Using Single Sign-On (SSO)

SL1 version 10.2.2

Table of Contents

Introduction 3
What is SSO? 3
SSO Terminology 4
How Can I Use SSO with SL1? 4
Importing User Accounts from Single Sign-On (SSO) 5
Required Tasks 6
Creating a User Policy for Imported Users 8
Creating an SSO Authentication Resource for Importing Users 10
Creating an Authentication Profile 17
Viewing Metadata 20
Using a Self-Signed SSL Certificate 20
Using Single Sign-On (SSO) for Authentication Only 21
Required Tasks 22
Creating a User Account that Will Be Authenticated with SSO 23
Manually Creating a User Account and Manually Defining Account Settings 23
Manually Creating a User Account and Using a User Policy to Define Account Settings 25
Creating an SSO Authentication Resource for Authenticating Users 28
Creating an Authentication Profile 31
Viewing Metadata 34
Using Your Own SSL Certificate 34

Chapter 1

Introduction

Overview

This manual is intended for administrators who create and manage user accounts. This manual assumes that you are familiar with Single Sign-On (SSO). If you are not familiar with SSO, you will need to work with your SSO administrator to perform the tasks in this manual.

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 the menu options, click the Advanced menu icon (⋯).

This chapter includes the following topics:

What is SSO? 3

SSO Terminology 4

How Can I Use SSO with SL1? 4

What is SSO?

SSO (Single Sign-On) allows a user to provide credentials only once and then be authenticated on multiple (or all, depending on configuration) applications. SL1 uses SAML (Security Assertion Markup Language) version 2.0 to exchange information with an IdP (identity provider). An IdP stores information about users in a database, frequently LDAP or Active Directory. In the SAML model, SL1 is considered a service provider.

SSO Terminology

- *SSO (Single Sign-On)*. SSO allows a user to provide credentials only once and then be authenticated on multiple (or all, depending on configuration) applications.
- *SP (Service Provider)*. An application that requires authentication. In our model, SL1 is considered a service provider. The SP passes authentication requests to the IdP.
- *IdP (Identify Provider)*. Stores information about users in a database, frequently LDAP or Active Directory, and passes authentication information to SPs.
- *SAML (Security Assertion Markup Language)*. XML-based standard for exchanging authentication data.
- *SAML Assertion*. A package of information about a user and the user's authentication status. A SAML assertion contains XML attributes.

How Can I Use SSO with SL1?

- You can configure SL1 to automatically *create user accounts in SL1* for existing Single Sign-On users and then always use Single Sign-On to authenticate those users when they access SL1.
- You can use Single Sign-On to *authenticate one or more existing ScienceLogic users* when they log in to SL1.

Chapter 2

Importing User Accounts from Single Sign-On (SSO)

Overview

If you have created SSO accounts for users and do not want to manually create accounts again in SL1, you can configure SL1 to automatically create accounts for SSO users.

Each SSO user accesses SL1 using a URL. SL1 authenticates the user via SSO and automatically creates an account for that user. Each subsequent time that user logs in to SL1, SL1 will use SSO to authenticate that user.

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 the menu options, click the Advanced menu icon (···).

This chapter includes the following topics:

Required Tasks *6*

Creating a User Policy for Imported Users *8*

Creating an SSO Authentication Resource for Importing Users *10*

Creating an Authentication Profile *17*

Viewing Metadata *20*

Using a Self-Signed SSL Certificate *20*

Required Tasks

To configure SL1 to automatically create accounts for SSO users, you must perform the following steps:

1. *Create one or more user policies* that define account properties and privilege keys in the SL1 for imported SSO users.

    - You can create more than one user policy for imported user accounts.

        - For example, suppose you want to import 100 user accounts. But suppose not all of these users require access to the same parts of SL1. You could define multiple user policies, each defining a unique set of ticket queue-memberships, organization memberships, and Access Keys.
        - For example, you could define a user policy for imported user accounts from the Sales department, another user policy for imported user accounts from the Support department, and yet another user policy for imported user accounts from the NOC department.

    - Later, in the SSO Auth Resource Editor (System > Settings > Authentication > create/edit SSO Resource), you specify the user policy to apply to imported user accounts.

        - If you have created only one user policy for all imported accounts, you select the option for *Static policy alignment* and then select the single user policy.
        - If you have created multiple user policies for imported user accounts, you select the option for *Dynamic policy alignment* and then assign a user policy to each type of imported user.

2. *Define the SSO Authentication Resource*.

> NOTE: SL1 supports SAML version 2.0.

- Specify how SL1 should communicate with the SAML IdP and exchange information with the SAML IdP.
- Specify how SL1 should map SSO attribute values to fields in the Account Properties page in SL1.
- Specifies whether SL1 should remain synced with the SAML IdP. If an SSO administrator makes changes to an SSO account, SL1 can automatically retrieve those updates and apply them to the user's account in SL1 (in the Account Properties page) the next time the user logs in to SL1.
- In the *Type* field, specify one of the following:

    - *Static policy alignment.* All user accounts imported from SSO will use a *single user policy*.
    - *Dynamic policy alignment*. You have created multiple user policies for imported SSO user accounts and do not want to use a single user policy for all imported user accounts.

- In the *Policy* field, if you selected *Static policy alignment* in the *Type* field, you must select a policy in the *Policy* field. All users who use the Authentication Resource will use this policy.

- In the *Policy* field, if you selected *Dynamic policy alignment* in the *Type* field, you must supply values in the *Attribute*, *Value*, and *Policy* fields:

    - In the *Attribute* field, specify the SAML attribute you want to use to differentiate imported user accounts. For example, you could select the attribute *department* and then assign different user policies to import user accounts from different departments.
    - In the *Value* field, specify the SAML attribute value. That is, you specify one of the possible values for the attribute (specified in the *Attribute* field).
    - In the corresponding *Policy* field, specify the policy you want to associate with that value. Select from a list of all user policies.
    - For example, suppose you specified *department* in the *Attribute* field. Suppose that the *department* attribute could have two possible values: *Sales* or *NOC*.
    - Suppose you created two user policies. One user policy, called *Sales User Policy*, includes the appropriate ticket queues and access keys for Sales personnel. Another user policy, called *NOC User Policy*, includes the appropriate ticket queues and access keys for NOC personnel.
    - In one of the *Value* fields, you could specify *Sales*. In the corresponding *Policy* field, you could then specify *Sales User Policy*.
    - You could then click on the plus-sign icon (+) and add another *Value* field and another *Policy* field.
    - In the next *Value* field, you could specify *NOC*. In the corresponding *Policy* field, you could specify *NOC User Policy*.
    - After defining these two *Value* fields and corresponding *Policy* fields, user accounts from the *Sales* department would be imported into SL1 using the *Sales User Policy*.
    - User accounts from the *NOC* department would be imported into SL1 using the *NOC User Policy*.

3. *Define one or more Authentication Profiles* that tell SL1 how to recognize SSO users and which *Authentication Resource* to use with those users.
4. After completing these steps:

    - SSO users can attempt to connect to SL1 by entering the URL for an page.
    - SL1 will examine the hostname or IP address in the incoming URL request to align the user with an *Authentication Profile*.
    - The *Authentication Profile* tells SL1 which *SSO Authentication Resource(s)* to use to authenticate the user.
    - The *SSO Authentication Resource* tells SL1 the settings to use to communicate with the SSO IdP. The SSO IdP will then attempt to authenticate each user.
    - Optionally, SL1 will use the mappings and the user policy specified in the *SSO Authentication Resource* to create each user account.

Creating a User Policy for Imported Users

User Policies allow you to define a custom set of account properties and privileges (from the Account Permissions page) and then save them as a policy.

A user policy allows you to define:

- Login State
- Authentication Method
- Ticket Queue Memberships
- Primary Organization and other Organization Memberships
- Theme
- Time Zone
- Access Keys

When you configure SL1 to automatically create user accounts for SSO users, you must define one or more user policies for those imported accounts. Because you will not be creating the accounts manually and then manually defining the account properties, SL1 uses the user policy to define the properties for the user account.

You can create more than one user policy for imported user accounts.

For example, suppose you want to import 100 user accounts from SOS. But suppose not all these users require access to the same parts of SL1. You could define multiple user policies, each defining a unique set of ticket queue memberships, organization membership, and Access Keys.

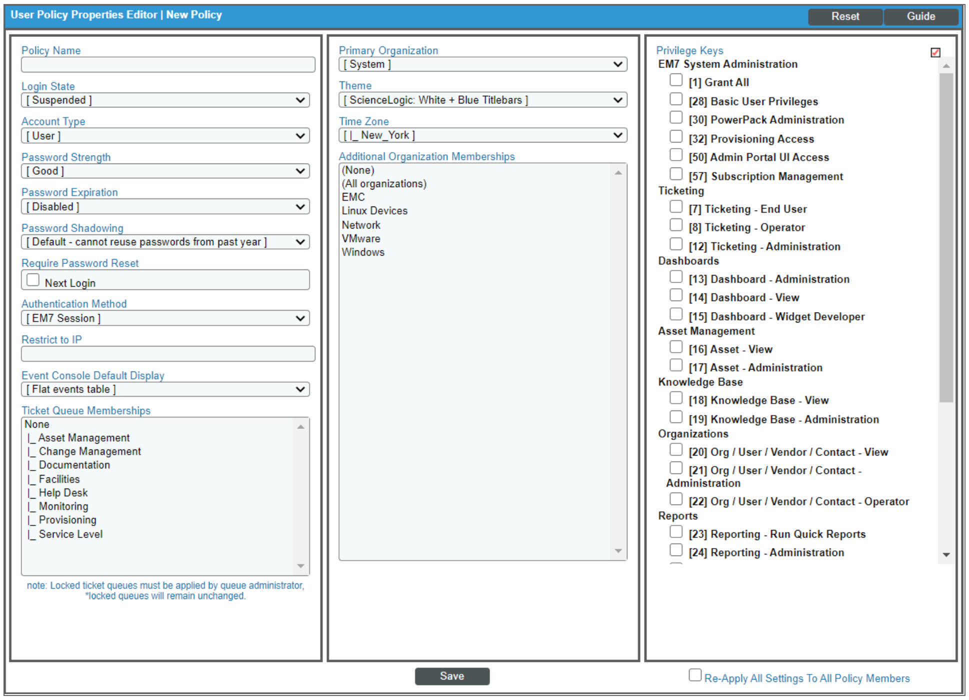
For example, you could define a user policy for imported user accounts from the Sales department, another user policy for imported user accounts from the Support department, and yet another user policy for imported user accounts from the NOC department.

Later, in the SSO Auth Resource Editor page (System > Settings > Authentication > create/edit SSO Resource), you specify the user policy to apply to imported user accounts. When doing this, you could tell SL1 to examine the value of the attribute "department" to determine the department associated with each user account. You could then tell SL1 to assign the sales policy to users from the sales department, the support policy to users from the support department, and so on.

To create a user policy that will configure imported user accounts:

1. Go to the User Policies page (Registry > Accounts > User Policies).

2. In the User Policies page, click the [Create] button. The User Policy Properties Editor page appears.



User Policy Properties Editor | New Policy

Policy Name

Login State
[Suspended]

Account Type
[User]

Password Strength
[Good]

Password Expiration
[Disabled]

Password Shadowing
[Default - cannot reuse passwords from past year]

Require Password Reset
□ Next Login

Authentication Method
[EM7 Session]

Restrict to IP

Event Console Default Display
[Flat events table]

Ticket Queue Memberships
None
|_ Asset Management
|_ Change Management
|_ Documentation
|_ Facilities
|_ Help Desk
|_ Monitoring
|_ Provisioning
|_ Service Level

note: Locked ticket queues must be applied by queue administrator,
*locked queues will remain unchanged.

Primary Organization
[System]

Theme
[ScienceLogic: White + Blue Titlebars]

Time Zone
[|_ New_York]

Additional Organization Memberships
(None)
(All organizations)
EMC
Linux Devices
Network
VMware
Windows

Privilege Keys ☑
EM7 System Administration
□ [1] Grant All
□ [28] Basic User Privileges
□ [30] PowerPack Administration
□ [32] Provisioning Access
□ [50] Admin Portal UI Access
□ [57] Subscription Management
Ticketing
□ [7] Ticketing - End User
□ [8] Ticketing - Operator
□ [12] Ticketing - Administration
Dashboards
□ [13] Dashboard - Administration
□ [14] Dashboard - View
□ [15] Dashboard - Widget Developer
Asset Management
□ [16] Asset - View
□ [17] Asset - Administration
Knowledge Base
□ [18] Knowledge Base - View
□ [19] Knowledge Base - Administration
Organizations
□ [20] Org / User / Vendor / Contact - View
□ [21] Org / User / Vendor / Contact - Administration
□ [22] Org / User / Vendor / Contact - Operator
Reports
□ [23] Reporting - Run Quick Reports
□ [24] Reporting - Administration

□ Re-Apply All Settings To All Policy Members

3. In the User Policy Properties Editor page, supply a value in each field:

- *Policy Name*. Name of the user policy. Can be any combination of alphanumeric characters, up to 64 characters in length.
- *Login State*. Specifies whether user accounts created with the policy can log in to SL1. Choices are:
  - *Active*. Means user accounts created with this policy are active and can log in to SL1.
  - *Suspended*. Means that user accounts created with this policy are not active and cannot log in to SL1.

NOTE: The *Login State* must be set to *Active* before you can successfully import users from SSO.

- *Account Type*. This drop-down list contains an entry for each standard account type. These account types affect the list of Access Keys for the user. The choices are:
  - *Administrator.* By default, administrators are granted all permissions available in SL1. Administrators can access all tabs and pages and perform all actions and tasks.
  - *User.* Accounts of type "user" are assigned Access Keys. Access Keys are customizable by the administrator, and grant users access to pages and tabs and permit users to view information and perform tasks in SL1. These Access Keys are defined by the system administrator from the Access Keys page (System > Manage > Access Keys).

- *Authentication Method*. You can select a value or leave this field blank.

NOTE: For users who are authenticated with SSO, SL1 ignores the *Authentication Method* field.

- *Restrict to IP*. If selected, the user will be allowed to access SL1 only from the specified IP. Specify the IP address in standard dotted-decimal notation.
- *Ticket Queue Memberships*. Highlight one or more ticket queues of which users will be members.
- *Primary Organization*. Specifies the primary organization. This will be the default organization for user accounts created with this policy. You can select from a list of all organizations in SL1.
- *Theme*. Backgrounds, colors, fonts, and graphics that will appear when a user logs in. Themes are defined in the Theme Management page (System > Customize > Themes). You can select from a list of all themes in SL1.
- *Time Zone*. The time zone to associate with each user account created with this user policy. Dates and times in SL1 will be displayed for the selected time zone.
- *Additional Organization Memberships*. User accounts created with this user policy will be members of each selected organization. This allows users to view and access elements from multiple organizations. To select, highlight one or more organizations.
- *Privilege Keys*. The Privilege Keys pane displays a list of Access Keys that can be assigned to the user's account. Access Keys define the tabs and pages users have access to and the actions that a user may perform. These Access Keys are defined by the system administrator from the Access Keys page (System > Manage > Access Keys).
    - To assign an Access Key to a user, select the checkbox. A check mark appears.
    - To deny an Access Key to a user, do not select it.
    - After clicking the [Save] button, all selected Access Keys will appear in red.

4. Click the [Save] button to save your new user policy.
5. Repeat these steps to create additional user policies for user accounts that will be imported from SSO.

Creating an SSO Authentication Resource for Importing Users

An *Authentication Resource* is a configuration policy that describes how SL1 should communicate with a user store. In this manual, the user store is an SSO IdP.

The SSO Auth Resource Editor page allows you to define an Authentication Resource for use with an SSO user store. An SSO Authentication Resource specifies the connector (communication software) to use to communicate with the SAML IdP and the URLs to use to send and retrieve information from the SAML IdP. An SSO Authentication Resource can also map attributes from the user's SSO account to fields in the user account on SL1.

NOTE: SL1 supports SAML version 2.0.

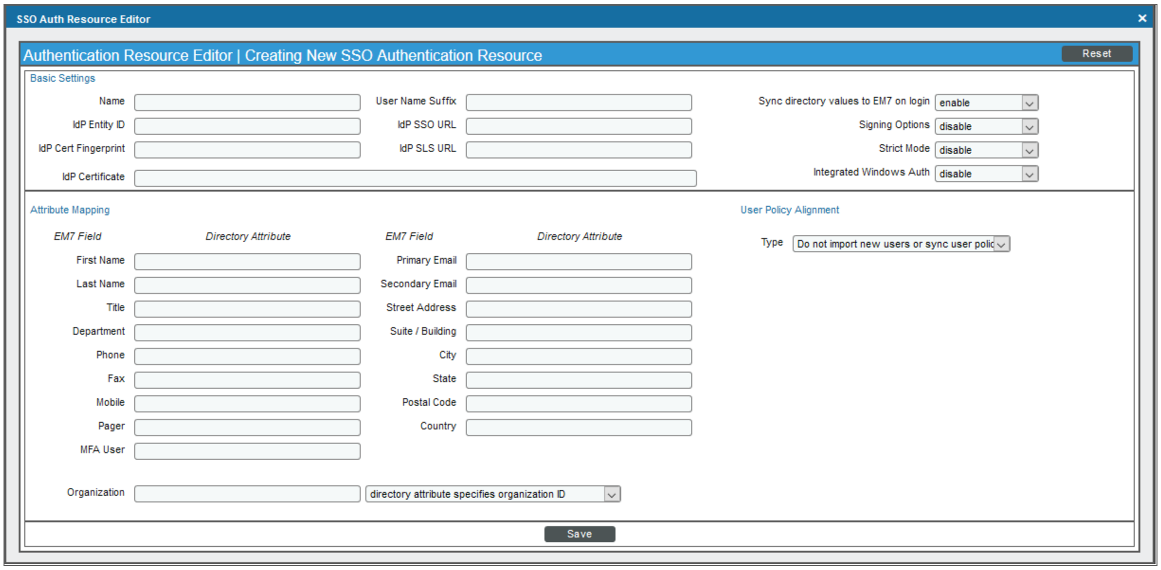
In the SSO Auth Resource Editor page (System > Settings > Authentication > create/edit SSO Resource), you can:

- Specify how SL1 should communicate with the SAML IdP and exchange information with the SAML IdP.
- Specify how SL1 should map SSO attribute values to fields in the Account Properties page.
- Specify whether SL1 should remain synced with the SAML IdP. If an SSO administrator makes changes to an SSO account, SL1 can automatically retrieve those updates and apply them to the user's account in SL1 (in the Account Properties page) the next time the user logs in to SL1.

Additionally, *Authentication Profiles* are policies that align user accounts with one or more Authentication Resources. *Authentication Profiles* are described later in this chapter.

To create an SSO authentication resource that imports existing SSO users:

1. Go to the Authentication Resource Manager page (System > Settings > Authentication > Resources).
2. Click the [Actions] menu and then select *Create SSO Resource*. The SSO Auth Resource Editor page appears.



SSO Auth Resource Editor

Authentication Resource Editor | Creating New SSO Authentication Resource

Basic Settings

Sync directory values to EM7 on login: enable
Signing Options: disable
Strict Mode: disable
Integrated Windows Auth: disable

Attribute Mapping

Organization: directory attribute specifies organization ID

User Policy Alignment

Type: Do not import new users or sync user polic

3. Enter values in the following fields:

Basic Settings

- *Name*. Name of the SSO authentication resource.
- *IdP Entity ID*. Globally unique name used as a SAML identifier configured on the IdP, usually in the format of an absolute URL.

- *IdP Cert Fingerprint*. The SHA1 certificate fingerprint, provided by the identity provider or service provider. Note that this field is not the serial number of the certificate.
- *IdP Certificate*. To ensure that communication between the IdP and EM7 is signed, type the full, PEM-encoded certificate from the IdP.
- *User Name Suffix*. Optional field. If you don't supply a value in this field, SL1 retrieves the SAML *NameID* attribute and uses that value as the ScienceLogic username.
    - You can supply the variable *%u* in this field, and the SL1 retrieves the SAML *NameID* attribute and uses that value as the ScienceLogic user name.
    - You can supply the value %*attribute_name*%, where attribute name is a SAML attribute other than *NameID*. SL1 will use the value of the attribute as the ScienceLogic user name.
    - Because a user can authenticate against multiple SSO servers, there is a risk of collision among user names. In this field, you can enter a string to append to the ScienceLogic user name to minimize risk of collision. For example:
        - You can enter a string, with no SAML attribute specified. When you don't specify a SAML attribute in this field, SL1will retrieve the SAML *NameID* attribute and append the string you specify in this field.

          Suppose we entered *@sciencelogic.local* in this field.

          Suppose the next SSO user logs in to SL1 with the SAML *NameID* of *bishopbrennan*.

          SL1 will log in that user as *bishopbrennan@sciencelogic.local*.

        - You can enter one or more SAML attribute names, surrounded by percent signs (%), with text preceding it and/or text appended. SL1 will retrieve the value of the SAML attribute and use that value plus any preceding text or appended text as the the ScienceLogic user name.

          Suppose we entered *%sn%-external* in this field.

          Suppose the next SSO user logs in to SL1 with their SAML *sn* (last name) attribute of *krilly*

          SL1 will log in that user as *krilly-external*.

NOTE: A best practice to avoid collisions is to use email addresses as user names.

- *IdP SSO URL*. The URL to which SL1 will send login requests to the IdP. This field must contain an absolute URL.
- *IdP SLS URL*. Optional field. If you want each user to be automatically logged out of the IdP when that user logs out of SL1, enter the URL to which SL1 will post the logout request to the IdP. If you leave this field blank, a user can log out of SL1 without automatically logging out of the IdP.

- *Sync directory values to EM7 on login*. If an SSO administrator makes changes to an SSO account, SL1 will automatically retrieve those updates and apply them to the user's account in the Account Properties page the next time the user logs in to SL1. (For more information about user account properties, see the *Organizations & Users* manual.)

- *Signing Options*. Specifies whether digital signing is required for communication between the IdP and SL1. Choices are:

  - *Disable*. No digital signature is required.
  - *IdP Response*. Messages from the IDP to SL1 must be signed. SL1 will use the value in the *IdP Certificate* field to validate the signature.
  - *SP Request and IdP Response*. Messages from the IDP to SL1 must be signed. SL1 will use the value in the *IdP Certificate* field to validate the signature. Messages from SL1 to the IdP must also be signed.

- *Strict Mode*. If you selected *IdP Response* or *SP Request and IdP Response* in the Signing Options field, this field is automatically set to *enable*. This field enforces validation of the SAML response and its attributes. As a best practice, disable this field while initially configuring SL1 and the IdP. As a best practice, enable this field for production use.
- *Integrated Windows Auth*. If you are using Active Directory Federation Services (ADFS) as your IdP, select *Enable* in this field.

Attribute Mapping

If you have configured SL1 to automatically create ScienceLogic accounts for SSO users, these fields specify the SAML attribute value that will be automatically inserted into each field in each user's Account Properties page. (For more information about user account properties, see the *Organizations & Users* manual.)

SL1 automatically populates as many of these fields as possible. You can edit or delete the default values provided by SL1. For example, SL1 automatically inserts the value of the SAML attribute "sn" (surname) into the *Last Name* field in each user's Account Properties page.

> NOTE: SL1 requires that the SAML attribute name that you specify in each field uses all lowercase characters.

- *First Name*. Specifies the SAML attribute value that will be automatically inserted into the *First Name* field in each user's Account Properties page. By default, SL1 inserts the value of the SAML attribute "givenname" into this field.
- *Last Name*. Specifies the SAML attribute value that will be automatically inserted into the *Last Name* field in each user's Account Properties page. By default, SL1 inserts the value of the SAML attribute "sn" into this field.
- *Title*. Specifies the SAML attribute value that will be automatically inserted into the *Title* field in each user's Account Properties page.
- *Department*. Specifies the SAML attribute value that will be automatically inserted into the *Department* field in each user's Account Properties page.

- *Phone*. Specifies the SAML attribute value that will be automatically inserted into the *Phone* field in each user's Account Properties page. By default, SL1 inserts the value of the SAML attribute "telephonenumber" into this field.
- *Fax*. Specifies the SAML attribute value that will be automatically inserted into the *Fax* field in each user's Account Properties page.
- *Mobile*. Specifies the SAML attribute value that will be automatically inserted into the *Mobile* field in each user's Account Properties page. By default, SL1 inserts the value of the SAML attribute "mobile" into this field.
- *Pager*. Specifies the SAML attribute value that will be automatically inserted into the *Pager* field in each user's Account Properties page.
- *Primary Email*. Specifies the SAML attribute value that will be automatically inserted into the *Primary Email* field in each user's Account Properties page. By default, SL1 inserts the value of the SAML attribute "mail" into this field.
- *Secondary Email*. Specifies the SAML attribute value that will be automatically inserted into the *Secondary Email* field in each user's Account Properties page.
- *Street Address*. Specifies the SAML attribute value that will be automatically inserted into the *Street Address* field in each user's Account Properties page. By default, SL1 inserts the value of the SAML attribute "streetaddress" into this field.
- *Suite/Building*. Specifies the SAML attribute value that will be automatically inserted into the *Suite/Building* field in each user's Account Properties page.
- *City*. Specifies the SAML attribute value that will be automatically inserted into the *City* field in each user's Account Properties page. By default, SL1 inserts the value of the SAML attribute "l" into this field.
- *State*. Specifies the SAML attribute value that will be automatically inserted into the *State* field in each user's Account Properties page. By default, SL1 inserts the value of the SAML attribute "st" into this field.
- *Postal Code*. Specifies the SAML attribute value that will be automatically inserted into the *Postal Code* field in each user's Account Properties page. By default, SL1 inserts the value of the SAML attribute "postalcode" into this field.
- *Country*. Specifies the SAML attribute value that will be automatically inserted into the *Country* field in each user's Account Properties page.
- *Organization*. Specifies the SAML attribute value that will be used to automatically define the *Primary Organization* field in each user's Account Permissions page. You must also specify one of the following:
    - *directory attribute specifies organization ID*. The attribute in the *Organization* field specifies an organization ID.
    - *directory attribute specifies organization name*. The attribute in the *Organization* field specifies an organization name.
    - *directory attribute specifies organization CRM ID*. The attribute in the *Organization* field specifies the CRM ID of an organization.

NOTE: To use Attribute Mapping for *Organization*, your SAML schema must include an attribute that maps to ScienceLogic Organization names, ScienceLogic Organization IDs, or ScienceLogic Organization CRM IDs.

NOTE: When you create a new SSO user, you must align a user policy with that user. If the aligned user policy specifies an organization for the user, the value from the user policy will overwrite the value from Attribute Mapping.

User Policy Alignment

- *Type*. Specifies whether SL1 should automatically create ScienceLogic accounts for each SSO user, whether SL1 should simply use SSO to authenticate one or more users, or whether SL1 will refuse to authenticate specific users. Choices are:
  - *Do not import new users or sync user policy authenticate new users*. Only those users who have an account already created in SL1 can log in to SL1, which will authenticate those users with SSO using the settings specified in this page.*If you have have configured SL1 to authenticate only using SSO*, select this option.
  - *If you have configured SL1 to automatically create ScienceLogic accounts for SSO users*, select one of the following options:
  - *Static policy alignment*. If an SSO user tries to access SL1, SL1 will automatically create an account for that user. SL1 will use one user policy (specified in the *Policy* field) to create the imported SSO user accounts for this authentication resource. SL1 will also use the settings specified in this page when creating the account.
  - *Dynamic policy alignment*. If an SSO users tries to access SL1, SL1 will automatically create an account for that user. SL1 will choose from among multiple user policies to create imported SSO user accounts for this authentication resource. For example, some imported user accounts might use "user policy A"; other imported user accounts might use "user policy B". SL1 will also use the settings specified in this page when creating the account.

NOTE: If you selected *Static policy alignment* in the *Type* field, you must supply a value in the *Policy* field.

- *Policy*. If you selected a *Type* of *Static policy alignment*, this field specifies the policy to use to create the user account. Select from a list of all user policies.Specifies the user policy to use to automatically create a ScienceLogic account for each SSO user.

NOTE: If you selected *Dynamic policy alignment* in the *Type* field, you must supply values in the *Attribute*, *Value*, and *Policy* fields.

- *Attribute*. If you selected a *Type* of *Dynamic policy alignment*, this field Sspecifies the SAML attribute you want to use to differentiate imported user accounts. For example, you could select the attribute *department* and then assign different user policies to import user accounts from different departments. You can also use this field to exclude SSO accounts for which you do not want to allow authentication.
- *Value*. If you selected a *Type* of *Dynamic policy alignment*, this field Sspecifies the SAML attribute value. That is, you specify one of the possible values for the attribute (specified in the *Attribute* field). SL1 will compare the value in this field to the retrieved value for the *Attribute*.
- *Policy*. If you selected a *Type* of *Dynamic policy alignment*, this field specifies *the policy you want to associate with the attribute/value pair*. Select from a list of all user policies.
    - For example, suppose you specified *department* in the *Attribute* field. Suppose that the *department* attribute could have two possible values: *Sales* or *NOC*.
    - Suppose you created two user policies. One user policy, called *Sales User Policy*, includes the appropriate ticket queues and access keys for Sales personnel. Another user policy, called *NOC User Policy*, includes the appropriate ticket queues and access keys for NOC personnel.
    - In one of the *Value* fields, you could specify *Sales*. In the corresponding *Policy* field, you could then specify *Sales User Policy*.
    - You could then click on the plus-sign icon (+) and add another *Value* field and another *Policy* field.
    - In the next *Value* field, you could specify *NOC*. In the corresponding *Policy* field, you could specify *NOC User Policy*.
    - After defining these two *Value* fields and the corresponding *Policy* fields, user accounts from the *Sales* department would be imported into SL1 using the *Sales User Policy*.
    - User accounts from the *NOC* department would be imported into SL1 using the *NOC User Policy*.
    - *Do Not Authenticate*. If the retrieved value of the specified *Attribute* matches the value in the *Value* field, the user is not authenticated. This setting applies to new users for whom SSO would have to create a new account in SL1 and for users who already have an account in SL1.
        - In the *Attribute* field, you could also specify *status*. Suppose that the *status* attribute could have two possible values: *active* or *terminated*.
        - In the next *Value* field, you could specify *terminated*. In the corresponding *Policy* field, you could specify *Do Not Authenticate*.
        - Whenever an LDAP or AD entry for a user included the *status* attribute with the value *terminated*, SL1 could apply the policy *Do Not authenticate*.
- To define additional *Value* and *Policy* fields, click on the green plus-sign icon (+).

4. Click the [Save] button to save your changes to the new authentication resource.

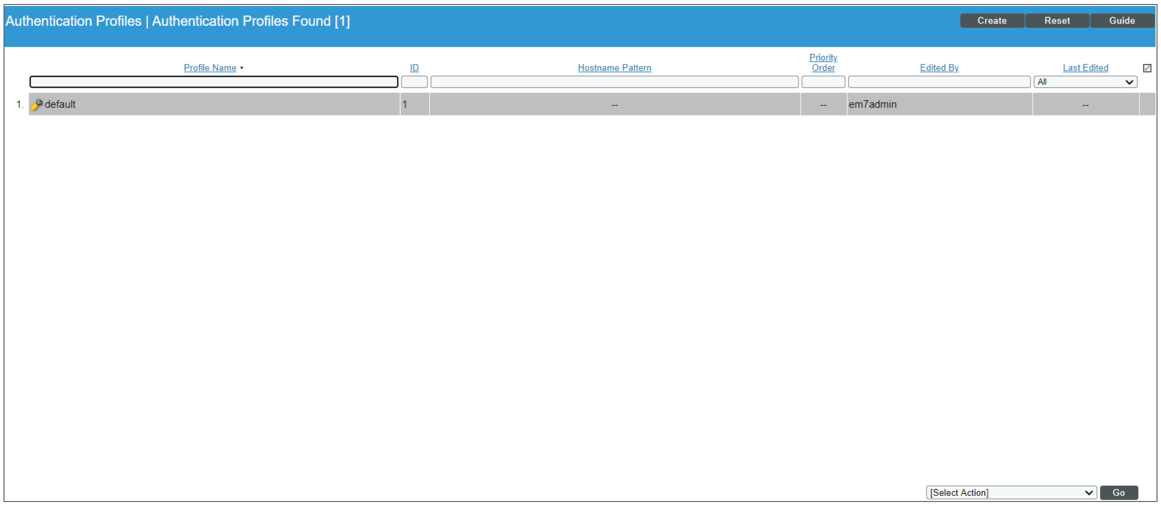
Creating an Authentication Profile

An *Authentication Profile* is a policy for user authentication. Authentication Profiles align user accounts with one or more *Authentication Resources*.

- *Alignment by pattern matching*. SL1 uses 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 criteria specified in an authentication profile, SL1 will automatically use the matching profile to perform user authentication.
- *Credential Source*. Specifies from where SL1 should extract the user name and password or certificate to be authenticated. These credentials are passed to SL1 via HTTP. SL1 then passes the credentials to each Authentication Resource specified in the Authentication Profile. The Authentication Resources authenticate the credentials with user stores.
- *Authentication Resource*. Specifies the connector to use to communicate with the user store and the URLs to examine during authentication. Also maps attributes from the user's account in the user store to fields in SL1 user account.

The Authentication Profiles page allows you to create a new authentication profile. To do so:

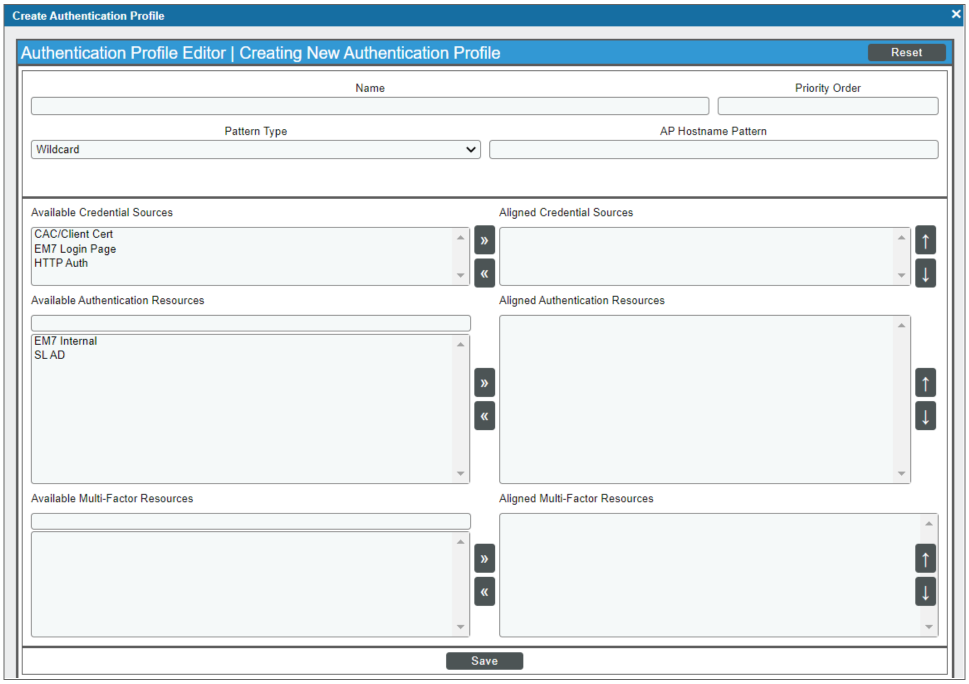
1. Go to the Authentication Profiles page (System > Settings > Authentication > Profiles).



Authentication Profiles | Authentication Profiles Found [1]

	Profile Name	ID	Hostname Pattern	Priority Order	Edited By	Last Edited
1.	default	1	--	--	em7admin	--

2. In the Authentication Profiles page, click the [Create] button.


Create Authentication Profile
Authentication Profile Editor | Creating New Authentication Profile
Reset
Name
Priority Order
Pattern Type
AP Hostname Pattern
Available Credential Sources
Aligned Credential Sources
Available Authentication Resources
Aligned Authentication Resources
Available Multi-Factor Resources
Aligned Multi-Factor Resources
»
«
Save

Pattern Type: Wildcard

Available Credential Sources:
CAC/Client Cert
EM7 Login Page
HTTP Auth

Available Authentication Resources:
EM7 Internal
SL AD

3. The Authentication Profile Editor modal page appears. In this page, you can define the new authentication profile.

   - *Name*. Name of the Authentication Profile.
   - *Priority Order*. If SL1 includes multiple Authentication Profiles, SL1 evaluates the Authentication Profiles in priority order, ascending. SL1 will apply the first 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 Appliance 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 username and password from SL1 login page fields.
  - *HTTP Auth*. SL1 will retrieve a username 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 finds 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. You must select at least one Authentication Resource and can select more than one.
- *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 EM7 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 select the right-arrow button. For details on creating a Multi-factor Resource, see the guide for the Multi-factor Resource Editor.
- *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 Resources successfully authenticates the user, the Authentication Profile stops executing any remaining Multi-factor Resources in the list.

NOTE: Best practice for SSO includes multi-factor authentication when connecting to the Identity Provider, not when logging in to SL1. For details on configuring multi-factor authentication, see the manual *Using Multi-Factor Authentication*.

4. Click the [Save] button to save your changes to the new authentication profile.

Viewing Metadata

To view the metadata for OneLogin SAML (the EM7 imlementation of SSO), enter the following URL in a browser:

```
https://hostname_or_ip_of_EM7_appliance/samlsp.em7?action=metadata
```

Using a Self-Signed SSL Certificate

By default, SL1 uses a self-signed certificate generated by SL1 during installation from ISO. SL1 uses the default SSL certificate from nginx as the certificate for communication with the Identity Provider.

If you want to use your own certificate for communication between SL1 and the Identity Provider, perform the following:

1. Go to the console of the Administration Portal or start an SSH session to the Administration Portal.
2. Either generate a self-signed SSL certificate of type .pem and an SSL key or acquire these files from a certificate authority. Save the certificate files with names that will not conflict with the default files *silossl.pem* and *silossl.key*.
3. Copy the certificate files to the /etc/nginx directory.
4. Using vi or another text editor, edit the file /etc/nginx/conf.d/em7ngx_web_ui.conf
5. Edit the following lines:

```
ssl_certificate /etc/nginx/silossl.pem;
ssl_certificate_key /etc/nginx/silossl.key;
```

   - Replace silossl.pem with the .pem file for your new certificate.
   - Replace silossl.key with the .key file for your new certificate.

6. Save and quit the file.

Chapter

3

Using Single Sign-On (SSO) for Authentication Only

Overview

If you have already created accounts for users in SL1, you can use SSO to authenticate one or more of those users. Each time an SSO user tries to access SL1, SL1 will use SSO to authenticate that user.

1. Each user logs in to SL1 by entering the URL for the All-In-One Appliance, Administration Portal, or Database Server.
2. SL1 examines the URL from which the request originates and applies the appropriate Authentication Profile (and the appropriate Authentication Resource).
3. If the user is not yet logged in to the SAML IdP:
    - The user will be directed to the login page for the SAML IdP.
    - After successfully logging in to the SAML IdP, the SAML IdP will send a message to SL1 via the user's browser (a SAML assertion), informing SL1 that the user is authenticated.
4. If the user is already logged in to the SAML IdP:
    - The SAML IdP will send a message to SL1 via the user's browser (a SAML assertion), informing SL1 that the user is authenticated.
5. SL1 displays the user's default page.

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 the menu options, click the Advanced menu icon (⋯).

This chapter includes the following topics:

Required Tasks *22*
Creating a User Account that Will Be Authenticated with SSO *23*
Manually Creating a User Account and Manually Defining Account Settings *23*
Manually Creating a User Account and Using a User Policy to Define Account Settings *25*
Creating an SSO Authentication Resource for Authenticating Users *28*
Creating an Authentication Profile *31*
Viewing Metadata *34*
Using Your Own SSL Certificate *34*

Required Tasks

To configure SL1 to automatically create accounts for SSO users, you must perform the following steps:

1. *Create a user account in SL1*. You can either create the account manually or you can use a user policy to create the account.

2. *Define the SSO Authentication Resource*.

    - Specify how SL1 should communicate with the SSO IdP and exchange information with the SSO IdP.
    - In the *Type* field, specify the following:

        - *Do not import new users or sync user policies.*SL1 will use SSO only to authenticate users and will not create a new user each time an SSO user attempts to connect to SL1.

3. *Define one or more Authentication Profiles* that tell SL1 how to recognize SSO users and which Authentication Resource to use with those users.
4. After completing these steps:

    - SSO users can attempt to connect to SL1 by entering the URL for an page.
    - SL1 will examine the hostname or IP address in the incoming URL request to align the user with an *Authentication Profile*.
    - The *Authentication Profile* tells SL1 which *SSO Authentication Resource(s)* to use to authenticate the user.
    - The *SSO Authentication Resource* tells SL1 the settings to use to communicate with the SSO IdP. The SSO IdP will then attempt to authenticate each user.

Creating a User Account that Will Be Authenticated with SSO

User accounts allow users to log in to SL1 and access pages and features in SL1. If you have already created a user account for a user in SSO, you can create a separate user account for that user in SL1 and then ask SSO to authenticate the user account.

There are two ways to create a user account in SL1:

- Manually create a user account and define all account settings.
- Manually create a user account and then apply a user policy to define additional account settings. User policies allow you to define a custom set of account properties and privileges and then save them as a policy.

Both options are described in this chapter.

Manually Creating a User Account and Manually Defining Account Settings

You can manually create a user account in SL1.

If you want to use SSO to authenticate the user when he/she logs in to SL1, you must:

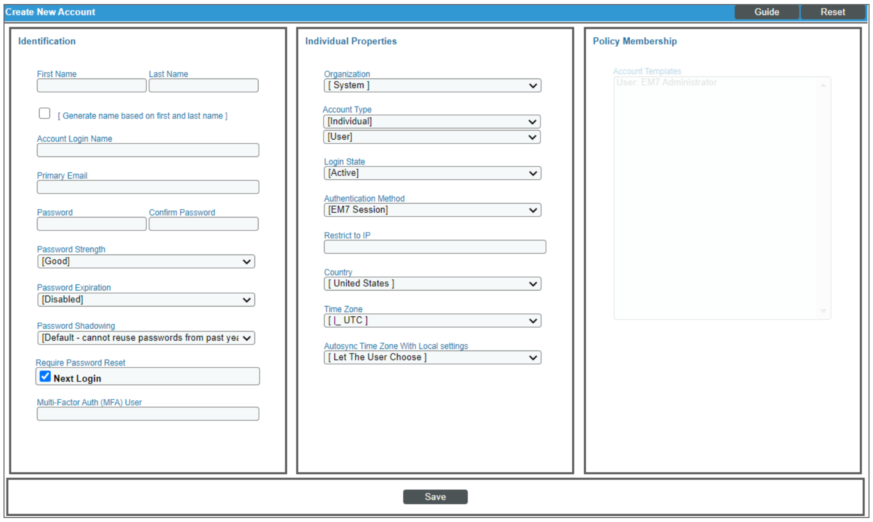
- Manually create a user account in SL1.

NOTE: The value in the *Account Login Name* must match the value of the SAML attribute *uid*.

To manually create a user account and apply a user policy to that account:

1. Go to the User Accounts page (Registry > Accounts > User Accounts).
2. In the User Accounts page, click the [Create] button.

3. The Create New Account page appears.



First Name
Last Name
□ [Generate name based on first and last name]
Account Login Name
Primary Email
Password
Confirm Password
Password Strength: [Good]
Password Expiration: [Disabled]
Password Shadowing: [Default - cannot reuse passwords from past yea
Require Password Reset: ☑ Next Login
Multi-Factor Auth (MFA) User

Organization: [System]
Account Type: [Individual] [User]
Login State: [Active]
Authentication Method: [EM7 Session]
Restrict to IP
Country: [United States]
Time Zone: [|_ UTC]
Autosync Time Zone With Local settings: [Let The User Choose]

Account Templates: User: EM7 Administrator

4. In the Create New Account page, enter values in each of the following fields:

- *First Name*. User's first name. This value can be up to 24 characters in length.
- *Last Name*. User's last name. This value can be up to 24 characters in length.
- *Generate a unique name based on first and last name*. Do not select this option.
- *Account Login Name* The same value as is stored in the SAML attribute *uid*.
- *Primary Email*. User's email address. This field can be up to 64 characters in length.
- *Password*. You can enter any password that meets the minimum security requirements. The password must be at least four characters in length and can be up to 64 characters in length.

NOTE: During authentication, SSO will ignore the value in the *Password* field and instead use the password stored in the IDP.

- *Confirm Password*. The user's password again. This value must be at least four characters in length and can be up to 64 characters in length. This password will be overwritten with the SSO password on first login.
- *Password Strength*. Required strength of the user's password. Must be set to *Strong*. The password will not be able to be changed through SL1.
- *Password Expiration*. Set this field to *Disabled*. The password will not be able to be changed through SL1.
- *Password Shadowing*. Set this field to *Default*. The password cannot be changed through SL1.
- *Require Password Reset*. Do not select this option. The password cannot be changed through SL1.

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

NOTE: : Best practice for SSO includes multi-factor authentication when connecting to the Identity Provider, not when logging in to SL1. For details on configuring multi-factor authentication, see the manual *Using Multi-Factor Authentication*.

- *Organization*. The organization of which the new user account will be a member. Users can select from among all organizations in SL1.
- *Account Type*. Specifies whether the user is a member of a user policy. Choices are:
  - *Individual*. User account is not a member of a user policy.
  - *Policy Membership*. Select this option. User will be defined with a user policy. When selected, the *Policy Membership* field becomes active.
- *Login State*. Default login state for the user account. The choices are:
  - *Suspended*. Account is not active. User cannot log in to SL1.
  - *Active*. Account is active. User can log in to SL1.
- *Authentication Method*. Specifies how the user's username and password will be authenticated. Select one of the following:
  - *EM7 Session*. User’s user-name and password are authenticated by SL1.
  - *LDAP/Active Directory*. User's username and password are authenticated by an LDAP server or Active Directory server.

NOTE: For users who are authenticated with SSO, you must set the *Authentication Method* field to "LDAP/Active Directory" to support automatic user policy alignment updates in case attributes change.

- *Restrict to IP*. The user will be allowed to access SL1 only from the specified IP. Specify the IP address in standard dotted-decimal notation.
- *Time Zone*. Select the appropriate time zone to associate with the user account.

5. Click the [Save] button to save the new user.

Manually Creating a User Account and Using a User Policy to Define Account Settings

You can manually create a user account and then apply a user template to that user account.

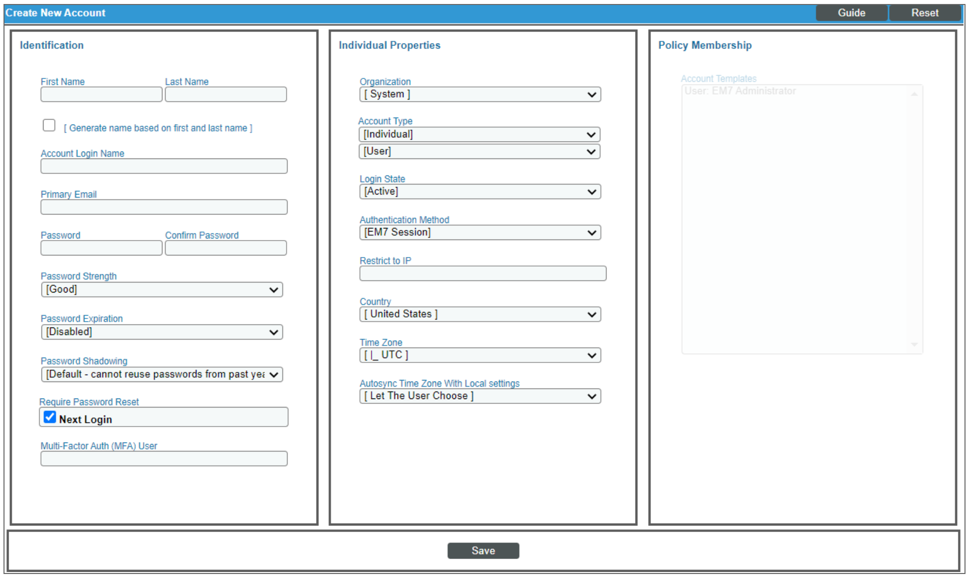
If you want to use SSO to authenticate the user when he/she logs in to SL1, you must:

- Define a user policy before creating the user account. For SSO authentication, there are no requirements for the user policy. You can define the user policy as you wish. For details on creating a user policy, see the manual *Organizations and Users*.
- Define the user account in SL1.

NOTE: The value in the *Account Login Name* must match the value of the SAML attribute *uid*.

To manually create a user account and apply a user policy to that account:

1. Go to the User Accounts page (Registry > Accounts > User Accounts).
2. In the User Accounts page, click the [Create] button.
3. The Create New Account page appears.



Identification

First Name
Last Name
□ [Generate name based on first and last name]
Account Login Name
Primary Email
Password
Confirm Password
Password Strength: [Good]
Password Expiration: [Disabled]
Password Shadowing: [Default - cannot reuse passwords from past yea
Require Password Reset: ☑ Next Login
Multi-Factor Auth (MFA) User

Individual Properties

Organization: [System]
Account Type: [Individual] [User]
Login State: [Active]
Authentication Method: [EM7 Session]
Restrict to IP
Country: [United States]
Time Zone: [|_ UTC]
Autosync Time Zone With Local settings: [Let The User Choose]

Policy Membership

Account Templates
User: EM7 Administrator

4. In the Create New Account page, enter values in each of the following fields:

    - *First Name*. User's first name. This value can be up to 24 characters in length.
    - *Last Name*. User's last name. This value can be up to 24 characters in length.
    - *Generate name based on first and last name*. Do not select this option.
    - *Account Login Name* The same value as is stored in the SAML attribute *uid*.
    - *Primary Email*. User's email address. This field can be up to 64 characters in length.
    - *Password*. You can any password that meets the minimum security requirements. The password must be at least four characters in length and can be up to 64 characters in length.

NOTE: During authentication, SSO will ignore the value in the *Password* field and instead use the password stored in the IDP.

- *Confirm Password*. The user's password again. This value must be at least four characters in length and can be up to 64 characters in length. This password will be overwritten with the SSO password on first login.
- *Password Strength*. Required strength of the user's password. Must be set to *Strong*. The password will not be able to be changed through SL1.
- *Password Expiration*. Set this field to *Disabled*. The password will not be able to be changed through SL1.
- *Password Shadowing*. Set this field to *Default*. The password cannot be changed through SL1.
- *Require Password Reset*. Do not select this option. The password cannot be changed through SL1.
- *Multi-Factor Auth (MFA) User*. If this user requires a different user name for Multi-factor authentication, enter the MFA user name in this field.

NOTE: Best practice for SSO includes multi-factor authentication when connecting to the Identity Provider, not when logging in to SL1. For details on configuring multi-factor authentication, see the manual *Using Multi-Factor Authentication*.

- *Organization*. The organization of which the new user account will be a member. Users can select from among all organizations in SL1.
- *Account Type*. Specifies whether the user is a member of a user policy. Choices are:
  - *Individual*. User account is not a member of a user policy.
  - *Policy Membership*. Select this option. User will be defined with a user policy. When selected, the *Policy Membership* field becomes active.

  After you select *Policy Membership*, all remaining fields except *Account Templates* are disabled. This is because those fields are defined in the user policy.
- *Policy Membership*. If you selected *Policy Membership* in the *Account Type* field, the *Policy Membership* field is activated. In this field, you can select a user policy to apply to the new user account.
  - When a user policy is applied to a user's account, the user inherits the Access Keys specified in the user policy. Administrators cannot add additional Access Keys or delete Access Keys from the user's account unless they edit the user policy.
  - When a user policy is edited, each user account that is a member of that template will be dynamically updated.

5. Click the [Save] button to save the new user.

Creating an SSO Authentication Resource for Authenticating Users

An *Authentication Resource* is a configuration policy that describes how SL1 should communicate with a user store. In this manual, the user store is an SSO IdP.

The SSO Auth Resource Editor page allows you to define an Authentication Resource for use with an SSO user store. An SSO Authentication Resource specifies the connector (communication software) to use to communicate with the SAML IdP and the URLs to use to send and retrieve information from the SAML IdP. An SSO Authentication Resource can also map attributes from the user's SSO account to fields in the user account on SL1.

NOTE: SL1 supports SAML version 2.0.

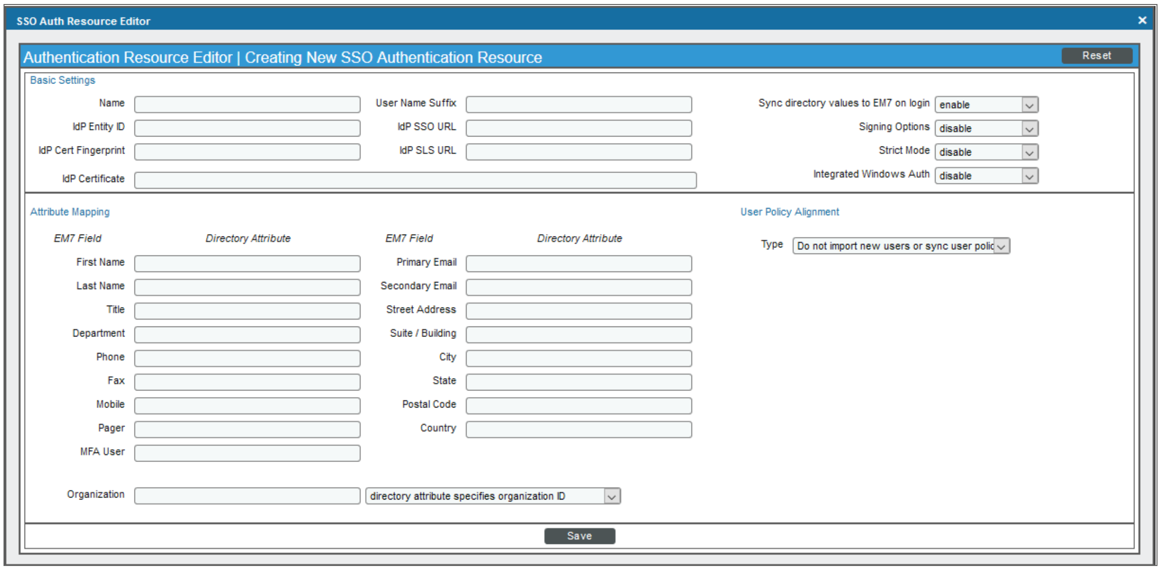
In the SSO Auth Resource Editor page (System > Settings > Authentication > create/edit SSO Resource), you can:

- Specify how SL1 should communicate with the SAML IdP and exchange information with the SAML IdP.

Additionally, *Authentication Profiles* are policies that align user accounts with one or more Authentication Resource. *Authentication Profiles* are described later in this chapter.

To create an SSO authentication resource that authenticates existing users in SL1:

1. Go to the Authentication Resource Manager page (System > Settings > Authentication > Resources).
2. Click the [Actions] menu and then select *Create SSO Resource*. The SSO Auth Resource Editor page appears.



SSO Auth Resource Editor

Authentication Resource Editor | Creating New SSO Authentication Resource

Sync directory values to EM7 on login: enable

Signing Options: disable

Strict Mode: disable

Integrated Windows Auth: disable

Type: Do not import new users or sync user polic

Organization: directory attribute specifies organization ID

3. Enter values in the following fields:

   <u>Basic Settings</u>

   - *Name*. Name of the SSO authentication resource.
   - *IdP Entity ID*. Globally unique name used as a SAML identifier configured on the IdP, usually in the format of an absolute URL.
   - *IdP Cert Fingerprint*. The SHA1 certificate fingerprint, provided by the identity provider or service provider. Note that this field is not the serial number of the certificate.
   - *IdP Certificate*. To ensure that communication between the IdP and EM7 is signed, type the full, PEM-encoded certificate from the IdP.
   - *User Name Suffix*. Optional field. If you don't supply a value in this field, SL1 retrieves the SAML *NameID* attribute and uses that value as the ScienceLogic username.
     - You can supply the variable *%u* in this field, and the SL1 retrieves the SAML *NameID* attribute and uses that value as the ScienceLogic user name.
     - You can supply the value %*attribute_name*%, where attribute name is a SAML attribute other than *NameID*. SL1 will use the value of the attribute as the ScienceLogic user name.
     - Because a user can authenticate against multiple SSO servers, there is a risk of collision among user names. In this field, you can enter a string to append to the ScienceLogic user name to minimize risk of collision. For example:
       - You can enter a string, with no SAML attribute specified. When you don't specify a SAML attribute in this field, SL1will retrieve the SAML *NameID* attribute and append the string you specify in this field.

         Suppose we entered *@sciencelogic.local* in this field.

         Suppose the next SSO user logs in to SL1 with the SAML *NameID* of *bishopbrennan*.

         SL1 will log in that user as *bishopbrennan@sciencelogic.local*.
       - You can enter one or more SAML attribute names, surrounded by percent signs (%), with text preceding it and/or text appended. SL1 will retrieve the value of the SAML attribute and use that value plus any preceding text or appended text as the the ScienceLogic user name.

         Suppose we entered *%sn%-external* in this field.

         Suppose the next SSO user logs in to SL1 with their SAML *sn* (last name) attribute of *krilly*

         SL1 will log in that user as *krilly-external*.

NOTE: A best practice to avoid collisions is to use email addresses as user names.

- *IdP SSO URL*. The URL to which SL1 will send login requests to the IdP. This field must contain an absolute URL.
- *IdP SLS URL*. Optional field. If you want each user to be automatically logged out of the IdP when that user logs out of SL1, enter the URL to which SL1 will post the logout request to the IdP. If you leave this field blank, a user can log out of SL1 without automatically logging out of the IdP.
- *Sync directory values to EM7 on login*. If an SSO administrator makes changes to an SSO account, SL1 will automatically retrieve those updates and apply them to the user's account in the Account Properties page the next time the user logs in to SL1. (For more information about user account properties, see the *Organizations & Users* manual.)
- *Signing Options*. Specifies whether digital signing is required for communication between the IdP and SL1. Choices are:
  - *Disable*. No digital signature is required.
  - *IdP Response*. Messages from the IDP to SL1 must be signed. SL1 will use the value in the *IdP Certificate* field to validate the signature.
  - *SP Request and IdP Response*. Messages from the IDP to SL1 must be signed. SL1 will use the value in the *IdP Certificate* field to validate the signature. Messages from SL1 to the IdP must also be signed.
- *Strict Mode*. If you selected *IdP Response* or *SP Request and IdP Response* in the Signing Options field, this field is automatically set to *enable*. This field enforces validation of the SAML response and its attributes. As a best practice, disable this field while initially configuring SL1 and the IdP. As a best practice, enable this field for production use.
- *Integrated Windows Auth*. If you are using Active Directory Federation Services (ADFS) as your IdP, select *Enable* in this field.

Attribute Mapping

These fields can be left blank or with their default values.

> NOTE: SL1 requires that the SAML attribute name that you specify in each field uses all lowercase characters.

User Policy Alignment

- *Type*. Select *Do not import new users or sync user profiles*.

4. Click the [Save] button to save your changes to the new authentication resource.

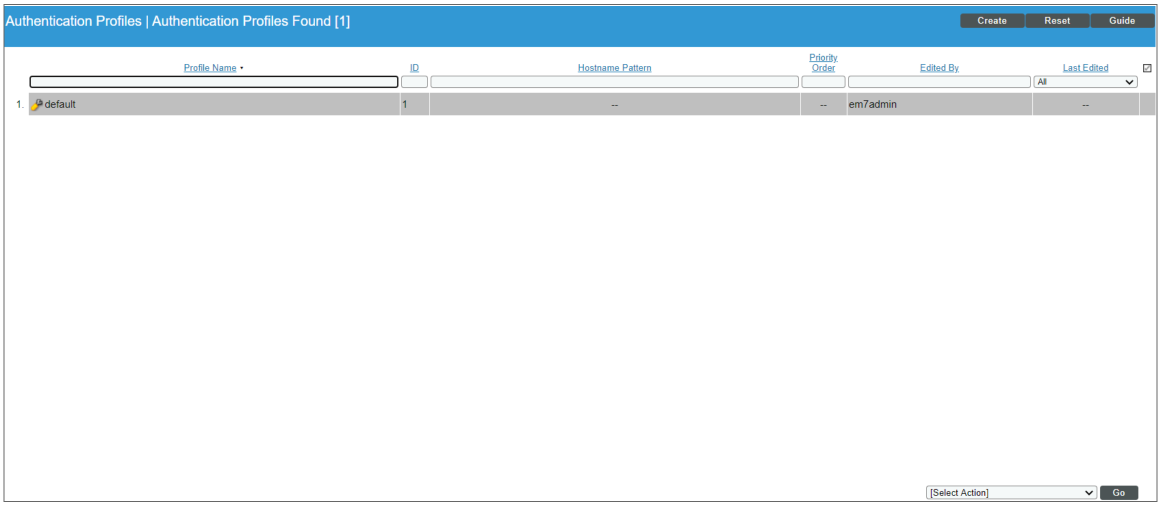
Creating an Authentication Profile

An *Authentication Profile* is a policy for user authentication. Authentication Profiles align user accounts with one or more *Authentication Resources*.

- *Alignment by pattern matching*. SL1 uses 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 criteria specified in an authentication profile, SL1 will automatically use the matching profile to perform user authentication.
- *Credential Source*. Specifies from where SL1 should extract the username and password or certificate to be authenticated. These credentials are passed to SL1 via HTTP. SL1 then passes the credentials to each Authentication Resource specified in the Authentication Profile. The Authentication Resources authenticate the credentials with user stores.
- *Authentication Resource*. Specifies the connector to use to communicate with the user store and the URLs to examine during authentication. Also maps attributes from the user's account in the user store to fields in the SL1 user account.

The Authentication Profiles page allows you to create a new authentication profile. To do so:

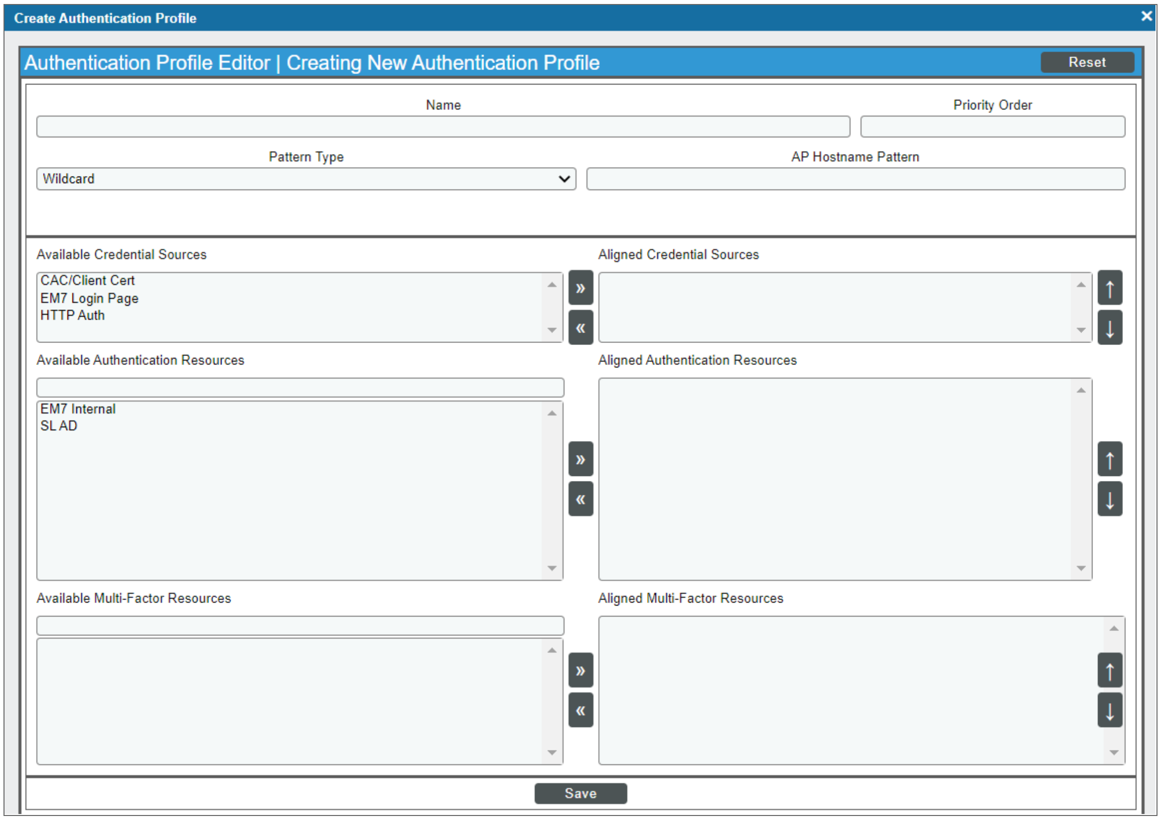
1. Go to the Authentication Profiles page (System > Settings > Authentication > Profiles).



Authentication Profiles | Authentication Profiles Found [1]

	Profile Name	ID	Hostname Pattern	Priority Order	Edited By	Last Edited
1.	default	1	--	--	em7admin	--

2. In the Authentication Profiles page, click the [Create] button.


Create Authentication Profile
Authentication Profile Editor | Creating New Authentication Profile
Reset
Name
Priority Order
AP Hostname Pattern
Aligned Credential Sources
Aligned Authentication Resources
Available Multi-Factor Resources
Aligned Multi-Factor Resources
»
«
Save

Pattern Type: Wildcard

Available Credential Sources:
CAC/Client Cert
EM7 Login Page
HTTP Auth

Available Authentication Resources:
EM7 Internal
SL AD

3. The Authentication Profile Editor modal page appears. In this page, you can define the new authentication profile.

    - *Name*. Name of the Authentication Profile.
    - *Priority Order*. If SL1 includes multiple Authentication Profiles, SL1 evaluates the Authentication Profiles in priority order, ascending. SL1 will apply the first 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 Appliance 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 username and password from the SL1 login page fields.
  - *HTTP Auth*. SL1 will retrieve a username 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 finds 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. You must select at least one Authentication Resource and can select more than one.
- *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 EM7 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 select the right-arrow button. For details on creating a Multi-factor Resource, see the guide for the Multi-factor Resource Editor.

- *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 Resources successfully authenticates the user, the Authentication Profile stops executing any remaining Multi-factor Resources in the list.

NOTE: Best practice for SSO includes multi-factor authentication when connecting to the Identity Provider, not when logging in to SL1. For details on configuring multi-factor authentication, see the manual *Using Multi-Factor Authentication*.

4. Click the [Save] button to save your changes to the new authentication profile.

Viewing Metadata

To view the metadata for OneLogin SAML (the EM7 imlementation of SSO), enter the following URL in a browser:

```
https://hostname_or_ip_of_EM7_appliance/samlsp.em7?action=metadata
```

Using Your Own SSL Certificate

By default, SL1 uses a self-signed certificate generated by SL1 during installation from ISO. SL1 uses the default SSL certificate from nginx as the certificate for communication with the Identity Provider.

If you want to use your own certificate for communication between SL1 and the Identity Provider, perform the following:

1. Go to the console of the Administration Portal or start an SSH session to the Administration Portal.
2. Either generate a self-signed SSL certificate of type .pem and an SSL key or acquire these files from a certificate authority. Save the certificate files with names that will not conflict with the default files *silossl.pem* and *silossl.key*.
3. Copy the certificate files to the /etc/nginx directory.
4. Using vi or another text editor, edit the file /etc/nginx/conf.d/em7ngx_web_ui.conf
5. Edit the following lines:

```
ssl_certificate /etc/nginx/silossl.pem;
ssl_certificate_key /etc/nginx/silossl.key;
```

   - Replace silossl.pem with the .pem file for your new certificate.
   - Replace silossl.key with the .key file for your new certificate.

6. Save and quit the file.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

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

ScienceLogic

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

International: +1-703-354-1010