Authentication

Skylar One version 12.5.20

Table of Contents

Introduction 5
- Overview and Core Concepts 7
  - How Authentication Is Used In Skylar One 7
  - Authentication vs. Authorization 7
- How Authentication Works 7
  - High-Level Authentication Flow 8
  - Local Authentication vs. External Identity Providers (IdP) 8
  - Authentication Decision Points 8
- Authentication Building Blocks 8
  - Authentication Profiles Overview 8
  - Authentication Resources Overview 9
  - Relationship Between Profiles and Resources 9
- Authentication Methods at a Glance 9
  - Local Authentication 9
  - Directory-Based Authentication (Active Directory and LDAP) 9
  - Single Sign-On (SSO) 10
  - SAML Authentication 10
  - Multi-Factor Authentication (MFA) 10
  - CAC Authentication 11
  - API Authentication (REST and Token-Based Access) 11
  - Choosing an Authentication Method 11

Authentication Profiles and Resources 12
- Authentication Profiles 13
  - Viewing the List of Authentication Profiles 13
  - The "Default" Authentication Profile 14
  - Creating an Authentication Profile 15
  - Editing an Authentication Profile 17
  - Deleting One or More Authentication Profiles 17
- Authentication Resources 17
  - Viewing the List of Authentication Resources 18
  - The "Internal" Resource 19

Creating an LDAP/AD Authentication Resource 19
Creating an SSO Authentication Resource 25
Editing an Authentication Resource 31
Deleting an Authentication Resource 32
Relationship Between Profiles and Resources 32
Single Sign-On (SSO) 33
What is SSO? 34
SSO Terminology 34
How Can I Use SSO with Skylar One? 34
Importing User Accounts from Single Sign-On (SSO) 34
Prerequisites 35
Required Tasks 35
Creating a User Policy for Imported Users 37
Creating an SSO Authentication Resource for Importing Users 39
Creating an Authentication Profile 46
Viewing Metadata 48
Using a Self-Signed SSL Certificate 48
Using Single Sign-On (SSO) for Authentication Only 49
Manually Creating a User Account and Using a User Policy to Define Account Settings 49
Creating an SSO Authentication Resource for Authenticating Users 51
Creating an Authentication Profile 54
Viewing Metadata 56
Using Your Own SSL Certificate 56
Multi-Factor Authentication 58
What is Multi-Factor Authentication? 58
Configuring Multi-Factor Authentication 59
Caveats 59
Prerequisites 59
Configuration Steps 59
Defining a Multi-factor Resource 60
Creating or Editing an Authentication Profile 61
Creating an Authentication Profile for Local Authentication 61

Creating an Authentication Profile for Active Directory or LDAP 63
Directory-Based Authentication (Active Directory and LDAP) 65
What is LDAP? 66
What is Active Directory? 66
LDAP and Active Directory Terminology 66
How Can I Use LDAP or Active Directory with Skylar One? 68
LDAP Authentication Configurations 68
How Can I View My Company's Active Directory or LDAP? 70
Importing User Accounts from Active Directory or LDAP 71
CAC Authentication 72
Using CAC Authentication 74
Prerequisites 75
Importing SSL Certificates 76
Extracting the Common Name from a Certificate for Authentication 77
Defining the Client Certificate Chain 78
Verifying SSL Certificate File Import and Resolving Issues 80
Clearing the Skylar One Cache and Restarting NGINX 81
Testing the Configuration 81
Troubleshooting CAC Authentication 82
Failed to Identify Personal Identity Verification (PIV) Card 82
Failed CAC Authentication After Disaster Recovery (DR) Failover 83
Failed CAC Authentication After Setting Up High Availability (HA) 83
Accessing the Appliance without CAC Authentication 84
Special Circumstance: Multiple Levels of Intermediate Certificates 84

Chapter

1

Introduction

Overview

This manual is intended for administrators, system integrators, and support personnel who plan, configure, or maintain authentication for the platform. It provides an overview of the authentication methods supported by the platform. It is intended for administrators, system integrators, and support personnel who are planning an authentication strategy, evaluating available authentication options, or supporting existing authentication implementations.

This chapter explains how authentication works at a high level, introduces the core authentication concepts and components used by , and describes each authentication method, including when it is typically used and how it integrates with the platform. This chapter does not include configuration or setup instructions. Detailed architecture, configuration, and setup guidance for all authentication methods is provided in the following chapter.

This manual assumes that you are familiar with basic authentication and identity concepts, such as usernames and passwords, directory services, and single sign-on. Familiarity with Active Directory, LDAP, and common identity provider workflows is recommended.

NOTE: If you are not familiar with these technologies, you might need to work with your organization's directory services, identity management, or security administrators to complete the tasks described in this manual.

This chapter covers the following topics:

Overview and Core Concepts 7

How Authentication Works 7

Authentication Building Blocks *8*
Authentication Methods at a Glance *9*

Overview and Core Concepts

Authentication controls how users and systems prove their identity before gaining access to the platform. It is a foundational security capability that ensures access is granted only to verified identities and that authentication decisions can be consistently enforced across different access methods and integrations.

This guide describes the authentication mechanisms supported by the platform, how authentication decisions are evaluated, and how different authentication methods can be combined to meet organizational security and operational requirements. It is intended for administrators, architects, and support personnel who are responsible for planning, implementing, or maintaining authentication.

How Authentication Is Used In Skylar One

In Skylar One, authentication is the process of validating a user's or system's credentials against a defined authentication source. Authentication may be performed locally or delegated to an external identity provider, depending on how the environment is configured.

Authentication determines whether an identity is valid. Once authenticated, access is governed by authorization and policy controls, which are addressed separately from authentication.

Authentication vs. Authorization

Authentication and authorization are related but distinct aspects of access control. Understanding the difference between them is essential when designing, configuring, or troubleshooting access to the platform.

Authentication is the process of verifying the identity of a user or system. It answers the question: Who is attempting to access the system? Authentication validates credentials such as a username and password, a smart card certificate, or a token issued by an external identity provider. If authentication succeeds, the identity is considered trusted; if it fails, access is denied immediately.

Authorization determines what an authenticated identity is allowed to do. It answers the question: What actions is this authenticated user or system permitted to perform? Authorization controls access to features, resources, and data based on roles, policies, or permissions associated with the authenticated identity.

In practice, authentication always occurs before authorization. A user or system must first successfully authenticate before any authorization rules are evaluated. While authentication establishes identity, authorization governs access.

How Authentication Works

Authentication follows a consistent evaluation model regardless of the specific method being used. Understanding this high-level flow helps administrators design authentication configurations and diagnose authentication failures.

High-Level Authentication Flow

At a high level, authentication proceeds through the following stages:

1. A user or system presents credentials.
2. The platform evaluates the credentials using one or more configured authentication mechanisms.
3. If authentication succeeds, the identity is established and access proceeds.
4. If authentication fails, access is denied and the authentication attempt ends.

The exact steps involved depend on how authentication is configured, but the overall decision flow remains consistent.

Local Authentication vs. External Identity Providers (IdP)

Skylar One supports both local authentication and authentication through external identity providers.

Local authentication validates credentials that are managed directly within the platform. This approach is often used in small or isolated environments, for initial access, or for service and emergency accounts.

External identity provider (IdP) authentication delegates credential validation to systems such as directory services or single sign-on providers. This approach allows organizations to centralize identity management, enforce consistent security policies, and integrate authentication with existing enterprise systems.

Organizations commonly use a combination of local and external authentication depending on operational and security requirements.

Authentication Decision Points

Authentication decisions are made by evaluating configured authentication components in a defined order. These components determine which authentication methods are attempted and how credential validation is performed. While the specific configuration is addressed later in this guide, understanding that authentication is evaluated through ordered decision points is key to understanding authentication behavior.

Authentication Building Blocks

Authentication behavior is defined using a small set of core components. These components work together to determine how authentication attempts are processed.

Authentication Profiles Overview

Authentication profiles define how authentication attempts are evaluated. A profile determines which authentication mechanisms are attempted and the order in which they are applied. Profiles allow authentication behavior to be tailored for different users, access paths, or integration scenarios.

Authentication Resources Overview

Authentication resources define how the platform communicates with a specific authentication source, such as a directory service or external identity provider. A resource contains the connection and integration details required to validate credentials against that source.

Relationship Between Profiles and Resources

Authentication profiles reference one or more authentication resources. During authentication, the platform evaluates the resources associated with a profile in sequence until authentication succeeds or all options are exhausted. This separation allows authentication behavior to be reused, extended, and modified without redefining individual integrations.

NOTE: For more information, see the chapter on *Authentication Profiles and Resources*.

Authentication Methods at a Glance

Skylar One supports multiple authentication methods to address a wide range of deployment models and security requirements. Each method differs in how credentials are validated, how identity is managed, and how access is enforced.

The following sections provide a high-level overview of each supported authentication method. Detailed configuration, troubleshooting, and escalation guidance is provided in later chapters.

Local Authentication

Local authentication validates credentials that are created and managed directly within Skylar One. User accounts and credentials are stored locally and authenticated without relying on external identity systems.

Local authentication is typically used for initial system access, service accounts, or environments where external identity integration is not required. It is also commonly retained as a fallback authentication method for administrative or recovery purposes.

Directory-Based Authentication (Active Directory and LDAP)

Directory-based authentication allows users to authenticate using credentials managed in an external directory service, such as Microsoft Active Directory or an LDAP-compliant directory.

In this model, Skylar One delegates credential validation to the directory service while maintaining control over user accounts, policies, and access within the platform. Directory-based authentication is widely used in enterprise environments to centralize identity management and enforce consistent authentication policies.

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 Skylar One is also used by LDAP and Active Directory.

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.

NOTE: For more information, see the chapter on *Directory-Based Authentication*.

Single Sign-On (SSO)

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

SSO is commonly used in environments that require centralized authentication, improved user experience, and integration with corporate identity platforms. SSO can also be combined with additional authentication controls, such as multi-factor authentication, depending on the IdP configuration.

NOTE: For more information, see the chapter on *Single Sign-On Authentication*.

SAML Authentication

SAML authentication is a standards-based form of single sign-on that uses Security Assertion Markup Language (SAML) to exchange authentication information between an identity provider and Skylar One.

In a SAML-based integration, the identity provider authenticates the user and issues a signed assertion that Skylar One uses to establish the user’s identity. SAML authentication is typically used in enterprise or regulated environments where standards-based federation is required or where an existing SAML-enabled identity provider is already in place.

Multi-Factor Authentication (MFA)

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

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

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

In Skylar One, MFA is commonly used to protect privileged access, administrative accounts, or externally accessible login paths. MFA can be used alongside other authentication methods, such as local authentication, directory-based authentication, or SSO.

NOTE: For more information, see the chapter on *Multi-Factor Authentication*.

CAC Authentication

CAC authentication uses smart cards and certificate-based credentials to authenticate users. This method relies on physical authentication factors and cryptographic certificates to establish identity.

CAC authentication is typically used in high-security or regulated environments where strong, hardware-based authentication is required. It is often deployed alongside directory or identity management systems to meet compliance and security standards.

NOTE: For more information, see the chapter on *CAC Authentication*.

API Authentication (REST and Token-Based Access)

API authentication allows systems, scripts, and integrations to authenticate programmatically when interacting with ScienceLogic through RESTful APIs.

Rather than authenticating as an interactive user, API authentication uses credentials such as tokens or keys to grant controlled access to specific API operations. This approach is commonly used for automation, integrations with external systems, and service-to-service communication, where interactive login is not appropriate.

In Skylar One 12.5.20 and later, you can assign a "Read-only API User" user policy to any user that you want to have read-only API access.

Choosing an Authentication Method

Organizations often use a combination of authentication methods to meet different access requirements. Interactive users, administrators, services, and integrations may each use different authentication approaches depending on security needs and operational constraints.

Each authentication method described above is covered in detail in its own chapter, including configuration steps, troubleshooting guidance, and escalation considerations.

Chapter

2

Authentication Profiles and Resources

Overview

Authentication behavior is defined using a small set of core components. These components work together to determine how authentication attempts are processed.

This chapter describes the following topics:

- ***Authentication Profiles***. Policies that align user accounts with one or more types of authentication.
- ***Authentication Resources***. Configuration policies that describe how Skylar One should communicate with a user store.

NOTE: If you are not familiar with these technologies, you may need to work with your organization's directory services, identity management, or security administrators to complete the tasks described in this manual.

This chapter covers the following topics:

Authentication Profiles 13

Authentication Resources 17

Relationship Between Profiles and Resources 32

Authentication Profiles

Authentication profiles define how authentication attempts are evaluated. A profile determines which authentication mechanisms are attempted and the order in which they are applied. Profiles allow authentication behavior to be tailored for different users, access paths, or integration scenarios.

Authentication profiles are policies that align user accounts with one or more types of authentication:

- ***Alignment by pattern matching***. Skylar One examines 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, Skylar One will automatically use the matching profile to perform user authentication.
- ***Credential Source***. Specifies from where Skylar One should extract the username and password or certificate to be authenticated. These credentials are passed to Skylar One through HTTP. Skylar One then passes the credentials to each authentication resource specified in the authentication profile (for example, CAC/
Client Cert). The authentication resources communicate with user stores that can authenticate the credentials entered by a user.
- ***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), such as your Active Directory server, and the URLs to examine during authentication. Authentication Resource also maps attributes from the user's account in the user store to fields in the ScienceLogic user account. For details on creating an authentication resource, see the section on *Authentication Resources*.

NOTE: If you will be using Single Sign-On (SSO) as your method of authentication, your SSO resource must be placed in its own Authentication Profile, since it will take priority over any other authentication method defined. If you have multiple SSO resources, each *must* be in its own profile.

Viewing the List of Authentication Profiles

To view a list of all authentication profiles in Skylar One:

1. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).
2. The following information is displayed about each authentication profile:
   - ***Profile Name***. Name of the authentication profile.
   - ***Access***. Indicates whether the authentication profile is shared with all organizations or is private.

   > **NOTE:** The ***Access*** column displays only for Administrator user accounts and user accounts assigned to the System organization.

   - ***ID***. Unique numeric ID, automatically assigned by Skylar One to each authentication profile.
   - ***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, Skylar One applies the authentication profile to the user for the current session.
   - ***Priority Order***. If your Skylar One System includes multiple authentication profiles, Skylar One evaluates the authentication profiles in priority order, ascending. This column displays the priority order value for the authentication profiles, where 0 (zero) is the highest priority.
   - ***Edited By***. The user who created or last edited the authentication profile.
   - ***Last Edited***. Date and time the authentication profile was created or last edited.

> **TIP:** To sort the list of authentication profiles, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The ***Last Edited*** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

The "Default" Authentication Profile

Skylar One includes a *default* authentication profile, for which the following rules apply:

- You cannot delete the *default* profile.
- If an ***AP Hostname Pattern*** fails to match all the other authentication profiles, Skylar One applies the *default* authentication profile.
- In ISO systems, initially the *default* profile is pre-configured to allow ScienceLogic administrators to log in via *CAC/Client Certificate*, *HTTP Auth*, or the Skylar One *Login Page* and the authentication resource *Internal*. This allows administrators to log in and perform initial configuration on the Skylar One system. After initial configuration, administrators can edit the *default* profile as best fits their organization.

- In patched systems, the *default* profile is included in the patch and is pre-configured to allow ScienceLogic administrators to log in via the ScienceLogic login page and the authentication resource *Internal*. It allows credentials via *CAC/Client Certificate*, *HTTP Auth*, or the Skylar One *Login Page*. It can also use the legacy authentication resources *SSO (legacy)*, *LDAP/AD (legacy)*, and *Internal*.

Creating an Authentication Profile

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.
    - ***Sharing Permission***. Indicates if the authentication profile is shared or private. Choices are:
        - *Shared with all organizations*. The authentication profile is shared with users across all organizations.
        - *Private (visible to System organization only)*. The authentication profile is private to only user accounts assigned to the System organization.

    > **NOTE:** The ***Sharing Permission*** field displays only for Administrator user accounts and user accounts assigned to the System organization.

    - ***Priority Order***. If your Skylar One System includes multiple authentication profiles, Skylar One evaluates the authentication profiles in ascending priority order. Skylar One 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 Skylar One will evaluate the value in the ***AP Hostname Pattern*** field. Choices are:
        - *Wildcard*. Skylar One will perform a text match, with wildcard characters (asterisks).
        - *Regex*. Skylar One 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, Skylar One applies the authentication profile to the user for the current session.
        - For example, if you specify "*" (asterisk), any IP address or URL will match. Skylar One 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", Skylar One 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", Skylar One 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.

> **NOTE:** Do not include underscores (_) in the ***AP Hostname Pattern*** field. URLs with underscores are not considered valid in Skylar One authentication profiles.

- ***Available Credential Sources***. This field tells Skylar One how to retrieve the user's credentials from the HTTP request to Skylar One. 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:** If you will be using CAC authentication, align the CAC/Client Cert credential source. If this is your primary method of logging in to Skylar One, align CAC/Client Cert as the number one credential source. ScienceLogic recommends having Login Page aligned, as well, for administrator or maintenance access.

  - *CAC/Client Cert*. Skylar One will retrieve a certificate from the HTTP request.
  - *HTTP Auth*. Skylar One will retrieve a user name and password from the HTTP request.
  - *Login Page*. Skylar One will retrieve a user name and password from the ScienceLogic login page fields.

> **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 Skylar One.

- ***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 Skylar One 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.

Editing an Authentication Profile

The **Authentication Profiles** page allows you to edit an existing authentication profile. To do so:

1. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).
2. Find the authentication profile that you want to edit. Click its wrench icon (🔧).
3. The **Authentication Profile Editor** modal page appears. In this page, you can edit the value of one or more fields.
4. Click the **[Save]** button to save your changes to the authentication profile.

Deleting One or More Authentication Profiles

The **Authentication Profiles** page allows you to delete one or more authentication profiles from Skylar One. To do so:

1. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).
2. Select the checkbox of each authentication profile that you want to delete.
3. Click the ***Select Actions*** menu (in the lower right), select *DELETE Authentication Profile*, and then click the **[Go]** button. The selected authentication profiles will be deleted.

> **NOTE:** You cannot delete the ***default*** authentication profile.

Authentication Resources

An authentication resource is a configuration policy that describes how Skylar One should communicate with a user store. An 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. An authentication resource also maps attributes from the user's account in the user store to fields in the ScienceLogic user account.

Authentication resources define how the platform communicates with a specific authentication source, such as a directory service or external identity provider. A resource contains the connection and integration details required to validate credentials against that source.

Viewing the List of Authentication Resources

The **Authentication Resource Manager** page displays a list of all authentication resources in the Skylar One System.

To view the list of authentication resources :

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).
2. The following information is displayed about each authentication resource:

> **TIP:** To sort the list of authentication resources, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The ***Last Edited*** column sorts by descending order on the first click; to sort by ascending order, click the column heading again

- ***Resource Name***. Name of the authentication resource.
- ***Access***. Indicates whether the authentication resource is shared with all organizations or is private.

  > **NOTE:** The ***Access*** column displays only for Administrator user accounts and user accounts assigned to the System organization.

- ***ID***. Unique numeric ID, automatically assigned by Skylar One to each authentication resource.
- ***Type***. Specifies the user store that is associated with the resource. Possible types are:
  - *Internal*. The authentication resource communicates and passes information to and from the ScienceLogic Database.
  - *LDAP/AD*. The authentication resource communicates and passes information to and from an LDAP server or Active Directory server.
  - *SSO*. The authentication resource communicates and passes information to and from a SAML Identity Provider (IdP) or Service Provider (SP).
- ***Connector***. The software that allows communication between the authentication resource and the user store. Possible connectors are:
  - *Internal*. Software that communicates with the ScienceLogic Database.
  - *LDAP/AD*. Software that communicates with an LDAP server or Active Directory server.

- *LDAP/AD - Legacy*. Software that communicates with an LDAP server or Active Directory server for ScienceLogic servers that were configured prior to version 7.8 of Skylar One. Skylar One systems that were upgraded to version 7.8 using patches can continue to use the same authentication methods without making changes to user accounts or the LDAP server or Active Directory server.
- *OneLogin*. Software that communicates with a SAML Identity Provider (IdP).
- *SimpleSAML - Legacy*. Software that communicates with a SAML Identity Provider (IdP) and Service Provider (SP) for ScienceLogic servers that were configured prior to version 7.8 of Skylar One. Skylar One systems that were upgraded to version 7.8 using patches can continue to use the same authentication methods without making changes to user accounts, the SAML configuration, or the SSO provider.

- ***Edited By***. The user who created or last edited the authentication resource.
- ***Last Edited***. Date the time the authentication resource was created or last edited.

The "Internal" Resource

The *Internal* resource allows you to access the user store in the ScienceLogic database.

- By default, each Skylar One System includes the *Internal* authentication resource.
- You cannot create an *Internal* authentication resource.
- You cannot edit or delete the *Internal* authentication resource included with your Skylar One System.
- Each Skylar One System can include only one the *Internal* authentication resource.

Creating an LDAP/AD Authentication Resource

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 ScienceLogic user account.

ScienceLogic administrators can use LDAP or Active Directory to authenticate ScienceLogic users. There are two ways to use LDAP or Active Directory authentication with Skylar One:

- You can configure Skylar One to automatically create user accounts for existing LDAP or Active Directory users and then always use LDAP or Active Directory to authenticate those users when they log in to Skylar One.
- You can use LDAP or Active Directory to authenticate one or more ScienceLogic users when they log in to Skylar One.

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** modal page appears.
3. Enter values in the following fields:

Basic Settings

- ***Name***. Name of the LDAP/AD authentication resource.
- ***Sharing Permission***. Indicates if the authentication resource is shared or private. Choices are:
    - *Shared with all organizations*. The authentication resource is shared with users across all organizations.
    - *Private (visible to System organization only)*. The authentication resource is private to only user accounts assigned to the System organization.

> **NOTE:** The ***Sharing Permission*** field displays only for Administrator user accounts and user accounts assigned to the System organization.

- ***Read Credential***. Credential that allows Skylar One 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 Skylar One 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*.
- ***User Name Suffix***. Optional field. Because Skylar One 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 to minimize the risk of collision. For example:
    - Suppose we entered ***@ad.local*** in this field.
    - Suppose the next LDAP/AD user logs in to Skylar One with the user name ***bishopbrennan***.
    - Skylar One will log that user in as ***bishopbrennan@ad.local***.

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

- ***User Display Name***. Select what name to display from the following options:
    - *disable*. Uses the current default behavior, which displays the user's username in the Skylar One user interface and logs.
    - *email address*. Displays the user's email address in the Skylar One user interface and logs.

- *user principal name*. Displays the value from the UPN field on this page in the Skylar One user interface and logs.

- ***UPN***. "User principal name." If you select *user principal name* in the ***User Display Name*** field, then the value from this field displays in the Skylar One user interface and audit logs. Enter one of the following:
  - *email address*. Displays the user's email address in the Skylar One user interface and audit logs.
  - *user principal name*. Displays the value from the UPN field on this page in the Skylar One user interface and audit logs.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Read Credential*** field and the ***Write Credential*** field. For details, see the ***Discovery & Credentials*** manual.

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

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

  You can use the following variables in the search filter:

  - **[%u]**. ScienceLogic login name.
  - *%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 ScienceLogic login name (entered when the user logs in to Skylar One 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 ScienceLogic login name (entered when the user logs in to Skylar One and then stored in the variable %u).

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

- ***Sync directory values on login***. If an LDAP or AD administrator makes changes to an LDAP or AD account, Skylar One will automatically retrieve those updates and apply them to the user's account in Skylar One (in the **Account Properties** page) the next time the user logs in to Skylar One. (For more information about user account properties, see the ***Organizations & Users*** manual.)
- ***Sync account values to directory on save***. If a ScienceLogic administrator made changes to the ScienceLogic account, Skylar One will automatically write those changes to the user's account in LDAP or Active Directory.

> **NOTE:** The ***Sync account values to directory on save*** option requires a write credential.

Attribute Mapping

If you have configured Skylar One to automatically create ScienceLogic accounts 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. (For more information about user account properties, see the ***Organizations & Users*** manual.)

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

> **NOTE:** Skylar One requires that the LDAP or AD attribute name that you specify in each field uses ***all lower-case 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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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.
- ***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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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*. If selected, the attribute in the ***Organization*** field specifies an organization ID.
    - *directory attribute specifies organization name*. If selected, the attribute in the ***Organization*** field specifies an organization name.
    - *directory attribute specifies organization CRM ID*. If selected, 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 ScienceLogic Organization names, Organization IDs, or Organization CRM IDs.

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 Skylar One should automatically create ScienceLogic accounts for each LDAP or Active Directory user in the search base (which is specified in the credential), whether Skylar One should simply use LDAP or Active Directory to authenticate one or more users, or whether Skylar One 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 Skylar One can log in to Skylar One. However, if one or more users' **Account Permissions** page specifies *LDAP /Active Directory* in the ***Authentication Method*** field, Skylar One 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 Skylar One using the LDAP or AD attribute specified in the ***Search Filter*** field, Skylar One will automatically create an account for that user. Skylar One will use ***one user policy*** (specified in the ***Policy*** field) to create all imported LDAP or AD user accounts. Skylar One 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 Skylar One using the LDAP or AD attribute specified in the ***Search Filter*** field, Skylar One will automatically create an account for that user. Skylar One 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". Skylar One will also use the settings and credentials specified in this page when creating the account.

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

- ***Policy***. Specifies the user policy to use to automatically create a ScienceLogic account for each LDAP or AD user. Select from a list of all user policies that specify *LDAP /Active Directory* in the ***Authentication Method*** field.

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

- ***Attribute***. Specifies 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 a ScienceLogic account.
- ***Value***. Specifies the LDAP or AD attribute value. That is, you specify one of the possible values for the attribute (specified in the ***Attribute*** field). Skylar One will compare the value in this field to the retrieved value for the ***Attribute***.
- ***Policy***. Choose one of the following:
    - *Do Not Authenticate*. If selected, if the retrieved value of the specified ***Attribute*** matches the value in the ***Value*** field, the user is not authenticated. This setting applies to new users for whom LDAP or Active Directory would have to create a new account in Skylar One and for users who already have an account in Skylar One.
    - *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", include 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 Skylar One using the Sales User Policy. User accounts from the NOC department would be imported into Skylar One using the NOC User Policy.
- To define additional ***Value*** and ***Policy*** fields, click on the plus-sign icon (+).

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

Creating an SSO Authentication Resource

The **SSO Auth Resource Editor** page allows you to define an authentication resource for use with a SAML IdP. An SSO authentication resource specifies the connector (communication software) to use to communicate with the SAML IdP and the URLs to use to send and retrieve information from the SAML IdP. An SSO authentication resource can also maps attributes from the user's SSO account to fields in the ScienceLogic user account.

ScienceLogic administrators can use SSO to authenticate ScienceLogic users. There are two ways to use SSO authentication with Skylar One:

- You can configure Skylar One to automatically create user accounts for existing SSO users and then always use SSO to authenticate those users when they log in to Skylar One.
- You can use SSO to authenticate one or more ScienceLogic users when they log in to Skylar One.

To create an SSO authentication resource:

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

   Basic Settings

   - ***Name***. Name of the SSO authentication resource.
   - ***IdP Entity ID***. Globally unique name used as a SAML identifier configured on the IdP, usually in the format of an absolute URL.
   - ***IdP Cert Fingerprint***. The SHA1 certificate fingerprint, provided by the identity provider or service provider. Note that this field is not the serial number of the certificate.

   > **NOTE:** If you supply the IdP certificate when you configure the SSO Authentication Resource, the IdP certificate fingerprint is not required and will not be used for IdP response validation. Instead, the full certificate that you provide in the ***IdP Certificate*** field will be used.

   - ***IdP Certificate***. To ensure that communication between the IdP and Skylar One is signed, type the full, PEM-encoded certificate from the IdP.
   - ***Sharing Permission***. Indicates if the authentication resource is shared or private. Choices are:
     - *Shared with all organizations*. The authentication resource is shared with users across all organizations.
     - *Private (visible to System organization only)*. The authentication resource is private to only user accounts assigned to the System organization.

   > **NOTE:** The ***Sharing Permission*** field displays only for Administrator user accounts and user accounts assigned to the System organization.

   - ***User Name Suffix***. Optional field. If you don't supply a value in this field, Skylar One retrieves the SAML ***NameID*** attribute and uses that value as the ScienceLogic username.
     - You can supply the variable ***%u*** in this field, and the Skylar One retrieves the SAML ***NameID*** attribute and uses that value as the ScienceLogic user name.
     - You can supply the value **%***attribute_name***%**, where attribute name is a SAML attribute other than ***NameID***. Skylar One will use the value of the attribute as the ScienceLogic user name.

- Because a user can authenticate against multiple SSO servers, there is a risk of collision among user names. In this field, you can enter a string to append to the ScienceLogic user name to minimize risk of collision. For example:
  - You can enter a string, with no SAML attribute specified. When you don't specify a SAML attribute in this field, Skylar Onewill retrieve the SAML ***NameID*** attribute and append the string you specify in this field.

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

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

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

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

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

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

    Skylar One will log in that user as ***krilly-external***.

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

- ***IdP SSO URL***. The URL to which Skylar One will send login requests to the IdP. This field must contain an absolute URL.
- ***IdP SLS URL***. Optional field. If you want each user to be automatically logged out of the IdP when that user logs out of Skylar One, enter the URL to which Skylar One will post the logout request to the IdP. If you leave this field blank, a user can log out of Skylar One without automatically logging out of the IdP.
- ***Sync directory values on login***. If an SSO administrator makes changes to an SSO account, Skylar One will automatically retrieve those updates and apply them to the user's account in the **Account Properties** page the next time the user logs in to Skylar One. (For more information about user account properties, see the ***Organizations & Users*** manual.)
- ***Signing Options***. Specifies whether digital signing is required for communication between the IdP and Skylar One. Choices are:
  - *Disable*. No digital signature is required.
  - *IdP Response*. Messages from the IDP to Skylar One must be signed. Skylar One will use the value in the ***IdP Certificate*** field to validate the signature.

- *SP Request and IdP Response*. Messages from the IDP to Skylar One must be signed. You can specify the signing algorithm in the ***Request Signature Algorithm*** field. Also, Skylar One will use the value in the ***IdP Certificate*** field to validate the signature. Messages from Skylar One to the IdP must also be signed.

- ***Request Signature Algorithm***. Select a signing algorithm for this resource. Your options include *RSA-SHA256*, *RSA-SHA384*, or *RSA-SHA512*. You must select *SP Request and IDP Response* in the ***Signing Options*** field to enable this field.
- ***Strict Mode***. If you selected *IdP Response* or *SP Request and IdP Response* in the Signing Options field, this field is automatically set to *enable*. This field enforces validation of the SAML response and its attributes. As a best practice, disable this field while initially configuring Skylar One and the IdP. As a best practice, enable this field for production use.
- ***Integrated Windows Auth***. If you are using Active Directory Federation Services (ADFS) as your IdP, select *Enable* in this field.

Attribute Mapping

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

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

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

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

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

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

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

<u>User Policy Alignment</u>

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

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

- ***Policy***. Specifies the user policy to use to automatically create a ScienceLogic account for each SSO user. Select from a list of all user policies.

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

- ***Attribute***. Specifies the SAML attribute you want to use to differentiate imported user accounts. For example, you could select the attribute *department* and then assign different user policies to import user accounts from different departments. You can also use this field to exclude SSO accounts for which you **do not want to allow authentication**.
- ***Value***. Specifies the SAML attribute value. That is, you specify one of the possible values for the attribute (specified in the ***Attribute*** field). Skylar One will compare the value in this field to

the retrieved value for the ***Attribute***.

- ***Policy***. Choose one of the following:
    - *Do Not Authenticate*. If the retrieved value of the specified ***Attribute*** matches the value in the ***Value*** field, the user is not authenticated. This setting applies to new users for whom SSO would have to create a new account in Skylar One and for users who already have an account in Skylar One.
    - *the policy you want to associate with that value*. Select from a list of all user policies that specify *SSO* 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*.
        - You could then click on the plus-sign icon (+) and add another ***Value*** field and another ***Policy*** field.
        - In the next ***Value*** field, you could specify *NOC*. In the corresponding ***Policy*** field, you could specify *NOC User Policy*.
        - After defining these two ***Value*** fields and the corresponding ***Policy*** fields, user accounts from the *Sales* department would be imported into Skylar One using the *Sales User Policy*.
        - User accounts from the *NOC* department would be imported into Skylar One using the *NOC User Policy*.
- To define additional ***Value*** and ***Policy*** fields, click on the plus-sign icon (+).

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

Editing an Authentication Resource

The **Authentication Resource Manager** page allows you to edit an existing authentication resource. To do so:

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).
2. Find the authentication resource that you want to edit. Click its wrench icon (🔧).
    - For LDAP/AD Resources, the **LDAP/AD Auth Resource Editor** page appears. In this page, you can you can edit the values for one or more fields. For more information, see the *Creating an LDAP/AD Authentication Resource* section.

- For SSO Resources, SSO Auth Resource Editor page appears. In this page, you can you can edit the values for one or more fields. For more information, see the *Creating an SSO Authentication Resource* section.

3. Click the **[Save]** button to save your changes to the authentication resource.

Deleting an Authentication Resource

The **Authentication Resource Manager** page allows you to delete one or more authentication resources from Skylar One. To do so:

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).
2. Select the checkbox of each authentication resource that you want to delete.
3. Click the ***Select Actions*** menu (in the lower right), select *DELETE Authentication Resource*, and then click the **[Go]** button. The selected authentication resources will be deleted.

NOTE: You cannot delete the *Internal* authentication resource.

Relationship Between Profiles and Resources

Authentication profiles reference one or more authentication resources. During authentication, the platform evaluates the resources associated with a profile in sequence until authentication succeeds or all options are exhausted. This separation allows authentication behavior to be reused, extended, and modified without redefining individual integrations.

Chapter

3

Single Sign-On (SSO)

Overview

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

This chapter covers the following topics:

What is SSO? ... 34

SSO Terminology ... 34

How Can I Use SSO with Skylar One? ... 34

Importing User Accounts from Single Sign-On (SSO) ... 34

Using Single Sign-On (SSO) for Authentication Only ... 49

Creating an SSO Authentication Resource for Authenticating Users ... 51

Creating an Authentication Profile ... 54

Viewing Metadata ... 56

Using Your Own SSL Certificate ... 56

What is SSO?

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

SSO Terminology

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

How Can I Use SSO with Skylar One?

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

Importing User Accounts from Single Sign-On (SSO)

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

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

Prerequisites

When setting up SAML-based SSO accounts for Skylar One, you will need to configure several URLs in the SAML application on the Identity Provider (IdP) side, such as in Azure or Okta.

> **NOTE:** The terminology for these URLs might vary based on the IdP used.

At a minimum, you must provide the following URLs:

- Service Provider (SP) Entity ID (Audience URI): https://*<hostname_or_IP_of_Skylar_One_appliance>*/samlsp.em7?action=metadata
- SP Assertion Consumer Service (ACS) URL (Single sign-on URL): https://*<hostname_or_IP_of_Skylar_One_appliance>*/samlsp.em7?action=acs

If you want single logout capabilities, then you must also configure this URL:

- SP Single Logout Service (SLS) URL: https://*<hostname_or_IP_of_Skylar_One_appliance>*/samlsp.em7?action=sls

Required Tasks

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

1. *Create one or more user policies* that define account properties and privilege keys in the Skylar One for imported SSO users.
    - You can create more than one user policy for imported user accounts.
        - For example, suppose you want to import 100 user accounts. But suppose not all of these users require access to the same parts of Skylar One. You could define multiple user policies, each defining a unique set of ticket queue-memberships, organization memberships, and Access Keys.
        - For example, you could define a user policy for imported user accounts from the Sales department, another user policy for imported user accounts from the Support department, and yet another user policy for imported user accounts from the NOC department.
    - Later, in the **SSO Auth Resource Editor** (System > Settings > Authentication > create/edit SSO Resource), you specify the user policy to apply to imported user accounts.
        - If you have created only one user policy for all imported accounts, you select the option for ***Static policy alignment*** and then select the single user policy.
        - If you have created multiple user policies for imported user accounts, you select the option for ***Dynamic policy alignment*** and then assign a user policy to each type of imported user.

2. *Define the SSO Authentication Resource*.

> **NOTE:** Skylar One supports SAML version 2.0.

- Specify how Skylar One should communicate with the SAML IdP and exchange information with the SAML IdP.
- Specify how Skylar One should map SSO attribute values to fields in the **Account Properties** page in Skylar One.
- Specifies whether Skylar One should remain synced with the SAML IdP. If an SSO administrator makes changes to an SSO account, Skylar One can automatically retrieve those updates and apply them to the user's account in Skylar One (in the **Account Properties** page) the next time the user logs in to Skylar One.
- In the ***Type*** field, specify one of the following:
  - *Static policy alignment.* All user accounts imported from SSO will use a ***single user policy***.
  - *Dynamic policy alignment*. You have created multiple user policies for imported SSO user accounts and do not want to use a single user policy for all imported user accounts.
- In the ***Policy*** field, if you selected *Static policy alignment* in the ***Type*** field, you must select a policy in the ***Policy*** field. All users who use the Authentication Resource will use this policy.
- In the ***Policy*** field, if you selected *Dynamic policy alignment* in the ***Type*** field, you must supply values in the ***Attribute***, ***Value***, and ***Policy*** fields:
  - In the ***Attribute*** field, specify the SAML attribute you want to use to differentiate imported user accounts. For example, you could select the attribute *department* and then assign different user policies to import user accounts from different departments.
  - In the ***Value*** field, specify the SAML attribute value. That is, you specify one of the possible values for the attribute (specified in the ***Attribute*** field).
  - In the corresponding ***Policy*** field, specify the policy you want to associate with that value. Select from a list of all user policies.
  - For example, suppose you specified *department* in the ***Attribute*** field. Suppose that the *department* attribute could have two possible values: *Sales* or *NOC*.
  - Suppose you created two user policies. One user policy, called *Sales User Policy*, includes the appropriate ticket queues and access keys for Sales personnel. Another user policy, called *NOC User Policy*, includes the appropriate ticket queues and access keys for NOC personnel.
  - In one of the ***Value*** fields, you could specify *Sales*. In the corresponding ***Policy*** field, you could then specify *Sales User Policy*.
  - You could then click on the plus-sign icon (+) and add another ***Value*** field and another ***Policy*** field.
  - In the next ***Value*** field, you could specify *NOC*. In the corresponding ***Policy*** field, you could specify *NOC User Policy*.

   - After defining these two ***Value*** fields and corresponding ***Policy*** fields, user accounts from the *Sales* department would be imported into Skylar One using the *Sales User Policy*.
   - User accounts from the *NOC* department would be imported into Skylar One using the *NOC User Policy*.
3. *Define one or more Authentication Profiles* that tell Skylar One how to recognize SSO users and which ***Authentication Resource*** to use with those users.
4. After completing these steps:
   - SSO users can attempt to connect to Skylar One by entering the URL for an page.
   - Skylar One will examine the hostname or IP address in the incoming URL request to align the user with an ***Authentication Profile***.
   - The ***Authentication Profile*** tells Skylar One which ***SSO Authentication Resource(s)*** to use to authenticate the user.
   - The ***SSO Authentication Resource*** tells Skylar One the settings to use to communicate with the SSO IdP. The SSO IdP will then attempt to authenticate each user.
   - Optionally, Skylar One will use the mappings and the user policy specified in the ***SSO Authentication Resource*** to create each user account.

Creating a User Policy for Imported Users

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

A user policy allows you to define:

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

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

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

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

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

Later, in the **SSO Auth Resource Editor** page (System > Settings > Authentication > create/edit SSO Resource), you specify the user policy to apply to imported user accounts. When doing this, you could tell Skylar One to examine the value of the attribute "department" to determine the department associated with each user account. You could then tell Skylar One 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 Skylar One. Choices are:
        - *Active*. Means user accounts created with this policy are active and can log in to Skylar One.
        - *Suspended*. Means that user accounts created with this policy are not active and cannot log in to Skylar One.

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

- ***Account Type***. This drop-down list contains an entry for each standard account type. These account types affect the list of Access Keys for the user. The choices are:
    - *Administrator.* By default, administrators are granted all permissions available in Skylar One. 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 Skylar One. These Access Keys are defined by the system administrator from the **Access Keys** page (System > Manage > Access Keys).
- ***Authentication Method***. You can select a value or leave this field blank.

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

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

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

Creating an SSO Authentication Resource for Importing Users

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

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

NOTE: Skylar One supports SAML version 2.0.

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

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

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

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

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

   Basic Settings

   - ***Name***. Name of the SSO authentication resource.
   - ***IdP Entity ID***. Globally unique name used as a SAML identifier configured on the IdP, usually in the format of an absolute URL.
   - ***IdP Cert Fingerprint***. The SHA1 certificate fingerprint, provided by the identity provider or service provider. Note that this field is not the serial number of the certificate.

   > **NOTE:** If you supply the IdP certificate when you configure the SSO Authentication Resource, the IdP certificate fingerprint is not required and will not be used for IdP response validation. Instead, the full certificate that you provide in the IdP Certificate field will be used.

   - ***IdP Certificate***. To ensure that communication between the IdP and Skylar One is signed, type the full, PEM-encoded certificate from the IdP.
   - ***User Name Suffix***. Optional field. If you don't supply a value in this field, Skylar One retrieves the SAML ***NameID*** attribute and uses that value as the ScienceLogic username.
     - You can supply the variable ***%u*** in this field, and the Skylar One retrieves the SAML ***NameID*** attribute and uses that value as the ScienceLogic user name.
     - You can supply the value **%***attribute_name***%**, where attribute name is a SAML attribute other than ***NameID***. Skylar One will use the value of the attribute as the ScienceLogic user name.

- Because a user can authenticate against multiple SSO servers, there is a risk of collision among user names. In this field, you can enter a string to append to the ScienceLogic user name to minimize risk of collision. For example:
    - You can enter a string, with no SAML attribute specified. When you don't specify a SAML attribute in this field, Skylar Onewill retrieve the SAML ***NameID*** attribute and append the string you specify in this field.

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

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

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

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

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

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

      Skylar One will log in that user as ***krilly-external***.

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

- ***IdP SSO URL***. The URL to which Skylar One will send login requests to the IdP. This field must contain an absolute URL.
- ***IdP SLS URL***. Optional field. If you want each user to be automatically logged out of the IdP when that user logs out of Skylar One, enter the URL to which Skylar One will post the logout request to the IdP. If you leave this field blank, a user can log out of Skylar One without automatically logging out of the IdP.
- ***Sync directory values on login***. If an SSO administrator makes changes to an SSO account, Skylar One will automatically retrieve those updates and apply them to the user's account in the **Account Properties** page the next time the user logs in to Skylar One. (For more information about user account properties, see the ***Organizations & Users*** manual.)
- ***Signing Options***. Specifies whether digital signing is required for communication between the IdP and Skylar One. Choices are:
    - *Disable*. No digital signature is required.
    - *IdP Response*. Messages from the IDP to Skylar One must be signed. Skylar One will use the value in the ***IdP Certificate*** field to validate the signature.

  - *SP Request and IdP Response*. Messages from the IDP to Skylar One must be signed. You can specify the signing algorithm in the ***Request Signature Algorithm*** field. Also, Skylar One will use the value in the ***IdP Certificate*** field to validate the signature. Messages from Skylar One to the IdP must also be signed.
- ***Request Signature Algorithm***. Select a signing algorithm for this resource. Your options include *RSA-SHA256*, *RSA-SHA384*, or *RSA-SHA512*. You must select *SP Request and IDP Response* in the ***Signing Options*** field to enable this field.
- ***Strict Mode***. If you selected *IdP Response* or *SP Request and IdP Response* in the Signing Options field, this field is automatically set to *enable*. This field enforces validation of the SAML response and its attributes. As a best practice, disable this field while initially configuring Skylar One and the IdP. As a best practice, enable this field for production use.
- ***Integrated Windows Auth***. If you are using Active Directory Federation Services (ADFS) as your IdP, select *Enable* in this field.

Attribute Mapping

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

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

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

> **NOTE:** Depending on the identity provider (IdP) you are using, you might need to enter the complete URL shown in the SAML trace for the fields below. Attribute names are provided by the IdP, so the default ones might not work in all cases.

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

- ***Phone***. Specifies the SAML attribute value that will be automatically inserted into the ***Phone*** field in each user's **Account Properties** page. By default, Skylar One inserts the value of the SAML attribute "telephonenumber" into this field.
- ***Fax***. Specifies the SAML attribute value that will be automatically inserted into the ***Fax*** field in each user's **Account Properties** page.
- ***Mobile***. Specifies the SAML attribute value that will be automatically inserted into the ***Mobile*** field in each user's **Account Properties** page. By default, Skylar One inserts the value of the SAML attribute "mobile" into this field.
- ***Pager***. Specifies the SAML attribute value that will be automatically inserted into the ***Pager*** field in each user's **Account Properties** page.
- ***MFA User***. Specifies the SAML attribute value that will be automatically inserted into the ***MFA User*** field in each user's **Account Permissions** page.

> NOTE: : Best practice for SSO includes multi-factor authentication when connecting to the Identity Provider, not when logging in to Skylar One. For details on configuring multi-factor authentication, see the section on *using multi-factor authentication*.

- ***Primary Email***. Specifies the SAML attribute value that will be automatically inserted into the ***Primary Email*** field in each user's **Account Properties** page. By default, Skylar One inserts the value of the SAML attribute "mail" into this field.
- ***Secondary Email***. Specifies the SAML attribute value that will be automatically inserted into the ***Secondary Email*** field in each user's **Account Properties** page.
- ***Street Address***. Specifies the SAML attribute value that will be automatically inserted into the ***Street Address*** field in each user's **Account Properties** page. By default, Skylar One inserts the value of the SAML attribute "streetaddress" into this field.
- ***Suite/Building***. Specifies the SAML attribute value that will be automatically inserted into the ***Suite/Building*** field in each user's **Account Properties** page.
- ***City***. Specifies the SAML attribute value that will be automatically inserted into the ***City*** field in each user's **Account Properties** page. By default, Skylar One inserts the value of the SAML attribute "l" into this field.
- ***State***. Specifies the SAML attribute value that will be automatically inserted into the ***State*** field in each user's **Account Properties** page. By default, Skylar One inserts the value of the SAML attribute "st" into this field.
- ***Postal Code***. Specifies the SAML attribute value that will be automatically inserted into the ***Postal Code*** field in each user's **Account Properties** page. By default, Skylar One inserts the value of the SAML attribute "postalcode" into this field.
- ***Country***. Specifies the SAML attribute value that will be automatically inserted into the ***Country*** field in each user's **Account Properties** page.

- ***Organization***. Specifies the SAML attribute value that will be used to automatically define the ***Primary Organization*** field in each user's **Account Permissions** page. You must also specify one of the following:

    - *directory attribute specifies organization ID*. The attribute in the ***Organization*** field specifies an organization ID.
    - *directory attribute specifies organization name*. The attribute in the ***Organization*** field specifies an organization name.
    - *directory attribute specifies organization CRM ID*. The attribute in the ***Organization*** field specifies the CRM ID of an organization.

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

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

User Policy Alignment

- ***Type***. Specifies whether Skylar One should automatically create ScienceLogic accounts for each SSO user, whether Skylar One should simply use SSO to authenticate one or more users, or whether Skylar One will refuse to authenticate specific users. Choices are:

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

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

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

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

- ***Attribute***. If you selected a ***Type*** of *Dynamic policy alignment*, this field specifies the SAML attribute you want to use to differentiate imported user accounts. For example, you could select the attribute *department* and then assign different user policies to import user accounts from different departments. You can also use this field to exclude SSO accounts for which you **do not want to allow authentication**.
- ***Value***. If you selected a ***Type*** of *Dynamic policy alignment*, this field specifies the SAML attribute value. That is, you specify one of the possible values for the attribute (specified in the ***Attribute*** field). Skylar One will compare the value in this field to the retrieved value for the ***Attribute***.
- ***Policy***. If you selected a ***Type*** of *Dynamic policy alignment*, this field specifies *the policy you want to associate with the attribute/value pair*. Select from a list of all user policies.
    - For example, suppose you specified *department* in the ***Attribute*** field. Suppose that the *department* attribute could have two possible values: *Sales* or *NOC*.
    - Suppose you created two user policies. One user policy, called *Sales User Policy*, includes the appropriate ticket queues and access keys for Sales personnel. Another user policy, called *NOC User Policy*, includes the appropriate ticket queues and access keys for NOC personnel.
    - In one of the ***Value*** fields, you could specify *Sales*. In the corresponding ***Policy*** field, you could then specify *Sales User Policy*.
    - You could then click on the plus-sign icon (+) and add another ***Value*** field and another ***Policy*** field.
    - In the next ***Value*** field, you could specify *NOC*. In the corresponding ***Policy*** field, you could specify *NOC User Policy*.
    - After defining these two ***Value*** fields and the corresponding ***Policy*** fields, user accounts from the *Sales* department would be imported into Skylar One using the *Sales User Policy*.
    - User accounts from the *NOC* department would be imported into Skylar One using the *NOC User Policy*.

- *Do Not Authenticate*. If the retrieved value of the specified ***Attribute*** matches the value in the ***Value*** field, the user is not authenticated. This setting applies to new users for whom SSO would have to create a new account in Skylar One and for users who already have an account in Skylar One.
  - In the ***Attribute*** field, you could also specify *status*. Suppose that the ***status*** attribute could have two possible values: *active* or *terminated*.
  - In the next ***Value*** field, you could specify *terminated*. In the corresponding ***Policy*** field, you could specify *Do Not Authenticate*.
  - Whenever an LDAP or AD entry for a user included the ***status*** attribute with the value *terminated*, Skylar One could apply the policy ***Do Not authenticate***.
- To define additional ***Value*** and ***Policy*** fields, click on the plus-sign icon (+).

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

Creating an Authentication Profile

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

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

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

1. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).
2. In the **Authentication Profiles** page, click the **[Create]** button.
3. The **Authentication Profile Editor** modal page appears. In this page, you can define the new authentication profile.
   - ***Name***. Name of the Authentication Profile.
   - ***Priority Order***. If Skylar One includes multiple Authentication Profiles, Skylar One evaluates the Authentication Profiles in priority order, ascending. Skylar One will apply the first Authentication Profile that matches the Hostname or IP in the current URL **AND** has the lowest value in the ***Priority Order*** field.
   - ***Pattern Type***. Specifies how Skylar One will evaluate the value in the ***AP Hostname Pattern*** field. Choices are:

- *Wildcard*. Skylar One will perform a text match, with wildcard characters (asterisks).
- *Regex*. Skylar One 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, Skylar One applies the Authentication Profile to the user for the current session.
  - For example, if you specify "*" (asterisk), any IP address or URL will match. Skylar One 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", Skylar One 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”, Skylar One 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.

> **NOTE:** Do not include underscores (_) in the ***AP Hostname Pattern*** field. URLs with underscores are not considered valid in Skylar One authentication profiles.

- ***Available Credential Sources***. This field tells Skylar One how to retrieve the user's credentials from the HTTP request to Skylar One. To align a credential source with the Authentication Profile, highlight the credential source and click the right-arrow button. You can select zero, one, or multiple credential sources for the Authentication Profile. Initially, this pane displays a list of all the credential sources:
  - *CAC/Client Cert*. Skylar One will retrieve a certificate from the HTTP request.
  - *Login Page*. Skylar One will retrieve a username and password from Skylar One login page fields.
  - *HTTP Auth*. Skylar One will retrieve a username and password from the HTTP request.
- ***Aligned Credentials Sources***. This field displays the list of credential sources that have been aligned with the Authentication Profile. The Authentication Profile will examine each credential source in the order in which it appears in this list. When the Authentication Profile finds the user's credential, the Authentication Profile stops examining any remaining credential sources in the list.
- ***Available Authentication Resources***.This field tells Skylar One which Authentication Resources to use to authenticate the retrieved credentials. To align an Authentication Resource with the Authentication Profile, highlight the Authentication Resource and click the right-arrow button. You must select at least one Authentication Resource and can select more than one.

- ***Aligned Authentication Resources***. This field displays the list of Authentication Resources that have been aligned with the Authentication Profile. The Authentication Profile will examine each Authentication Resource in the order in which it appears in this list. When an Authentication Resource successfully authenticates the user, the Authentication Profile stops executing any remaining Authentication Resources in the list.
- ***Available Multi-factor Resources***. This field tells Skylar One which Multi-factor Resources to use to perform multi-factor authentication. To align an Multi-factor Resource with the Authentication Profile, highlight the Multi-factor Resource and select the right-arrow button. For details on creating a Multi-factor Resource, see the guide for the Multi-factor Resource Editor.
- ***Aligned Multi-factor Resources***. This field displays the list of Multi-factor Resources that have been aligned with the Authentication Profile. The Authentication Profile will examine each Multi-factor Resources in the order in which it appears in this list. When a Multi-factor Resources successfully authenticates the user, the Authentication Profile stops executing any remaining Multi-factor Resources in the list.

NOTE: Best practice for SSO includes multi-factor authentication when connecting to the Identity Provider, not when logging in to Skylar One. For details on configuring multi-factor authentication, see the section on *using multi-factor authentication*.

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

Viewing Metadata

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

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

Using a Self-Signed SSL Certificate

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

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

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

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

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

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

6. Save and quit the file.

Using Single Sign-On (SSO) for Authentication Only

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

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

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

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

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

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

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

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

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, click the **[Create]** button.
3. The **Create New Account** page appears.
4. In the **Create New Account** page, enter values in each of the following fields:
    - ***First Name***. User's first name. This value can be up to 24 characters in length.
    - ***Last Name***. User's last name. This value can be up to 24 characters in length.
    - ***Generate name based on first and last name***. **Do not select this option**.
    - ***Account Login Name*** The same value as is stored in the SAML attribute ***uid***.
    - ***Primary Email***. User's email address. This field can be up to 64 characters in length.
    - ***Password***. You can any password that meets the minimum security requirements. The password must be at least four characters in length and can be up to 64 characters in length.

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

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

> **NOTE**: Best practice for SSO includes multi-factor authentication when connecting to the Identity Provider, not when logging in to Skylar One. For details on configuring multi-factor authentication, see the section on *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 Skylar One.
- ***Account Type***. Specifies whether the user is a member of a user policy. Choices are:

    - *Individual*. User account is not a member of a user policy.
    - *Policy Membership*. **Select this option**. User will be defined with a user policy. When selected, the *Policy Membership* field becomes active.

    After you select *Policy Membership*, all remaining fields except ***Account Templates*** are disabled. This is because those fields are defined in the user policy.

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

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

Creating an SSO Authentication Resource for Authenticating Users

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

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

NOTE: Skylar One supports SAML version 2.0.

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

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

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

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

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

2. Click the **[Actions]** menu and then select *Create SSO Resource*. The **SSO Auth Resource Editor** page appears.
3. Enter values in the following fields:

Basic Settings

- ***Name***. Name of the SSO authentication resource.
- ***IdP Entity ID***. Globally unique name used as a SAML identifier configured on the IdP, usually in the format of an absolute URL.
- ***IdP Cert Fingerprint***. The SHA1 certificate fingerprint, provided by the identity provider or service provider. Note that this field is not the serial number of the certificate.

> **NOTE:** If you supply the IdP certificate when you configure the SSO Authentication Resource, the IdP certificate fingerprint is not required and will not be used for IdP response validation. Instead, the full certificate that you provide in the IdP Certificate field will be used.

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

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

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

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

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

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

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

Skylar One will log in that user as ***krilly-external***.

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

- ***IdP SSO URL***. The URL to which Skylar One will send login requests to the IdP. This field must contain an absolute URL.
- ***IdP SLS URL***. Optional field. If you want each user to be automatically logged out of the IdP when that user logs out of Skylar One, enter the URL to which Skylar One will post the logout request to the IdP. If you leave this field blank, a user can log out of Skylar One without automatically logging out of the IdP.
- ***Sync directory values on login***. If an SSO administrator makes changes to an SSO account, Skylar One will automatically retrieve those updates and apply them to the user's account in the **Account Properties** page the next time the user logs in to Skylar One. (For more information about user account properties, see the ***Organizations & Users*** manual.)
- ***Signing Options***. Specifies whether digital signing is required for communication between the IdP and Skylar One. Choices are:
  - *Disable*. No digital signature is required.
  - *IdP Response*. Messages from the IDP to Skylar One must be signed. Skylar One will use the value in the ***IdP Certificate*** field to validate the signature.
  - *SP Request and IdP Response*. Messages from the IDP to Skylar One must be signed. You can specify the signing algorithm in the ***Request Signature Algorithm*** field. Also, Skylar One will use the value in the ***IdP Certificate*** field to validate the signature. Messages from Skylar One to the IdP must also be signed.
- ***Request Signature Algorithm***. Select a signing algorithm for this resource. Your options include *RSA-SHA256*, *RSA-SHA384*, or *RSA-SHA512*. You must select *SP Request and IDP Response* in the ***Signing Options*** field to enable this field.
- ***Strict Mode***. If you selected *IdP Response* or *SP Request and IdP Response* in the Signing Options field, this field is automatically set to *enable*. This field enforces validation of the SAML response and its attributes. As a best practice, disable this field while initially configuring Skylar One and the IdP. As a best practice, enable this field for production use.
- ***Integrated Windows Auth***. If you are using Active Directory Federation Services (ADFS) as your IdP, select *Enable* in this field.

Attribute Mapping

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

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

User Policy Alignment

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

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

Creating an Authentication Profile

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

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

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

1. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).
2. In the **Authentication Profiles** page, click the **[Create]** button.
3. The **Authentication Profile Editor** modal page appears. In this page, you can define the new authentication profile.
   - ***Name***. Name of the Authentication Profile.
   - ***Priority Order***. If Skylar One includes multiple Authentication Profiles, Skylar One evaluates the Authentication Profiles in priority order, ascending. Skylar One will apply the first Authentication Profile that matches the Hostname or IP in the current URL **AND** has the lowest value in the ***Priority Order*** field.
   - ***Pattern Type***. Specifies how Skylar One will evaluate the value in the ***AP Hostname Pattern*** field. Choices are:
     - *Wildcard*. Skylar One will perform a text match, with wildcard characters (asterisks).
     - *Regex*. Skylar One 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, Skylar One applies the Authentication Profile to the user for the current session.

   - For example, if you specify "*" (asterisk), any IP address or URL will match. Skylar One 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", Skylar One 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”, Skylar One 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.

   > **NOTE:** Do not include underscores (_) in the ***AP Hostname Pattern*** field. URLs with underscores are not considered valid in Skylar One authentication profiles.

- ***Available Credential Sources***. This field tells Skylar One how to retrieve the user's credentials from the HTTP request to Skylar One. To align a credential source with the Authentication Profile, highlight the credential source and click the right-arrow button. You can select zero, one, or multiple credential sources for the Authentication Profile. Initially, this pane displays a list of all the credential sources:
   - *CAC/Client Cert*. Skylar One will retrieve a certificate from the HTTP request.
   - *Login Page*. Skylar One will retrieve a username and password from the Skylar One login page fields.
   - *HTTP Auth*. Skylar One will retrieve a username and password from the HTTP request.
- ***Aligned Credentials Sources***. This field displays the list of credential sources that have been aligned with the Authentication Profile. The Authentication Profile will examine each credential source in the order in which it appears in this list. When the Authentication Profile finds the user's credential, the Authentication Profile stops examining any remaining credential sources in the list.
- ***Available Authentication Resources***.This field tells Skylar One which Authentication Resources to use to authenticate the retrieved credentials. To align an Authentication Resource with the Authentication Profile, highlight the Authentication Resource and click the right-arrow button. You must select at least one Authentication Resource and can select more than one.
- ***Aligned Authentication Resources***. This field displays the list of Authentication Resources that have been aligned with the Authentication Profile. The Authentication Profile will examine each Authentication Resource in the order in which it appears in this list. When an Authentication Resource successfully authenticates the user, the Authentication Profile stops executing any remaining Authentication Resources in the list.

- ***Available Multi-factor Resources***. This field tells Skylar One which Multi-factor Resources to use to perform multi-factor authentication. To align an Multi-factor Resource with the Authentication Profile, highlight the Multi-factor Resource and select the right-arrow button. For details on creating a Multi-factor Resource, see the guide for the Multi-factor Resource Editor.
- ***Aligned Multi-factor Resources***. This field displays the list of Multi-factor Resources that have been aligned with the Authentication Profile. The Authentication Profile will examine each Multi-factor Resources in the order in which it appears in this list. When a Multi-factor Resources successfully authenticates the user, the Authentication Profile stops executing any remaining Multi-factor Resources in the list.

> **NOTE**: Best practice for SSO includes multi-factor authentication when connecting to the Identity Provider, not when logging in to Skylar One. For details on configuring multi-factor authentication, see the section on *using multi-factor authentication*.

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

Viewing Metadata

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

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

Using Your Own SSL Certificate

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

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

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

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

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

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

6. Save and quit the file.

Chapter

4

Multi-Factor Authentication

Overview

This chapter explains how to configure your Skylar One systems to use RSA SecurID for multi-factor authentication during login to Skylar One.

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

This chapter covers the following topics:

What is Multi-Factor Authentication? 58

Configuring Multi-Factor Authentication 59

What is Multi-Factor Authentication?

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

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

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

Configuring Multi-Factor Authentication

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

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

Caveats

- ***Default User Interface (AP2)***. You currently cannot use multi-factor authentication with the default user interface (AP2).
- ***API***. You currently cannot use multi-factor authentication with the ScienceLogic API.
- ***SSO***. Best practice for Single Sign-On (SSO) includes multi-factor authentication when connecting to the Identity Provider, not when logging in to Skylar One. This chapter does not describe how to configure SSO authentication and multi-factor authentication during login to Skylar One.

Prerequisites

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

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

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

Configuration Steps

To configure multi-factor authentication:

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

Defining a Multi-factor Resource

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

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

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

1. Go to the **Multi-factor Resource Manager** page System > Settings > Authentication > Multi-factor.
2. In the **Multi-factor Resource Manager** page, select the**[Actions]** menu and then select the following:
    - ***Create RSA Resource***. The **Multi-Factor Resource Editor** page appears.
3. In the **Multi-Factor Resource Editor** page, you can define the new Multi-factor Resource.
4. In the **Multi-Factor Resource Editor** page, supply values in the following fields:
    - ***Name***. Enter the name of the Multi-Factor Resource.
    - ***WEB Agent ID***. Enter the IP address or hostname of the Agent registered with RSA.
    - ***Access Key***. Enter the Access Key for the RSA SecurID endpoint.
    - ***User Name Suffix***. Enter a suffix that will be applied to all user names before submitting them to RSA SecurID for authentication.
        - If you have not specified a a value in the ***Multi-factor Auth (MFA) User*** field in either the **Create New Account** page (Registry > Accounts > User Accounts > Create button)or the **Account Permissions** page (Registry > Accounts > User Accounts > edit user account), the value in the ***User Name Suffix*** field will be appended to the value in the ***Account Login Name*** field in either the **Create New Account** page or the **Account Permissions** page.
        - If you have specified a a value in the ***Multi-factor Auth (MFA) User*** field in either the **Create New Account** page (Registry > Accounts > User Accounts > Create button)or the **Account Permissions** page (Registry > Accounts > User Accounts > edit user account), the value in the ***User Name Suffix*** field will be appended to the value in the he ***Multi-factor Auth (MFA) User*** field in either the **Create New Account** page or the **Account Permissions** page.

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

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

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

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

Creating or Editing an Authentication Profile

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

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

NOTE: Skylar One supports SAML version 2.0.

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

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

Creating an Authentication Profile for Local Authentication

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

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

- ***Multi-Factor Auth (MFA) User***. Optional. If this user requires a different user name for Multi-factor authentication, enter the MFA user name in this field.
- ***Authentication Method***. Specifies how the user's user name and password will be authenticated. Select *local*. The user name and password are authenticated by the database in Skylar One.

3. Create an authentication profile for the user. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).
4. In the **Authentication Profiles** page, click the **[Create]** button. The Authentication Profile Editor modal page appears.
5. Enter values in the following fields:
   - ***Name***. Name of the Authentication Profile.
   - ***Priority Order***. If your Skylar One system includes multiple Authentication Profiles, Skylar One evaluates the Authentication Profiles in priority order, ascending. Skylar One 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 Skylar One will evaluate the value in the ***AP Hostname Pattern*** field. Choices are:
     - *Wildcard*. Skylar One will perform a text match, with wildcard characters (asterisks).
     - *Regex*. Skylar One 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, Skylar One applies the Authentication Profile to the user for the current session.

     For example, if you specify "*" (asterisk), any IP address or URL will match. Skylar One 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", Skylar One will apply the Authentication Profile to each session on an Administration Portal, Database Server, or All-In-One Appliances where the user enters "192.168.38.235" into the browser.

     If you enter "*.sciencelogic.local", Skylar One 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.

NOTE: Do not include underscores (_) in the ***AP Hostname Pattern*** field. URLs with underscores are not considered valid in Skylar One authentication profiles.

   - ***Available Credential Sources***. This field tells Skylar One how to retrieve the user's credentials from the HTTP request to Skylar One. To align a Credential Source with the Authentication profile, highlight the credential source and click the right-arrow button. You can select zero, one, or multiple credential sources for the Authentication Profile. Initially, this pane displays a list of all the credential sources:

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

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

Creating an Authentication Profile for Active Directory or LDAP

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

1. Create a user account or user policy for Active Directory or LDAP users.For details on creating a user account or user policy for use with Actve Directory or LDAP, see the ***Directory-Based Authentication (Active Directory and LDAP)*** chapter.
2. In either the **Create New Account** page or the Account Permissions page (Registry > Accounts > User Accounts), inspect the following fields:
    - ***Multi-Factor Auth (MFA) User***. Optional. If this user requires a different user name for Multi-factor authentication, enter the MFA user name in this field.

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

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

3. Define a credential that allows Skylar One to communicate with Active Directory or LDAP. For details, see the ***Directory-Based Authentication (Active Directory and LDAP)*** chapter.
4. Define an Authentication Resource for Active Directory or LDAP. For details, see the ***Directory-Based Authentication (Active Directory and LDAP)*** chapter.
5. Define an Authentication Profile for Active Directory or LDAP. For details, see the ***Directory-Based Authentication (Active Directory and LDAP)*** chapter.
6. Either while defining an Authentication Profile for Active Directory or LDAP or editing an existing Authentication Profile for Active Directory or LDAP, edit the following fields:
   - ***Available Multi-factor Resources***. This field tells Skylar One which Multi-factor Resources to use to perform multi-factor authentication. To align an Multi-factor Resource with the Authentication Profile, highlight the Multi-factor Resource and click the right-arrow button. *Select the Multi-Factor Resource you created earlier* in this chapter.
   - ***Aligned Multi-factor Resources***. This field displays the list of Multi-factor Resources that have been aligned with the Authentication Profile. The Authentication Profile will examine each Multi-factor Resources in the order in which it appears in this list. When a Multi-factor Resource successfully authenticates the user, the Authentication Profile stops executing any remaining Multi-factor Resources in the list.
   - **Save**. Saves a new Authentication Profile or changes to an existing Authentication Profile.
7. Users that are authenticated with Active Directory or LDAP will now also be prompted to enter their RSA SecurID token during login.

Chapter

5

Directory-Based Authentication (Active Directory and LDAP)

Overview

This chapter is intended for administrators who create and manage user accounts. This chapter assumes that you are familiar with LDAP (Lightweight Directory Access Protocol) 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 chapter.

This chapter covers the following topics:

What is LDAP? 66

What is Active Directory? 66

LDAP and Active Directory Terminology 66

How Can I Use LDAP or Active Directory with Skylar One? 68

How Can I View My Company's Active Directory or LDAP? 70

Importing User Accounts from Active Directory or LDAP 71

NOTE: If you are not familiar with these technologies, you may need to work with your organization's directory services, identity management, or security administrators to complete the tasks described in this manual.

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 Skylar One 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 Skylar One, 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 Skylar One.
- ***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 Skylar One?

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

1. You can configure Skylar One to ***automatically create user accounts in Skylar One*** 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 Skylar One.
   - Each user logs in to Skylar One, either through the login page, a CAC card or certificate, or HTTP. The user logs in to Skylar One using an LDAP or AD attribute value as a login name and the LDAP or AD password.
   - Skylar One examines the login request and applies the appropriate Authentication Profile (and the appropriate Authentication Resource).
   - Skylar One then authenticates the user by communicating with the LDAP or Active Directory server.
   - Skylar One then creates a ScienceLogic account for the user, using both the mappings defined in the Authentication Resource and a ScienceLogic user policy.
   - Skylar One displays the default page in Skylar One.
2. You can use LDAP or Active Directory to authenticate one or more users when they log in to Skylar One. You can also specify that Skylar One won't authenticate other LDAP or Active Directory users.
   - Each user logs in to Skylar One, either through the login page, a CAC card or certificate, or HTTP. The user logs in to Skylar One using an LDAP or AD attribute value as a login name and the LDAP or AD password.
   - Skylar One examines the login request and applies the appropriate Authentication Profile (and the appropriate Authentication Resource(s)).
   - Skylar One then authenticates the user by communicating with the LDAP or Active Directory server.

LDAP Authentication Configurations

This section describes the various LDAP authentication configurations that are supported in Skylar One.

> CAUTION: If you are using an LDAP configuration other than one that is listed below, you should contact ScienceLogic Support or your Customer Success Manager to explain your use case. Non-supported configurations will be deprecated in a future release.

Configuration 1: Basic LDAP Authentication

- Configure an authentication profile that lists *Login Page* as the aligned credential source.
- The aligned authentication resource is associated with an LDAP/AD credential.
- It does not matter if the aligned LDAP/AD credential uses the %u or %e variables in its RDN string or if the RDN string is a defined value. If it is a defined value, it must also include a bind password.
- Optionally, an SSL certificate has been imported and installed if you are using LDAP over SSL.

> **NOTE:** You can log in through REST API using an LDAP configuration.

Configuration 2: LDAP Configuration for CAC Authentication

- Configure one authentication profile, for most uses:
  - The authentication profile lists *CAC/Client Cert* as the aligned credential source.
  - The aligned authentication resource is associated with an LDAP/AD credential.
  - The aligned LDAP/AD credential uses a defined RDN string with a bind password; it cannot use the %u or %e variables in its RDN string.
- Configure a second authentication profile for administrator or maintenance access:
  - The authentication profile lists *Login Page* as the aligned credential source.
  - The aligned authentication resource is the *Internal* resource.

> **NOTE:** You cannot log in through REST API using CAC authentication.

> **NOTE:** You cannot have both CAC and non-CAC LDAP users on the same Skylar One system.

> **NOTE:** To disable a user's CAC authentication access, remove the user from the LDAP/AD server.

Configuration 3: Multiple LDAP Authentication Resources Used in the Same Authentication Profile

- Configure an authentication profile that lists *Login Page* as the aligned credential source.
- The authentication profile lists multiple aligned authentication resources, all of which are associated with LDAP/AD credentials.
- It does not matter if the aligned LDAP/AD credentials use the %u or %e variables in their RDN strings or if the RDN strings are a defined value. If they are defined values, they must also include bind passwords.
- Optionally, an SSL certificate has been imported and installed if you are using LDAP over SSL.

Configuration 4: One LDAP Authentication Resource Used in Multiple Authentication Profiles

- Configure one authentication profile:
  - The authentication profile lists *Login Page* as the aligned credential source.
  - The aligned authentication resource is associated with an LDAP/AD credential.
  - It does not matter if the aligned LDAP/AD credential uses the %u or %e variables in its RDN string or if the RDN string is a defined value. If it is a defined value, it must also include a bind password.
  - Optionally, an SSL certificate has been imported and installed if you are using LDAP over SSL.
- Configure a second authentication profile:
  - The authentication profile lists *Login Page* as the aligned credential source.
  - The aligned authentication resource is same one used in the first authentication profile.

Configuration 5: Basic HTTP Authentication with LDAP

- Configure an authentication profile that lists *HTTP Auth* as the aligned credential source.
- The aligned authentication resource is associated with an LDAP/AD credential.
- It does not matter if the aligned LDAP/AD credential uses the %u or %e variables in its RDN string or if the RDN string is a defined value. If it is a defined value, it must also include a bind password.
- Optionally, an SSL certificate has been imported and installed if you are using LDAP over SSL.

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.

Importing User Accounts from Active Directory or LDAP

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

Each Active Directory or LDAP user logs in to Skylar One using his or her Active Directory or LDAP username and password, and Skylar One automatically creates an account for that user. Each subsequent time that user logs in to Skylar One, Skylar One will use Active Directory or LDAP to authenticate that user.

Chapter

6

CAC Authentication

Overview

This chapter describes how Skylar One (formerly SL1) supports Common Access Card (CAC) authentication. The **Client Certificate & CAC Authentication** page (System > Settings > Authentication > Admin SSL Certificates, or System > Settings > Authentication > SSL Certificates in the classic Skylar One user interface) allows you to define a check for SSL certificate that controls whether the login page is displayed to the end user.

This feature is primarily used to authenticate Common Access Card (CAC) users against a Department of Defense (DoD) issued server-side certificate; however, based on your business needs, this feature can also be used with your own client/server certificates.

> **NOTE:** You can use CAC authentication to log in to either the default Skylar One user interface ("AP2") or the classic Skylar One user interface. Follow the steps described in this chapter to configure your CAC authentication, regardless of which user interface you use.

> **NOTE:** Currently, Skylar One does not support client-side certificate authentication for login to the console, either through SSH or through a keyboard connected to the appliance.

This chapter covers the following topics:

Using CAC Authentication 74

Prerequisites 75

Importing SSL Certificates 76

Extracting the Common Name from a Certificate for Authentication 77
Defining the Client Certificate Chain 78
Verifying SSL Certificate File Import and Resolving Issues 80
Clearing the Skylar One Cache and Restarting NGINX 81
Testing the Configuration 81
Troubleshooting CAC Authentication 82
Accessing the Appliance without CAC Authentication 84
Special Circumstance: Multiple Levels of Intermediate Certificates 84

Using CAC Authentication

Skylar One supports CAC authentication. The **Client Certificate & CAC Authentication** page allows you to define a check for SSL certificate that controls whether the login page is displayed to the end user. This feature is primarily used to authenticate Common Access Card (CAC) users against a Department of Defense (DoD) issued server-side certificate; however, based on your business needs, this feature can also be used with your own client/server certificates.

The CAC is a United States DoD smartcard issued as standard identification for Active Duty Military personnel, reserve personnel, civilian employees, and eligible contractor personnel. A User Principal Name (UPN) is recommended, and in some instances required, when using CAC.

CAC provides applications with a more secure way to authenticate the identity of a user, application, or device. However, even if a user authenticates with a certificate, it does not mean that they user is authorized to access the requested data. For more information on authentication and authorization, see the DoD documentation on authentication and authorization for DoD web servers.

DoD has implemented an external interoperability strategy for secure information sharing with external partners. Some DoD industry partners have implemented corporate PKIs, and others have obtained certificates from approved commercial PKIs. Some DoD international allied and coalition partners also have established PKIs to issue certificates to their personnel. Systems and applications with user populations that hold approved external credentials should be configured to accept those credentials rather than requiring the users to obtain Common Access Cards (CACs) or External Certification Authority (ECA) certificates. For the complete list of DoD approved external PKIs and interoperability tools, see the DoD documentation on interoperarability.

DoD policy requires that external credentials have an assurance level of medium hardware or higher, so systems accepting external credentials must have an assurance level enforcement capability. Depending on technology, this can be accomplished through use of the Interoperability Root CAs (IRCAs) or implementation of a local certificate policy object identifier (OID) filtering solution such as the DoD PKE Trust Anchor Constraints Tools (TACT). For a complete list of approved partner OIDs, see the DoD documentation on the approved assurance levels from external partner PKIs.

Systems and applications typically have configuration properties that control security settings related to PKI functionality. Security settings should be configured to support all desired PKI functions and comply with DoD authentication policy.

Skylar One allows you to configure appliances that provide the user interface (Administration Portal, All-In-One Appliance, or the Database Server) for use with DoD certificates or your own certificates.

The CAC is used as the user's authentication to Skylar One. If the Authentication Profile (System > Settings > Authentication > Profiles) contains both the "CAC/Client Cert" and "Login Page" credential sources *and* a CAC is not presented or is invalid, then the ScienceLogic login page is presented to the end user.

NOTE: You can use CAC authentication to log in to either the default Skylar One user interface ("AP2") or the classic Skylar One user interface. Follow the steps described in this chapter to configure your CAC authentication, regardless of which user interface you use.

NOTE: Currently, Skylar One does not support client-side certificate authentication for login to the console, either through SSH or through a keyboard connected to the appliance.

Prerequisites

To use client certificate authentication with Skylar One, you must first meet the following requirements:

1. Organizations must be created and configured. For more information, see "Creating and Editing Organizations" in the ***Organizations and Users*** manual.
2. An LDAP or AD Credential must be configured with a Service Account that has the appropriate permissions to query AD, typically read access.
3. Create one or more User Policies if you will use Skylar One authentication. You do not need to configure user policies if you are using Active Directory (AD) or LDAP. For more information, see "Creating a User Policy" in the ***Organizations and Users*** manual.
4. If you are using LDAP or Active Directory as your user store, you must configure this as your Authentication Resource before setting up your Authentication Profile. For more information, see *Authentication Resources*.
5. Configure an Authentication Profile for CAC authentication. When setting up your Authentication Profile for CAC, align the "CAC/Client Cert" credential with the profile as the first credential source. You can align the Login Page as a secondary credential source for administrator access, but this is not required. For more information, see *Creating an Authentication Profile*.
6. Configure an emergency account ("break glass" account) for the Database Server. Because CAC will work only with the Database Server's DNS name, an emergency account ensures that the em7admin account is used only as a last resort.
7. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles). Select the wrench icon ( ) for the default profile. In the **Authentication Profile Editor** page, in the ***Aligned Credential Sources*** field, delete any existing CAC/Client Cert credentials.
8. Your users must have either:
   - Valid CACs with valid client-side certificates already loaded onto the cards, or
   - Valid client-side certificates installed in their web browser.
9. If CACs are used, the browser through which the user logs on to the user interface must be able to read security certificates from the cards.
10. The Administration Portal, All-In-One Appliance, or the Database Server will request a certificate from the CAC or client web server only when the appliance uses HTTPS. In Skylar One 12.2.0 and above, the use of HTTPS is enforced by default. In Skylar One versions prior to 12.2.0, you must go to the **Behavior Settings** page (System > Settings > Behavior), and select the ***Force Secure HTTPS*** setting checkbox.

> **NOTE:** In Skylar One 12.2.0 and above, the ***Force Secure HTTPS*** setting does not appear as an option on the **Behavior Settings** page.

11. On the **SSL Certificates** page (System > Settings > Authentication > Admin SSL Certificates, or System > Settings > Authentication > SSL Certificates in the classic Skylar One user interface), you must install the certificate chain in PEM format on the Administration Portal, All-In-One Appliance, or the Database Server. A certificate chain usually includes a root CA certificate and an intermediate certificate. Your organization might require multiple intermediate certificates to provide access to all users. To learn more about importing a certificate, see the section *Importing an SSL Certificate*.

> **NOTE:** If you want to extract part of the Common Name to customize the username that is displayed in Skylar One after CAC authentication, you can edit the ScienceLogic configuration file to customize the displayed username. You do not need to do this if you are using the msUPN. For more information, see *Extracting the Common Name from a Certificate for Authentication*.

12. In the **Client Certificate & CAC Authentication** page (System > Settings > Authentication > CAC Client Cert Auth, or System > Settings > Authentication > CAC/ClientCert Auth in the classic Skylar One user interface), you must configure the server-side certificate and test it against your client-side certificate. For more information, see *Defining the Client Certificate Chain*.

Importing SSL Certificates

Secure Sockets Layer, or SSL, is a protocol for securely transmitting data via the Internet. SSL uses a private key to encrypt data to be transferred over an Internet connection. In Skylar One, you can import server-side SSL certificate files, including DoD certificate files used in CAC authentication, to the Administration Portal, All-In-One Appliance, or the Database Server.

Note the following:

- You must have one root certificate and one certificate for each intermediate authority in the client certificate chain. If you have users with CACs issued by different intermediate authorities, you must import SSL certificates for all possible client authentication chains into Skylar One.
- All SSL certificates must be in PEM format.
- You can test your SSL certificate files by using the following command, where <certificate_file_ name> is the full name of the certificate file:

```
openssl x509 -text -noout -in <certificate_file_name>
```

> **TIP:** It is a best practice to check each certificate file before attempting to import the file. If you encounter an error, resolve that error before you continue.

To import an SSL certificate for CAC authentication:

1. Go to the **SSL Certificates** page (System > Settings > Authentication > Admin SSL Certificates, or System > Settings > Authentication > SSL Certificates in the classic Skylar One user interface).
2. In the **SSL Certificates** page, click the **[Actions]** menu. Select ***Import PEM Certificate File***. The **Import Certificate File (PEM format)** modal appears.
3. In the **Import Certificate File (PEM format)** modal, enter the following:
    - ***Description***. Description of the certificate.
    - ***CA File***. Browse for the server-side certificate file on your local computer.
4. Click the **[Save]** button to load the certificate to the Administration Portal, All-In-One Appliance, or the Database Server.
5. Repeat these steps for each certificate file you want to import. When finished, verify that all of your certificates appear in the listing shown on the SSL Certificates page (System > Settings > Authentication > Admin SSL Certificates, or System > Settings > Authentication > SSL Certificates in the classic Skylar One user interface).

TIP: A best practice is to make note of the value in the Hash field shown for each certificate and verify that the hash values match the symlink files in the /var/lib/em7/certs directory on the appliance after completing the configuration of your client certificate chain. You will use these hash values in *Verifying SSL Certificate File Import and Resolving Issues*.

Extracting the Common Name from a Certificate for Authentication

By default, the certificate configuration file (em7_certificate.conf) is configured to display the full common name (CN) of the CAC user as the username in Skylar One after authentication. If this meets your requirements, then you do not need to update the configuration file and can skip this section.

NOTE: If you are using the Microsoft User Principal Name (MS UPN) in your certificates, you do not need to make any edits in the configuration file.

However, if you require that Skylar One use only a portion of the CN, then you can edit the certificate configuration file to parse out a username from the CN in the certificate.

For example, in some instances you might want to use an employee's ID number as the username. To do that, you must edit the Nginx configuration file.

To do so:

1. Log in to the console of the Skylar One appliance as the root user.
2. Navigate to the directory **/etc/nginx/conf.d/** :

```
cd /etc/nginx/conf.d/
```

3. Open the file em7_certificate.conf with a text editor like vi:

```
vi em7_certificate.conf
```

4. Modify the file to extract the CN from the full Distinguished Name (DN) found in the certificate based on how you want to map the username to an LDAP system or how you want the usernames to look if you are using Skylar One internal as the backend of your authentication configuration.

   This is the default configuration of the file:

```
# Create the Username for EM7 to use from the Certificate
# Default: Pull the Common Name from the DN.
map $ssl_client_s_dn $ssl_client_username {
~/?CN=(?<CN>[^/,]+) $CN;
}
```

   Modify the string to extract the name. The following is a regular expression that extracts the CN from the full DN) found in the certificate:

```
map $ssl_client_s_dn $ssl_client_username { ~/CN=[A-Z\.]+(?<num>[0-9]+)
$num; }
```

5. Save and quit (:wq) the file.

Defining the Client Certificate Chain

After importing your SSL Certificates, you must consolidate the SSL PEM certificates into a combined file (emt_combined.crt). On the CAC/ClientCert Auth menu, select all of the desired SSL PEM certificates. After saving, Skylar One will update the em7_combined.crt file with all of the selected SSL PEM certificates. Skylar One will then use only the selected PEM certificates for validating and authenticating users.

You can also define some custom settings for client-side certificate authentication. You can define error messages that are displayed to the end user if authentication fails. Optionally, you can also define IP addresses in this modal for which the user interface will not perform certificate authentication, if you have not already created an Authentication Profile for this purpose. See *Accessing the Appliance without CAC Authentication* for more information.

When authentication is successful, the user interface displays the **ScienceLogic Login** page to the user.

To define the authentication settings:

1. Access the user interface with your CAC or a browser with your client-side certificate installed.
2. Go to the **Client Certificate & CAC Authentication** page (System > Settings > Authentication > CAC Client Cert Auth, or System > Settings > Authentication > CAC/ClientCert Auth in the classic Skylar One user interface).
3. Supply a value in each of the following fields:

- ***Root CA Certificates***. Select *all* root and intermediate certificates that make up the chain from a list of certificates installed on the **SSL Certificates** page (System > Settings > Authentication > Admin SSL Certificates, or System > Settings > Authentication > SSL Certificates in the classic Skylar One user interface). Your client-side certificate will be authenticated against the selected server-side root and intermediate certificates.
- ***Auth Failure Message***. Enter text for the error message that appears to users if authentication fails.

> CAUTION: You cannot save your authentication settings until you enter text in the "Auth Failure Message" field.

- ***Ignore Networks***. In this field, you can enter a list of networks and hosts from which certificate authentication ***is not required***. During each login, the platform will compare the client's IP address to the list entered in this field. If the client's IP address is included in this field, Skylar One will not require certificate authentication from that client.

> **NOTE:** If you are using Authentication Profiles to configure access from specific resources from which certificate authentication is not required, you do not need to use the *Ignore Networks* field. For more information, see *Accessing the Appliance without CAC Authentication*.

  - In the *Ignore Networks* field, you can enter one or more IP addresses, each separated by a new-line character (press the **[<Enter>]** key).
  - In the list of IPs to ignore, you can enter only the first octet, only the first and second octet, only the first, second, and third octet, or all four octets. Skylar One will interpret the entry as if the rightmost octet is followed by * (asterisk).

    For example:

    - 192.168.10.142 will allow a single host to log in to the user interface without certificate authentication
    - 192 behaves the same as entering 192*. This will allow all hosts included in 192.0.0.1 through 192.254.254.254 to log in to the user interface without certificate authentication
    - 192.168.10.24 behaves the same as entering 192.168.10.24*. This will allow all hosts 192.168.10.24, 192.168.10.240, 192.168.10.241, 192.168.10.242, 192.168.10.243, 192.168.10.244, 192.168.10.245, 192.168.10.246, 192.168.10.247, 192.168.10.248, and 192.168.10.249

4. Click the **[Save]** button to save your settings. The user interface displays the message:

```
Settings Saved Successfully. Configuration must be tested in
order to take effect.
```

CAUTION: *Do not* click the Test link at this time.

Verifying SSL Certificate File Import and Resolving Issues

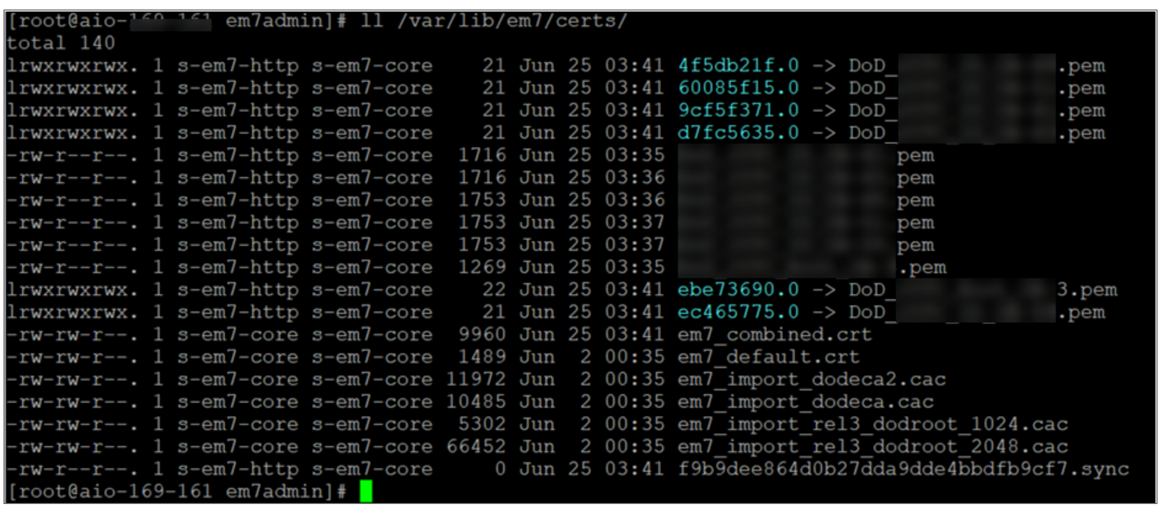
After you have imported your SSL certificates and configured your client certificate chain, it is important to verify the your certificate files were imported correctly and are valid in Skylar One.

To verify that your SSL certificate files were imported correctly:

1. Either go to the console of the Skylar One appliance where you imported the SSL certificates, or use SSH to log in.
2. Navigate to the /var/lib/em7/certs directory. At the shell prompt, enter:

    ```
    ls -l
    ```

3. Review the list of hash symlink files in the directory and compare them to the list of certificates on the SSL Certificates page. Ensure that the hash values shown in Skylar One match the hash symlink files. Note that the hash symlink in the /var/lib/em7/certs directory (in blue text) for a certificate file is appended with ".0", as shown in the image below.

    All of the following must be true. If any of these are not true, then the certificate file was not imported and saved correctly in Skylar One:

    - One hash symlink file should exist in the directory for each of the imported certificate files.
    - The file size of the "em7_combined.crt" file is equal to the combined file sizes of all of the certificate (.pem) files. (The file "em7_combined.crt" *is not* equal to the "em7_default.crt" file.)

- When you view the contents of the "em7_combined.crt" file using `cat` or similar command, the file is the concatenation of all of the certificate (.pem) files. NGINX references the "em7_combined.crt" file as the file containing the client certificate chain.

4. If any of the conditions listed above are not true, then the certificate file was not imported and saved correctly in Skylar One. To resolve the problem:
   a. Log in to the Skylar One appliance user interface.
   b. Go to the **Client Certificate & CAC Authentication** page (System > Settings > Authentication > CAC Client Cert Auth, or System > Settings > Authentication > CAC/ClientCert Auth in the classic Skylar One user interface).
   c. Edit the *Auth Failure Message* field. Make a change to the section.
   d. Click **[Save]**.
   e. Repeat steps 1-3 to verify your certificate files.

Clearing the Skylar One Cache and Restarting NGINX

Before you proceed to testing the configuration, you must clear the Skylar One cache, restart nginx, and close any browsers you have open. This will ensure the best outcome when testing.

1. Log in to the user interface on the Skylar One appliance.
2. Click on the **[Toolbox]** button ( ) and choose Misc > *Clear Skylar One System Cache*.
3. Log out of the Skylar One appliance.
4. Either go to the console of the Skylar One appliance where you imported the SSL certificates, or use SSH to log in to the appliance.
5. Run the following command to restart nginx:

```
sudo systemctl restart nginx
```

6. Close any open browsers that have been used to access the appliance.

Testing the Configuration

After you define the certificate authentication settings, you must test your client-side certificate against the server-side certificate you selected in the ***Root CA Certificates*** field. Testing your configuration is required to prevent an incorrect configuration from preventing administrator access to the user interface. If the test is successful, the certificate authentication settings will be applied. If the test is unsuccessful, the certificate authentication settings will not be applied.

To test certificate authentication settings:

1. With your CAC inserted in the reader, access the user interface of your Skylar One appliance using the IP address or domain name defined in the ***AP Hostname Pattern*** field of the CAC Authentication Profile (System > Settings > Authentication > Profiles). Log in with an administrator account.

2. Go to the **Client Certificate & CAC Authentication** page (System > Settings > Authentication > CAC Client Cert Auth, or System > Settings > Authentication > CAC/ClientCert Auth in the classic Skylar One user interface).
3. After defining the certificate, you will see the following message at the top of the pane:

```
Configuration must be tested in order to take effect: TEST.
```

4. Click the **TEST** link. Skylar One will attempt to authenticate your client-side certificate against the selected server-side certificate.
5. If the test authentication is successful, Skylar One will display the following message at the top of the pane and end users with the appropriate client certificate or CAC can now access the user interface using client certificate authentication:

```
Configuration verified and enabled.
```

6. A new field, ***Client Cert / CAC Auth***, appears with a default value of *Allowed*. Do not edit this field.
7. Set the *Certificate User Field* to "Common Name" (default) or "MS UPN".

> **NOTE:** If you are using LDAP or Active Directory (AD) for user authentication, set this field to "MS UPN".

8. Select the **[Save]** button to save the setting in the ***Client Cert / CAC Auth field***.
9. If the test authentication is unsuccessful, the user interface will display the following message at the top of the pane. The settings will not be applied, and client certificate authentication will not be used until the problem is corrected:

```
ERROR: configuration was not successfully tested with CAC or Client
Certificate.
```

> **NOTE:** If you experience the error above, double-check the following: verify there are not any simple mistakes by reviewing any information you manually entered; check to see if there is a mismatch between the certificate chain installed in nginx versus what the browser uses; make sure the cert file names do not contain spaces or blanks in the file name.

Troubleshooting CAC Authentication

There are a few common issues you might experience while testing CAC authentication. If your test is unsuccessful, review the following troubleshooting steps.

Failed to Identify Personal Identity Verification (PIV) Card

If you receive the "Failed to identify PIV card" message, verify the following:

- All root and intermediate certificates have been uploaded in a PEM format.
- All root and intermediate certificates have not expired and are configured properly.
- The client certificate has not expired.
- Customer username information is in the Microsoft User Principal Name (MS UPN and not the Common Name (CN).

Failed CAC Authentication After Disaster Recovery (DR) Failover

If your CAC authentication testing fails after DR failover, verify the following:

- The DR node domain has been added to the Auth Profile for pattern matching.
- The DR has all of the required certificates. (You might be required to manually upload and save the certificates again.)

> **NOTE:** For more information, see the chapter on "Disaster Recovery with Two Appliances" in the ***High Availability and Disaster Recovery Configuration*** manual.

Failed CAC Authentication After Setting Up High Availability (HA)

Assuming you have deployed a Skylar One distributed system with one Database Server and two or more Administration Portals and your CAC authentication testing fails after setting up HA, you must ensure the following:

- The first Administration Portal where you configured CAC is working and you authenticated with CAC before verifying that the second or third Administration Portal actually works. You should not have the CAC/Client Cert in the aligned credential source on the default profile but in a new profile created for CAC only.

> **NOTE:** ScienceLogic suggests having at least two profiles (a default profile and a CAC profile). You should enter an AP Hostname Pattern on the CAC profile but keep the AP Hostname Pattern blank on the default profile.

- Upon successful CAC login on the first Administration Portal, you will notice that any login attempts to the second or third Administration Portal will fail. For this, you need to first verify that the content of the /var/lib/em7/certs contains the PEM files that are identical to the first Administration Portal. You must also ensure that the hash files representing your PEM files are identical to the first Administration Portal and that the combined file is identical to the first Administration Portal.
- Once verified, restart nginx on the second and third Administration Portals and ensure that nginx is running correctly.

- Verify that you can log in with CAC from the second or third Administration Portals as you have done with the first Administration Portal.

> **NOTE:** For more information, see the chapter on "High Availability with Two Appliances" in the ***High Availability and Disaster Recovery Configuration*** manual.

Accessing the Appliance without CAC Authentication

In certain circumstances, you might need to access your Skylar One appliance without using CAC authentication. For example, the following are some reasons you might want to use another authentication type:

- For use during initial setup
- For appliance access when a certificate has expired
- For maintenance or administrator accounts
- For certain internal networks that will not require certificate authentication

You can configure the appliance to accept a login in these cases in two ways:

- By configuring an Authentication Profile to use an alternative authentication resource (for example, Internal) for certain networks or hosts. For more information, see the section on *Authentication Profiles*.
- By using the Ignore Networks field on the **Client Certificate & CAC Authentication** page (System > Settings > Authentication > CAC Client Cert Auth, or System > Settings > Authentication > CAC/ClientCert Auth in the classic Skylar One user interface). For more information, see *Defining the Client Certificate Chain*.

Special Circumstance: Multiple Levels of Intermediate Certificates

By default, Skylar One is configured to handle the typical certificate hierarchy, which comprises three levels: root, intermediate, and client certificates. This represents a depth of 2 from the root to the client certificate. If your organization will use CAC authentication in which you have multiple levels of intermediate certificates in the hierarchy, you will need to change this setting (**ssl_verify_depth**) as described in the procedure below.

To update the value of **ssl_verify_depth**:

1. Log in to the console of the ScienceLogic appliance as the root user.
2. Navigate to the directory **/etc/ngnix/conf.d/** :

```
cd /etc/ngnix/conf.d/
```

3. Open the file em7ngx_web_ui.conf with a text editor like vi:

```
vi em7ngx_web_ui.conf
```

4. Edit the ssl_verify_depth value to be the depth from client certificate to the root certificate (for example, 3):

```
ssl_verify_depth 3;
```

5. Save and quit (:wq) the file.

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

International: +1-703-354-1010