RSA SecurID Access Implementation Guide

ZPE Systems, Inc

Nodegrid 4.1

Certified: August 21, 2019

Table of Contents

Solution Summary

This section describes the way in which ZPE Nodegrid can integrate with RSA SecurID Access.

Use Case

User sign in - When integrated, users must authenticate with RSA SecurID Access in order to sign in to Nodegrid. User sign in can be integrated with RSA SecurID Access using **SecurID Authentication API**.

Integration Types

SecurID Authentication API integrations can provide a rich user interface with all RSA SecurID Access features within the partner application. Refer to the Supported Features section in this guide see which features this partner application has implemented.

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 contains the steps to integrate RSA SecurID Access with ZPE Nodegrid for each integration type.

ZPE Nodegrid Integration with RSA Cloud Authentication Service

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

ZPE Nodegrid Integration with RSA Authentication Manager

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

✔ Supported

- Not supported

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

Configuration Summary

The following links provide instructions on how to integrate ZPE Nodegrid with RSA SecurID Access.

This document is not intended to suggest optimum installations or configurations. It assumes 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 ZPE Nodegrid components must be installed and working prior to the integration.

Integration Configuration

- SecurID Authentication API with AM
- SecurID Authentication API with CAS

Use Case Configuration

- User sign in

Certification Details

Date of testing: August 6, 2019

RSA Cloud Authentication Service

RSA Authentication Manager 8.3

ZPE Nodegrid 4.1

Known Issues

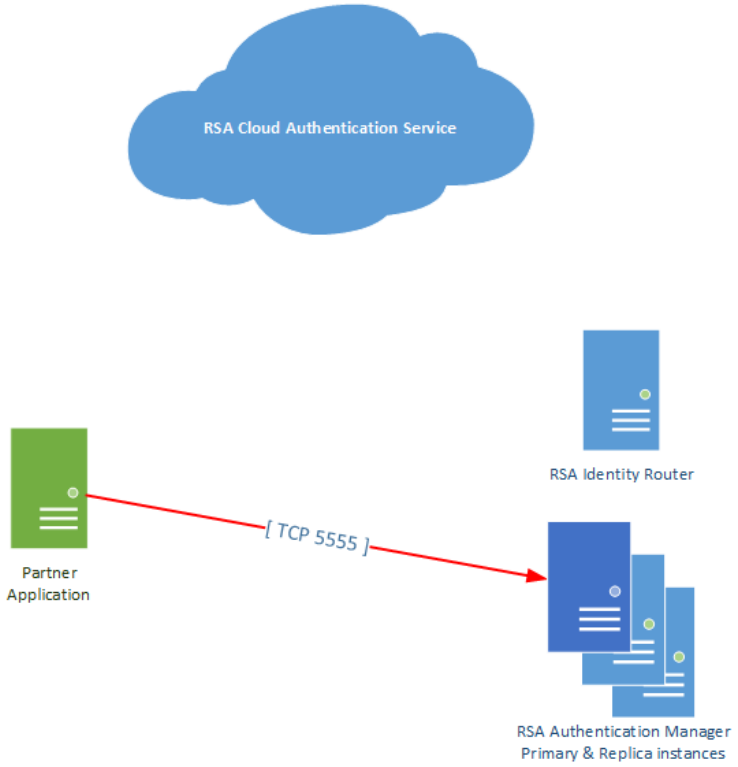
No known issues

Integration Configuration

SecurID Authentication API with AM

This section describes how to integrate ZPE Nodegrid with RSA Authentication Manager using SecurID Authentication API.

Architecture Diagram



Configure RSA Authentication Manager

To configure the integration with RSA Authentication Manager, you must enable the REST Service and then create an authentication agent.

Sign into the **Security Console** and browse to **Setup** > **System Settings** > **REST Service**, mark the checkbox to enable **REST Service** and make note of the **Agent Credentials**. The Agent Credentials will be needed during configuration of the agent.

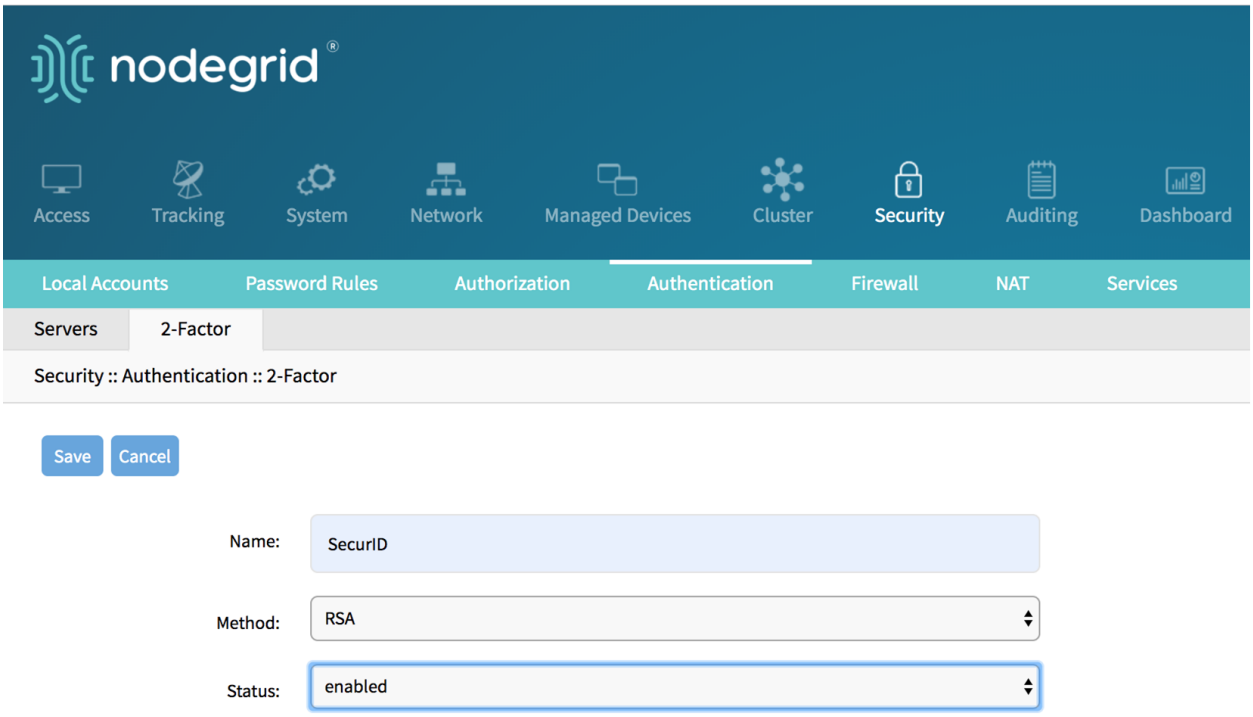
Browse to **Access** > **Authentication Agents** and click **Add New**. Enter the name of your authentication agent in the **Hostname** field and click **Save**.

Configure ZPE Nodegrid

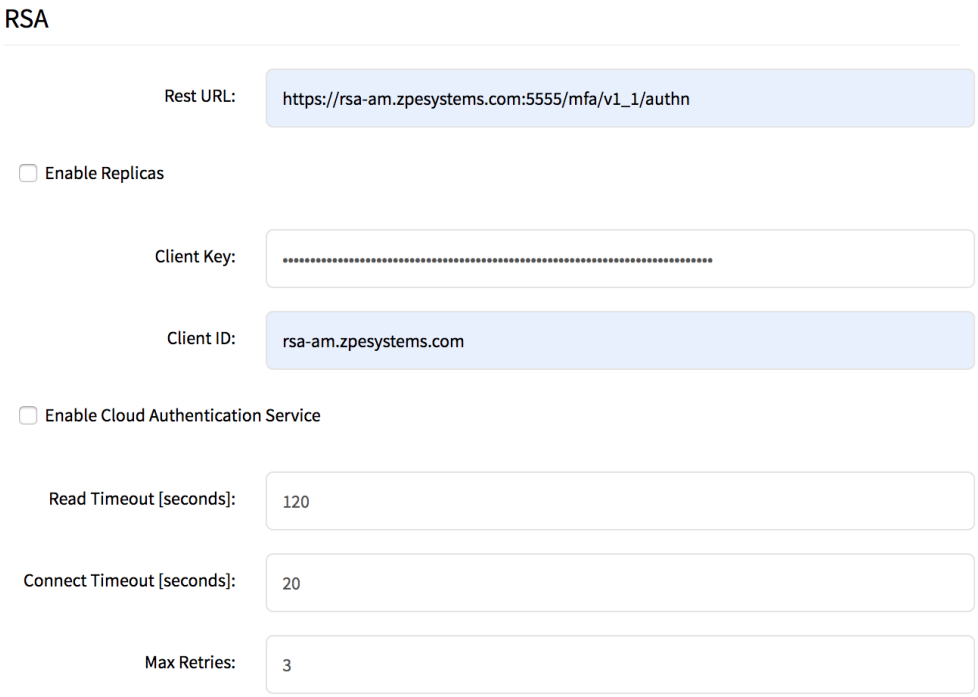
Perform these steps to configure ZPE Nodegrid as an authentication API client to RSA Authentication Manager.

Procedure

1. Sign into Nodegrid Web Interface as admin, browse to **Security** > **Authentication** > **2-Factor** and click **Add**.
2. Configure the 2-Factor settings and then scroll down to the **RSA** section.
   a. Enter a **Name** to identify the method. For example: SecurID
   b. Select **RSA** from the Method drop-down menu.
   c. Select **enabled** from the Status drop-down menu.



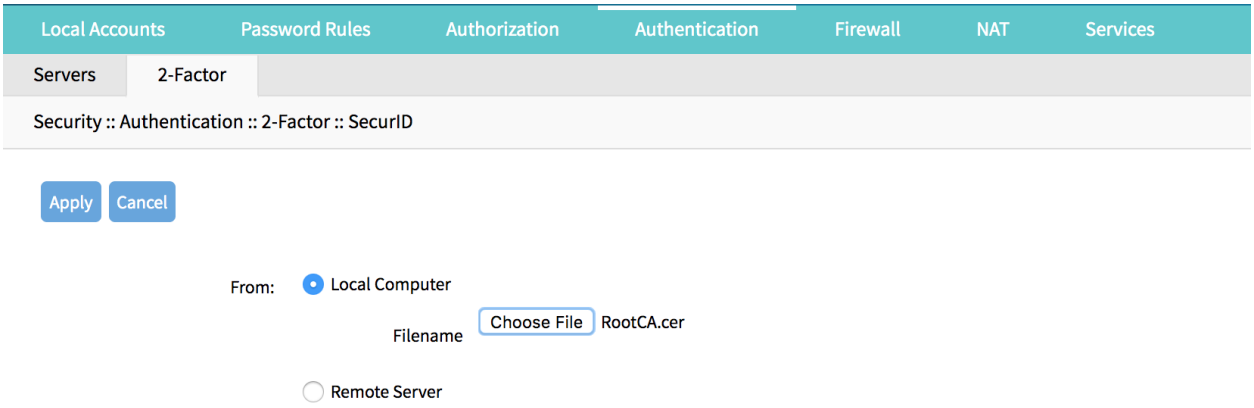
3. Configure the RSA server settings and click **Save**.
   a. **REST URL**: Enter the REST URL for the RSA Authentication Manager you wish to authenticate with. For example: https://am1.domain.local:5555/mfa/v1_1/authn
   b. **Enable Replicas**: Mark the check box and enter up to 15 AM replica REST URLs (one per line).
   c. **Client Key**: Enter the RSA SecurID Authentication API Access Key located in the RSA Authentication Manager Security Console.
   d. **Client ID**: Enter the name of the corresponding authentication agent host name as specified in the RSA Authentication Manager Security Console.



4. After saving, edit the RSA 2-Factory method and upload the certificate which allows Nodegrid to trust RSA Authentication Manager.

a. Follow the steps in this link to acquire the certificate for RSA Authentication Manager.

b. Click the **Certificate** button, upload the certificate file and click **Apply**.

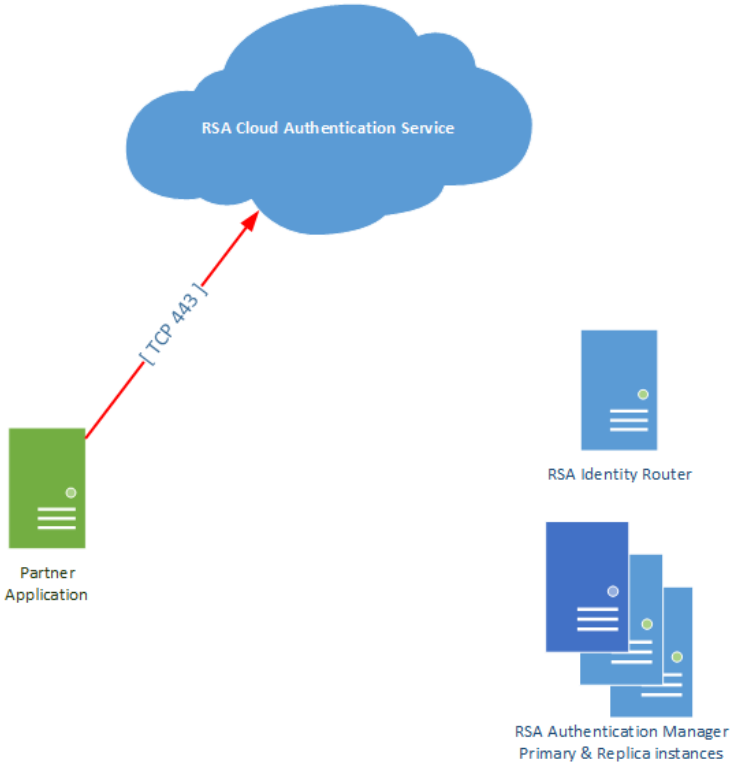


Next Step: Proceed to the Use case configuration section for the steps to apply this configuration to the use case.

SecurID Authentication API with CAS

This section describes how to integrate ZPE Nodegrid with RSA Cloud Authentication Service using SecurID Authentication API.

Architecture Diagram



Configure RSA Cloud Authentication Service

To configure the integration with RSA Cloud Authentication Service, you must first collect the Authentication API key and Authentication Service Domain for your RSA SecurID Access tenant.

Sign into the Cloud Administration Console and browse to **My Account** > **Company Settings** > **Authentication API Keys** and copy the Description and Key.

Browse to **Platform** > **Identity Routers** > **Edit** > **Registration** and copy the **Authentication Service Domain**.

Configure ZPE Nodegrid

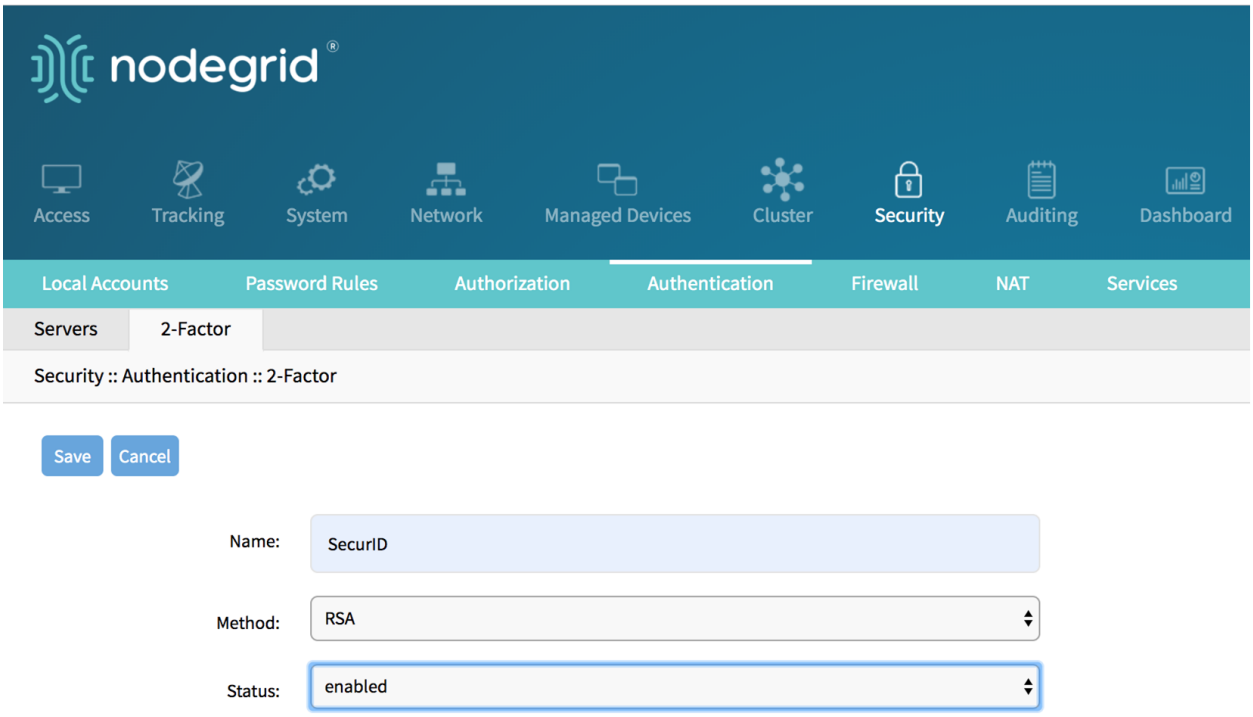
Perform these steps to configure ZPE Nodegrid as an authentication API client to RSA Cloud Authentication Service.

Procedure

1. Sign into Nodegrid Web Interface as admin, browse to **Security** > **Authentication** > **2-Factor** and click **Add**.

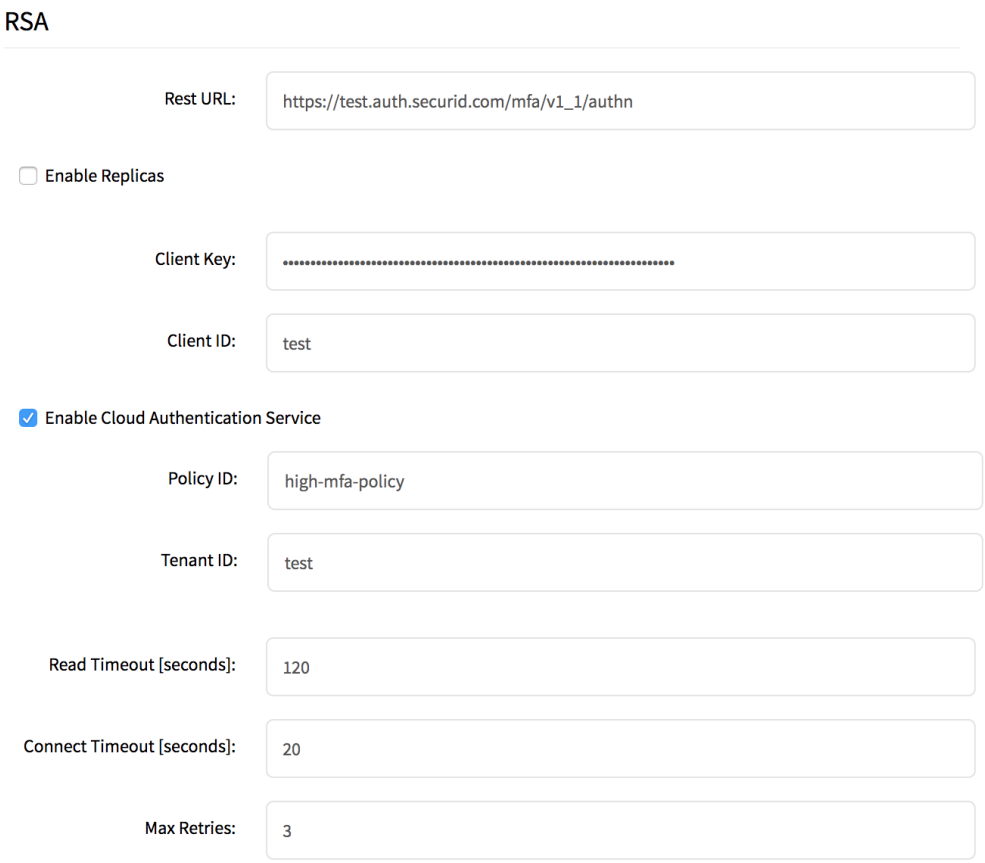
2. Configure the 2-Factor settings and then scroll down to the **RSA** section.

   a. Enter a **Name** to identify the method. For example: SecurID
   b. Select **RSA** from the Method drop-down menu.
   c. Select **enabled** from the Status drop-down menu.



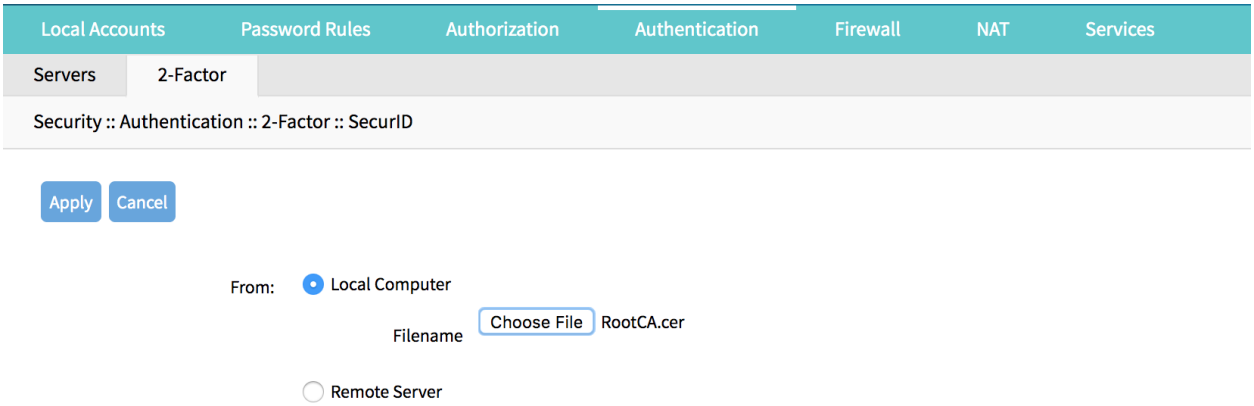
3. Configure the RSA server settings and click **Save**.

   a. **REST URL**: Enter the REST URL for the RSA Cloud Authentication Service. For example: https://test.auth.securid.com/mfa/v1_1/authn
   b. **Enable Replicas**: Leave the check box unmarked. High availability is handled internally by RSA Cloud Authentication Service.
   c. **Client Key**: Enter the Authentication API Key from the RSA Cloud Administration Console.
   d. **Client ID**: Enter the name you wish to be displayed in the RSA Authenticate App's push notifications. Example notification: "Sign in request for: Nodegrid"
   e. Mark the check box for **Enable Cloud Authentication Service**.
   f. **Policy ID**: Enter the name of the access policy you wish to authenticate with as specified in RSA Cloud Administration Console.
   g. **Tenant ID**: Enter the RSA Cloud Authentication Service Company ID



4. After saving, edit the RSA 2-Factory method and upload the certificate which allows Nodegrid to trust RSA Cloud Authentication Service.

a. Follow the steps in this link to acquire the certificate for RSA Cloud Authentication Service.
b. Click the **Certificate** button, upload the certificate file and click **Apply**.



Next Step: Proceed to the Use case configuration section for the steps to apply this configuration to the use case.

Use Case Configuration

Configure User sign in

Follow the instruction steps in this section to apply your**SecurID Authentication API** configuration to ZPE Nodegrid 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

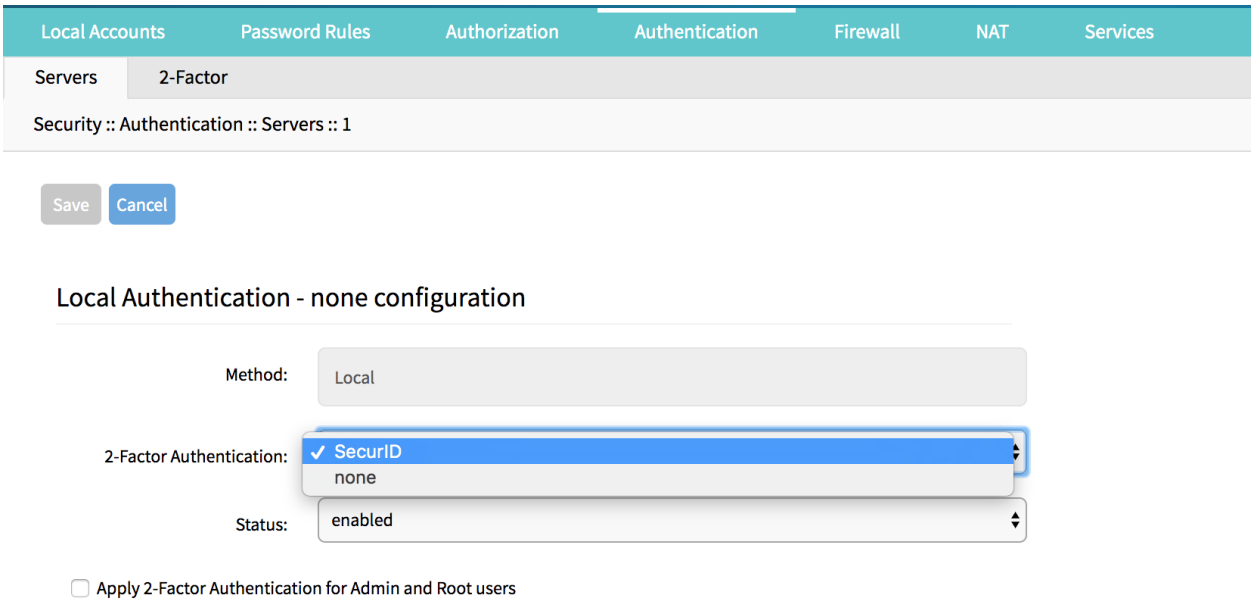
1. Sign in to Nodegrid Web Interface as admin and browse to **Security** > **Authentication** > **Servers** and choose the method to wish to use with RSA authentication. Options are: Local, LDAP/AD, RADIUS, TACACS or Kerberos.

Note: In order to sign in using RSA 2-Factor method, users must have accounts with both methods. For example: If layering RSA SecurID with local authentication, the user must have both a local account and an account in RSA Authentication Manager.

2. Configure the method 2-Factor settings and click **Save**.

   a. **2-Factor Authentication**: Select the RSA method you created in the previous section.

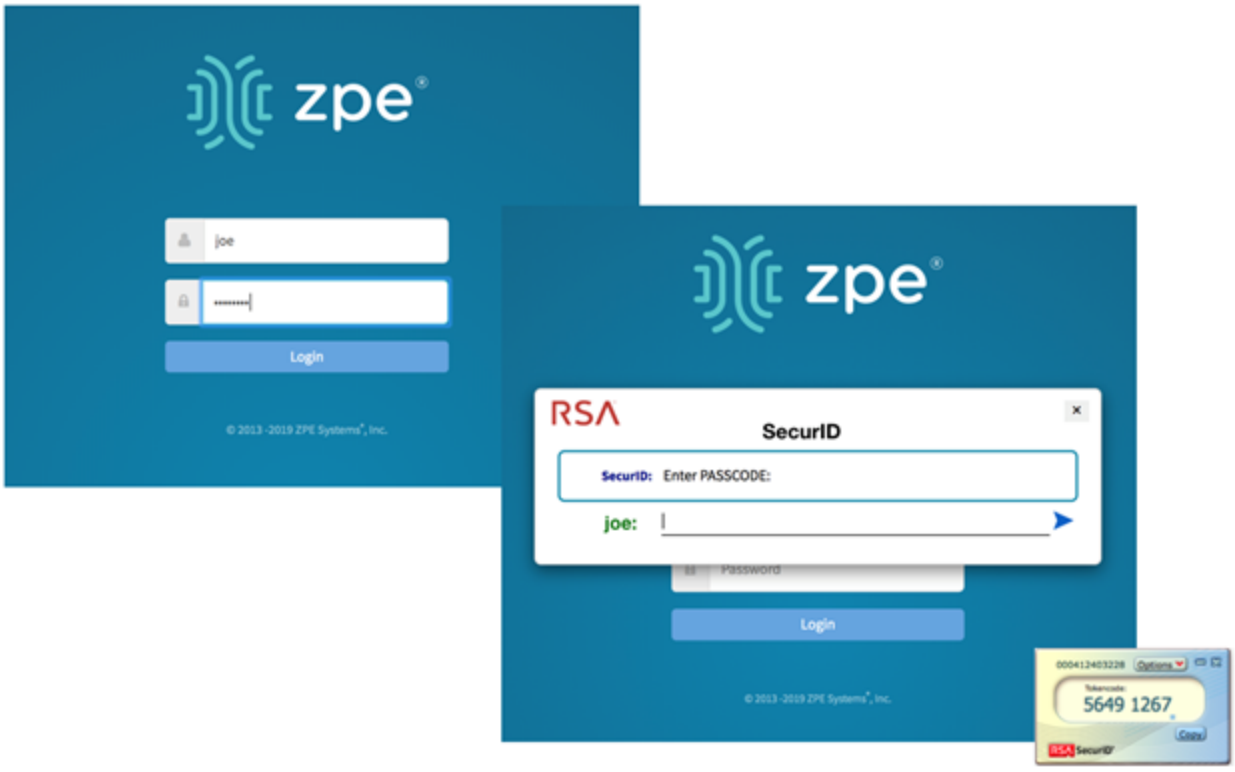
   b. **Status**: Set to enabled.



Note: It is possible to enforce or skip 2-factor authentication for admin and root users when using the Local authentication method.

Configuration is complete.

User Experience



Return to the main page for more certification related information.