RSA Two Factor Authentication

Feature Description

UPDATED: 20 March 2021

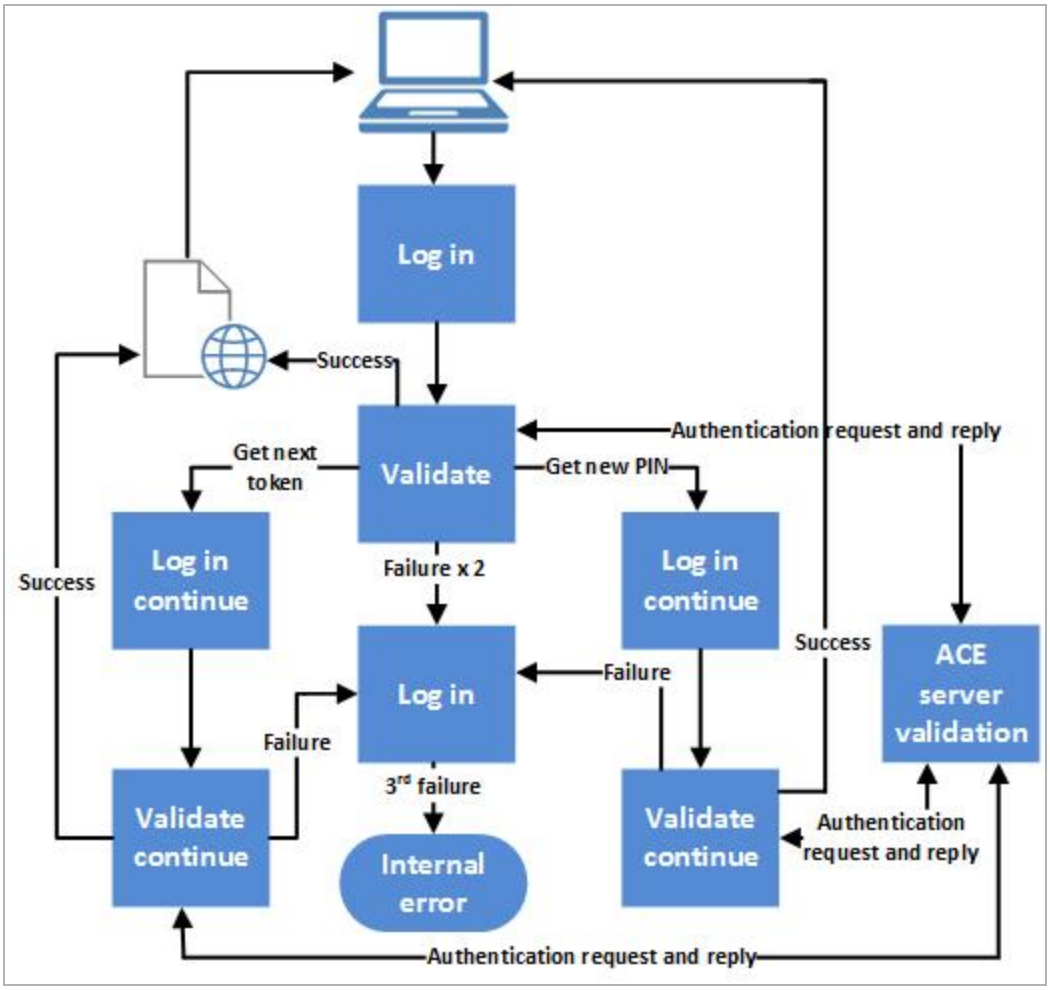
Copyright Notices

Table of Contents

1 Introduction

As part of the Kemp Edge Security Pack (ESP), the LoadMaster supports the RSA SecurID authentication scheme. This scheme authenticates the user on an RSA SecurID Server. When RSA is enabled as the authentication method, during the login process the user is prompted to enter a password that is a combination of two numbers – a Personal Identification Number (PIN) and a token code which is the number displayed on the RSA SecurID authenticator (dongle).

There are two additional challenge-response modes: next token and new PIN. These are described in the sections below.



The above diagram shows both next token and new pin modes which are only applicable under the conditions described below. This flow allows for three login attempts, after which login failure is final. The actual number of login attempts users are allowed to have is configurable.

1.1 Next Token Mode

Next token mode is applied in cases where the authentication process requires additional verification of the token code. The user is asked to enter the next token code, that is, wait for the number that is currently displayed on the authenticator to change, and enter the new number (without the PIN).

> When using RSA and Kerberos Constrained Delegation (KCD), the user password will not be authenticated which may result in unsecured access – particularly if RSA operates in token code only mode. While many RSA implementations use token code and PIN, others just use token code.

1.2 New PIN Mode

New PIN mode is applied in cases where the authentication process requires additional verification of the PIN. In this case, the user must use a new PIN. Depending on the configuration of the RSA ACE/Server, the user is prompted to select and enter a new PIN, or the server supplies the user with a new PIN. The user then re-authenticates with the new PIN. The use of new PIN mode is optional and can be enabled or disabled in the authentication server.

1.3 Document Purpose

This document describes how to configure the LoadMaster to use the RSA two factor authentication method.

The RSA Security Console screenshots and steps in this document are examples. Kemp will not be notified of any changes made in the RSA Security Console so please refer to the RSA documentation for the latest information, if needed.

1.4 Intended Audience

This document is intended to be read by anyone who is interested in finding out how to use RSA authentication with the Kemp LoadMaster.

1.5 Related Firmware Version

Published with LMOS version 7.2.48.4 LTS. This document has not required substantial changes since 7.2.48.4 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

1.6 Prerequisites

The following are required in order to use RSA as an authentication method:

- A configured RSA SecurID Server

  The LoadMaster can only use one RSA server at a time.

- RSA Authentication Manager 8.1
- SecurID dongles

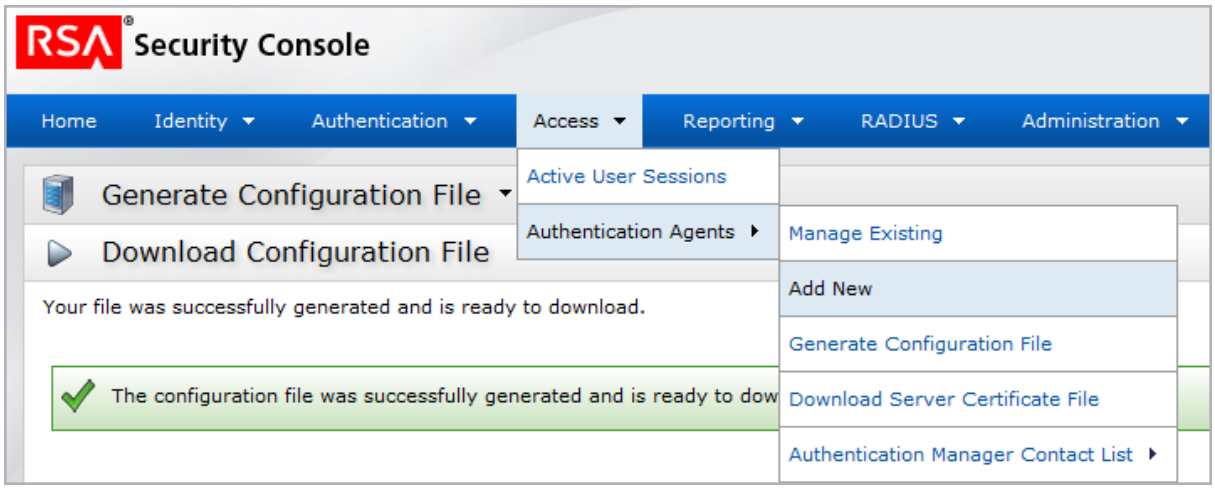
2 Configure RSA SecurID Multi-Factor Authentication

You need to complete three steps in order to configure RSA multi-factor authentication on the LoadMaster. These are outlined in the sections below.

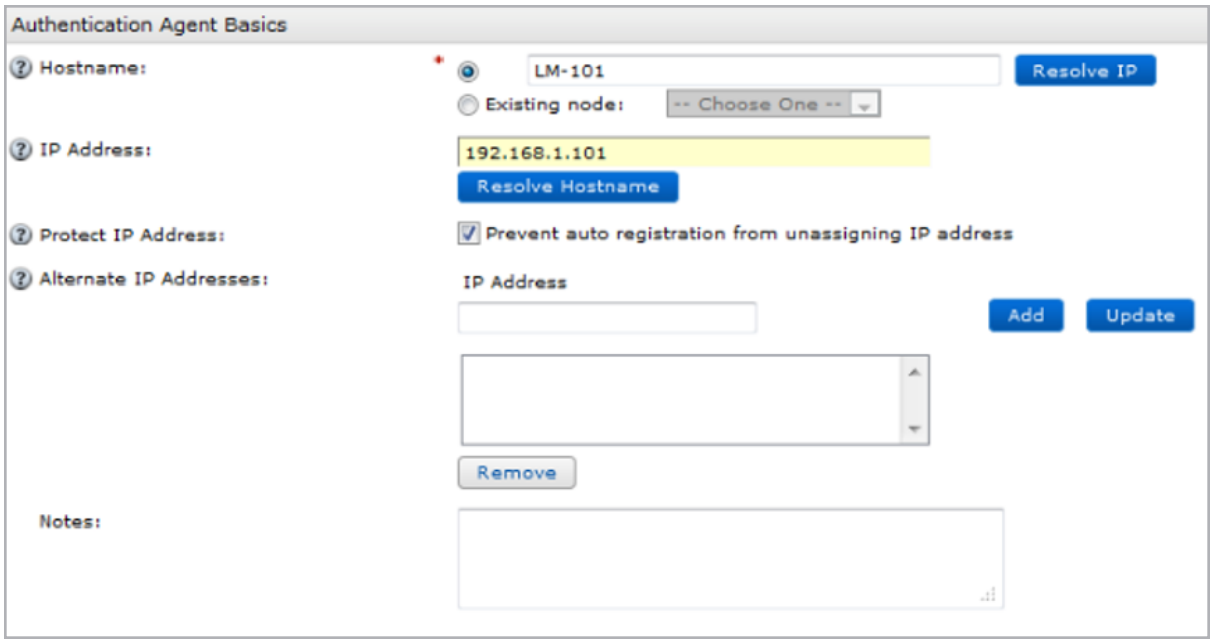
If multiple domains are configured, sign-on can then be authenticated all at once. More information on this option can be found in **ESP, Feature Description**.

2.1 Generate an Authentication Agent Entry

An Authentication Agent Entry needs to be generated for the LoadMaster in the RSA Authentication Manager. To do this, in the RSA Security Console, follow the steps below:



1. Select **Access > Authentication Agents** and click **Add New**.

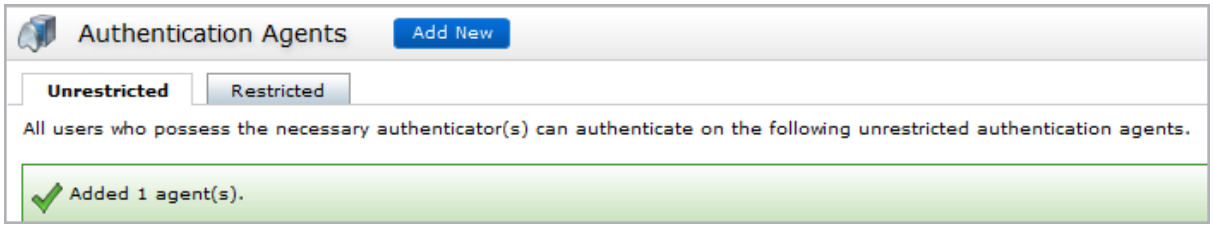


2. Enter the LoadMaster IP address in the **IP Address** text box.

   For a HA cluster, add all three LoadMaster IP addresses (unit 1, unit 2 and the shared IP address).

   If the source IP address of traffic from the LoadMaster to the RSA server changes as a result of interface IP changes or routing changes, please note that a new RSA-Config file will need to be generated.

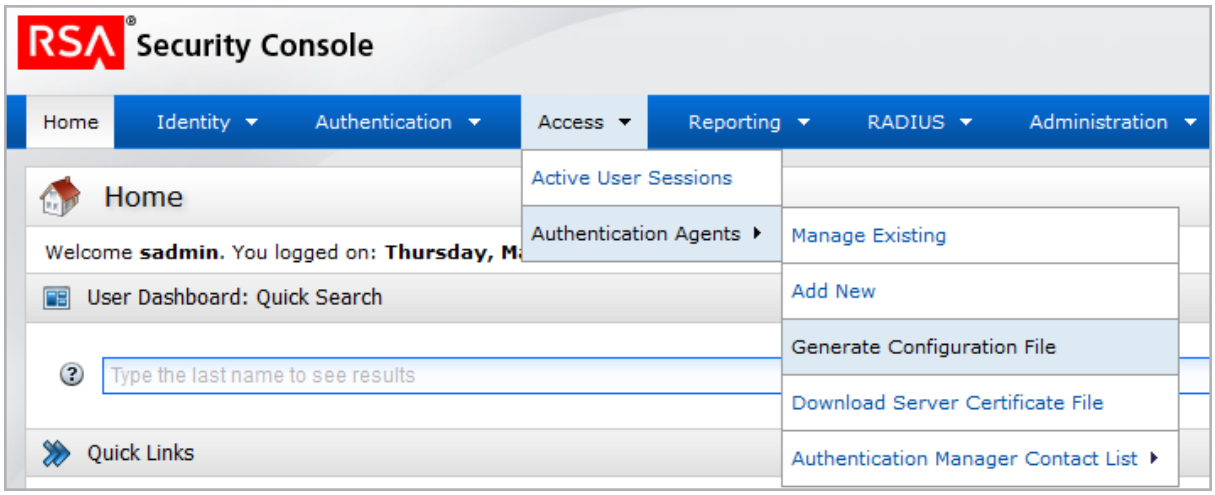
3. Click the **Resolve Hostname** button. The **Hostname** field will auto-populate.
4. Fill out the remaining fields as required on the form.
5. Click **Save**.



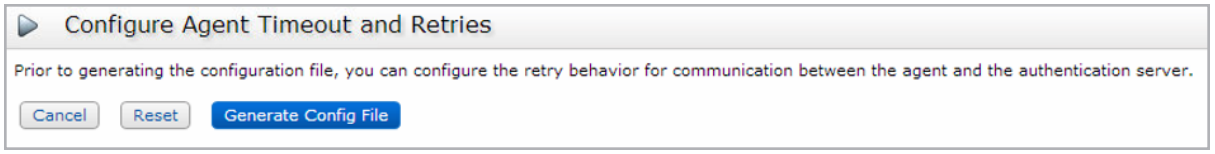
A message will appear confirming that the agent was added.

2.2 Export the Authentication Manager Configuration

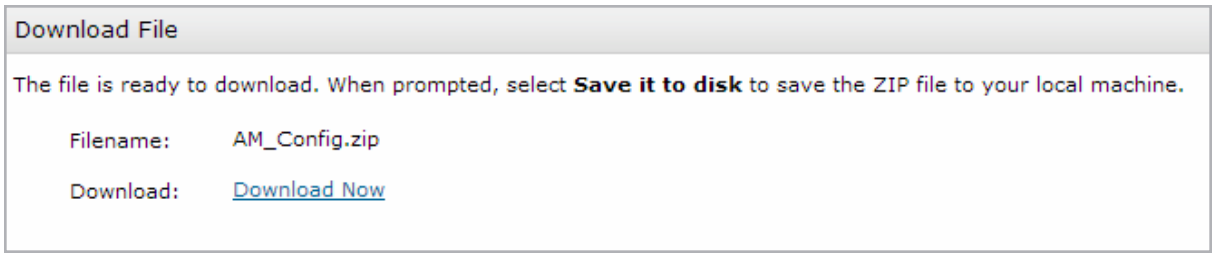
Before uploading the Authentication Manager configuration, it needs to be exported from the RSA Security Console. To do this, follow the steps below:



1. Select **Access > Authentication Agents** and click **Generate Configuration File**.



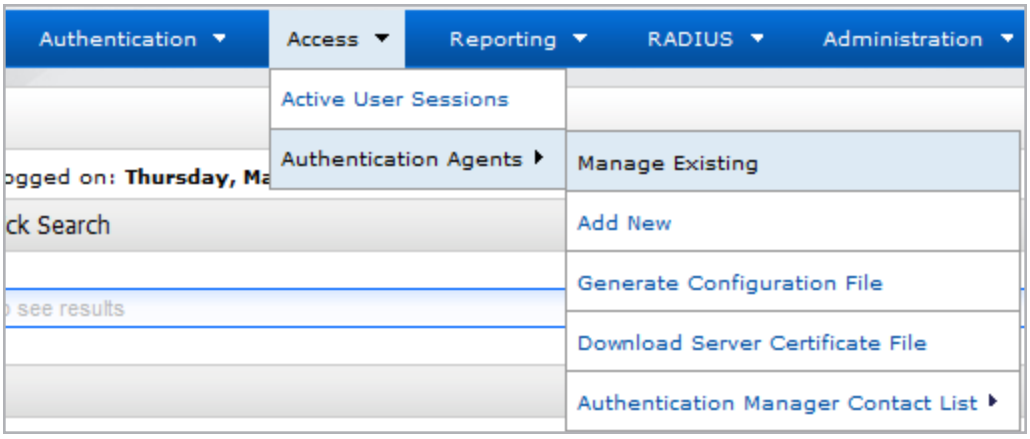
2. Click **Generate Config File**.



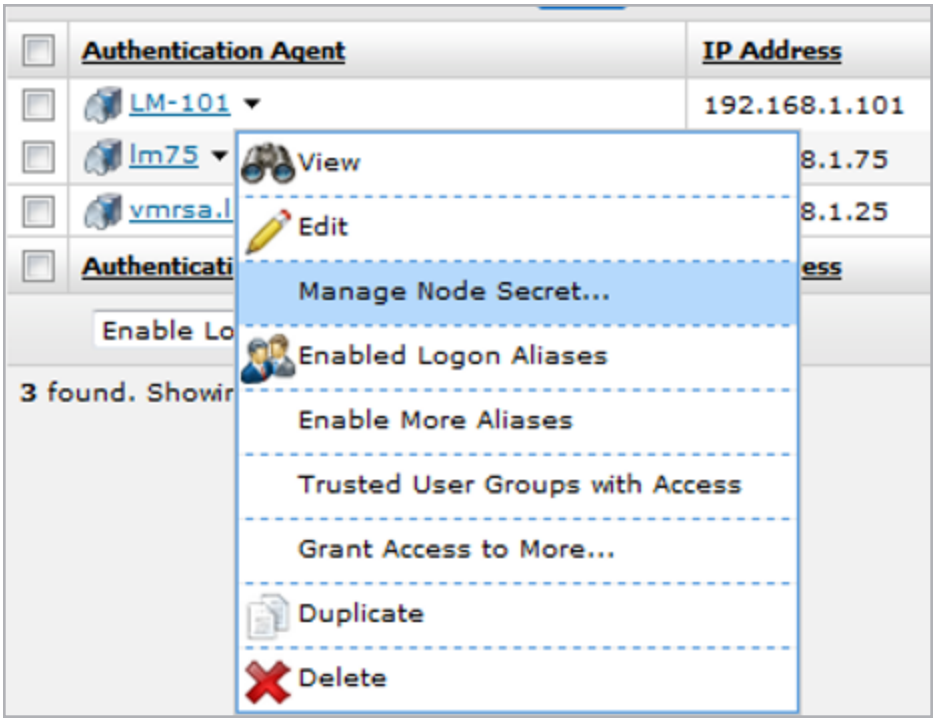
3. Click **Download Now** to download the configuration file.

2.3 Generate a Node Secret File

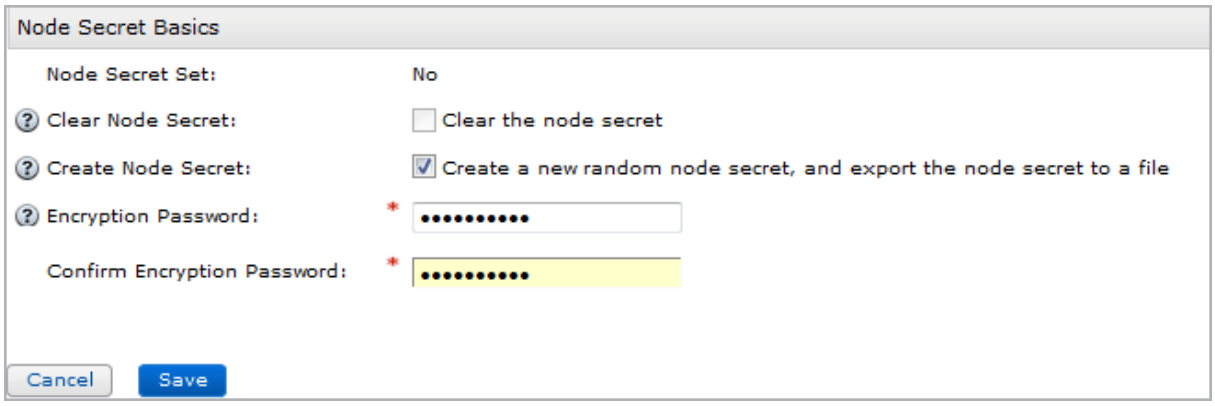
First, generate a Node Secret in the RSA Security Console by following the steps below:



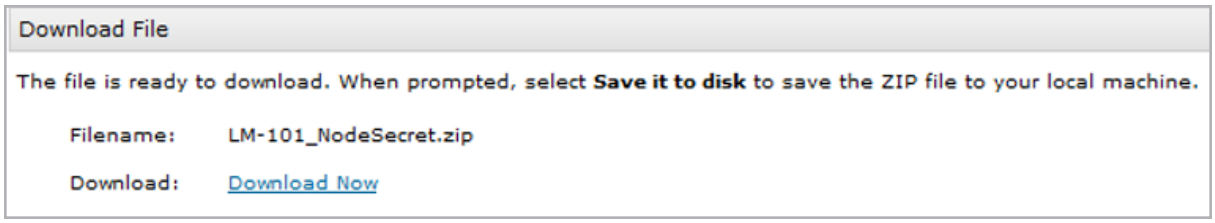
1. Select **Access > Authentication Agents > Manage Existing**.



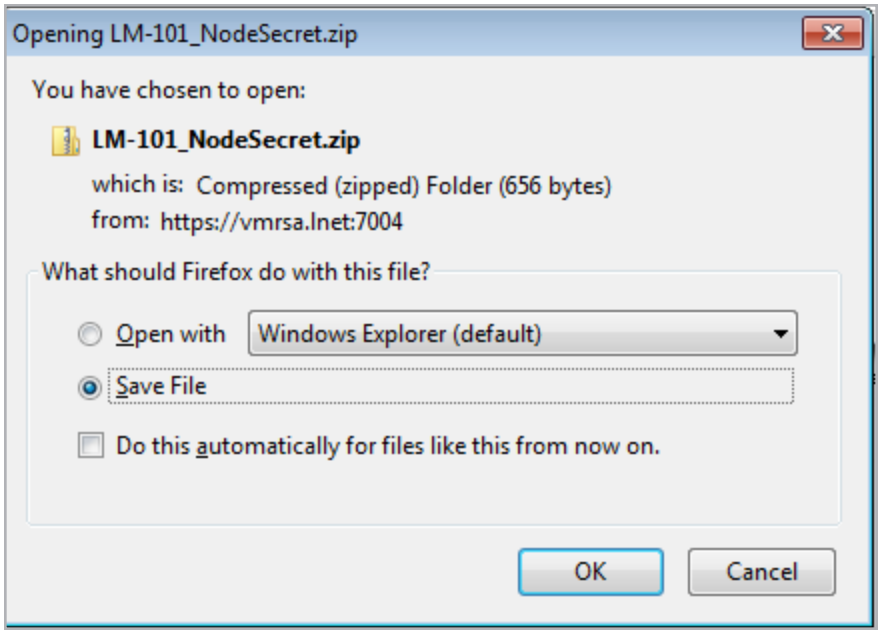
2. Right click the LoadMaster entry and click **Manage Node Secret**.



3. Select the **Create a new random node secret, and export the node secret to a file** check box.
4. Enter an **Encryption Password** for the node secret file.
5. Confirm the encryption password.
6. Click **Save**.



7. Click **Download Now**.



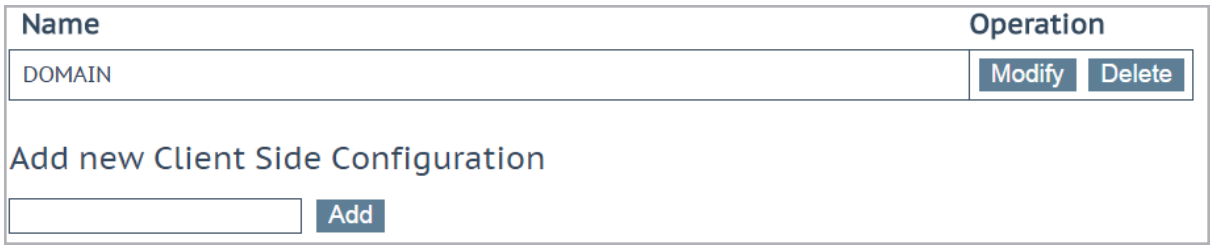
8. Save the file.

2.4 Configure the LoadMaster

> The LoadMaster can only use one RSA server at a time.

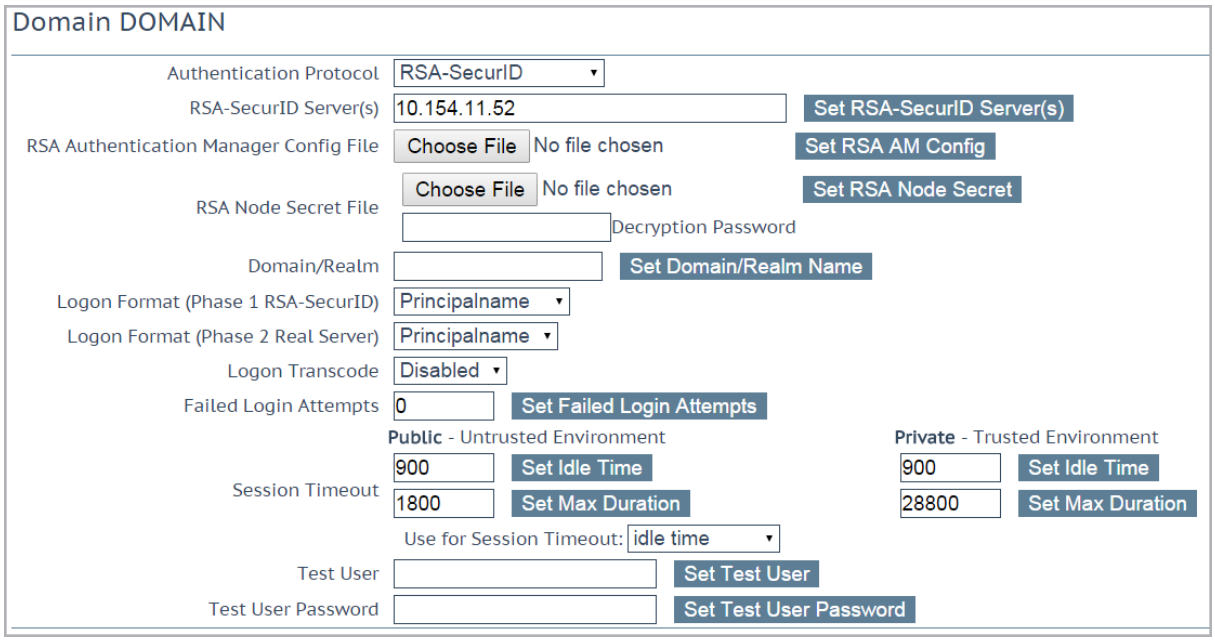
In the LoadMaster Web User Interface (WUI), follow the steps below:

1. In the main menu, select **Virtual Services** and **Manage SSO**.



> For steps on how to configure an SSO domain and ESP, refer to the **ESP, Feature Description** document.

2. Click **Modify** on the relevant SSO domain.



3. Select RSA-SecurID as the Authentication protocol.

> It is also possible to select **RSA-SecurID and LDAP** as the **Authentication Protocol**. If this is selected, the **LDAP Endpoint** will also need to be selected.

4. In the **RSA-SecurID Server(s)** text box, enter the address(es) of the RSA-SecurID server(s) that are used to validate this domain.

5. Click **Set RSA-SecurID Server(s)**.

6. In the **RSA Authentication Manager Config File** field, click **Choose File**.

7. Browse to and select the file exported in the **Export the Authentication Manager Configuration** section.

8. Click **Set RSA AM Config**.

9. Enter the login domain to be used in the **Domain/Realm** text box.

> This is also used with the logon format to construct the normalized username, for example;
> - **Principalname:** <username>@<domain>
> - **Username:** <domain>\<username>

> If the **Domain/Realm** field is not set, the **Domain** name set when initially adding an SSO domain is used as the **Domain/Realm** name.

10. Select the relevant option for **Logon Format (Phase 1 RSA-SecurID)**.
11. Select the relevant option for **Logon Format (Phase 2)**.

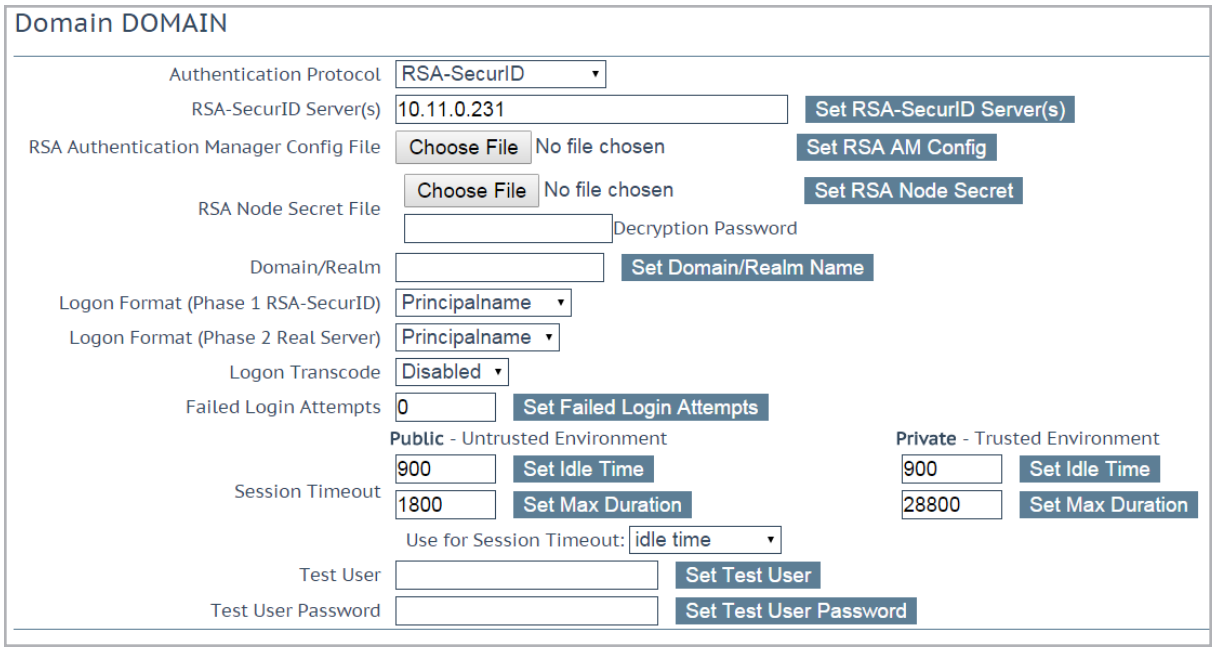
> The different logon formats are described below:
> - **Not Specified:** The username will have no normalization applied to it - it is taken as it is typed.
> - **Principalname:** Selecting this as the **Logon format** means that the client does not need to enter the domain when logging in, for example **username@domain**. The SSO domain added in the corresponding text box is used as the domain in this case.
> - **Username:** Selecting this as the **Logon format** means that the client needs to enter the domain and username, for example **domain\username**.
> - **Username Only:** Selecting this as the **Logon Format** means that the text entered is normalized to the username only (the domain is removed).

12. Enter the **Test User** and click **Set Test User**.
13. Enter the **Test User Password** and click **Set Test User Password**.

> The LoadMaster will use this test information in a health check of the SecurID Server. These details are static and should be set in the RSA management WUI. This health check is performed every 20 seconds.

2.4.1 Upload a Node Secret File for the LoadMaster

Upload the node secret in the LoadMaster. In the Manage SSO screen on the LoadMaster WUI, follow the steps below:



1. In the **RSA Node Secret File** field, click **Choose File**.

2. Browse to and select the Node Secret file generated in the **Generate a Node Secret File** section.

> It is not possible to upload the RSA node secret file until the RSA Authentication Manager configuration file is uploaded. The node secret file is dependent on the configuration file.

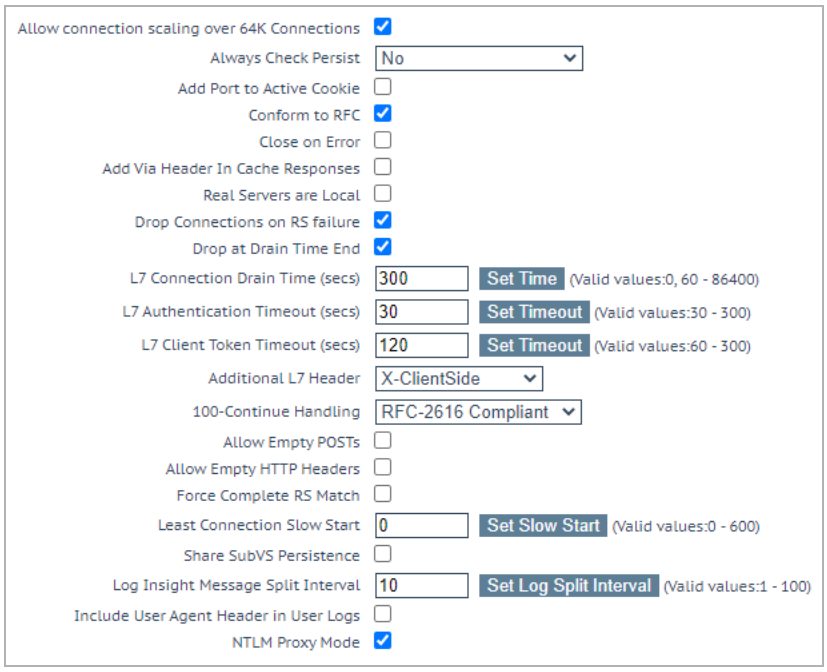
3. Enter the **Decryption Password**.

4. Click **Set RSA Node Secret**.

2.4.2 Set the L7 Client Token Timeout Value

The L7 Client Token Timeout is the duration of time (in seconds) to wait for the client token while the process of authentication is ongoing. The default L7 client token timeout is set to 120 seconds. This can be modified as needed in the LoadMaster WUI. The range of valid values is 60 to 300. To configure the timeout value, follow the steps below:

1. In the main menu, go to **System Configuration > Miscellaneous Options > L7 Configuration**.

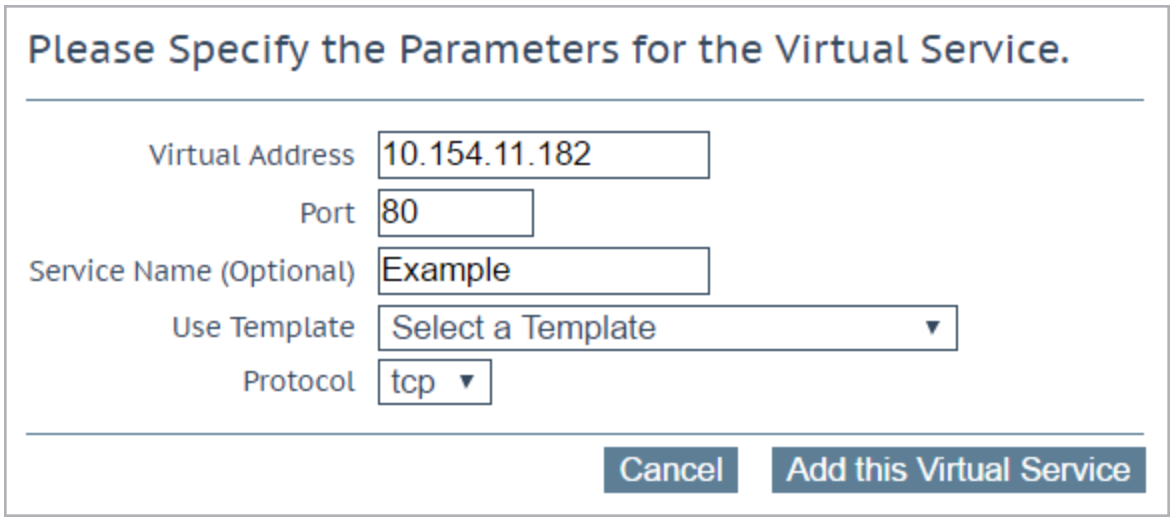


2. Enter the new value in the **L7 Client Token Timeout** text box and click **Set Timeout**.

2.4.3 Create a Virtual Service

Follow the steps below to create a Virtual Service in the LoadMaster WUI:

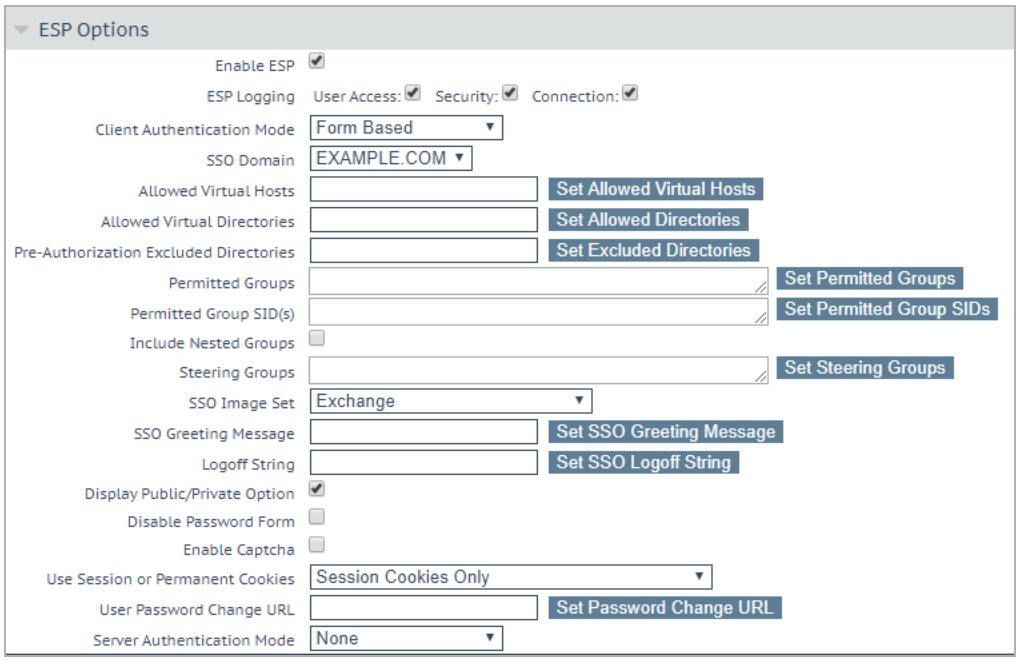
1. In the main menu, expand **Virtual Services** and click **Add New**.



2. Enter a valid **Virtual Address**.
3. Fill out any other details as needed.

4. Click **Add this Virtual Service**.

5. Expand the **ESP Options** section.



6. Select the **Enable ESP** check box.

7. Select **Form Based** as the **Client Authentication Mode**.

8. Select the SSO domain created previously from the **SSO Domain** drop-down list.

9. Fill out any other details as needed.

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

ESP, Feature Description

Web User Interface, Configuration Guide

Last Updated Date

This document was last updated on 20 March 2021.