Using Active Directory and LDAP

ScienceLogic Version 8.6.0

Table of Contents

Introduction 3
What is LDAP? 3
What is Active Directory? 4
LDAP and Active Directory Terminology 4
How Can I use LDAP or Active Directory with SL1? 5
How Can I View My Company's Active Directory or LDAP? 6
Importing User Accounts from Active Directory or LDAP 7
Required Tasks 8
Creating a User Policy for Imported Users 10
Defining a Credential for Importing Users from Active Directory or LDAP 13
Creating an LDAP/AD Authentication Resource 15
Creating an Authentication Profile 23
Using Active Directory or LDAP for Authentication Only 27
Required Tasks 28
Creating a User Account that Will Be Authenticated with Active Directory or LDAP 29
Manually Creating a User Account and Manually Defining Account Settings 29
Manually Creating a User Account and Using a User Policy to Define Account Settings 32
Defining a Credential for Authenticating with Active Directory or LDAP 34
Creating an LDAP/AD Authentication Resource 36
Creating an Authentication Profile 40
Example of Importing User Accounts Using Active Directory 44
Required Tasks 45
Example Entry in Active Directory 46
Creating a User Policy 46
Creating a Credential for Active Directory 48
Creating an LDAP/AD Authentication Resource 50
Creating an Authentication Profile 54
User Login to SL1 57
Example of Only Authenticating User Accounts Using LDAP 59
Required Tasks 60
Example Entry in LDAP 61
Creating a User Account that Will Be Authenticated with Active Directory or LDAP 61
Defining a Credential for Authentication with LDAP 63
Creating an LDAP/AD Authentication Resource 65
Creating an Authentication Profile 67
User Login to SL1 71

Chapter 1

Introduction

Overview

This manual is intended for administrators who create and manage user accounts. This manual assumes that you are familiar with LDAP and/or Active Directory. If you are not familiar with LDAP or Active Directory, you will need to work with your LDAP or Active Directory 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 LDAP? 3
What is Active Directory? 4
LDAP and Active Directory Terminology 4
How Can I use LDAP or Active Directory with SL1? 5
How Can I View My Company's Active Directory or LDAP? 6

What is LDAP?

LDAP (Lightweight Directory Access Protocol) is an application protocol for directory services that runs over TCP/IP. An LDAP directory server provides system administrators with a centralized tool for authenticating users and managing user access on a network and the devices in the network.

What is Active Directory?

Active Directory is Microsoft's implementation of LDAP. Although Active Directory includes some platform-specific features that differ from a standard LDAP implementation, the terminology used in SL1 is also used by LDAP and Active Directory.

LDAP and Active Directory Terminology

A directory (either LDAP or Active Directory) is organized in a tree structure. To understand how directories work with SL1, you should understand the following terms:

- ***Entry***. A directory tree is made up of entries. Each entry can have a parent entry and multiple child entries. An entry is made up of attributes.
- ***Object Class***. All LDAP and AD entries in the directory have a type. That is, each entry belongs to one or more object classes that identify the type of data represented by the entry. The object class specifies the mandatory and optional attributes that can be associated with an entry of that class. The object classes for all objects in the directory form a class hierarchy. The classes "top" and "alias" are at the root of the hierarchy. For example, the "organizationalPerson" object class is a subclass of the "Person" object class, which in turn is a subclass of "top". When creating a new entry, you must always specify all of the object classes to which the new entry belongs.
- ***Attribute***. Each entry in the directory is made up of attributes. Each attribute is made up of an attribute name and one or more attribute values. For example, for the attribute "SN", the name of the attribute is "SN", short for surname. The value could be "Jones". The combination of SN and its value make up an attribute.
- ***Domain***. Usually the root of a directory tree. Each directory system includes at least one domain. The domain includes the directory server and its clients. Most directories use DNS names as domain names. For example, a directory could use the domain "acme.com".
- ***DC***. A domain is made up of DC (domain components). If a directory uses the domain "acme.com", the directory will have two DCs: "dc=acme, dc=com".
- ***DN***. Each entry is assigned a DN (distinguished name). The DN is a unique identifier for the entry. The DN includes an RDN (relative distinguished name) constructed from some attribute(s) in the entry, followed by the parent entry's DN. Think of the DN as a full filename and the RDN as a relative filename in a folder. An entry's DN might change over the lifetime of the entry. For example, an entry's DN might change when parent and child entries are moved within the directory tree.
- ***RDN***. The RDN (relative distinguished name) is a unique identifier for the entry. For a user, the RDN is frequently the user's full name. An RDN is made up of one or more attributes.
- ***OU***. An OU (organizational unit) allows you to create a hierarchical structure to your directory tree. Some common OUs are "ou=people" or "ou=devices". An OU is referenced with its full path, for example "ou=Users, ou=ScienceLogicHQ, DC=ScienceLogic, DC=local".
- ***Search Base***. A search base specifies the location in the directory from which to begin a search. Search base is specified with a DN.

- ***Bind***. In directory applications, a bind operation authenticates and allows access to the server where the directory resides.
- ***uid***. Attribute for user ID. This attribute can be used in SL1.
- ***CN***. Attribute for common name. This attribute is usually assigned a value that contains the user's first name and last name.

LDAP and Active Directory are binary protocols. However, you can use LDIF (LDAP data interface format) to view directory data. In LDIF, a directory entry for a user might look like this:

```
dn: cn=John Doe,dc=company,dc=com
cn: John Doe
givenName: John
sn: Doe
uid: jdoe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1234
mail: jdoe@company.com
street: 123 Commonwealth Avenue
l: Boston
st: Massachusetts
postalCode: 02134
manager: cn=Sally Smith,dc=company,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

- **dn** is the unique identifier for the entry. The combination of CN plus the root domain uniquely identifies this entry. Note that a dn is an identifier and not an attribute.
    - "**cn=John Doe**" is the entry's RDN (Relative Distinguished Name). The value of the CN attribute uniquely identifies this entry within its groups and domain.
    - "**dc=company,dc=com**" is the DN of the parent entry, where dc denotes Domain Component. So the parent entry for John Doe is the domain "company" within the domain "com".
- The remaining lines display the attributes for this entry. Attribute names are usually mnemonic strings, like "sn" for surname, "givenname" for first name, and "st" for state.

How Can I use LDAP or Active Directory with SL1?

Administrators can use LDAP or Active Directory to authenticate users. There are two ways to use LDAP or Active Directory authentication with SL1:

1. You can configure SL1 to ***automatically create user accounts in SL1*** for all existing LDAP or Active Directory users and then always use LDAP or Active Directory to authenticate those users when they log in to SL1.

- Each user logs in to SL1, either through the login page, a CAC card or certificate, or HTTP. The user logs in to SL1 using an LDAP or AD attribute value as a login name and the LDAP or AD password.
- SL1 examines the login request and applies the appropriate Authentication Profile (and the appropriate Authentication Resource).
- SL1 then authenticates the user by communicating with the LDAP or Active Directory server.
- SL1 then creates a ScienceLogic account for the user, using both the mappings defined in the Authentication Resource and a ScienceLogic user policy.
- SL1 displays the default page in SL1.

2. You can use LDAP or Active Directory to authenticate one or more users when they log in to SL1. You can also specify that SL1 won't authenticate other LDAP or Active Directory users.

    - Each user logs in to SL1, either through the login page, a CAC card or certificate, or HTTP. The user logs in to SL1 using an LDAP or AD attribute value as a login name and the LDAP or AD password.
    - SL1 examines the login request and applies the appropriate Authentication Profile (and the appropriate Authentication Resource(s)).
    - SL1 then authenticates the user by communicating with the LDAP or Active Directory server.

How Can I View My Company's Active Directory or LDAP?

Some of the steps in this manual require you to be familiar with the structure of your company's Active Directory implementation or LDAP implementation.

To view your company's Active Directory structure, talk to your Active Directory administrator, and try using a tool like ldp.exe.

- To download ldp.exe, go to http://technet.microsoft.com/en-us/library/cc772839(WS.10).aspx and follow the instructions.
- For information on using ldp.exe, see http://support.microsoft.com/kb/224543.

To view your company's LDAP structure, talk to your LDAP administrator, and try using a tool like phpLDAPAdmin.

- To download phpLDAPAdmin, go to http://phpldapadmin.sourceforge.net/wiki/index.php/Download.
- For information on using phpLDAPAdmin, see http://phpldapadmin.sourceforge.net/wiki/index.php/Main_Page.

Chapter 2

Importing User Accounts from Active Directory or LDAP

Overview

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

Each Active Directory or LDAP user logs in to SL1 using his or her Active Directory or LDAP username and password, and SL1 automatically creates an account for that user. Each subsequent time that user logs in to SL1, SL1 will use Active Directory or LDAP 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 8
Creating a User Policy for Imported Users 10
Defining a Credential for Importing Users from Active Directory or LDAP 13
Creating an LDAP/AD Authentication Resource 15
Creating an Authentication Profile 23

Required Tasks

To configure SL1 to automatically create accounts for existing LDAP or AD users, you must perform the following steps:

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

    - When creating the user policy, you must select *LDAP/Active Directory* in the ***Authentication Method*** field.
    - 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 these users require access to the same parts of SL1. You could define multiple user policies, each defining a unique sets 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 **LDAP/AD Auth Resource Editor** page (System > Settings > Authentication > Resources > create/edit LDAP/AD 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, based on an LDAP or AD attribute. For example, "department".

2. *Create an LDAP or AD credential* that allows SL1 to read from (and optionally, write to) the LDAP or AD directory.
3. *Define the LDAP/AD Authentication Resource*.

    - Specify how SL1 should communicate with the LDAP or Active Directory server and exchange information with the LDAP or Active Directory server.
    - Specify how SL1 should map LDAP or AD attribute values to fields in the **Account Properties** page.
    - Specify whether SL1 should remain synced with the LDAP/AD server. If an LDAP or AD administrator makes changes to an account, SL1 can automatically retrieve those updates and apply them to the user's account in SL1 (in the **Account Propertiess** 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 LDAP or AD will use a ***single user policy***.
        - *Dynamic policy alignment*. User accounts imported from LDAP or AD will use ***multiple user policies***.

- If you selected *Static policy alignment* in the ***Type*** field, then you must select a policy in the ***Policy*** field. All users who use the Authentication Resource will use this policy.
- If you selected *Dynamic policy alignment* in the ***Type*** field, then you must supply values in the ***Attribute***, ***Value***, and ***Policy*** fields.
    - In the ***Attribute*** field, specify the LDAP or AD) 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 one of the possible values for the LDAP or AD 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.
    - Click the plus-sign icon ( ) to add additional values and policies, as needed.
    - 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*.

4. *Define one or more Authentication Profiles* that tell SL1 how to recognize LDAP/AD users and which Authentication Resource to use with those users.
5. After completing these steps:
    - Each LDAP/AD user must log in to SL1 using the LDAP or AD user name and the LDAP or AD password.
    - 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 Authentication Resources to use to authenticate the user.
    - SL1 will use the settings and the credentials defined in the LDAP/AD Authentication Resource to query the LDAP or AD directory to authenticate each user.
    - Optionally, SL1 will use the mappings and the user policy specified in the LDAP/AD Authentication Resource to create each user account. The user name will match the ***Search Field*** in the LDAP/AD Authentication Resource.

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 Active Directory users or LDAP 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.

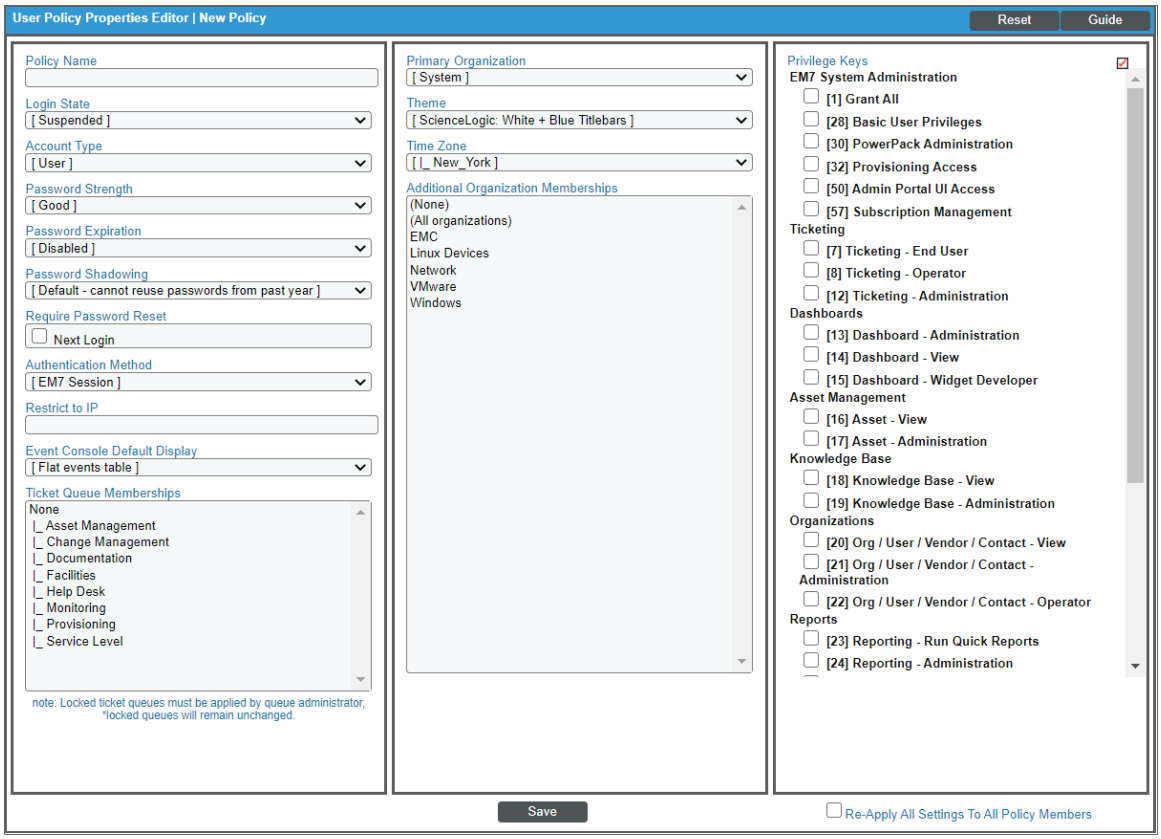
For example, suppose you want to import 100 user accounts from Active Directory. But suppose not all these users require access to the same parts of SL1. You could define multiple user policies, each defining a unique set of ticket queue memberships, organization membership, and Access Keys.

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 **LDAP/AD Auth Resource Editor** page (System > Settings > Authentication > Resources > create/edit LDAP/AD 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.



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 Active Directory or LDAP.

   - ***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).

- ***Password Strength***, ***Password Expiration***, ***Password Shadowing***, ***Require Password Reset***. These fields aren't used for LADAP/AD Authentication, so you can skip these fields.
- ***Authentication Method***. Select *LDAP/Active Directory*. The user's username and password will then be authenticated by the Active Directory server or the LDAP server.
- ***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.
- ***Event Console Default Display***. Specifies how the Event Console page will appear by default. Choices are:
  - *Flat events table*. Displays all events, grouped by severity. The filter-while-you-type fields and the advanced filter tool apply to the entire list of events. You can apply a single filter to events in multiple organizations.
  - *Group events table by organization*. Events will be grouped by organization in the Event Console page. The filter-while-you-type fields and the advanced filter tool will appear for each organization grouping and will act only on the events in that organization grouping. You will not be able to apply a single filter to events in multiple organizations.
- ***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.
- ***Re-Apply All settings to All Policy Members***. Because the ***Require Password Reset*** field is not used by LDAP/Ad Authentication, you can skip this field.

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 Active Directory or LDAP.

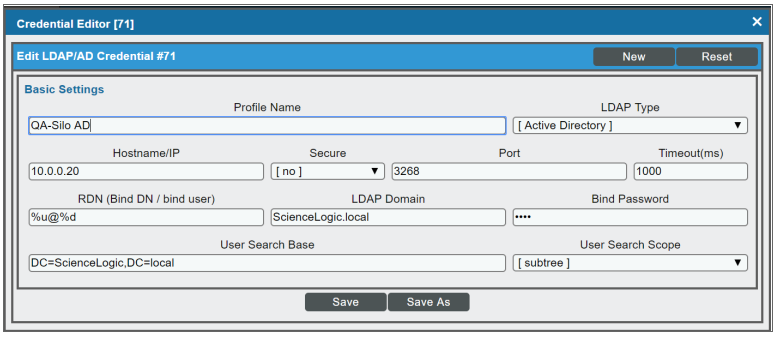
Defining a Credential for Importing Users from Active Directory or LDAP

Credentials are access profiles (username and password plus additional information) for external systems. These profiles allow SL1 to access external systems while maintaining the security of the access accounts. Users see only the name of the credential, not the username, password, and network information contained in the credential.

When you configure SL1 to automatically create user accounts for Active Directory users or LDAP users, you must define one or more credentials so SL1 can communicate with the Active Directory server or LDAP server. SL1 must communicate with the AD server or LDAP server, both to authenticate each user and to retrieve information about each user to include in each user's account.

To define a credential for accessing Active Directory or LDAP:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. In the **Credential Management** page, click the **[Actions]** drop-down menu. Select *Create LDAP/AD Credential*.
3. The **Credential Editor** modal page appears. In this page, you can define the new credential.



4. Supply a value in each of the following fields:

    - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters.
    - ***LDAP Type***. Specifies the type of LDAP implementation running on the directory server. Choices are *LDAP* or *Active Directory*.
    - ***Hostname/IP.*** Hostname or IP address of the LDAP or Active Directory server.
    - ***Secure***. Specifies whether you are using LDAP over SSL.
    - ***Port***. Port number on the LDAP or Active Directory server to which SL1 will send requests. If you specified *No* in the ***Secure*** field, the default value is *389*. If you specified *Yes* in the ***Secure*** field, the default value is *636*. However, you can specify a custom port used by your organization.
    - ***Timeout***. Number of milliseconds during which the credential should continue to try to contact the LDAP or Active Directory server. After this time elapses, the credential will stop trying to contact the LDAP or Active Directory server.
    - ***RDN (Bind DN / bind user)***. To configure SL1 to automatically create accounts when a user logs in with an AD name and password or LDAP name and password, ***you must include the %u variable in this field***.

        - If the LDAP or Active Directory structure ***does not*** contain all users ***in a single branch***, in this field, you must ***specify a Bind DN that is allowed to search the LDAP or Active Directory*** for the user who is logging in. You must also supply a password for this Bind DN in the ***Bind Password*** field. SL1 will use the specified Bind DN and password to search the entire LDAP or Active Directory structure for the user who is logging in. When SL1 finds the user who is logging in, it will perform a bind using that user's Bind DN and the password supplied during login.
        - If the LDAP or Active Directory structure contains all users in a single branch, you can use a variable for username and then explicitly specify the appropriate ou and dc. In many LDAP or AD configurations, each user has read-access to his/her own account. Therefore, you might find it most useful to include the %u variable in this field. When an LDAP or AD user logs in to SL1, SL1 stores the username in the %u variable. SL1 then uses the %u variable to build the bind DN, uses the bind DN to communicate with the LDAP or AD server, and then authenticates the current user.
        - An example entry in the RDN field might be: uid=%u, ou=People, dc=sciencelogic, dc=com
        - This creates a DN using the current ScienceLogic login name as the uid.
        - You can also include the %d variable in this field. The %d variable represents the name of the LDAP domain, as specified in the ***LDAP Domain*** field.

- ***Bind Password***. Password that allows access to the Active Directory server or the LDAP server. In most cases, when you specify a bind password in a credential, you are creating a "write" credential (that is, a credential that allows SL1 to make changes to the LDAP or AD server). Most Active Directory and LDAP configurations do not require a password for "read-only" access. To import information from the AD server or LDAP server and authenticate the imported user, SL1 requires only "read-only" access.
- ***LDAP Domain***. If your LDAP or Active Directory configuration includes multiple domains, specify the domain components to bind to in this field. For example, you could specify:

    dc=reston, dc=ScienceLogic, dc=local.

- This example would bind to the sub-domain "reston", in the domain "sciencelogic", in the domain "local".

- ***User Search Base***. Specify the area in the AD directory or LDAP directory where users to be authenticated and automatically added to SL1 reside, using RDN notation. The search base tells SL1 which part of the external directory tree to search. For example, if you want all users in the ou called "Users", in the parent ou called "ScienceLogicHQ", in the domain ScienceLogic.local to be automatically added to SL1, you could specify the RDN that includes those ous and that specific domain.

  ou=Users,ou=ScienceLogicHQ,dc=ScienceLogic, dc=local

  - This example would allow SL1 to authenticate users in the ou called "Users" in the parent ou "ScienceLogicHQ", and also authenticate all users in any ou underneath "Users".

NOTE: For details on search syntax for Active Directory, see http://msdn.microsoft.com/en-us/library/aa746475(VS.85).aspx. For details on the search syntax for LDAP, see http://www.faqs.org/rfcs/rfc2254.html.

- ***User Search Scope***. In this field, you specify whether SL1 should search only the directory specified in User Search Base or whether EM7 should search the directory specified in User Search Base and all its child branches.

  - *Subtree*. SL1 should search the directory specified in the ***User Search Base*** field and also search all its child branches.
  - *One Level*.SL1 should search only the directory specified in the ***User Search Base*** field.

5. Click the **[Save]** button to save your changes to the credential.

Creating an LDAP/AD Authentication Resource

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 LDAP or Active Directory user store. The **LDAP/AD Auth Resource Editor** page allows you to define an Authentication Resource for use with an LDAP/AD user store. An LDAP/AD Authentication Resource specifies the connector (communication software) to use to communicate with the LDAP/AD user store and the credential to use to connect to the user store. An LDAP/AD Authentication Resource can also map attributes from the user's LDAP/AD account to fields in the user account on SL1.

In the **LDAP/AD Auth Resource Editor** page (System > Settings > Authentication > Resources > create/edit LDAP/AD Resource), you can:

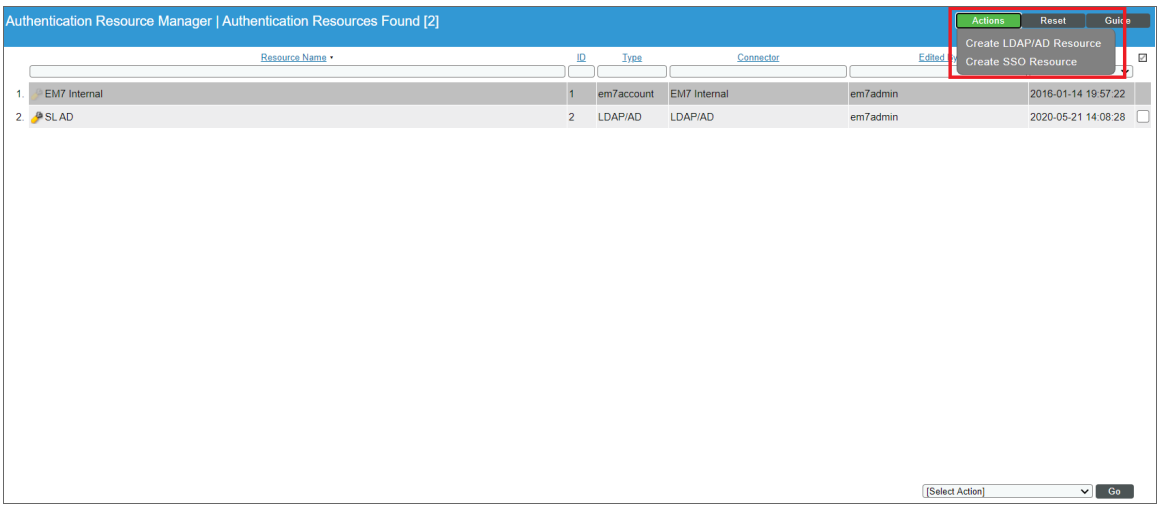
- Specify the credential that allows SL1 to communicate with the Active Directory server or the LDAP server.
- Specify the area in the Active Directory server or LDAP server that contains the users to be imported.
- Specify the user policy to use for each imported user account. You can use multiple user polices and map policies to user accounts (using AD attributes and LDAP attributes).

- Map the values from an Active Directory account or LDAP account to corresponding values in the new account.
- Specify whether SL1 should automatically update each user's account in SL1 when the corresponding account is edited in Active Directory or LDAP.
- Specify whether SL1 should automatically update each user's account in Active Directory or LDAP when the corresponding account is edited in SL1.

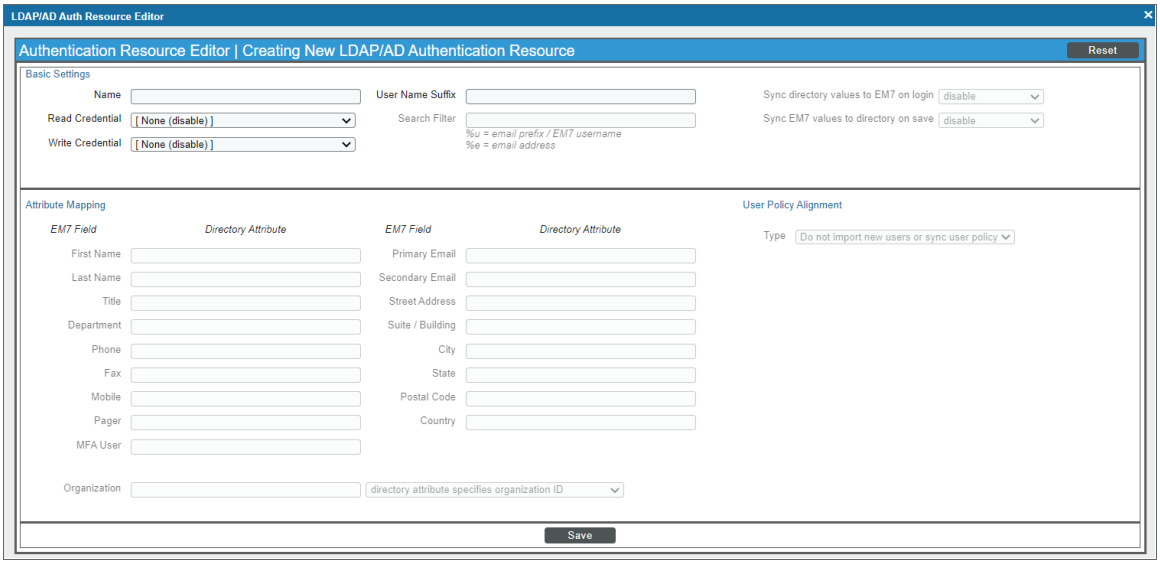
Additionally, ***Authentication Profiles*** are policies that align user accounts with one or more Authentication Resource. ***Authentication Profiles*** are described later in this chapter.

To create an LDAP/AD Authentication Resource:

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).



2. In the **Authentication Resource Manager** page, click the **[Actions]** menu and then select *Create LDAP/AD Resource*. The **LDAP/AD Auth Resource Editor** page appears.



3. Complete he following fields:

Basic Settings

- ***Name***. Name of the LDAP/AD Authentication Resource.
- ***Read Credential***. Credential that allows SL1 to read data from an LDAP or Active Directory server. Select from a list of all LDAP and Active Directory credentials to which you have access. If this field has been set to a credential to which you do not have access, this field will display the value *Restricted Credential*. If you set this field to a different credential, the entry for *Restricted Credential* will be removed from the field; you will not be able to re-align the field with the *Restricted Credential*.
- ***Write Credential***. Credential that allows SL1 to write data to an LDAP or Active Directory server. Select from a list of all LDAP and Active Directory credentials to which you have access. If this field has been set to a credential to which you do not have access, this field will display the value *Restricted Credential*. If you set this field to a different credential, the entry for *Restricted Credential* will be removed from the field; you will not be able to re-align the field with the *Restricted Credential*.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Read***

- ***User Name Suffix***. Optional field. Because SL1 can authenticate against multiple LDAP or Active Directory servers, there is a risk of collision among user names. In this field, you can enter a string to append to the user name in SL1, to minimize risk of collision. For example:
    - You can supply the value **%***attribute_name***%**, where *attribute_name* is an AD or LDAP attribute. SL1 will use the value of the attribute as the username.
    - You can enter one or more AD or LDAP attribute names, surrounded by percent signs (%), with text preceding it and/or text appended. SL1 will retrieve the value of the attribute and use that value plus any preceding text or appended text as the username.
    - You can enter a string, with no AD or LDAP attribute specified. When you don't specify an AD or LDAP attribute in this field, SL1 will retrieve the ***uid*** attribute and append the string you specify in this field. SL1 will then use the value in the the ***uid*** plus the appended string as the username.
    - Suppose we entered ***@ad.local*** in this field.

      Suppose the next LDAP/AD user logs into SL1 with the username ***bishopbrennan***.

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

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

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

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

NOTE: As a best practice, use email addresses as usernames to avoid collisions.

- ***Search Filter***. Specifies where to find the user's account information in LDAP or Active Directory. You must tell SL1 where to find the LDAP or AD attribute that maps to the user's account name in SL1.

  For example, an LDAP user might use his/her uid value to log in to SL1. In the user account in SL1, that uid value will then become the user's ***Account Login Name***.

  You can use the following variables in the search filter:

    - **[%u]**. Login name in SL1.
    - %e. Email address.
    - An example search filter for LDAP might be:

      ```
      (&(objectClass=person)(uid=%u))
      ```

      This says to search in the object class called "person" for the uid that matches the login name entered when the user logs in to SL1 and then stored in the variable %u.

- An example search filter for Active Directory might be:

  ```
  (samaccountname=%u)
  ```

  This says to search for the samaccountname attribute that matches the login name (entered when the user logs in to SL1 and then store in the variable %u).

- For more information on the syntax of LDAP and AD search filters, see RFC 4515.

- ***Sync directory values to EM7 on login***. If an LDAP or AD administrator makes changes to an LDAP or AD account, SL1 will 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.
- ***Sync EM7 values to directory on save***. If an administrator made changes to the user account in SL1, SL1 will automatically write those changes to the user's account in LDAP or Active Directory. ***This option requires a write credential***.

Attribute Mapping

If you have configured SL1 to automatically create accounts in SL1 for LDAP or AD users, these fields specify the LDAP or AD attribute value that will be automatically inserted into each field in each user's **Account Properties** page.

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 LDAP/AD attribute "sn" (surname) into the ***Last Name*** field in each user's **Account Properties** page (Registry > Devices > Device Manager.

NOTE: SL1 requires that the LDAP or AD attribute name that you specify in each field uses ***all lowercase characters***.

- ***First Name***. Specifies the LDAP or AD 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 LDAP/AD attribute "givenname" into this field.
- ***Last Name***. Specifies the LDAP or AD 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 LDAP/AD attribute "sn" into this field.
- ***Title***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Title*** field in each user's **Account Properties** page.
- ***Department***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Department*** field in each user's **Account Properties** page.
- ***Phone***. Specifies the LDAP or AD 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 LDAP/AD attribute "telephonenumber" into this field.
- ***Fax***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Fax*** field in each user's **Account Properties** page.

- ***Mobile***. Specifies the LDAP or AD 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 LDAP/AD attribute "mobile" into this field.
- ***Pager***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Pager*** field in each user's **Account Properties** page.
- ***MFA User***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***MFA User*** field in each user's Account Permissions page.

NOTE: For details on configuring multi-factor authentication, see the manual ***Using Multi-Factor Authentication***.

- ***Primary Email***. Specifies the LDAP or AD 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 LDAP/AD attribute "mail" into this field.
- ***Secondary Email***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Secondary Email*** field in each user's **Account Properties** page.
- ***Street Address***. Specifies the LDAP or AD 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 LDAP/AD attribute "streetaddress" into this field.
- ***Suite/Building***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Suite/Building*** field in each user's **Account Properties** page.
- ***City***. Specifies the LDAP or AD 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 LDAP/AD attribute "l" into this field.
- ***State***. Specifies the LDAP or AD 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 LDAP/AD attribute "st" into this field.
- ***Postal Code***. Specifies the LDAP or AD 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 LDAP/AD attribute "postalcode" into this field.
- ***Country***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Country*** field in each user's **Account Properties** page.
- ***Organization***. Specifies the LDAP or AD 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 LDAP/AD schema must include an attribute that maps to Organization names in SL1, Organization IDs in SL1, or Organization CRM IDs in SL1.

NOTE: When you create a new LDAP/AD 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 accounts in SL1 for each LDAP or Active Directory user in the search base (which is specified in the credential), whether SL1 should simply use LDAP or Active Directory to authenticate one or more users, or whether SL1 will refuse to authenticate specific users. Choices are:
  - *Do not authenticate new users from directory*. Only those users who have an account already created in SL1 can log in to SL1. However, if one or more users' ***Account Permissions page*** specifies *LDAP /Active Directory* in the ***Authentication Method*** field, SL1 will authenticate those users with either LDAP or Active Directory, using the settings and credentials specified in this page.
  - *Static policy alignment*. If an LDAP or AD user logs in to SL1 using the LDAP or AD attribute specified in the ***Search Filter*** field, SL1 will automatically create an account for that user. SL1 will use ***one user policy*** (specified in the ***Policy*** field) to create all imported LDAP or AD user accounts. SL1 will also use the settings and credentials specified in this page when creating the account.
  - *Dynamic policy alignment*. If an LDAP or AD user logs in to SL1 using the LDAP or AD attribute specified in the ***Search Filter*** field, SL1 will automatically create an account for that user. SL1 will ***choose from among multiple user policies*** to create imported LDAP or AD user accounts. 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 and credentials specified in this page when creating the account.

NOTE: If you have dynamic policy alignment configured, each time a user logs in using an account that is aligned with a user policy that uses LDAP/AD authentication, SL1 will perform the attribute match and reassign a user policy if the attribute has changed.

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

- ***Policy***. Specifies the user policy to use to automatically create an account in SL1 for each LDAP or AD user. Select from a list of all user policies that specify *LDAP /Active Directory* in the ***Authentication Method*** 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 LDAP or AD 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 LDAP or AD accounts for which you ***do not want to create an account in SL1***.
- In the ***Value*** field, specify one of the possible LDAP or AD attribute values (specified in the ***Attribute*** field). SL1 will compare the value in this field to the retrieved value for the ***Attribute***.
- In the corresponding ***Policy*** field, choose one of the following:
  - *Do Not Authenticate*. If the retrieved value of the specified ***Attribute*** matches the value in the ***Value*** field, SL1 **will not authenticate the user**. This setting applies to new users for whom LDAP or Active Directory would have to create a new account in SL1 and for users who already have an account in SL1.
  - *the policy you want to associate with that value*. Select from a list of all user policies that specify *LDAP /Active Directory* in the ***Authentication Method*** field.
  - 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".
  - 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.
  - You could also specify ***status*** in the ***Attribute*** field. Suppose that the ***status*** attribute could have two possible values: *active* or *terminated*.
  - 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 the green plus-sign icon ( ).

NOTE: If a user matches multiple ***Value*** entries, SL1 will find the first match and then stop searching. Therefore, it is important to define the ***Value***/***Policy*** field pairs in the order in which you want them applied to users.

4. Click the **[Save]** button to save your changes to the new Authentication Resource.

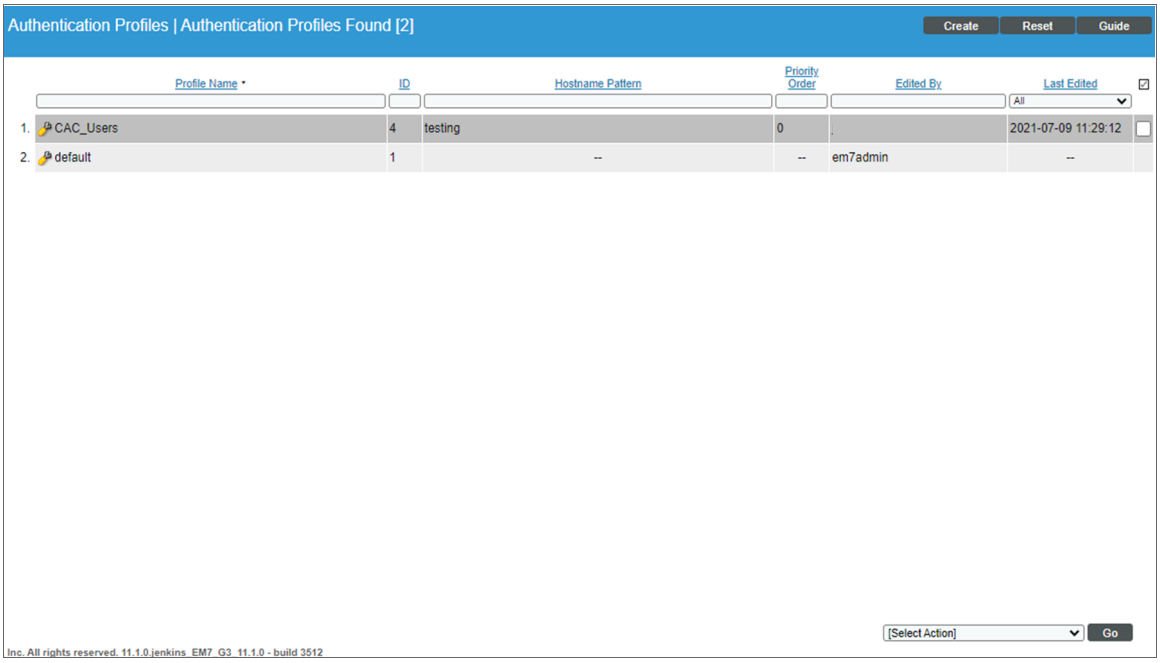
Creating an Authentication Profile

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

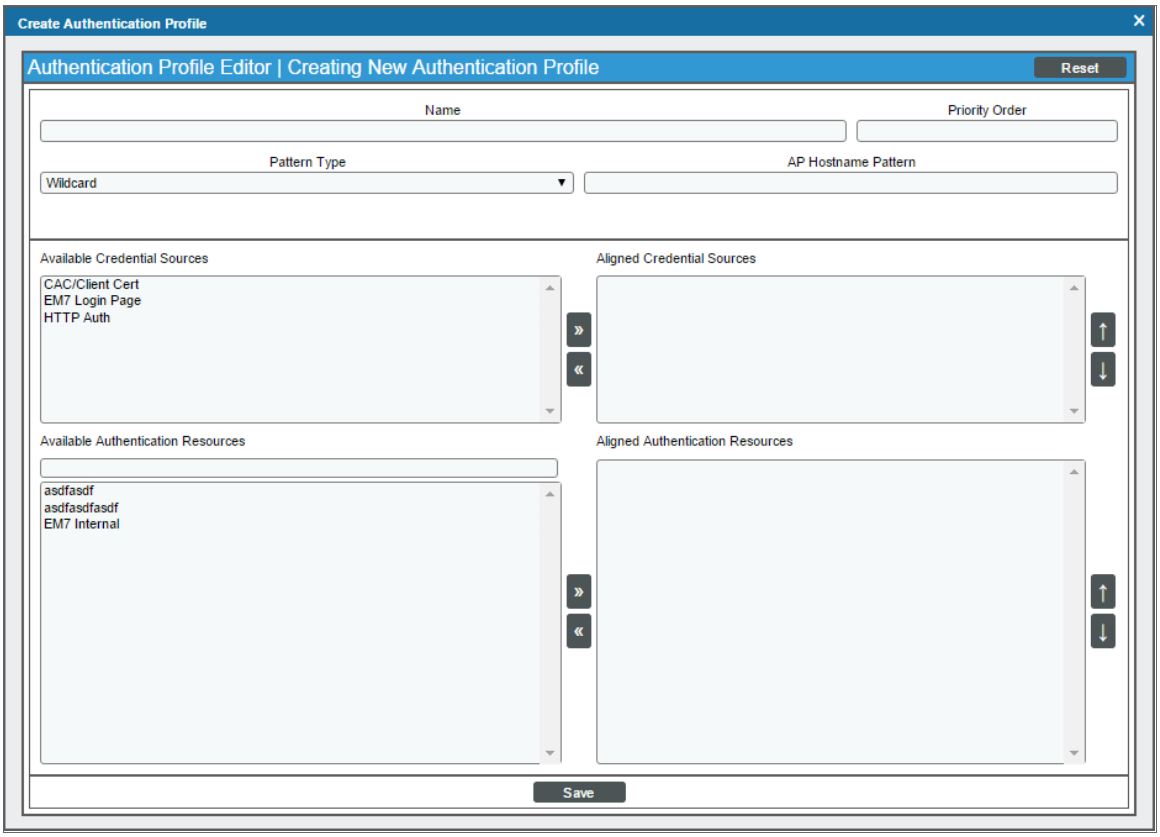
- ***Alignment by pattern matching***. SL1 uses the URL or IP address that a user enters in a browser to connect to an Administration Portal, Database Server, or All-In-One Appliance. If the URL or IP address matches the criteria specified in an authentication profile, SL1 will automatically use the 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, the credential to use to connect to the user store (if applicable), 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.
- ***Multi-factor Resource***. Specifies the connector to use to 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, and the URL of the RSA REST endpoint.

To create a new authentication profile:

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



2. Click the **[Create]** button. The **Authentication Profile Editor** modal appears.



3. 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 ascending priority order. 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 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:

    NOTE: For CAC authentication, align the CAC/Client Cert credential source. If this is your primary method of logging in to SL1, align CAC/Client Cert as the number one credential source. ScienceLogic recommends having EM7 Login Page aligned, as well, for administrator or maintenance access.

    - *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 ScienceLogic login page fields.
    - *HTTP Auth*. SL1 will retrieve a user name and password from the HTTP request.

    NOTE: If you are using Single Sign-On (SSO) authentication, the ***Available Credential Sources*** field is ignored. You do not have to align a credential source because credentials are submitted directly to an Identity Provider (IdP) instead of SL1.

    - ***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. You must select at least one authentication resource (but can select more than one). For details on creating an authentication resource, see the section on *Authentication Resources*.

- ***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.

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

Chapter 3

Using Active Directory or LDAP for Authentication Only

Overview

If you have already created accounts for users in SL1, you can use Active Directory or LDAP to authenticate one or more of those users. Each time an Active Directory or LDAP user logs in to SL1 using his/her Active Directory or LDAP username and password, SL1 will use Active Directory or LDAP 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 28
Creating a User Account that Will Be Authenticated with Active Directory or LDAP 29
Manually Creating a User Account and Manually Defining Account Settings 29
Manually Creating a User Account and Using a User Policy to Define Account Settings 32
Defining a Credential for Authenticating with Active Directory or LDAP 34
Creating an LDAP/AD Authentication Resource 36
Creating an Authentication Profile 40

Required Tasks

You can use LDAP or Active Directory to authenticate one or more users when they log in to SL1. You can also specify that SL1 should not authenticate other LDAP or Active Directory users.

- Each user logs in to SL1, either through the login page, a CAC card or certificate, or HTTP. The user logs in to SL1 using an LDAP or AD attribute value as a login name and the LDAP or AD password.
- SL1 examines the login request and applies the appropriate Authentication Profile (and the appropriate Authentication Resource(s)).
- SL1 then authenticates the user by communicating with the LDAP or Active Directory server.

If you want to use LDAP or Active Directory to only authenticate users (that is, you do not want SL1 to import user accounts from Active Directory or LDAP), you must manually create accounts in SL1 and specify LDAP or AD authentication. To do this:

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.

    - When creating the user policy, you must select *LDAP/Active Directory* in the ***Authentication Method*** field in the **User Policy Properties Editor** page (Registry > Accounts > User Policies > create/edit User Policy).
    - When creating the user account, you must specify select *LDAP/Active Directory* in the ***Authentication Method*** field in the **Account Permissions** page (Registry > Accounts > User Accounts > edit user account)

2. *Create an Active Directory or LDAP credential* that allows SL1 to read from (and optionally, write to) the AD or LDAP directory. This credential allows SL1 to connect to Active Directory or LDAP and authenticate user accounts.
3. *Define the LDAP/AD Authentication Resource*.

    - Specify how SL1 should communicate with the LDAP or Active Directory server and exchange information with the LDAP or Active Directory server.
    - In the ***Type*** field, select the following:

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

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

    - Each LDAP/AD user must log in to SL1 using the user name and password for SL1. This user name must be identical to the LDAP or AD user ID for the user; the password must be identical to the LDAP or AD password.

- 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 Authentication Resources to use to authenticate the user.
- SL1 will use the settings and the credentials defined in the LDAP/AD Authentication Resource to query the LDAP or AD directory to authenticate each user.

Creating a User Account that Will Be Authenticated with Active Directory or LDAP

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 Active Directory or LDAP, you can create a separate user account for that user in SL1 and then ask Active Directory or LDAP 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.

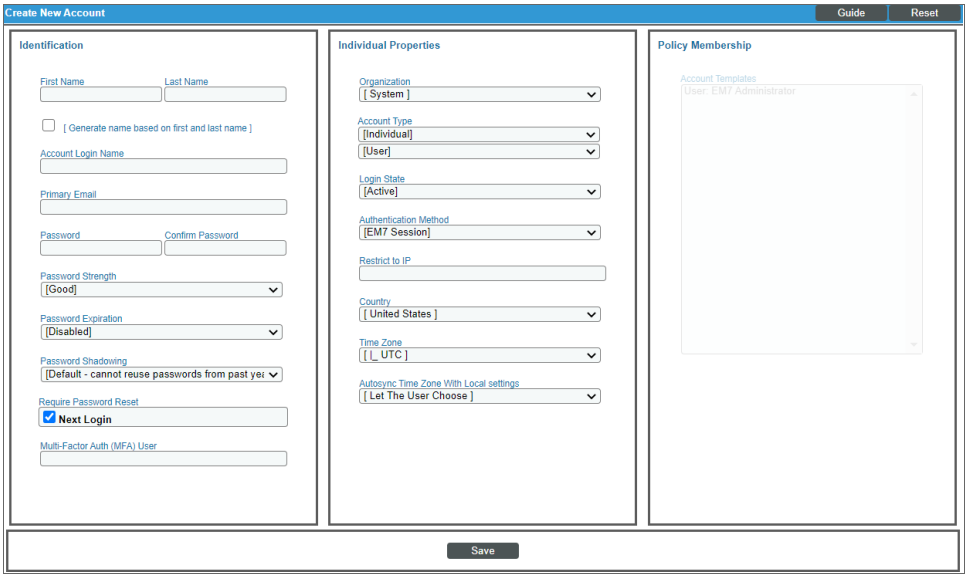
Both options will be described in the following sections.

Manually Creating a User Account and Manually Defining Account Settings

To manually create a new user account and manually define account settings:

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.



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*. **Enter a value that is included in the Active Directory entry or LDAP entry for the user.** For example, you could enter the uid value for the user from LDAP or AD. This value will then be the login name for the user. To enable AD or LDAP to authenticate the user, the login name must match a value in the AD or LDAP entry for the user.
   - ***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 passwordmust be at least four characters in length and can be up to 64 characters in length.

NOTE: During authentication, LDAP or AD will ignore the value in the ***Password*** field and instead use the password stored in LDAP or AD.

   - ***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 AD or LDAP 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**: 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*. **Select this option**.User account is not a member of a user policy.
  - *Policy Membership*. User will be defined with a user policy. When selected, the *Policy Membership* field becomes active.
- ***Account Type***. This drop-down 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).
- ***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 the following:
  - *LDAP/Active Directory*. **Select this option**. User's username and password are authenticated by an LDAP server or Active Directory server.
- ***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

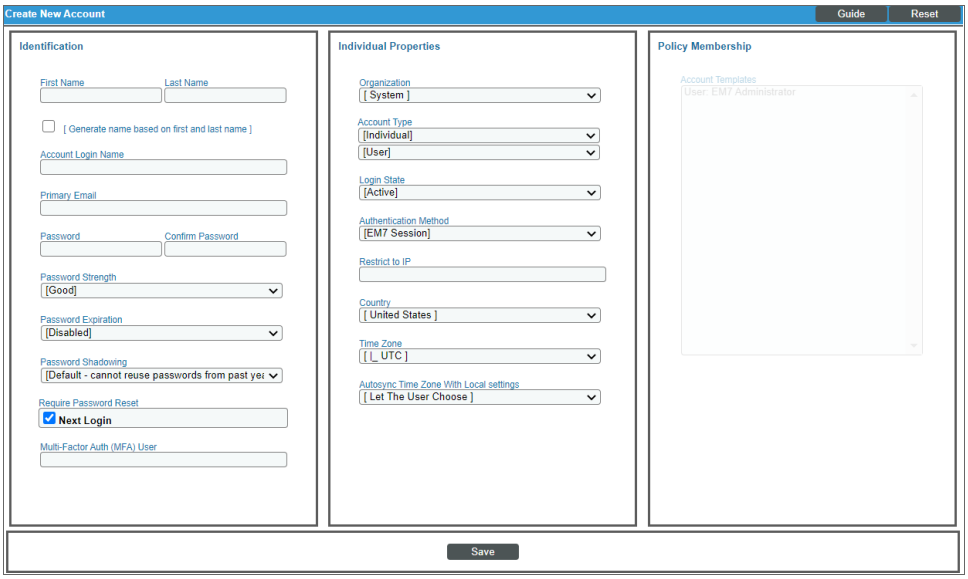
You can manually create a user account and then apply a user template to that user account.

If you want to use Active Directory or LDAP to authenticate the user when he/she logs in to SL1, you must:

- Define a user policy before creating the user account. With the exception of the ***Authentication Method*** field, there are no further requirements for LDAP or AD authentication. You can define the user policy as you wish. For details on creating a user policy, see the manual ***Organizations and Users***.
- Ensure that the user policy includes the following settings:
    - ***Authentication Method***. Specifies how the user's username and password will be authenticated. Select:
        - *LDAP/Active Directory*. **Select this option**. The user's username and password will be authenticated by an LDAP server or Active Directory server.

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.



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*. **Enter a value that is included in the Active Directory entry or LDAP entry for the user.** For example, you could enter the uid value for the user from LDAP or AD. This value will then be the login name for the user. To enable AD or LDAP to authenticate the user, the login name must match a value in the AD or LDAP entry for the user.
- ***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 passwordmust be at least four characters in length and can be up to 64 characters in length.

NOTE: During authentication, LDAP or AD will ignore the value in the ***Password*** field and instead use the password stored in LDAP or AD.

- ***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 AD or LDAP 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: 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.

NOTE: Ensure that you select a policy that specifies an ***Authentication Method*** of *LDAP/Active Directory*.

  - 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.

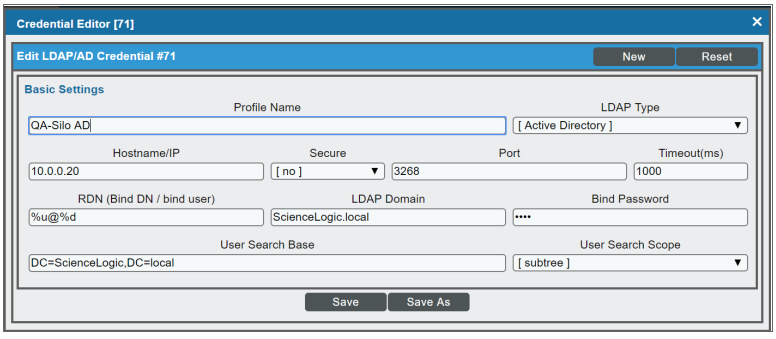
Defining a Credential for Authenticating with Active Directory or LDAP

Credentials are access profiles (username and password plus additional information) for external systems. These profiles allow SL1 to access external systems while maintaining the security of the access accounts. Users see only the name of the credential, not the username, password, and network information contained in the credential.

When you define user accounts that are authenticated with Active Directory or LDAP, you must define one or more credentials, so SL1 can communicate with the Active Directory server or LDAP server. SL1 must communicate with the AD server or LDAP server to authenticate each specified user.

To define a credential for accessing Active Directory or LDAP:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. In the **Credential Management** page, click the **[Actions]** drop-down menu. Select *Create LDAP/AD Credential*.
3. The **Credential Editor** modal page appears. In this page, you can define the new credential.



4. Supply a value in each of the following fields:

    - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters.
    - ***LDAP Type***. Specifies the type of LDAP implementation running on the directory server. Choices are *LDAP* or *Active Directory*.
    - ***Hostname/IP***. Hostname or IP address of the LDAP or Active Directory server.
    - ***Secure***. Specifies whether you are using LDAP over SSL.
    - ***Port***. Port number on the LDAP or Active Directory server to which SL1 will send requests. If you specified *No* in the ***Secure*** field, the default value is *389*. If you specified *Yes* in the ***Secure*** field, the default value is *636*. However, you can specify a custom port used by your organization.
    - ***Timeout***. Number of milliseconds during which the credential should continue to try to contact the LDAP or Active Directory server. After this time elapses, the credential will stop trying to contact the LDAP or Active Directory server.
    - ***RDN (Bind DN / bind user)***. To configure SL1 to automatically create accounts when a user logs in with an AD name and password or LDAP name and password, ***you must include the %u variable in this field***.

        - If the LDAP or Active Directory structure ***does not*** contain all users ***in a single branch***, in this field, you must ***specify a Bind DN that is allowed to search the LDAP or Active Directory*** for the user who is logging in. You must also supply a password for this Bind DN in the ***Bind Password*** field. SL1 will use the specified Bind DN and password to search the entire LDAP or Active Directory structure for the user who is logging in. When SL1 finds the user who is logging in, it will perform a bind using that user's Bind DN and the password supplied during login.
        - If the LDAP or Active Directory structure contains all users in a single branch, you can use a variable for username and then explicitly specify the appropriate ou and dc. In many LDAP or AD configurations, each user has read-access to his/her own account. Therefore, you might find it most useful to include the %u variable in this field. When an LDAP or AD user logs in to SL1, SL1 stores the username in the %u variable. SL1 then uses the %u variable to build the bind DN, uses the bind DN to communicate with the LDAP or AD server, and then authenticates the current user.
        - An example entry in the RDN field might be: uid=%u, ou=People, dc=sciencelogic, dc=com
        - This creates a DN using the current ScienceLogic login name as the uid.
        - You can also include the %d variable in this field. The %d variable represents the name of the LDAP domain, as specified in the ***LDAP Domain*** field.

- ***Bind Password***. Password that allows access to the Active Directory server or the LDAP server. In most cases, when you specify a bind password in a credential, you are creating a "write" credential (that is, a credential that allows SL1 to make changes to the LDAP or AD server). Most Active Directory and LDAP configurations do not require a password for "read-only" access. To import information from the AD server or LDAP server and authenticate the imported user, SL1 requires only "read-only" access.
- ***LDAP Domain***. If your LDAP or Active Directory configuration includes multiple domains, specify the domain components to bind to in this field. For example, you could specify:

    dc=reston, dc=ScienceLogic, dc=local.

- This example would bind to the sub-domain "reston", in the domain "sciencelogic", in the domain "local".

- ***User Search Base***. Specify the area in the AD directory or LDAP directory where users to be authenticated and automatically added to SL1 reside, using RDN notation. The search base tells SL1 which part of the external directory tree to search. For example, if you want all users in the ou called "Users", in the parent ou called "ScienceLogicHQ", in the domain ScienceLogic.local to be automatically added to SL1, you could specify the RDN that includes those ous and that specific domain.

  ou=Users,ou=ScienceLogicHQ,dc=ScienceLogic, dc=local

  - This example would allow SL1 to authenticate users in the ou called "Users" in the parent ou "ScienceLogicHQ", and also authenticate all users in any ou underneath "Users".

NOTE: For details on search syntax for Active Directory, see http://msdn.microsoft.com/en-us/library/aa746475(VS.85).aspx. For details on the search syntax for LDAP, see http://www.faqs.org/rfcs/rfc2254.html.

- ***User Search Scope***. In this field, you specify whether SL1 should search only the directory specified in User Search Base or whether EM7 should search the directory specified in User Search Base and all its child branches.

  - *Subtree*. SL1 should search the directory specified in the ***User Search Base*** field and also search all its child branches.
  - *One Level*.SL1 should search only the directory specified in the ***User Search Base*** field.

5. Click the **[Save]** button to save your changes to the credential.

Creating an LDAP/AD Authentication Resource

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 LDAP or Active Directory (AD) user store. The **LDAP/AD Auth Resource Editor** page allows you to define an Authentication Resource for use with an LDAP/AD user store. An LDAP/AD Authentication Resource specifies the connector (communication software) to use to communicate with the LDAP/AD user store and the credential to use to connect to the user store. An LDAP/AD Authentication Resource can also map attributes from the user's LDAP/AD account to fields in the user account on SL1.

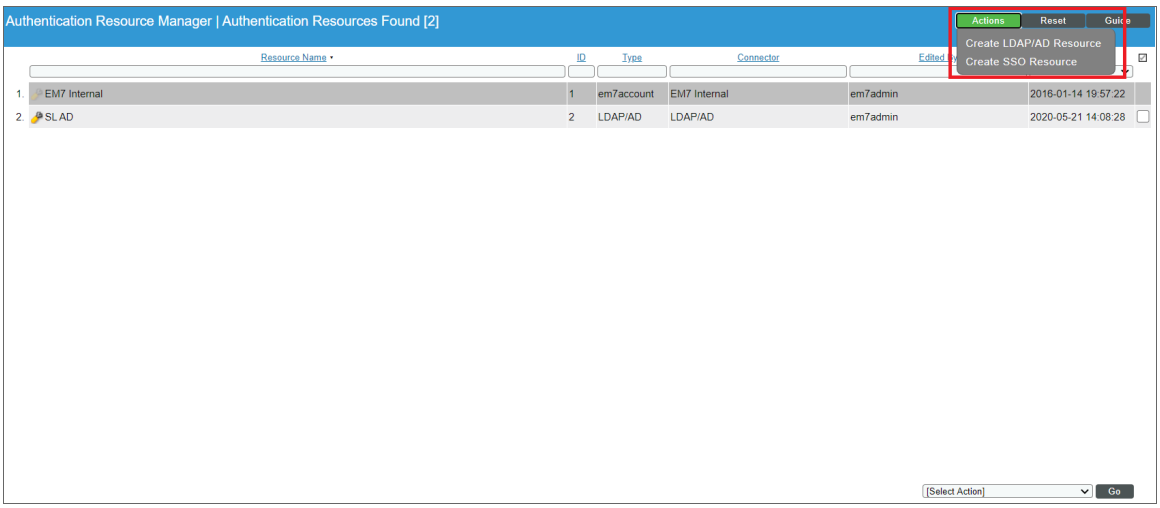
In the In the **LDAP/AD Auth Resource Editor** page (System > Settings > Authentication > Resources > create/edit LDAP/AD Resource), you can:

- Specify the credential that allows SL1 to communicate with the AD server or the LDAP server.
- Specify the area in the AD server or LDAP server where the user's records reside.
- Specify whether SL1 should automatically update each user's account in AD or LDAP when the corresponding account is edited in SL1.

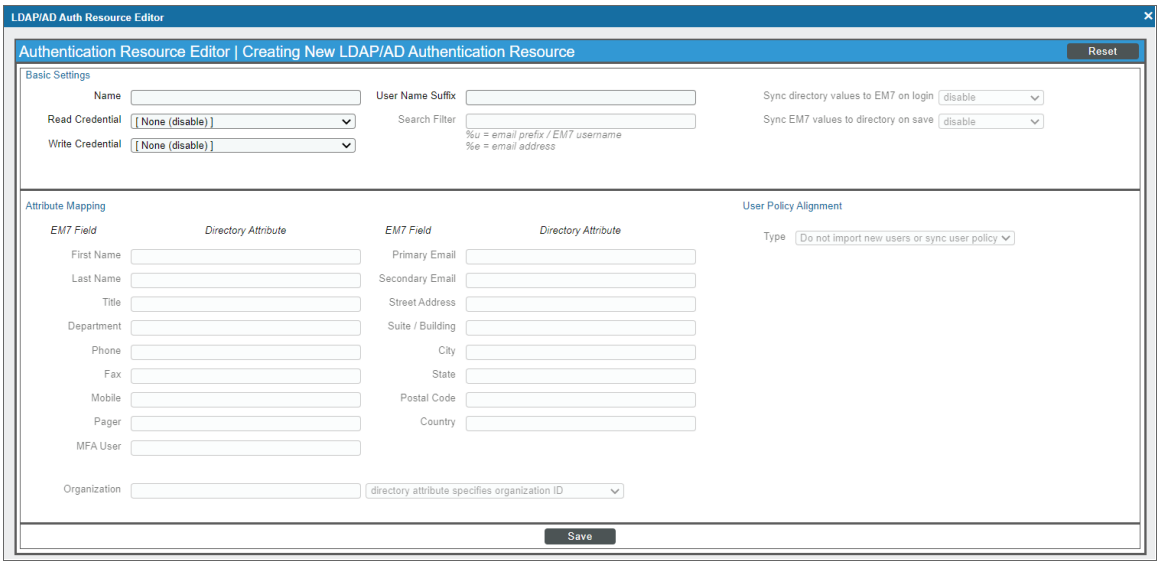
Additionally, ***Authentication Profiles*** are policies that align user accounts with one or more Authentication Resource. ***Authentication Profiles*** are described later in this chapter.

To create an LDAP/AD Authentication Resource:

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources)



2. In the **Authentication Resource Manager** page, click the **[Actions]** menu and then select *Create LDAP/AD Resource*. The **LDAP/AD Auth Resource Editor** page appears.



3. Complete the following fields:

Basic Settings

- ***Name***. Name of the LDAP/AD Authentication Resource.

- ***Read Credential***. Credential that allows SL1 to read data from an LDAP or AD server. Select from a list of all LDAP and AD credentials to which you have access. If this field has been set to a credential to which you do not have access, this field will display the value *Restricted Credential*. If you set this field to a different credential, the entry for *Restricted Credential* will be removed from the field; you will not be able to re-align the field with the *Restricted Credential*.
- ***Write Credential***. Credential that allows SL1 to write data to an LDAP or AD server. Select from a list of all LDAP and AD credentials to which you have access. If this field has been set to a credential to which you do not have access, this field will display the value *Restricted Credential*. If you set this field to a different credential, the entry for *Restricted Credential* will be removed from the field; you will not be able to re-align the field with the *Restricted Credential*.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Read Credential*** field and the ***Write Credential*** field.

- ***User Name Suffix***. Optional field. Because SL1 can authenticate against multiple LDAP or AD servers, there is a risk of collision among usernames. In this field, you can enter a string to append to the username in SL1, to minimize risk of collision. For example:
  - You can supply the value **%***attribute_name***%**, where *attribute_name* is an AD or LDAP attribute. SL1 will use the value of the attribute as the username.
  - You can enter one or more AD or LDAP attribute names, surrounded by percent signs (%), with text preceding it and/or text appended. SL1 will retrieve the value of the attribute and use that value plus any preceding text or appended text as the username.
  - You can enter a string, with no AD or LDAP attribute specified. When you don't specify an AD or LDAP attribute in this field, SL1 will retrieve the ***uid*** attribute and append the string you specify in this field. SL1 will then use the value in the the ***uid*** plus the appended string as the username.
  - Suppose we entered ***@ad.local*** in this field.

    Suppose the next LDAP/AD user logs into SL1 with the username ***bishopbrennan***.

    SL1 will log in that user as ***bishopbrennan@ad.local***.
  - Suppose we entered ***%sn%-external*** in this field.

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

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

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

- ***Search Filter***. Specifies where to find the user's account information in LDAP or AD. You must tell SL1 where to find the LDAP or AD attribute that maps to the user's account name in SL1.

For example, an LDAP user might use his/her uid value to log in to SL1. In the user account in SL1, that uid value will then become the user's ***Account Login Name***.

You can use the following variables in the search filter:

- **[%u]**. Login name in SL1.
- %e. Email address.
- An example search filter for LDAP might be:

```
(&(objectClass=person)(uid=%u))
```

This says to search in the object class called "person" for the uid that matches the login name entered when the user logs in to SL1 and then stored in the variable %u.

- An example search filter for AD might be:

```
(samaccountname=%u)
```

This says to search for the samaccountname attribute that matches the login name (entered when the user logs in to SL1 and then store in the variable %u).

- For more information on the syntax of LDAP and AD search filters, see RFC 4515.

- ***Sync directory values to EM7 on login***. Select *Disable*. This feature is used to automatically update accounts in the SL1 .
- ***Sync EM7 values to directory on save***. If an administrator made changes to the user account in SL1, SL1 will automatically write those changes to the user's account in LDAP or AD. ***This option requires a write credential***.

Attribute Mapping

Define these settings only if you have configured SL1 to automatically create accounts in SL1 for LDAP or AD users.

User Policy Alignment

- ***Type***. Specifies whether SL1 should automatically create accounts in SL1 for each LDAP or AD user in the search base (which is specified in the credential), whether SL1 should simply use LDAP or AD to authenticate one or more users, or whether SL1 will refuse to authenticate specific users. If you are using LDAP or AD to authenticate user but not automatically create new user accounts in SL1, your choices are:

  - *Do not authenticate new users from directory*. Only those users who have an account already created in SL1 can log in to SL1. However, if one or more users' ***Account Permissions page*** specifies *LDAP /Active Directory* in the ***Authentication Method*** field, SL1 will authenticate those users with either LDAP or AD, using the settings and credentials specified in this page.

4. Click the **[Save]** button to save your changes to the new Authentication Resource.

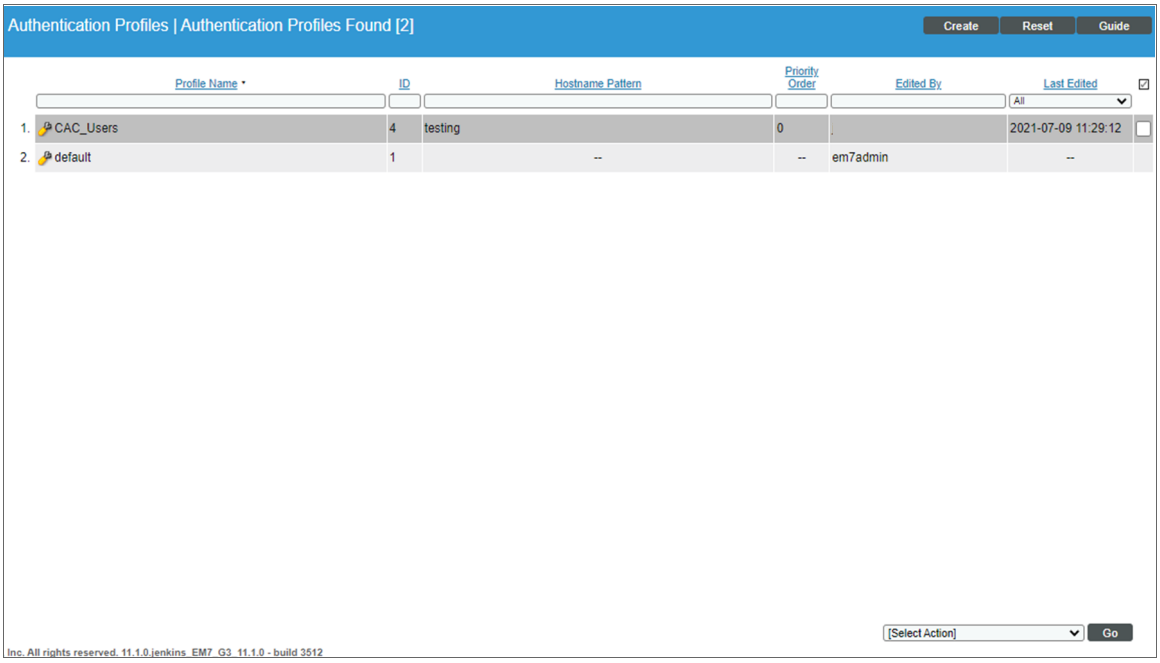
Creating an Authentication Profile

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

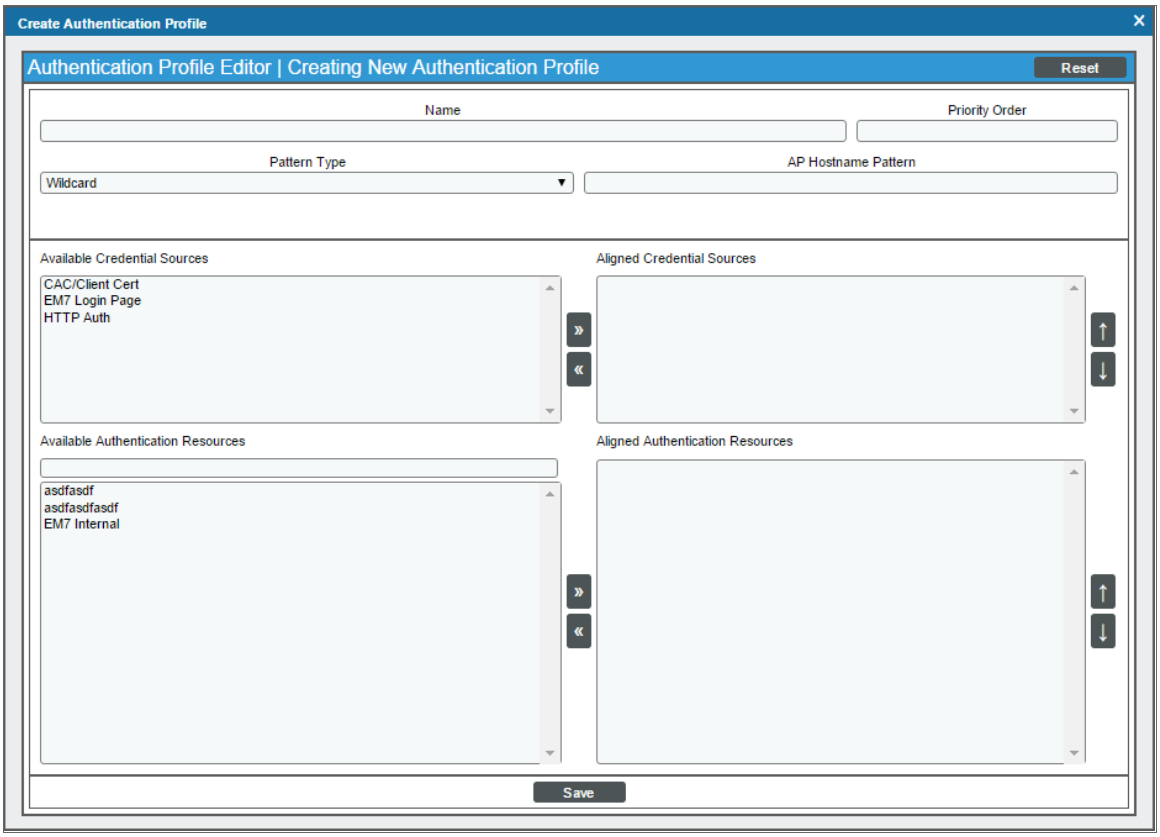
- ***Alignment by pattern matching***. SL1 uses the URL or IP address that a user enters in a browser to connect to an Administration Portal, Database Server, or All-In-One Appliance. If the URL or IP address matches the criteria specified in an authentication profile, SL1 will automatically use the 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, the credential to use to connect to the user store (if applicable), 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.
- ***Multi-factor Resource***. Specifies the connector to use to 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, and the URL of the RSA REST endpoint.

To create a new authentication profile:

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



2. Click the **[Create]** button. The **Authentication Profile Editor** modal appears.



3. 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 ascending priority order. 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 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:

> **NOTE:** For CAC authentication, align the CAC/Client Cert credential source. If this is your primary method of logging in to SL1, align CAC/Client Cert as the number one credential source. ScienceLogic recommends having EM7 Login Page aligned, as well, for administrator or maintenance access.

    - *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 ScienceLogic login page fields.
    - *HTTP Auth*. SL1 will retrieve a user name and password from the HTTP request.

> **NOTE:** If you are using Single Sign-On (SSO) authentication, the ***Available Credential Sources*** field is ignored. You do not have to align a credential source because credentials are submitted directly to an Identity Provider (IdP) instead of SL1.

- ***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. You must select at least one authentication resource (but can select more than one). For details on creating an authentication resource, see the section on *Authentication Resources*.

- ***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.

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

Example

1

Example of Importing User Accounts Using Active Directory

Overview

This chapter will walk you through an example of importing a user account from Active Directory. Although this chapter will illustrate the steps and concepts for this task, the values are specific to the example Active Directory server and will not work on your Active Directory system.

Although some of the values in this example are specific to Active Directory, you can use a very similar example to import user accounts from LDAP.

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 *45*

Example Entry in Active Directory *46*

Creating a User Policy *46*

Creating a Credential for Active Directory *48*

Creating an LDAP/AD Authentication Resource *50*

Creating an Authentication Profile *54*

User Login to SL1 ..... *57*

Required Tasks

To configure SL1 to automatically create accounts for existing LDAP or AD users, you must perform the following steps:

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

    - When creating the user policy, you must select *LDAP/Active Directory* in the ***Authentication Method*** field.
    - You can create more than one user policy for imported user accounts.
    - Later, in the **LDAP/AD Auth Resource Editor** page (System > Settings > Authentication > Resources > create/edit LDAP/AD Resource), you specify the user policy to apply to imported user accounts.

2. *Create an LDAP or AD credential* that allows SL1 to read from (and optionally, write to) the LDAP or AD directory.

3. *Define the LDAP/AD Authentication Resource*.

    - Specify how SL1 should communicate and exchange information with the LDAP or Active Directory server.
    - Specify how SL1 should map LDAP or AD attribute values to fields in the **Account Properties** page.
    - Specify whether SL1 should remain synced with the LDAP/AD server. If an LDAP or AD administrator makes changes to an 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.

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

    - Each LDAP/AD user must log in to SL1 using the LDAP or AD username and the LDAP or AD password.
    - 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 Authentication Resources to use to authenticate the user.
    - SL1 will use the settings and the credentials defined in the LDAP/AD Authentication Resource to query the LDAP or AD directory to authenticate each user.
    - Optionally, SL1 will use the mappings and the user policy specified in the LDAP/AD Authentication Resource to create each user account. The username will match the ***Search Field*** in the LDAP/AD Authentication Resource.

Example Entry in Active Directory

Suppose we have an entry in Active Directory that looks like this:

NOTE: For details on how the attribute names map to the page displays in Active Directory, see the appropriate Active Directory documentation.

```
# kgibson, Users, ScienceLogicHQ, sciencelogic.local
dn: samaccountname=kgibson,ou=Users,ou=ScienceLogicHQ,dc=sciencelogic,dc=local
samaccountname: kgibson
cn: Kate Gibson
userPassword:: ilovedocs!
department: documentation
streetaddress: 12369 Sunrise Valley Drive
l: Reston
st: VA
c: US
postalCode: 20191
mail: kgibson@sciencelogic.com
telephoneNumber: 703-354-1010
facsimiletelphonenumber: 571-336-8000
mobile: 703-354-1011
pager: 703-354-1111
givenName: Kate
sn: Gibson
```

In this entry, we have a user named "kgibson", who resides in the ou called "Users", in the ou called "ScienceLogicHQ" in the domain "sciencelogic.local". We'll use this information when configuring SL1 to authenticate this user.

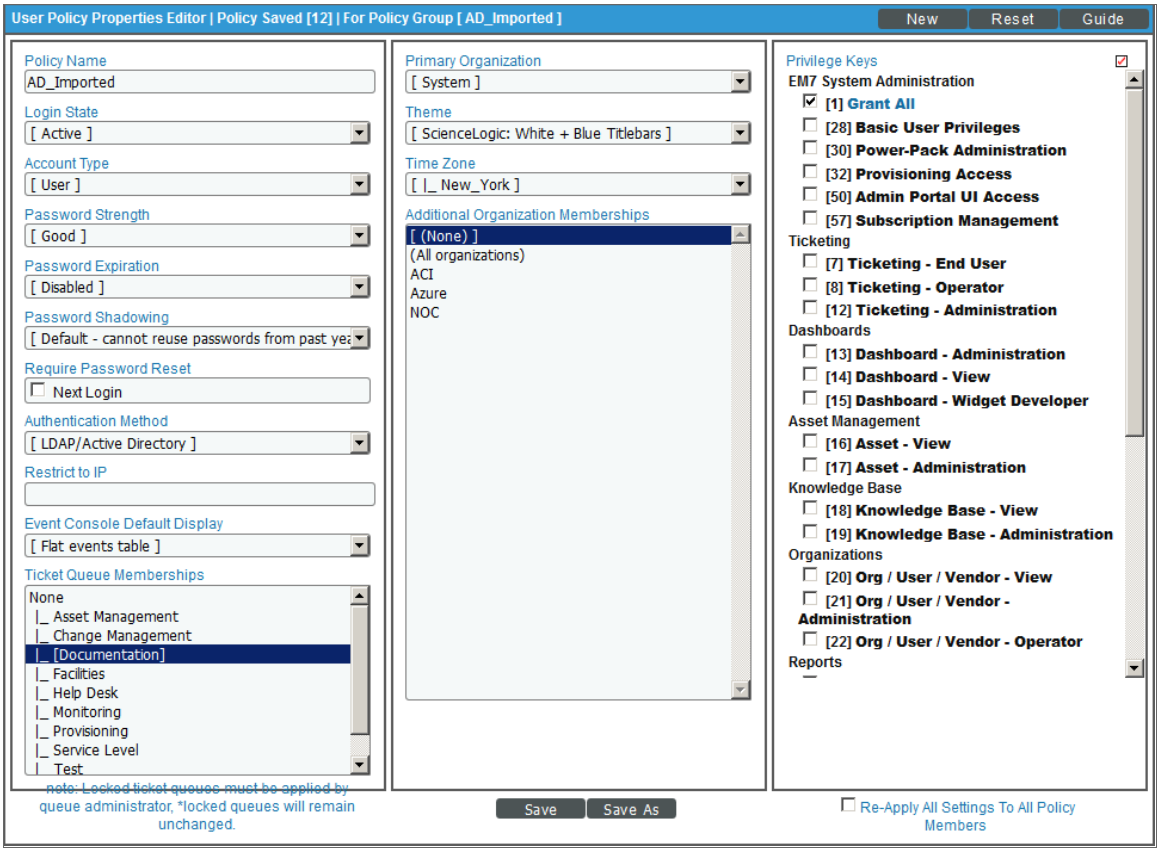
Creating a User Policy

When you configure SL1 to automatically create user accounts for Active Directory users or LDAP 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.

For our example, we performed the following:

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

2. Click the **[Create]** button. The **User Policy Properties Editor** page appears.



3. In the **User Policy Properties Editor** page, we supplied the following values:

   - ***Policy Name***. Name of the user policy. Can be any combination of alphanumeric characters, up to 64 characters in length. We entered ***AD_Imported***.
   - ***Login State***. Specifies whether user accounts created with the policy can log in to SL1. We selected **Active**. This means that as soon as the policy creates an account, the account user can log in to SL1.
   - ***Account Type***. This drop-down contains an entry for each standard account type. These account types affect the list of Access Keys for the user. We selected *User*.

     - *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).

   - ***Password Strength***, ***Password Expiration***, ***Password Shadowing***, ***Require Password Reset***. These fields aren't used for LADAP/AD Authentication, so you can skip these fields.
   - ***Password Strength***. We selected *Good*. The user's password must have a strength of *Good* to be authenticated.
   - ***Password Expiration***. We selected *60 days*. After 60 days the user will be forced to change their password.

- ***Password Shadowing***. We selected *Default*. The user will not be able to reuse any password from the past year.
- ***Require Password Reset***. We did not select this checkbox. The user will not have to reset their password at their next login.
- ***Authentication Method***. We selected *LDAP/Active Directory*. **This selection is required**. The user's username and password will then be authenticated by the Active Directory server or the LDAP server.
- ***Restrict to IP***. We left this field **blank**. If selected, the user will be allowed to access SL1 only from the specified IP. Specify the IP address in standard dotted-decimal notation.
- ***Event Console Default Display***. Specifies how the **Event Console** page will appear by default. We chose *Flat events table*.
- ***Ticket Queue Memberships***. We highlighted the ticket queues specifying which users will be members. In our example, this is *Documentation*.
- ***Primary Organization***. Specifies the primary organization. We selected *System*. 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. We selected *ScienceLogic: White + Blue Titlebars*.
- ***Time Zone***. The time zone to associate with each user account created with this user policy. We selected *New_York*. Dates and times in SL1 will be displayed for the selected time zone.
- ***Organization Memberships***. User accounts created with this user policy will be members of each selected organization. **We did not select any additional organizations**.
- ***Privilege Keys***. The **Privilege Keys** pane displays a list of Access Keys that can be assigned to the user's account. We selected *Grant All*. This means the user can access all parts of SL1 (but cannot create or edit additional Access Keys).
- ***Re-Apply All Settings to All Policy Members***. We left this field unchecked.

4. Click the **[Save]** button to save your new user policy.

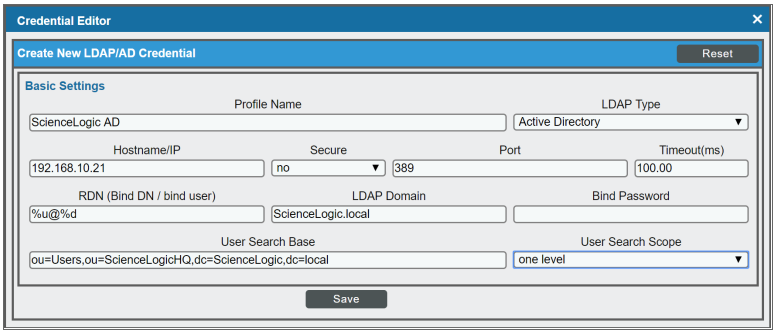
Creating a Credential for Active Directory

When you configure SL1 to automatically create user accounts for Active Directory users, you must define one or more credentials, so SL1 can communicate with the Active Directory server. SL1 must communicate with the AD server, both to authenticate each user and to retrieve information about each user to include in each user's user account.

For our example, we performed the following:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** menu, then select *LDAP/AD Credential*.

3. The **Credential Editor** modal page appears. In this page, you can define the new credential.



4. Supply a value in each of the following fields:
   - ***Profile Name***. Name of the credential. We specified *ScienceLogic AD*.
   - ***LDAP Type***. Specifies the type of LDAP implementation running on the directory server. We selected *Active Directory*.
   - ***Hostname/IP.*** Hostname or IP address of the Active Directory server. We supplied the IP address of the Active Directory server (**192.168.10.21**).
   - ***Secure***. Specifies whether you are using the "LDAP over SSL" protocol. We selected *No*.
   - ***Port.*** Port number on the LDAP or Active Directory server to which SL1 will send requests. We accepted the default port value (**389**).
   - ***Timeout***. We accepted the default value of *10000*.
   - ***RDN (Bind DN / bind user)***. This field specifies the ***bind DN***. The bind DN is an account on the Active Directory server or the LDAP server that is allowed to search the directory within the specified search base. We entered:

     %u@%d

     This says that the bind DN "kgibson@ScienceLogic.local" will allow SL1 to authenticate the user and retrieve information about that user.

     - In SL1, the %u variable stores the latest username from the login page.
     - In SL1, the %d variable stores the value specified in the field ***LDAP Domain***.
     - To configure SL1 to automatically create accounts when a user logs in with an AD name and password, ***you must include the %u variable in this field***.
     - When an AD user logs in to SL1, SL1 stores the username in the %u variable. SL1 then uses the %u variable to build the bind DN, uses the bind DN to communicate with the AD server, and then asks the AD server to authenticate the current user.

   - ***LDAP Domain***. If your LDAP or Active Directory configuration includes multiple domains, specify the domain components to bind to in this field. We entered *ScienceLogic.local*.

- ***Bind Password***. Password that allows access to the Active Directory server or the LDAP server. In most cases, when you specify a bind password in a credential, you are creating a "write" credential (that is, a credential that allows SL1 to make changes to the LDAP or AD server). We left this field **blank**.
- ***User Search Base***. Specify where in the AD directory to find the user accounts to import, using RDN notation. The search base tells SL1 which part of the external directory tree to search. We entered:

  ou=Users,ou=ScienceLogicHQ,dc=ScienceLogic,dc=local

  This specifies that SL1 can import any Active Directory account in the ou "Users", in the parent ou "ScienceLogicHQ", in the domain "ScienceLogic.local". Any users in any ou that is a child to the ou "Users" will also be imported.

NOTE: For details on search syntax for Active Directory, see http://msdn.microsoft.com/en-us/library/aa746475(VS.85).aspx. For details on the search syntax for LDAP, see http://www.faqs.org/rfcs/rfc2254.html.

- ***User Search Scope***. Specify whether SL1 should search only the directory specified in the ***User Search Base*** field or whether SL1 should search the directory specified in the ***User Search Base***field and all its child branches. We selected *One Level*.

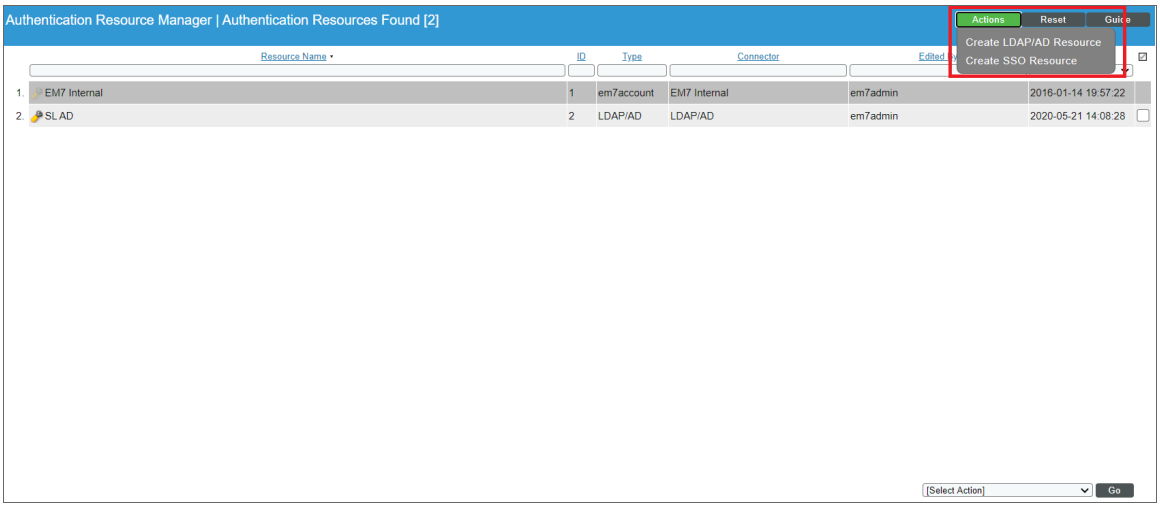
5. Click the **[Save]** button to save your changes to the credential.

Creating an LDAP/AD Authentication Resource

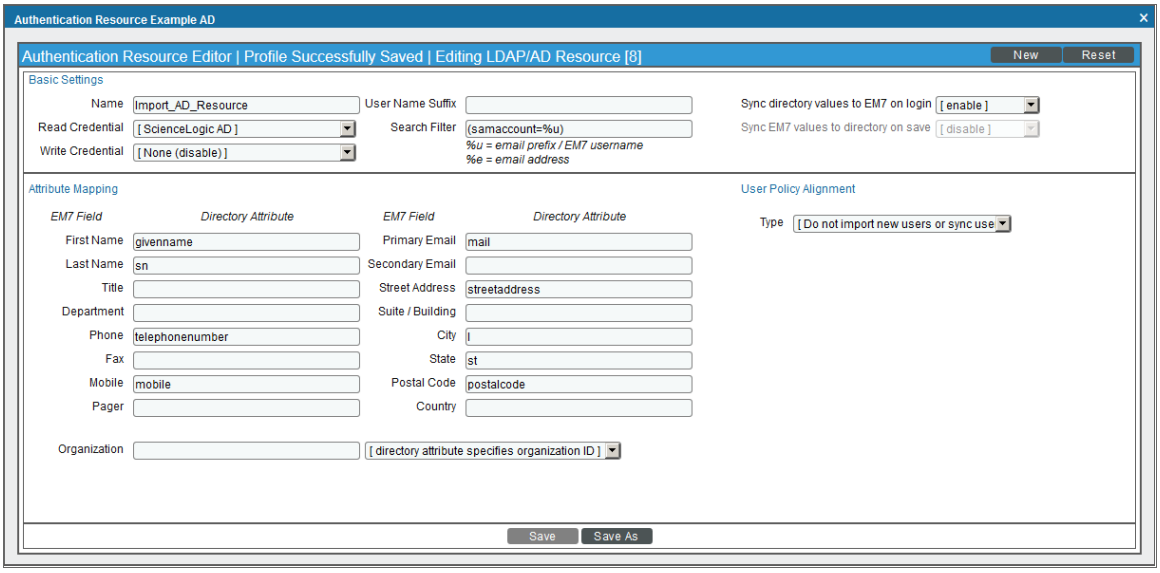
An ***Authentication Resource*** is a configuration policy that describes how SL1 should communicate with a user store. In this manual, the user store is an Active Directory user store. The **LDAP/AD Auth Resource Editor** page allows you to define an Authentication Resource for use with an AD user store. An LDAP/AD Authentication Resource specifies the connector (communication software) to use to communicate with the AD user store and the credential to use to connect to the user store. An LDAP/AD Authentication Resource can also map attributes from the user's AD account to fields in the user account on SL1.

To create an LDAP/AD Authentication Resource:

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).



2. In the **Authentication Resource Manager** page, click the **[Actions]** menu and then select *Create LDAP/AD Resource*. The **LDAP/AD Auth Resource Editor** page appears.



3. Enter values in the following fields:

Basic Settings

- ***Name***. Name of the LDAP/AD Authentication Resource. Enter *Import_AD_Resource*.
- ***Read Credential***. Select the credential we created earlier, ***ScienceLogic AD***. This credential allows SL1 to read data from an Active Directory server.

- ***Write Credential***. Leave this field blank.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Read Credential*** field and the ***Write Credential*** field.

- ***User Name Suffix***. Leave this field blank.
- ***Search Filter***. Specifies where to find the user's account information in Active Directory. Enter the following:

```
(samaccountname=%u)
```

  This says to search for the samaccountname attribute that matches the login name (entered when the user logs in to SL1 and then store in the variable %u).

- ***Sync directory values to EM7 on login***. If the AD administrator makes changes to an AD account, SL1 will 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.
- ***Sync EM7 values to directory on save***. If an administrator made changes to the user account in SL1, SL1 will automatically write those changes to the user's account in LDAP or Active Directory. ***This option requires a write credential***.

Attribute Mapping

If you have configured SL1 to automatically create accounts in SL1 for AD users, these fields specify the AD attribute value that will be automatically inserted into each field in each user's **Account Properties** page.

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 AD attribute "sn" (surname) into the ***Last Name*** field in each user's **Account Properties** page (Registry > Devices > Device Manager.

NOTE: SL1 requires that the LDAP or AD attribute name that you specify in each field uses ***all lowercase characters***.

- ***First Name***. Specifies the AD 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 AD attribute "givenname" into this field. We accepted the default value.
- ***Last Name***. Specifies the AD 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 AD attribute "sn" into this field. We accepted the default value.

- ***Phone***. Specifies the AD 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 AD attribute "telephonenumber" into this field. We accepted the default value.
- ***Mobile***. Specifies the AD 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 AD attribute "mobile" into this field. We accepted the default value.
- ***Primary Email***. Specifies the AD 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 AD attribute "mail" into this field. We accepted the default value.
- ***Street Address***. Specifies the AD 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 AD attribute "streetaddress" into this field. We accepted the default value.
- ***Suite/Building***. Specifies the AD attribute value that will be automatically inserted into the ***Suite/Building*** field in each user's **Account Properties** page.
- ***City***. Specifies the AD 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 AD attribute "l" into this field. We accepted the default value.
- ***State***. Specifies the AD 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 AD attribute "st" into this field. We accepted the default value.
- ***Postal Code***. Specifies the AD 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 AD attribute "postalcode" into this field. We accepted the default value.
- ***We accepted the default values (usually a blank field) in all other fields***.

User Policy Alignment

- ***Type***. Specifies whether SL1 should automatically create accounts in SL1 for each LDAP or Active Directory user in the search base (which is specified in the credential), whether SL1 should simply use LDAP or Active Directory to authenticate one or more users, or whether SL1 will refuse to authenticate specific users. We selected :
    - *Static policy alignment*. If an LDAP or AD user logs in to SL1 using the LDAP or AD attribute specified in the ***Search Filter*** field, SL1 will automatically create an account for that user. SL1 will use ***one user policy*** (specified in the ***Policy*** field) to create all imported LDAP or AD user accounts. SL1 will also use the settings and credentials specified in this page when creating the account.

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

- ***Policy***. Specifies the user policy to use to automatically create an account in SL1 for each LDAP or AD user. Select from a list of all user policies that specify *LDAP /Active Directory* in the ***Authentication Method*** field. We selected the User Policy we created earlier, *AD_Imported*.

4. Click the **[Save]** button to save your changes to the new Authentication Resource.

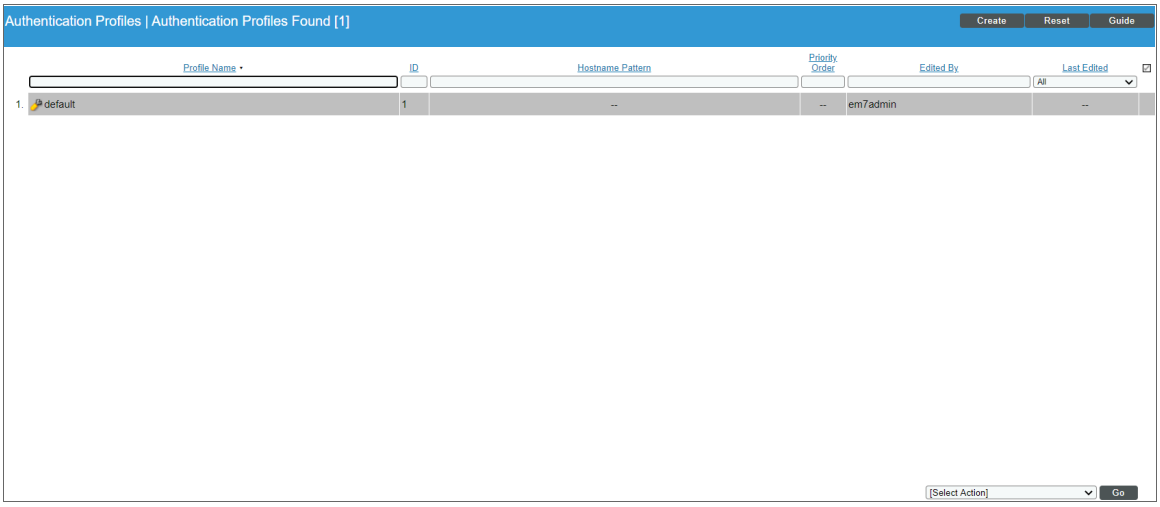
Creating an Authentication Profile

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

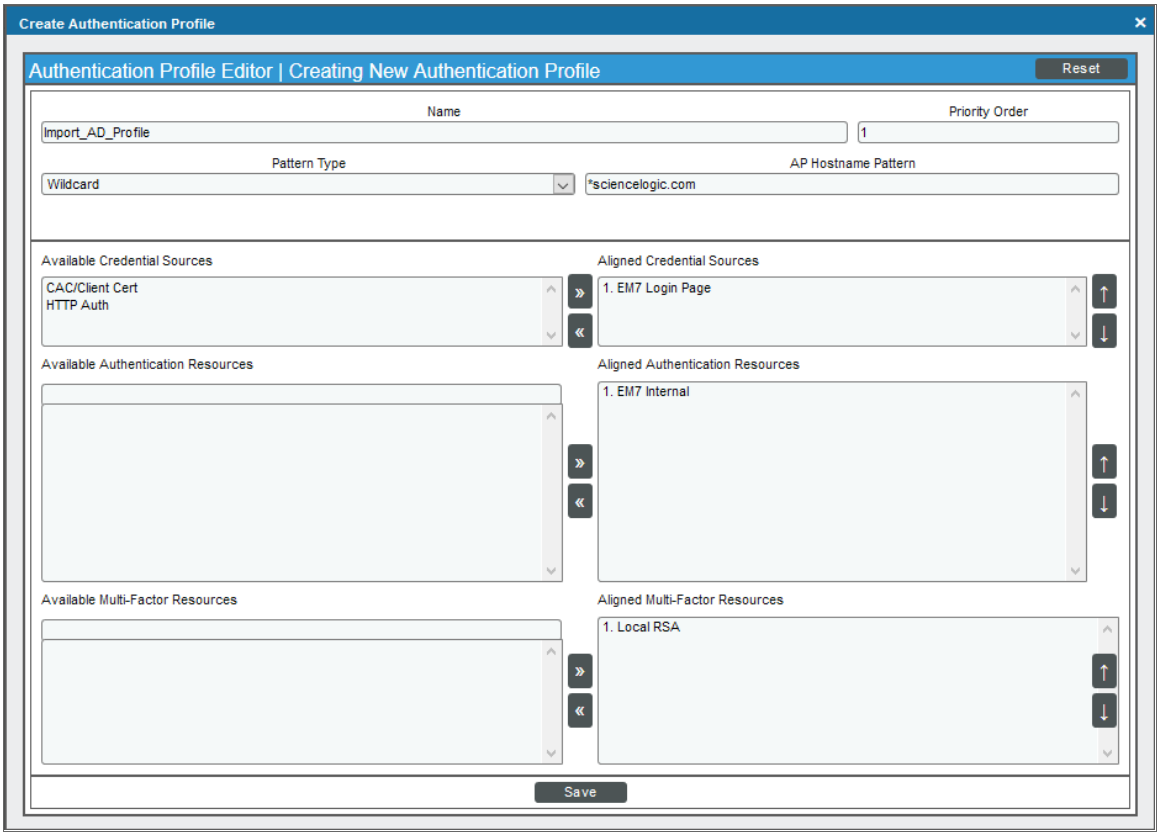
- ***Alignment by pattern matching***. SL1 uses the URL or IP address that a user enters in a browser to connect to an Administration Portal, Database Server, or All-In-One Appliance. If the URL or IP address matches the criteria specified in an authentication profile, SL1 will automatically use the 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, the credential to use to connect to the user store (if applicable), 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.
- ***Multi-factor Resource***. Specifies the connector to use to 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, and the URL of the RSA REST endpoint.

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).



2. Click the **[Create]** button. The **Authentication Profile Editor** modal page appears.



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

   - ***Name***. Name of the Authentication Profile. We entered *Import_AD_Profile*.
   - ***Priority Order***. If SL1 includes multiple Authentication Profiles, SL1 evaluates the Authentication Profiles in ascending priority order. 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. We accepted the default value, *1*.
   - ***Pattern Type***. Specifies how SL1 will evaluate the value in the ***AP Hostname Pattern*** field. We selected *Wildcard*. SL1 will perform a text match, with wildcard characters (asterisks).
   - ***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. We entered **.sciencelogic.com* in this field.

     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.com" 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. We selected:

    - *EM7 Login Page*. SL1 will retrieve a user name and password from SL1 login page fields.

- ***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. We selected *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 select the right-arrow button.
- ***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.

NOTE: 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.

User Login to SL1

After completing the steps in this chapter:

1. Suppose user "kgibson" logs in to SL1 with the following credentials:

   - ***Account***: kgibson
   - ***Password***: ilovedocs!

2. SL1 will look for an account with an ***Account Login Name*** of "kgibson".
3. When examining the user's account information, SL1 will discover that this user login is to be authenticated with AD.
4. SL1 will check the login request and match the originator's URL or IP address to an Authentication Profile. In our example, the originator's URL will match the Authentication Profile we created, ***Import_AD__Profile***.
5. The Authentication Profile will tell the platform to extract the user's credentials from the ScienceLogic Login page and to use the Authentication Resource we created, ***Import_AD_Resource***.
6. The Authentication Resource will tell SL1 to use the credential we created, **ScienceLogic AD**, to connect to the AD server. SL1 will connect to the AD server using the bind dn value from the ***RDN*** field in the credential. The value we entered was **%u %d**. So we will connect to the AD server using the username "kgibson" in the domain "sciencelogic.local".
7. SL1 will search the AD server using the value specified in ***Search Filter*** field in the Authentication Resource. In our example, SL1 will search for a record where the *samaccountname* attribute contains the login name (entered when the user logs in to SL1).
8. Based on the record found in the AD server, SL1 will ask the AD server to authenticate the username and password that were passed to the ScienceLogic Login page.

9. After authentication, SL1 will retrieve values from the AD server to populate fields in the user's **Account Properties** page.

Example

2

Example of Only Authenticating User Accounts Using LDAP

Overview

If you have already created Active Directory or LDAP accounts for users, you can use Active Directory or LDAP to authenticate one or more of those users. Each Active Directory or LDAP user logs in to SL1 using his/her Active Directory or LDAP username and password, and SL1 will use Active Directory or LDAP to authenticate that user.

This chapter will walk you through an example of authenticating a user using LDAP. Although this chapter will illustrate the steps and concepts for this task, the values are specific to the example LDAP server and will not work on your LDAP system.

Although some of the values in this example are specific to LDAP, you can use a very similar example to authenticate user accounts with Active Directory.

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 *60*

Example Entry in LDAP *61*

Creating a User Account that Will Be Authenticated with Active Directory or LDAP *61*

Defining a Credential for Authentication with LDAP *63*

Creating an LDAP/AD Authentication Resource *65*

Creating an Authentication Profile *67*

Required Tasks

You can use LDAP or Active Directory to authenticate one or more users when they log in to SL1. You can also specify that SL1 should not authenticate other LDAP or Active Directory users.

- Each user logs in to SL1, either through the login page, a CAC card or certificate, or HTTP. The user logs in to SL1 using an LDAP or AD attribute value as a login name and the LDAP or AD password.
- SL1 examines the login request and applies the appropriate Authentication Profile (and the appropriate Authentication Resource(s)).
- SL1 then authenticates the user by communicating with the LDAP or Active Directory server.

If you want to use LDAP or Active Directory to only authenticate users (that is, you do not want SL1 to import user accounts from Active Directory or LDAP), you must manually create accounts in SL1 and specify LDAP or AD authentication. To do this:

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.

    - When creating the user policy, you must select *LDAP/Active Directory* in the ***Authentication Method*** field in the **User Policy Properties Editor** page Registry > Accounts > User Policies > create/edit User Policy.
    - When creating the user account, you must select *LDAP/Active Directory* in the ***Authentication Method*** field in the **Account Permissions** page (Registry > Accounts > User Accounts > edit user account)

2. *Create an Active Directory or LDAP credential* that allows SL1 to read from (and optionally, write to) the AD or LDAP directory. This credential allows SL1 to connect to Active Directory or LDAP and authenticate user accounts.
3. *Define the LDAP/AD Authentication Resource*.

    - Specify how SL1 should communicate with the LDAP or Active Directory server and exchange information with the LDAP or Active Directory server.
    - In the ***Type*** field, select the following:

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

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

    - Each LDAP/AD user must log in to SL1 using the user name and password for SL1. This username must be identical to the LDAP or AD user ID for the user; the password must be identical to the LDAP or AD password.

- 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 Authentication Resources to use to authenticate the user.
- SL1 will use the settings and the credentials defined in the LDAP/AD Authentication Resource to query the LDAP or AD directory to authenticate each user.

Example Entry in LDAP

Suppose we have an entry like this in LDAP:

```
# tkrilly, People, sciencelogic.com
dn: uid=tkrilly,ou=People,dc=sciencelogic,dc=com
uid: tkrilly
cn: Ted Krilly
objectClass: top
objectClass: person
objectClass: inetOrgPerson
userPassword:: craggy
street: 100 Commonwealth Avenue
l: Boston
st: MA
postalCode: 02134
mail: tkrilly@company.com
telephoneNumber: 617-776-2661
mobile: 617-776-3000
givenName: Ted
sn: Krilly
```

In this entry, we have a user named "tkrilly", who resides in the ou called "People", in the domain "sciencelogic.com". We'll use this information when configuring SL1 to authenticate this user.

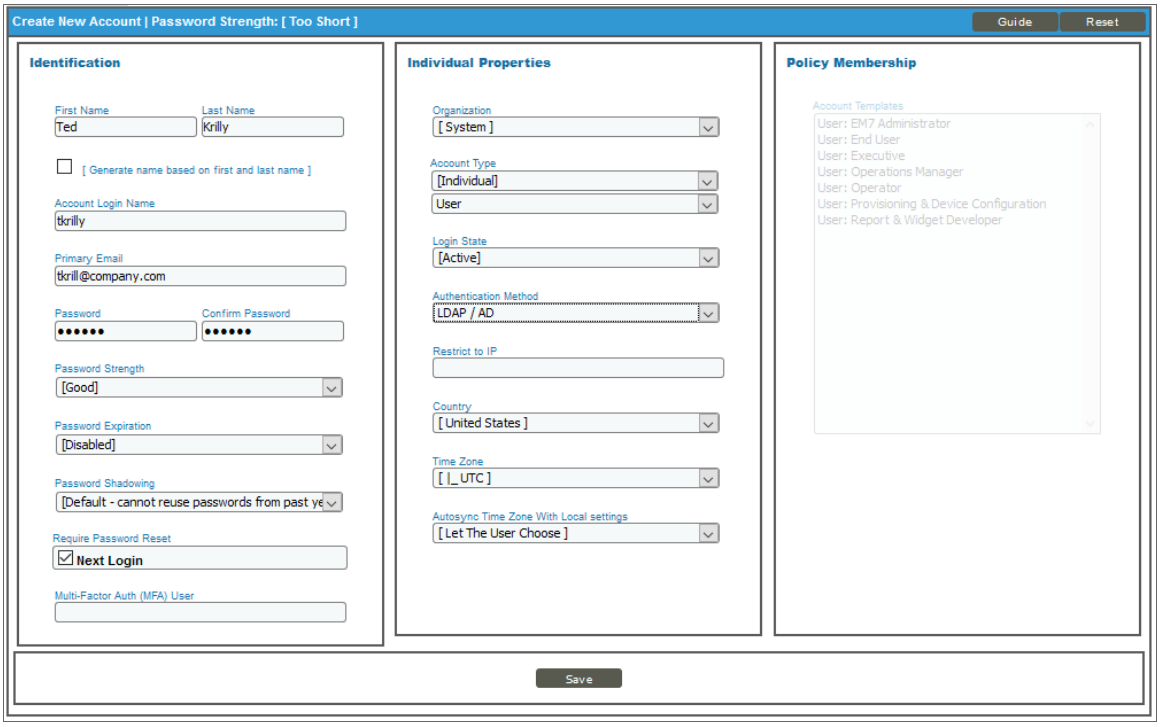
Creating a User Account that Will Be Authenticated with Active Directory or LDAP

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 LDAP, you can create a separate user account for that user in SL1 and then ask Active Directory or LDAP to authenticate the user account.

For our example, we performed the following:

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

2. Click the **[Create]** button. The **Create New Account** page appears.



3. 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. We entered **Ted**.
   - ***Last Name***. User's last name. This value can be up to 24 characters in length. We entered **Krilly**.
   - ***Generate a unique name based on first and last name***. **Do not select this option**.
   - *Account Login Name*. **Enter a value that is included in the Active Directory entry or LDAP entry for the user.** We entered the value of the **uid** for the user's account in LDAP. We entered **tkrilly**.
   - ***Primary Email***. The user's primary email address. We entered **tkrilly@company.com**.
   - ***Password***. **Enter the user's LDAP password**. We entered **craggy!**. To allow LDAP to authenticate the user, the password must match the user's password in LDAP.
   - ***Confirm Password***. The user's password again. We entered **craggy!** again.
   - ***Password Strength***. We selected *Good*. The user's password must have a strength of "Good" to be authenticated.
   - ***Password Expiration***. We selected *Disabled*.
   - ***Password Shadowing***. We selected *Default*. The user will not be able to reuse any password from the past year.
   - ***Require Password Reset***. We did not select this checkbox. The user will not have to reset their password at their next login.
   - ***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: 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. We selected *System*.
- ***Account Type***. Specifies whether the user is a member of a user policy.
  - *Individual*. **We selected this option**. User account is not a member of a user policy.
- ***Account Type***.This drop-down contains an entry for each standard account type. These account types affect the list of Access Keys for the user.
  - *User*. **We selected this option**. 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 a system administrator from the **Access Keys** page (System > Manage > Access Keys).
- ***Login State***. Default login state for the user account.
  - *Active*.**We selected this option**. Account is active, so the user can log in to SL1.
- ***Authentication Method***. Specifies how the user's username and password will be authenticated.
  - *LDAP/Active Directory*. **Select this option**. User's username and password are authenticated by an LDAP server or Active Directory server.
- ***Restrict to IP***. **We did not select this option and left the field blank**. When an IP address is entered in this field, the user will be allowed to access SL1 only from the specified IP.
- ***Time Zone***. Select the appropriate time zone to associate with the user account. We selected *America / New York*.

4. Click the **[Save]** button to save the new user.

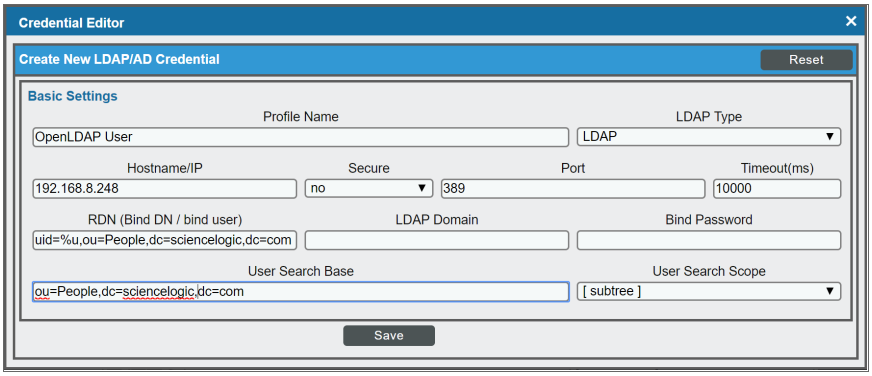
Defining a Credential for Authentication with LDAP

When you define user accounts that are authenticated with LDAP, you must define one or more credentials so SL1 can communicate with the LDAP server. SL1 must communicate with the LDAP server to authenticate the specified users.

For our example, we performed the following:

1. Go to the **Credential Management** page (Credential Management).
2. Click the **[Actions]** drop-down menu and then select *Create LDAP/AD Credential*.

3. The **Credential Editor** modal page appears. In this page, you can define the new credential.



4. Supply a value in each of the following fields:

   - ***Profile Name***. Name of the credential. We entered **OpenLDAP User**.
   - ***LDAP Type***. Specifies the type of LDAP implementation running on the directory server. We selected *LDAP*.
   - ***Hostname/IP*** . Hostname or IP address of the LDAP server. We entered **192.168.8.248**.
   - ***Secure***. Specifies whether you are using the "LDAP over SSL" protocol. We selected *no*.
   - ***Port*** . Port number on the LDAP server or Active Directory server to which SL1 will send requests. We accepted the default port, **389**.
   - ***Timeout***. We accepted the default value *10000*.
   - ***RDN (Bind DN / bind user)***. Specifies the ***bind DN***. The bind DN is an account on the Active Directory server or LDAP server that is allowed to search the directory within the specified search base.

     - In SL1, the %u variable stores the latest username from the login page.
     - In most LDAP configurations, each user has read-access to his or her own account.
     - You can include the variable %u in this field. When an LDAP user logs in to SL1, SL1 stores the username in the %u variable. SL1 then uses the %u variable to build the bind DN, uses the bind DN to communicate with the LDAP server, and then asks the LDAP server to authenticate the current user.

     We typed:

     uid=%u,ou=People,dc=sciencelogic,dc=com

     This creates a DN using the current login name as the uid. The bind DN will be the user's UID, in the ou "People" in the domain "sciencelogic.com".

   - ***LDAP Domain***. If your LDAP or Active Directory configuration includes multiple domains, specify the domain components to bind to in this field. Because our LDAP server includes only one domain, **we left this field blank**.

- ***Bind Password***. Password that allows access to the LDAP server. In most cases, when you specify a bind password in a credential, you are creating a "write" credential (that is, a credential that allows SL1 to make changes to the LDAP server). **We left this field blank**.
- ***User Search Base***. Specifies the area in the LDAP directory where the user to be authenticated resides, using RDN notation. The search base tells SL1 which part of the external directory tree to search. We entered:

  ou=People,dc=sciencelogic,dc=com

  This tells SL1 to search for users to authenticate in the ou called "People " in the domain "sciencelogic.com" and also authenticate all users in any ou underneath "People".

NOTE: For details on search syntax for Active Directory, see http://msdn.microsoft.com/en-us/library/aa746475(VS.85).aspx. For details on the search syntax for LDAP, see http://www.faqs.org/rfcs/rfc2254.html

- ***User Search Scope***. Specifies whether SL1 should search only the directory specified in the ***User Search Base*** field or whether SL1 should search the directory specified in the ***User Search Base*** field and all its child branches. We selected *Subtree*, so SL1 will search the specified directory and all child branches.

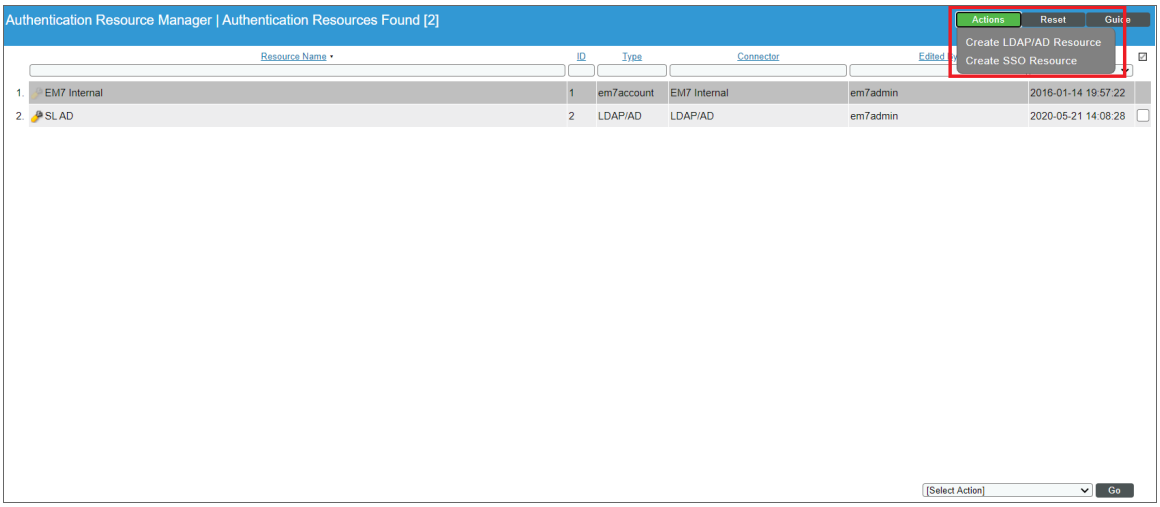
5. Click the **[Save]** button to save your changes to the credential.

Creating an LDAP/AD Authentication Resource

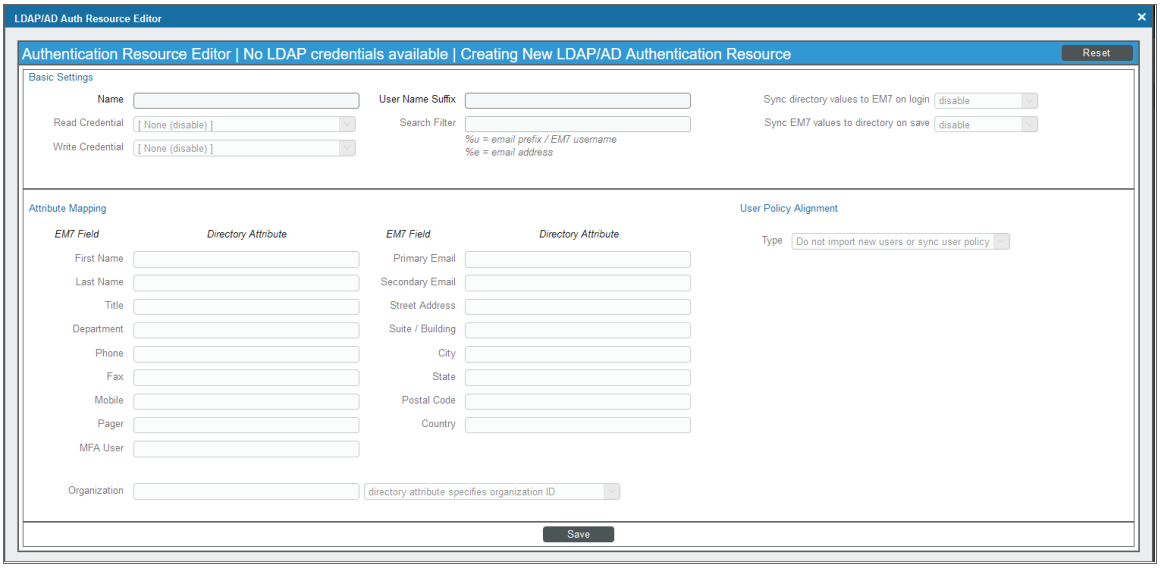
An ***Authentication Resource*** is a configuration policy that describes how SL1 should communicate with a user store. In this manual, the user store is an Active Directory user store. The **LDAP/AD Auth Resource Editor** page allows you to define an Authentication Resource for use with an AD user store. An LDAP/AD Authentication Resource specifies the connector (communication software) to use to communicate with the AD user store and the credential to use to connect to the user store. An LDAP/AD Authentication Resource can also map attributes from the user's AD account to fields in the user account on SL1.

To create an LDAP/AD Authentication Resource:

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).



2. Click the **[Actions]** menu and then select *Create LDAP/AD Resource*. The **LDAP/AD Auth Resource Editor** page appears.



3. Enter values in the following fields:

Basic Settings

- ***Name***. Name of the LDAP/AD Authentication Resource. Enter *Authenticate__LDAP_Resource*.
- ***Read Credential***. Select the credential we created earlier, ***OpenLDAP User***. This credential allows SL1 to read data from an Active Directory server.

- ***Write Credential***. Leave this field blank.

> **NOTE**: Your organization membership(s) might affect the list of credentials you can see in the ***Read Credential*** field and the ***Write Credential*** field.

- ***User Name Suffix***. Leave this field blank.
- ***Search Filter***. Specifies where to find the user's account information in LDAP . Enter the following:

```
(&(objectClass=person)(uid=%u))
```

  This says to search the object class ***person*** and search for the ***uid*** attribute that matches the login name (entered when the user logs in to SL1 and then store in the variable %u).

- ***Sync directory values to EM7 on login***. If the LDAP administrator makes changes to an LDAP account, SL1 will 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. Wee selected *enable*.
- ***Sync EM7 values to directory on save***. If an administrator made changes to the user account in SL1, SL1 will automatically write those changes to the user's account in LDAP or Active Directory. ***This option requires a write credential***. We accepted the default value of *disable*.

Attribute Mapping

In this example, SL1 uses LDAP to authenticate existing users. We therefore do not configure these settings. ***We deleted the default values and left each field blank.***

User Policy Alignment

- ***Type***. Specifies whether SL1 should automatically create accounts in SL1 for each LDAP or Active Directory user in the search base (which is specified in the credential), whether SL1 should simply use LDAP or Active Directory to authenticate one or more users, or whether SL1 will refuse to authenticate specific users. Because we are using LDAP or AD to authenticate users but not automatically create new user accounts in SL1, we selected the following:
  - *Do not authenticate new users from directory*. Only those users who have an account already created in SL1 can log in to SL1. However, if one or more users' ***Account Permissions page*** specifies *LDAP /Active Directory* in the ***Authentication Method*** field, SL1 will authenticate those users with either LDAP or Active Directory, using the settings and credentials specified in this page.

4. Click the **[Save]** button to save your changes to the new Authentication Resource.

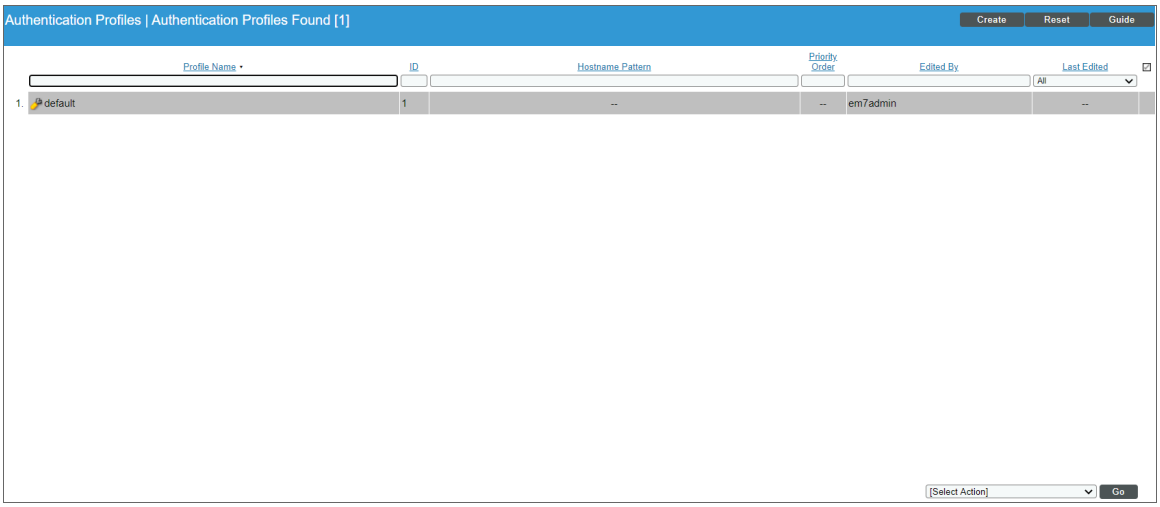
Creating an Authentication Profile

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

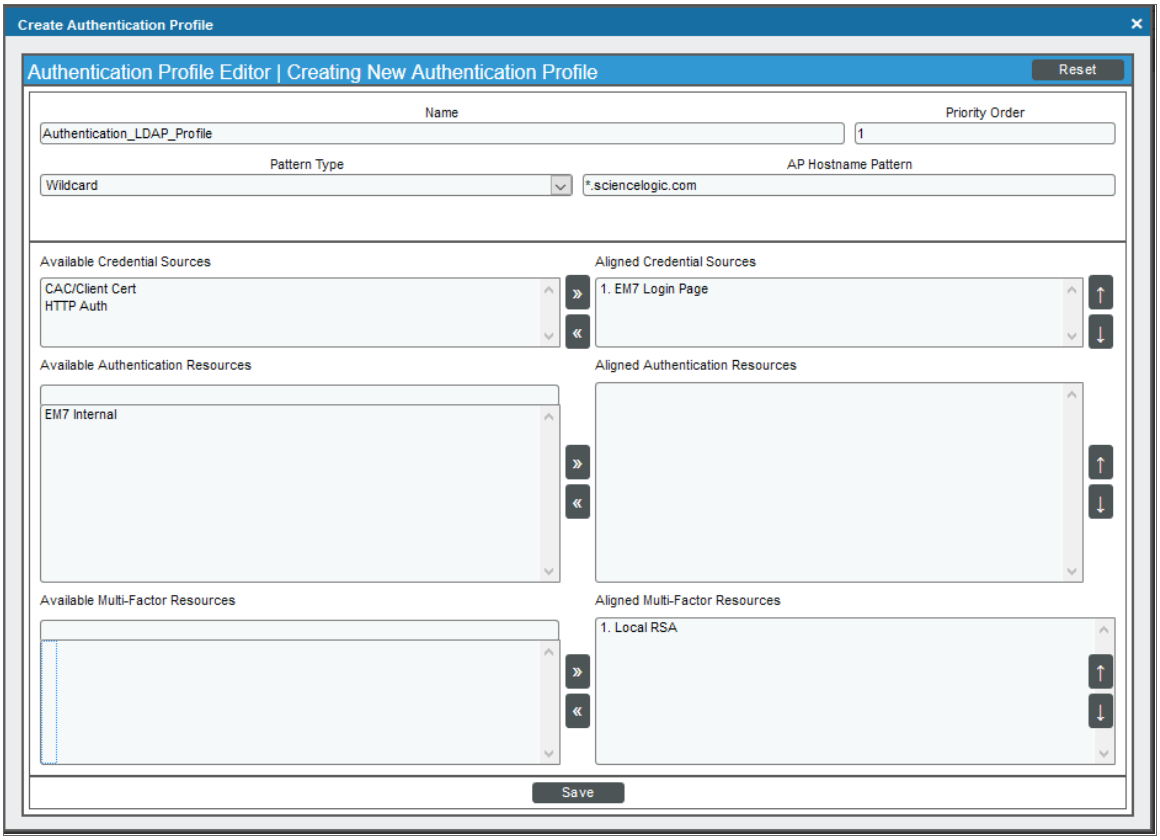
- ***Alignment by pattern matching***. SL1 uses the URL or IP address that a user enters in a browser to connect to an Administration Portal, Database Server, or All-In-One Appliance. If the URL or IP address matches the criteria specified in an authentication profile, SL1 will automatically use the 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, the credential to use to connect to the user store (if applicable), and the URLs to examine during authentication.
- ***Multi-factor Resource***. Specifies the connector to use to 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, and the URL of the RSA REST endpoint.

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).



2. Click the **[Create]** button. The **Authentication Profile Editor** modal page appears.



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

   - ***Name***. Name of the Authentication Profile. We entered *Authenticate_LDAP_Profile*.
   - ***Priority Order***. If SL1 includes multiple Authentication Profiles, SL1 evaluates the Authentication Profiles in ascending priority order. 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. We accepted the default value, *1*.
   - ***Pattern Type***. Specifies how SL1 will evaluate the value in the ***AP Hostname Pattern*** field. We selected *Wildcard*. SL1 will perform a text match, with wildcard characters (asterisks).
   - ***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. We entered **.sciencelogic.com* in this field.

     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.com" 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. We selected:

    - *EM7 Login Page*. SL1 will retrieve a user name and password from SL1 login page fields.

- ***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. We selected *Authenticate_LDAP_Resource*.
- ***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 select the right-arrow button.
- ***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.

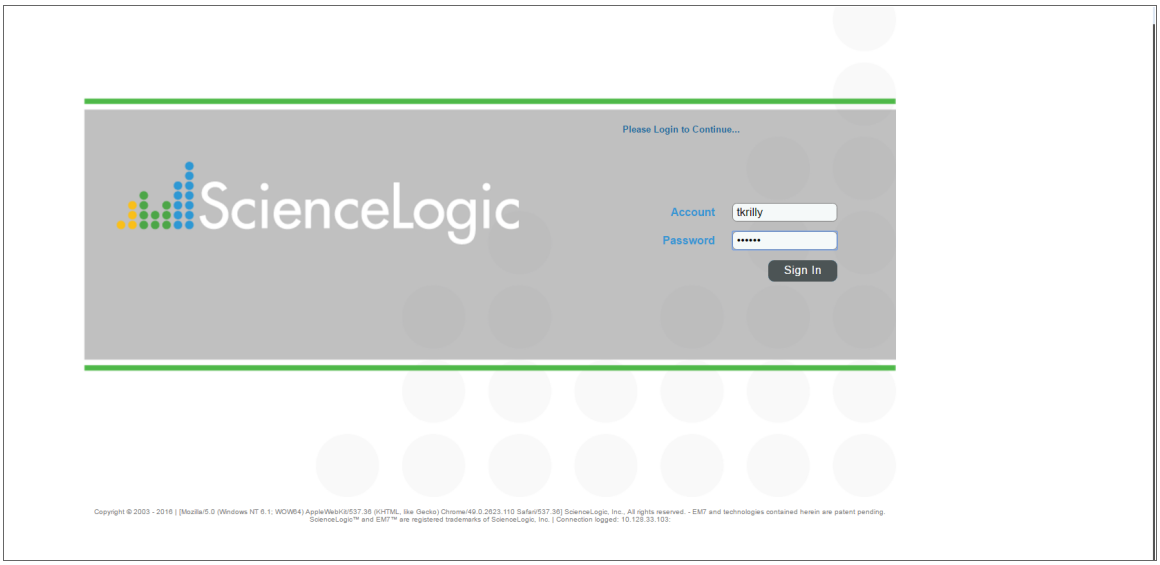
NOTE: For details on configuring multi-factor authentication, see the manual ***Using Multi-Factor Authentication***.

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

User Login to SL1

After completing the steps in this chapter:

1. Suppose user "tkrilly" logs in to SL1 with the following:



   - ***Account***: tkrilly
   - ***Password***: craggy

2. SL1 will look for an account with an ***Account Login Name*** of "tkrilly".
3. When examining the user's account information, SL1 will discover that this user login is to be authenticated with LDAP.
4. SL1 will check the login request and match the originator's URL or IP address to an Authentication Profile. In our example, the originator's URL will match the Authentication Profile we created, ***Authenticate_LDAP_Profile***.
5. The Authentication Profile will tell the platform to extract the user's credentials from the ScienceLogic Login page and to use the Authentication Resource we created, ***Authenticate_LDAP_Resource***.
6. The Authentication Resource will tell SL1to use the credential we created, **OpenLDAP User**, to connect to the LDAP server. SL1 will connect to the LDAP server using the value from the ***RDN*** field in the credential. The value we entered was **uid=%u,ou=People,dc=sciencelogic,dc=com**. So we will connect to the LDAP server using the user name "tkrilly", in the ou "People", in the domains "sciencelogic" and "com".
7. SL1 will search the LDAP server using the value specified in the ***Search Filter*** field in the Authentication Resource. In our example, SL1 will search the object class ***person*** and search for the ***uid*** attribute that matches the login name (entered when the user logs in to SL1).

8. Based on the matching record found in the LDAP server, SL1 will ask the LDAP server to authenticate the username and password that were passed to the ScienceLogic Login page.

© 2003 - 2022, ScienceLogic, Inc.

All rights reserved.

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

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

International: +1-703-354-1010