Using Multi-Factor Authentication (MFA)

ScienceLogic Version 8.6.0

Table of Contents

Chapter 1

Introduction

Overview

This manual will explain how to configure your SL1 systems to use RSA SecurID for multi-factor authentication during login to SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

NOTE: Currently, SL1 supports multi-factor authentication through RSA SecurID only.

What is Multi-Factor Authentication?

Multi-factor authentication adds an additional step to authentication. Users still must provide a user name and password, but multi-factor authentication requires an additional piece of information from the user.

Currently, SL1 supports multi-factor authentication from RSA SecurID. RSA SecurID generates a unique token delivered to a key fob or to an email address or mobile phone.

If you configure SL1 to use multi-factor authentication, after the user provides a user name and password, SL1 prompts the user to enter the token from RSA SecurID.

Chapter 2

Configuring Multi-Factor Authentication

Overview

You can configure your SL1 systems to use RSA SecurID for multi-factor authentication during login to SL1. You must still configure standard user authentication via EM7 Session or Active Directory/LDAP. Multi-factor authentication provides an additional level of security to standard authentication.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

This chapter includes the following topics:

NOTE: Currently, SL1 supports multi-factor authentication through RSA SecurID only.

Caveats

- ***New UI (Beta)***. You currently cannot use multi-factor authentication with the new user interface.
- ***API***. You currently cannot use multi-factor authentication with the ScienceLogic API.
- ***SSO***. Best practice for Single Sign-On (SSO) includes multi-factor authentication when connecting to the Identity Provider, not when logging in to SL1. This chapter does not describe how to configure SSO authentication and multi-factor authentication during login to SL1.

Prerequisites

Before configuring SL1 to use RSA SecurID for multi-factor authentication, you must first:

- Enable the RSA Authentication API on the SecurID server
- Define an Authentication Agent on the SecurID server
- Know the Web Agent ID of the agent registered with the SecurID server
- Know the Access Key for connecting to the SecurID server
- Know the RSA REST Endpoint for the SecurID server

For details on performing these tasks, see the documentation for RSA SecurID at https://community.rsa.com/docs/DOC-76573

Configuration Steps

To configure multi-factor authentication:

1. *Define a Multi-factor Resource*.
2. Optionally, if the user name in SL1 is different than the user name for multi-factor authentication, edit the Account Permissions page (or the **Create New Account** page) and enter the user name for multi-factor authentication.
3. *Create or edit one or more Authentication Profiles* and include a Multi-Factor Resource in the profile.

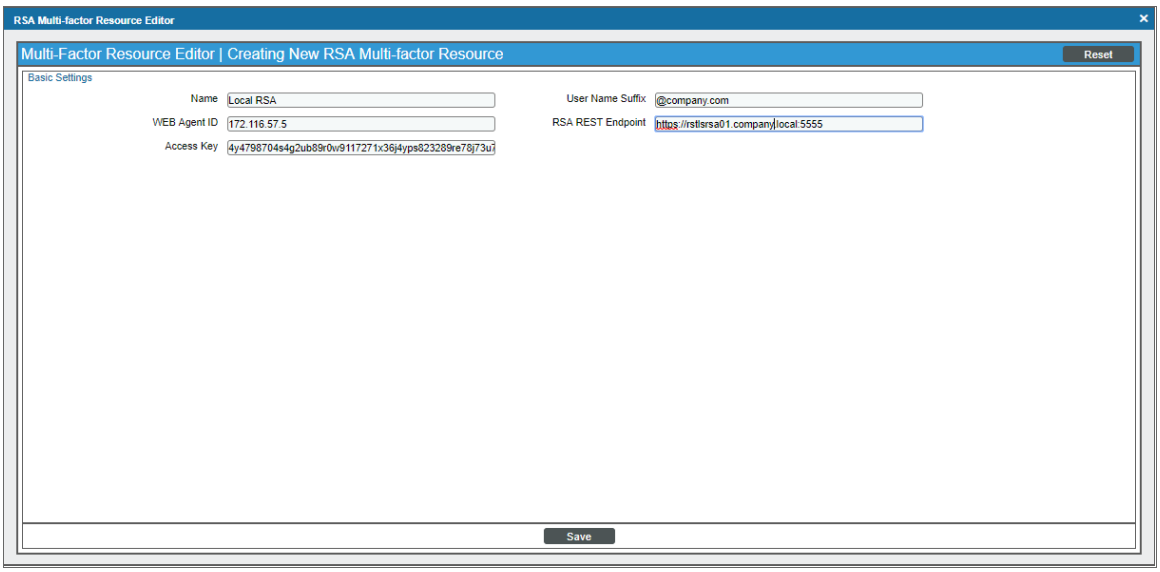
Defining a Multi-factor Resource

A ***Multi-Factor Resource*** is a configuration policy that describes how SL1 should communicate with the multi-factor endpoint. A Multi-factor Resource specifies:

- the hostname or IP address of the Authentication Agent
- the access key for communicating with the endpoint
- the URL of the RSA REST endpoint

The **Multi-factor Resource Manager** page allows you to create a new Multi-factor Resource. To do so:

1. Go to the **Multi-factor Resource Manager** page System > Settings > Authentication > Multi-factor.
2. In the **Multi-factor Resource Manager** page, select the **[Actions]** menu and then select the following:
    - ***Create RSA Resource***. The **Multi-Factor Resource Editor** page appears.
3. In the **Multi-Factor Resource Editor** page, you can define the new Multi-factor Resource.



4. In the **Multi-Factor Resource Editor** page, supply values in the following fields:
    - ***Name***. Enter the name of the Multi-Factor Resource.
    - ***WEB Agent ID***. Enter the IP address or hostname of the Agent registered with RSA.
    - ***Access Key***. Enter the Access Key for the RSA SecurID endpoint.
    - ***User Name Suffix***. Enter a suffix that will be applied to all user names before submitting them to RSA SecurID for authentication.
        - If you have not specified a a value in the ***Multi-factor Auth (MFA) User*** field in either the **Create New Account** page (Registry > Accounts > User Accounts > Create button)or the **Account Permissions** page (Registry > Accounts > User Accounts > edit user account), the value in the ***User Name Suffix*** field will be appended to the value in the ***Account Login Name*** field in either the **Create New Account** page or the **Account Permissions** page.
        - If you have specified a a value in the ***Multi-factor Auth (MFA) User*** field in either the **Create New Account** page (Registry > Accounts > User Accounts > Create button)or the **Account Permissions** page (Registry > Accounts > User Accounts > edit user account), the value in the ***User Name Suffix*** field will be appended to the value in the he ***Multi-factor Auth (MFA) User*** field in either the **Create New Account** page or the **Account Permissions** page.

Ideally, the user names in SL1 and the user names for RSA SecurID are the same. If they are not, you can use this field to map the user names in SL1 to the RSA SecurID user names.

- For example, suppose your SL1 uses Active Directory to authenticate users.
- Suppose each users name in Active Directory is configured as FirstnameLastname, for example "JohnSmith".
- Suppose the user names in RSA SecurID include an email address, like "JohnSmith@company.com".
- You could enter "@company.com" in this field.

- ***RSA REST Endpoint***. Enter the root URL of the REST API on the RSA SecurID endpoint. By default, this URL uses HTTPS and the default port "5555". For example, "https://rstlsrsa01.eng.sciencelogic.local:5555".

5. Click the **[Save]** button to save the new Multi-factor Resource.

Creating or Editing an Authentication Profile

To use multi-factor authentication, you must first define standard user authentication. ***Authentication*** is the method by which SL1 determines if a user can access the system. There are three methods of authentication:

- ***EM7 Session***. An administrator must define the user account in SL1. The user account has a user name and password. During login, the SL1 system checks its own databases to make sure that the user name and password are legitimate and accurate. For details on creating a user account, see the ***Organizations and Users*** manual.
- ***LDAP/Active Directory***. If the user has an account in Active Directory or on an LDAP server, the user can log in to SL1 with the Active Directory or LDAP user name and password. SL1 will communicate with Active Directory or the LDAP server to determine if the user name and password are legitimate and accurate. For details on defining authentication with Active Directory or LDAP, see the ***Using LDAP or Active Directory*** manual.
- ***SSO Authentication***. If the user has an SSO account, the user can enter a URL to access SL1. A SAML Identity Provider (IdP) will authenticate the user, with the user's browser acting as an intermediary. If the user is already logged in to the SAML IdP, SL1 will display the default page for the user. If the user is not yet logged in to the SAML IdP, the user will be prompted to login to the SAML IdP and then redirected to the default page in SL1.

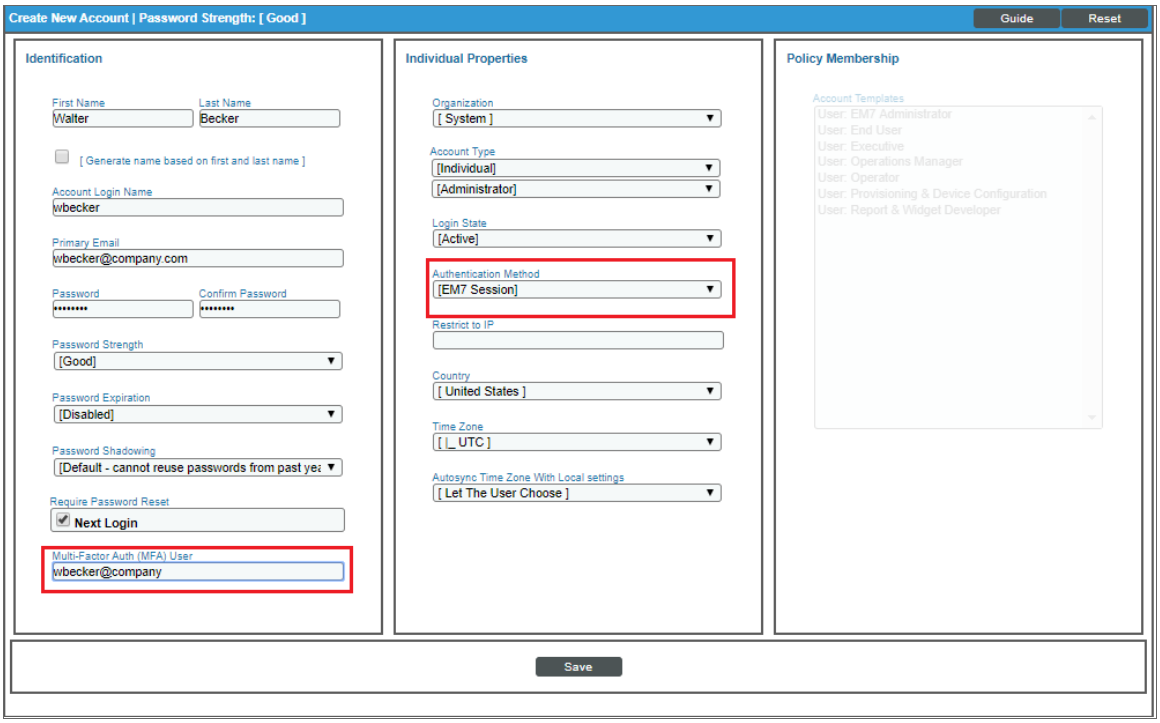
NOTE: Best practice for SSO is to include multi-factor authentication when connecting to the Identity Provider, not when logging in to SL1.

Authentication Profiles are policies that align user accounts with one or more types of authentication. Authentication Profiles use Multi-factor Resources to communicate with multi-factor endpoints.

Creating an Authentication Profile for EM7 Session

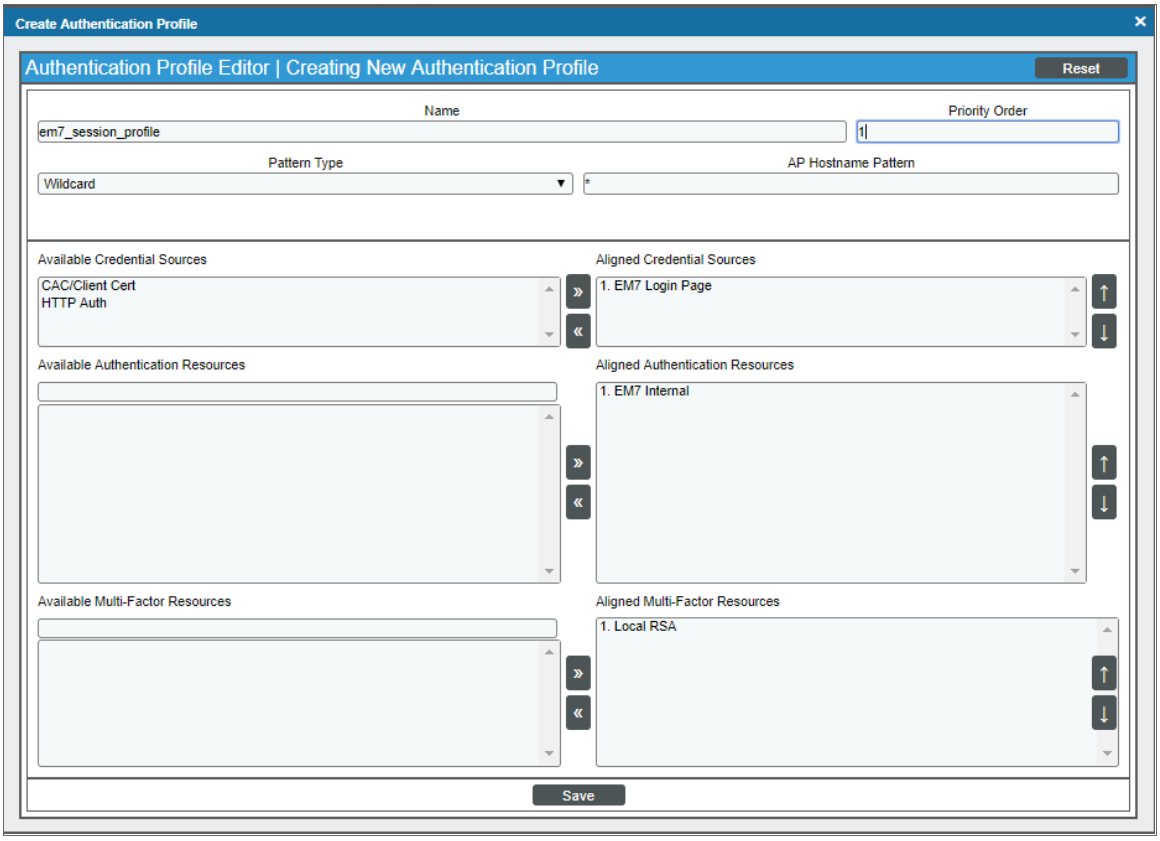
To use multi-factor authentication for users that use EM7 Session authentication, create an authentication profile and align a Multi-Factor Resource. This section explains how to perform these steps.

1. Create a user account for the user. For details on creating a user account, see the ***Organizations and Users*** manual.
2. In either the **Create New Account** page (Registry > Accounts > User Accounts > Create button)or the **Account Permissions** page (Registry > Accounts > User Accounts > edit user account), inspect the following fields:



   - ***Multi-Factor Auth (MFA) User***. Optional. If this user requires a different user name for Multi-factor authentication, enter the MFA user name in this field.
   - ***Authentication Method***. Specifies how the user's user name and password will be authenticated. Select *EM7 Session*. The user name and password are authenticated by the database in SL1.
3. Create an authentication profile for the user. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).

4. In the **Authentication Profiles** page, click the **[Create]** button. The Authentication Profile Editor modal page appears.



5. Enter values in the following fields:

   - ***Name***. Name of the Authentication Profile.
   - ***Priority Order***. If your SL1 system includes multiple Authentication Profiles, SL1 evaluates the Authentication Profiles in priority order, ascending. SL1 will apply the Authentication Profile that matches the Hostname or IP in the current URL AND has the lowest value in the Priority Order field.
   - ***Pattern Type***. Specifies how SL1 will evaluate the value in the ***AP Hostname Pattern*** field. Choices are:
     - *Wildcard*. SL1 will perform a text match, with wildcard characters (asterisks).
     - *Regex*. SL1 will use regular expressions to compare the AP Hostname Pattern to the current session information.
   - ***AP Hostname Pattern***. This field is used to match the URL or IP address that a user enters in a browser to connect to an Administration Portal, Database Server, or All-In-One Appliance. If the URL or IP address matches the value in this field, SL1 applies the Authentication Profile to the user for the current session.

For example, if you specify "*" (asterisk), any IP address or URL will match. SL1 will then apply this Authentication Profile to every session on an Administration Portal, Database Server, or All-In-One Appliance.

If you enter "192.168.38.235", SL1 will apply the Authentication Profile to each session on an Administration Portal, Database Server, or All-In-One Appliances where the user enters "192.168.38.235" into the browser.

If you enter "*.sciencelogic.local", SL1 will apply the Authentication Profile to each session on an Administration Portal, Database Server, or All-In-One Appliance where the user enters a URL ending with ".sciencelogic.local" into the browser.

- ***Available Credential Sources***. This field tells SL1 how to retrieve the user's credentials from the HTTP request to SL1. To align a Credential Source with the Authentication profile, highlight the credential source and click the right-arrow button. You can select zero, one, or multiple credential sources for the Authentication Profile. Initially, this pane displays a list of all the credential sources:
  - *CAC/Client Cert*. SL1 will retrieve a certificate from the HTTP request.
  - *EM7 Login Page*. SL1 will retrieve a user name and password from the login page fields.
  - *HTTP Auth*. SL1 will retrieve a user name and password from the HTTP request.
- ***Aligned Credentials Sources***. This field displays the list of credential sources that have been aligned with the Authentication Profile. The Authentication Profile will examine each credential source in the order in which it appears in this list. When the Authentication Profile find the user's credential, the Authentication Profile stops examining any remaining credential sources in the list.
- ***Available Authentication Resources***.This field tells SL1 which Authentication Resources to use to authenticate the retrieved credentials. To align an Authentication Resource with the Authentication Profile, highlight the Authentication Resource and click the right-arrow button. Select *EM7 Internal*.
- ***Aligned Authentication Resources***. This field displays the list of Authentication Resources that have been aligned with the Authentication Profile. The Authentication Profile will examine each Authentication Resource in the order in which it appears in this list. When an Authentication Resource successfully authenticates the user, the Authentication Profile stops executing any remaining Authentication Resources in the list.
- ***Available Multi-factor Resources***.This field tells SL1 which Multi-factor Resources to use to perform multi-factor authentication. To align an Multi-factor Resource with the Authentication Profile, highlight the Multi-factor Resource and click the right-arrow button. *Select the Multi-Factor Resource you created earlier* in this chapter
- ***Aligned Multi-factor Resources***. This field displays the list of Multi-factor Resources that have been aligned with the Authentication Profile. The Authentication Profile will examine each Multi-factor Resources in the order in which it appears in this list. When a Multi-factor Resource successfully authenticates the user, the Authentication Profile stops executing any remaining Multi-factor Resources in the list.
- **Save**. Saves a new Authentication Profile or changes to an existing Authentication Profile.

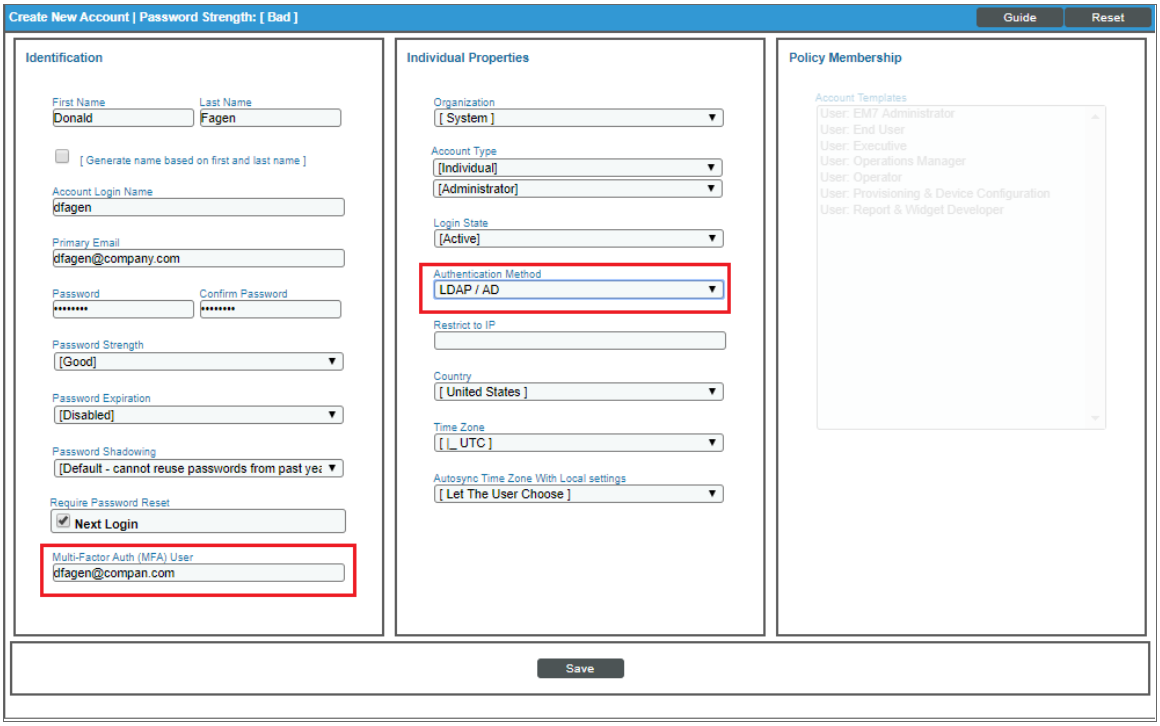
6. Users that are authenticated with EM7 Session will now also be prompted to enter their RSA SecurID token.

Creating an Authentication Profile for Active Directory or LDAP

To use multi-factor authentication for users that use "LDAP/Active Directory" authentication, you must create or edit an authentication profile and align a Multi-Factor Resource. This section explains how to perform these steps.

1. Create a user account or user policy for Active Directory or LDAP users. For details on creating a user account or user policy for use with Actve Directory or LDAP, see the ***Using LDAP or Active Directory*** manual.

2. In either the **Create New Account** page or the Account Permissions page (Registry > Accounts > User Accounts), inspect the following fields:

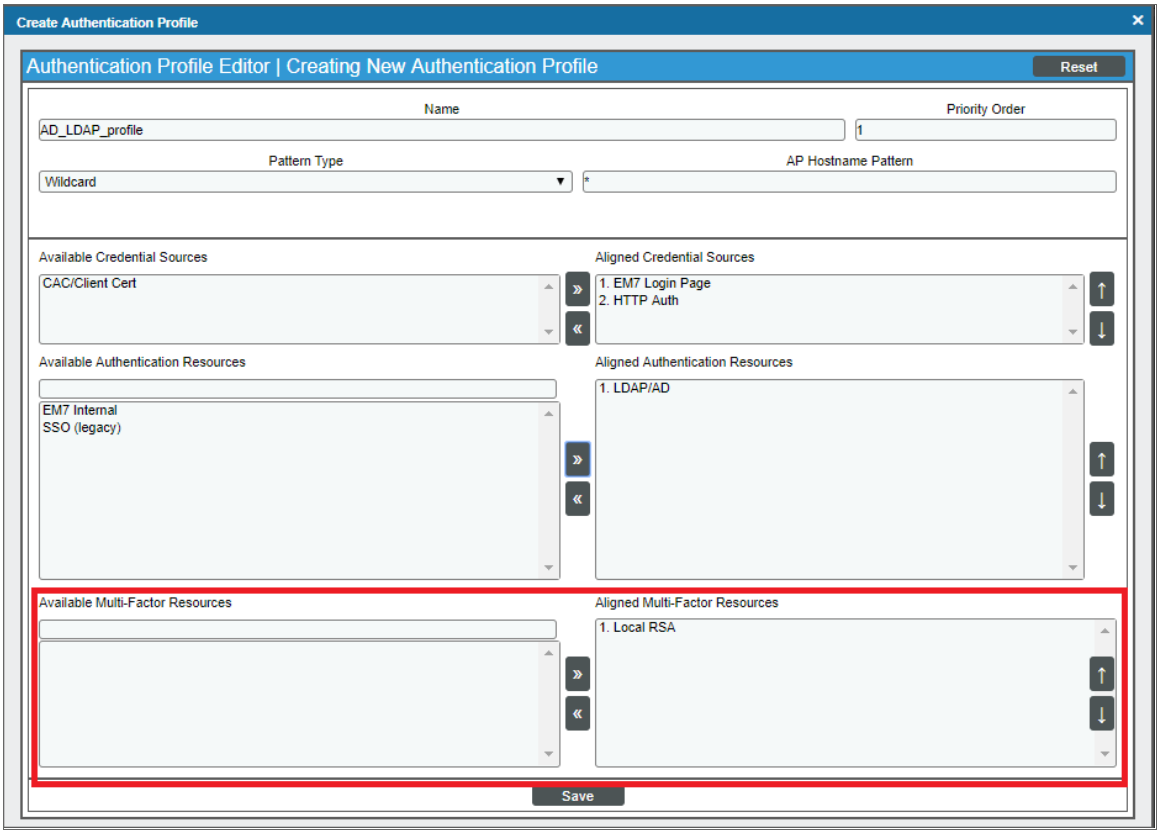


- ***Multi-Factor Auth (MFA) User***. Optional. If this user requires a different user name for Multi-factor authentication, enter the MFA user name in this field.

NOTE: If you specified a value in the ***MFA User*** field in the Attribute Mapping section of the **LDAP/AD Auth Resource Editor** page (System > Settings > Authentication > Resources > create/edit LDAP/AD Resource), the specified Active Directory or LDAP value will be inserted into this field. If you have manually entered a value in this field, the specified Active Directory or LDAP value will overwrite that value.

- ***Authentication Method***. Specifies how the user's user name and password will be authenticated. Select *LDAP/AD*. The user name and password are authenticated by an LDAP server or Active Directory server.

3. Define a credential that allows SL1 to communicate with Active Directory or LDAP. For details, see the ***Using LDAP or Active Directory*** manual.
4. Define an Authentication Resource for Active Directory or LDAP. For details, see the ***Using LDAP or Active Directory*** manual.
5. Define an Authentication Profile for Active Directory or LDAP. For details, see the ***Using LDAP or Active Directory*** manual.



6. Either while defining an Authentication Profile for Active Directory or LDAP or editing an existing Authentication Profile for Active Directory or LDAP, edit the following fields:

   - ***Available Multi-factor Resources***. This field tells SL1 which Multi-factor Resources to use to perform multi-factor authentication. To align an Multi-factor Resource with the Authentication Profile, highlight the Multi-factor Resource and click the right-arrow button. *Select the Multi-Factor Resource you created earlier* in this chapter.
   - ***Aligned Multi-factor Resources***. This field displays the list of Multi-factor Resources that have been aligned with the Authentication Profile. The Authentication Profile will examine each Multi-factor Resources in the order in which it appears in this list. When a Multi-factor Resource successfully authenticates the user, the Authentication Profile stops executing any remaining Multi-factor Resources in the list.
   - **Save**. Saves a new Authentication Profile or changes to an existing Authentication Profile.

7. Users that are authenticated with Active Directory or LDAP will now also be prompted to enter their RSA SecurID token during login.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010