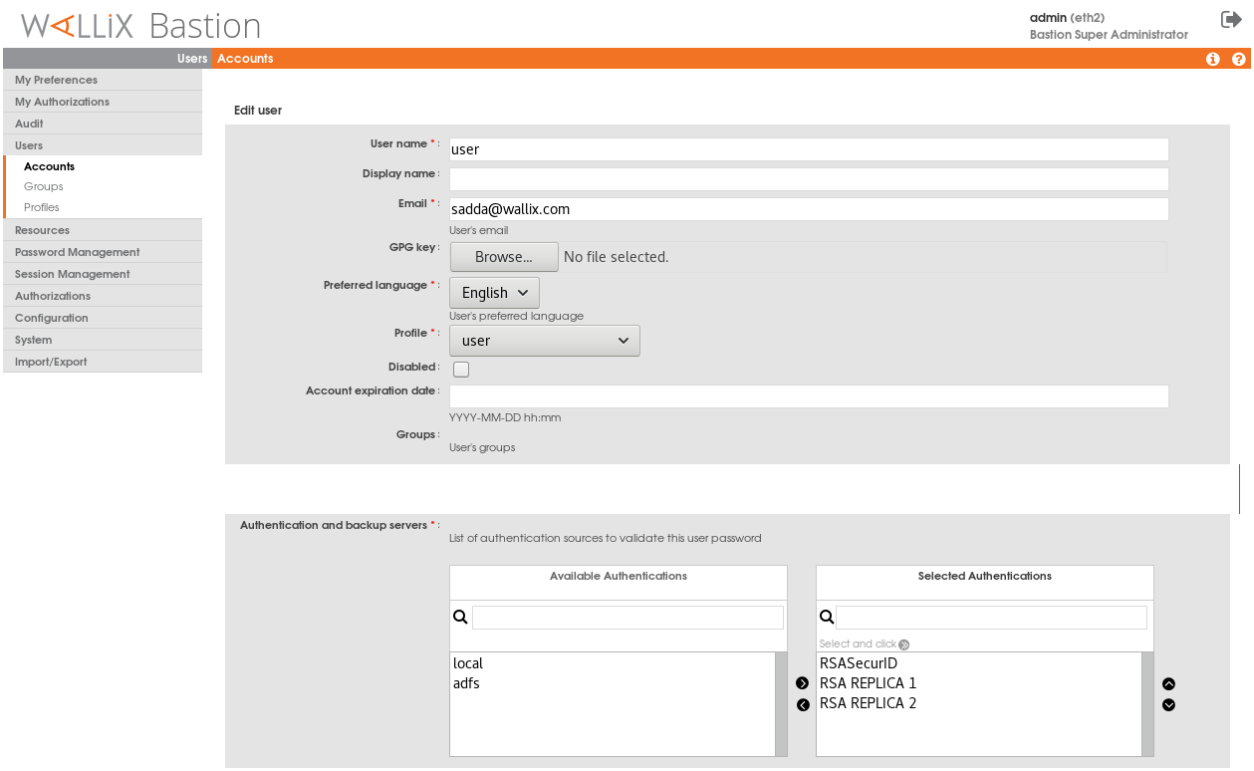
Follow the instruction steps in this section to apply your RADIUS configuration to WALLIX Bastion User Sign-In.

Before you begin: Configure the integration type that your use case will employ. Refer to the Integration Configuration Summary section for more information.

Procedure

1. Sign in to Wallix Bastion Administrative user interface and browse to **Users** > **Accounts** and click to add or edit the user that will authenticate using RSA SecurID Access.

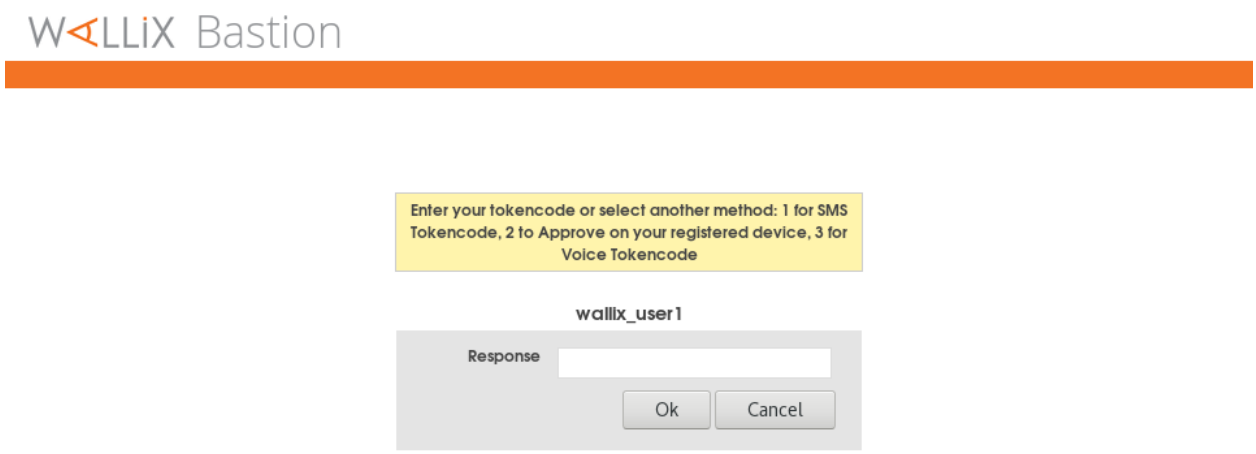
2. In the **Authentication and backup servers** section, move the appropriate RSA SecurID Access server(s) to the **Selected Authentications** field and click to apply.



Configuration is complete.

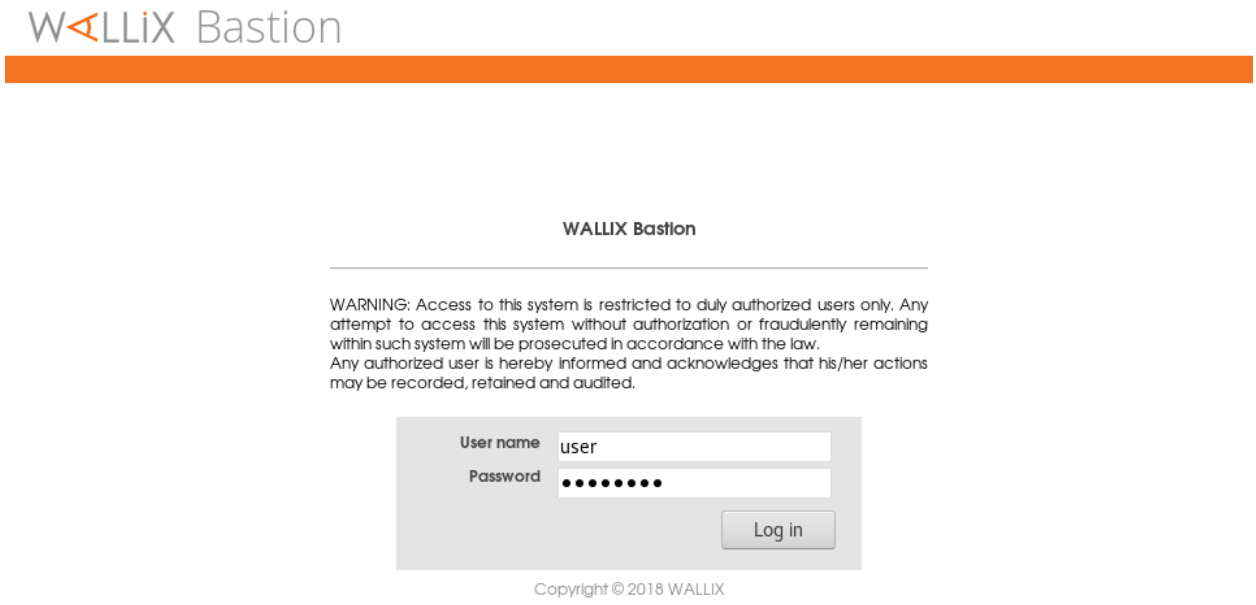
User Experience - RSA Cloud Authentication Service

Method selection screen

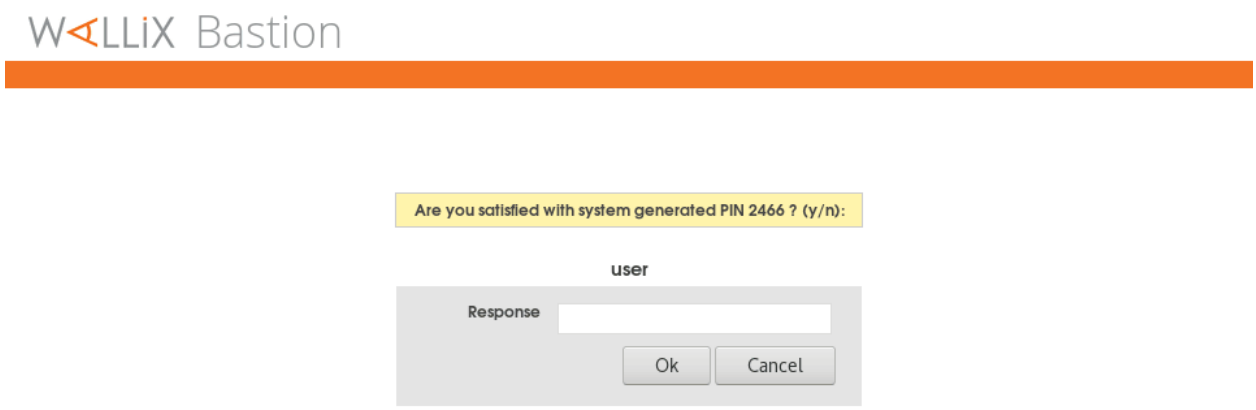


User Experience - RSA Authentication Manager

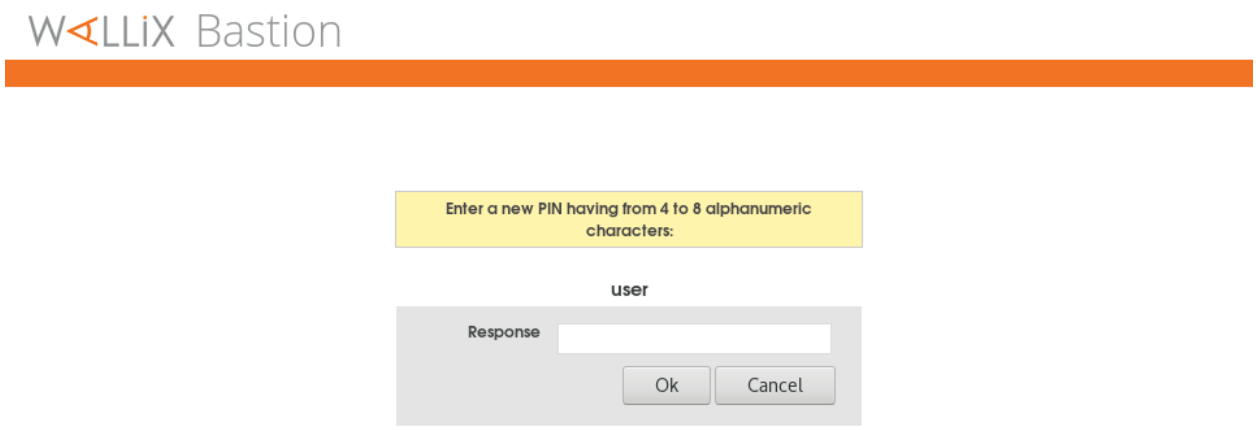
Login Page



System generated new PIN



User defined new PIN



Head back to the main page for more certification related information.