Passwordstate

Enterprise Password Management

RSA SecurID Configuration

Table of Contents

1 Introduction

This document will describe the process for initially configuring Passwordstate to use two-factor authentication with RSA's SecurID. It will also provide some guidance in troubleshooting authenticating users, as the response codes returned from an attempted authentication session can sometimes be unclear.

IMPORTANT

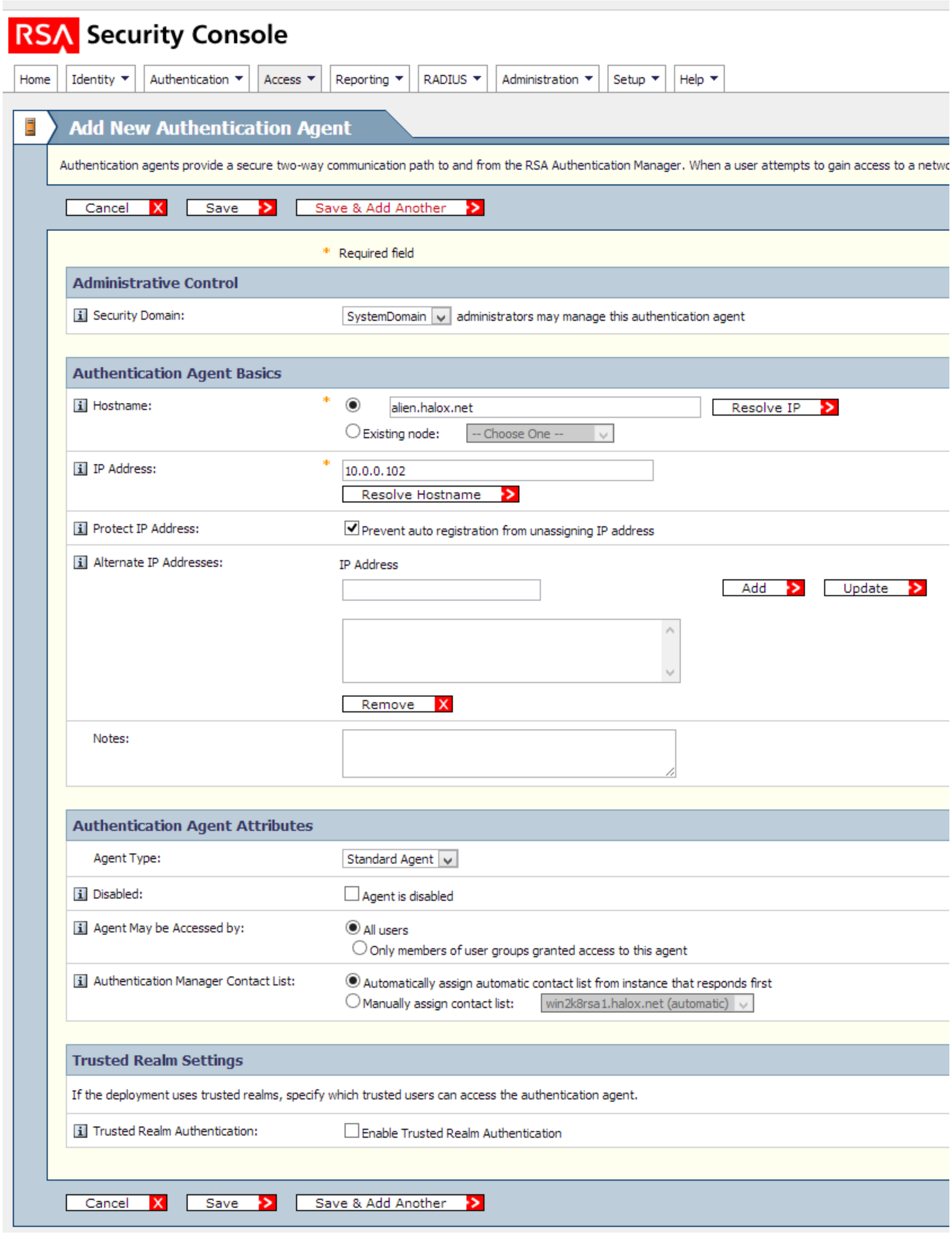
When following the instructions in this document, you must be logged into the RSA Security Console with a user account which has '**Auth Mgr Agent Admin**' rights.

2 Creating and Installing SecurID Configuration Files

Once Passwordstate is installed and operational, you must follow the steps below to create and copy across the SecurID configuration files. Please note these steps are based on RSA Authentication Manager 7.1 SP4 Patch 22, so the screens/instructions may be different for your version of Authentication Manager.

Create Authentication Agent(s)

- Logon onto your Authentication Manager Security Console
- Navigate to the menu Access -> Authentication Agents -> Add New
- Select the appropriate Security Domain, specify the fully qualified Hostname of your Passwordstate web server, and click the 'Resolve IP Address' button to ensure DNS is working correctly



Add New Authentication Agent

Authentication agents provide a secure two-way communication path to and from the RSA Authentication Manager. When a user attempts to gain access to a netwc

* Required field

Administrative Control

Security Domain: SystemDomain administrators may manage this authentication agent

Authentication Agent Basics

Hostname: * ● alien.halox.net
○ Existing node: -- Choose One --

IP Address: * 10.0.0.102

Protect IP Address: ☑ Prevent auto registration from unassigning IP address

Alternate IP Addresses: IP Address

Notes:

Authentication Agent Attributes

Agent Type: Standard Agent

Disabled: □ Agent is disabled

Agent May be Accessed by: ● All users
○ Only members of user groups granted access to this agent

Authentication Manager Contact List: ● Automatically assign automatic contact list from instance that responds first
○ Manually assign contact list: win2k8rsa1.halox.net (automatic)

Trusted Realm Settings

If the deployment uses trusted realms, specify which trusted users can access the authentication agent.

Trusted Realm Authentication: □ Enable Trusted Realm Authentication

- Click on the 'Save' button

Note 1: You may need to specify different settings on this screen for your environment i.e. Enable Trusted Realm Authentication, etc.

Note 2: If you are using the High Availability Instance of Passwordstate, you will also need to create an Authentication Agent for your HA web server host name, and perform the same steps below for your HA web server installation.

Create Node Secret

- Navigate to the menu Access -> Authentication Agents -> Manage Existing
- On the right-hand side of the Authentication Agent you just created, select 'Manage Node Secret' from the dropdown menu
- Click on the option 'Create a new random node secret, and export the node secret file'
- Specify an 'Encryption Password' to use, the click on the Save button
- Click on the 'Download Now' button, extract the zip file contents, and copy the files to the '/securid' folder in the Passwordstate web site

Create and Install Configuration File

- Navigate to the menu Access -> Authentication Agents -> Generate Configuration File
- Specify any 'Agent Timeout and Retries' settings applicable to your environment
- Click on the 'Generate Config file' button
- Download the configuration file, extract the zip file contents, and copy the files to the '/securid' folder in the Passwordstate web site

Generate the SecurID <no extension> File

- On your web server, open a command prompt with **Administrative Privileges**
- Change to the following folder c:\inetpub\passwordstate\securid\<32bit or 64bit>. The path to this folder may be different for your installation, and you will need to change to either the 32bit or 64bit operating system, depending on what Operating System Architecture you are using
- Type the command below, and enter the 'Encryption Password' you specified above when prompted. If the creation of the securid file is successful, you will see the message "The Node Secret is successfully loaded".

  ```
  agent_nsload.exe -f c:\inetpub\passwordstate\securid\nodesecret.rec -d c:\inetpub\passwordstate\securid
  ```

- When the securid file is created, it is created without any owner or any NTFS permissions. To correct this, please follow these instructions:
  - Using Windows Explorer, right-click on the file and select 'Properties'
  - Click on the 'Security' tab and then on the 'Advanced' button
  - Click on the 'Continue' button
  - Click on the option 'Include inheritable permissions from the object's parent', then click on the 'Apply' button
  - Click on the 'OK' button and close all remaining open windows

Note 1: It is important you fix the NTFS permissions on the securid file, otherwise the file cannot be backed up.

Note 2: Please wait at least 10 to 15 minutes before trying your first SecurID authentication in Passwordstate, as it can take a little time for the new Authentication Agent to be functional in RSA Authentication Manager.

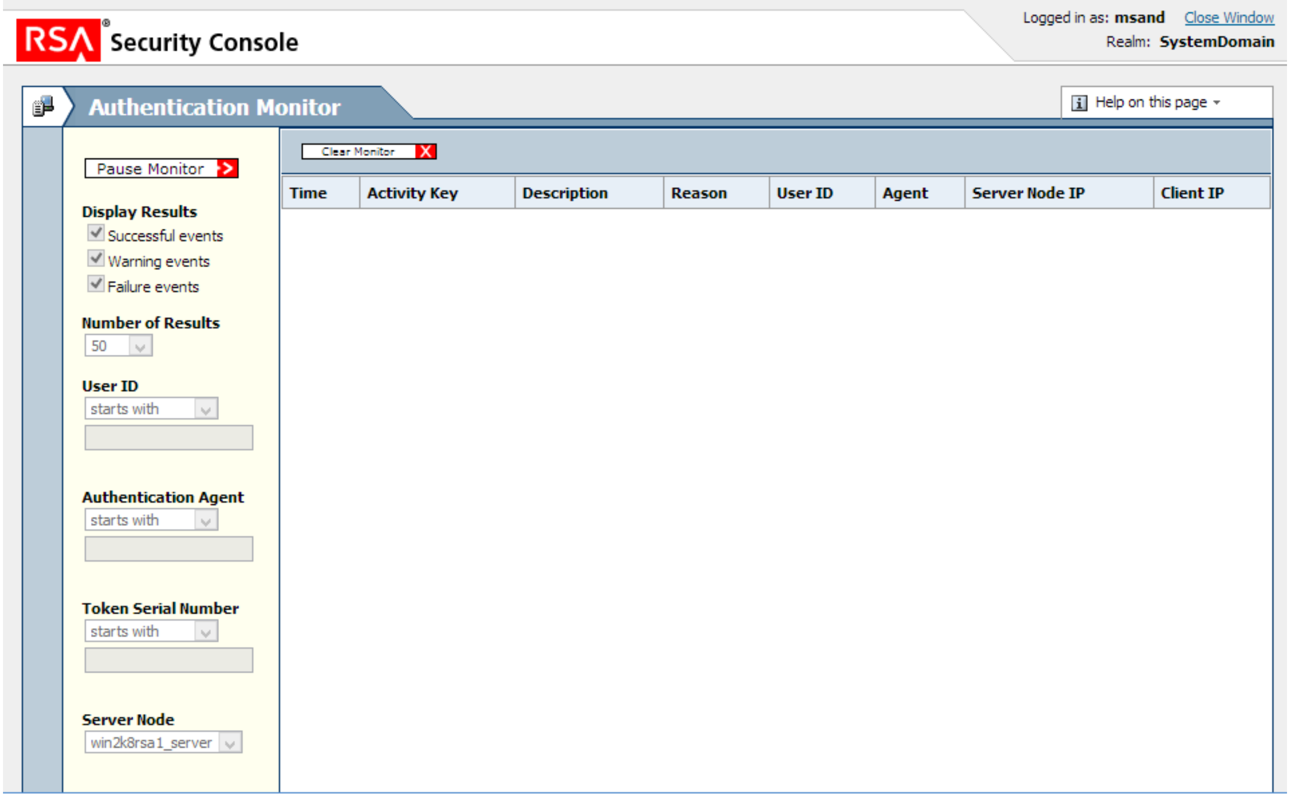
Note 3: If you see error messages in the Security Console Authentication Monitor saying 'Node secret mismatch: agent and server using different node secrets', then please restart IIS to see if this resolves the issue.

Note 1: If at any stage you decide to move your Passwordstate installation to a different web server with a different hostname/ip address, you will need to redo all these steps.

3 Troubleshooting Authentication Issues

There are multiple reasons why authentication can fail for a user, including an invalid sdconfig.rec file, or locked account, etc. Apart from error messages displayed in Passwordstate, the most effective means of determine what's causing the issue is my using the 'Real-Time Activity Monitors' feature in your Authentication Manager Security Console.

- Navigate to Reporting -> Real-Time Activity Monitors -> Authentication Activity Monitor
- Click on the 'Start Monitor' button, and retry your user authentication. Any errors or successful authentication attempts will now be displayed on the screen below. If you're still unable to determine what the cause is, please contact Click Studios and we will try to assist.



Logged in as: msand

Realm: SystemDomain

Display Results
☑ Successful events
☑ Warning events
☑ Failure events

Number of Results: 50

User ID: starts with

Authentication Agent: starts with

Token Serial Number: starts with

Server Node: win2k8rsa1_server

Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP

- If you see errors similar to 'Node secret mismatch: cleared on server but not on agent', or 'Node secret mismatch. Cleared on agent but not on server', then you may need to delete the 'Authentication Agent' you created, and redo all the steps above.