



# Cerner Healthcare Connector Guide

Version: 8.2 Patch 1

# Copyright and Trademark Notices

Copyright © 2021 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

"SailPoint," "SailPoint & Design," "SailPoint Technologies & Design," "Identity Cube," "Identity IQ," "IdentityAI," "IdentityNow," "SailPoint Predictive Identity" and "SecurityIQ" are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. <https://www.sailpoint.com/patents>

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce's Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

# Contents

---

<b>Overview .....</b>	<b>1</b>
<b>IdentityIQ for Cerner Healthcare .....</b>	<b>2</b>
Overview .....	2
Configuration Parameters .....	3
Schema Attributes .....	4
Provisioning Policy Attributes .....	6
Additional Information .....	7
Troubleshooting .....	8

## Overview

SailPoint Healthcare Integration Modules deliver extended value from standard IdentityIQ deployments. SailPoint is committed to providing design, configuration, troubleshooting and best practice information to deploy and maintain strategic integrations. SailPoint has modified the structure of this document to aid customers and partner deployments. The focus of this document is product configuration and integration. For more details on design, troubleshooting and deployment best practices, refer to the Connector and Integration Deployment Center in Compass, SailPoint's Online customer portal.

This document provides a guide to the integration between the Healthcare Connector and IdentityIQ.

This document is intended for the Healthcare Connector and IdentityIQ System Administrators and assumes an advance level of technical knowledge.

# IdentityIQ for Cerner Healthcare

The following topics are discussed in this chapter:

- [Overview](#)
- [Configuration Parameters](#)
- [Schema Attributes](#)
- [Provisioning Policy Attributes](#)
- [Additional Information](#)
- [Troubleshooting](#)

## Overview

Cerner Corporation is a global supplier of health care information technology (HCIT) solutions, services, devices and hardware. Cerner solutions optimize processes for health care organizations. The IdentityIQ for Cerner Healthcare is designed to provide automated way of provisioning through SailPoint IdentityIQ solution.

## Supported Features

IdentityIQ for Cerner Healthcare supports the following features:

### Account Management

- Aggregation, Refresh Account
- Create, Update, Delete
- Enable, Disable, Change Password
- Add/Remove Entitlements (position and organization groups)

### Account - Group Management

- Aggregation

## Prerequisites

The Cerner Enterprise Provisioning Service exposes the provisioning mechanism to external requests and responses using the SPML (Service Provisioning Markup Language), which is an standard Cerner Millennium provisioning language. Through this service, its possible to support external provisioning solutions to create and maintain users.

The following details are required:

These details are provided by Cerner to individual customer. Hence these details vary as per the customer.

- Provisioning Servlet: The Cerner connector accesses the provisioning servlet URL, an customer specific enterprise provisioning service to perform all the aggregation & provisioning related operations.

- **Target ID:** Along with the servlet, an customer specific target ID is required for IdentityIQ to connect to Cerner Provisioning adapter (through Cerner API's access)
- **Permissions:** The Cerner provisioning adapter requires one Millennium account having Manage Accounts privilege, which modifies the users within Millennium. The service account is mapped to TargetID which is required in order to make calls to the provisioning adapter.

All the above prerequisites are mandatory as Cerner does not define users having the authority to send requests in any method.

## Configuration Parameters

### **Cerner URL**

URL of the Provisioning Servlet and the Provisioning Servlet allows SailPoint Cerner connector to communicate with Cerner through SPML calls.

For example, <http://<hostName>/security-provisioning/ProvisioningServlet>

### **Target ID**

ID with required permission to get the data and to perform provisioning on Cerner. Enter Valid Target ID. Target ID is referred to as the Millennium ID that must be created and considered to be a service account used by the Cerner connector. Users must get the Millennium ID created from the Cerner through some form of Service Request.

For example, "millennium\_XXXXXX"

### **Manage Accounts**

Select the following appropriate user status to aggregate users:

- Active and Suspended
- Active
- All

## Additional Configuration Parameters

- Time out setting is required if the response is getting delayed from the Cerner system. By default, timeout is set to 1 minute. The timeout settings can be configured from the application debug page as follows:

```
<entry key="timeout" value="1"/>
```

- Cerner API's require version while executing the operations. Currently version 1.0 is supported. Version can be configured from the application debug page as follows:

```
<entry key="version" value="1.0"/>
```

- Cerner connector provides a generic delimiter accross the connector to aggregate/provision. The default value of the delimiter is - #~#

To change the value of the default value, add the following entry key in the application debug page:

```
<entryKey="cernerDelimiter" value="<anyothercharacter>"/>
```

Ensure that the same delimiter is used to provision as mentioned in aggregation.

## Schema Attributes

### Account Attributes

The following table lists the account attributes:

#### ***ID***

Identifies an object that exists on a target that is exposed by a provider

#### ***username***

The user name associated with the account. The value of the user name field must be unique within the target Cerner Millennium domain. Any value between 1 and 48 characters

#### ***directoryIndicator***

- True (LDAP user)
- False (non-LDAP user)

Contains an indicator if the user is an LDAP directory user or not.

#### ***birthdate***

Birthdate of the personnel.

#### ***firstname***

First name for the personnel.

#### ***lastname***

Surname (last name) for the personnel.

#### ***middleName***

Middle name of the personnel.

#### ***displayName***

Display name for the personnel.

#### ***suffix***

Suffix of the personnel.

#### ***privilege***

Privileges assigned to the Cerner account.

#### ***gender***

A coded value representing the gender of the personnel.

#### ***restriction***

A restriction to be assigned to or unassigned from the account.

#### ***title***

Title (or list of titles) for the personnel. For example, Dr. Mr. and so on.

#### ***physicianInd***

An indicator if the personnel is a physician or not.

#### ***position***

A coded value representing the position assigned to the personnel which is treated as Group entity.

***beginEffectiveDate******Time***

Date/time at which the personnel becomes/became effective.

***endEffectiveDate******Time***

Date/time at which the personnel ceases/ceased to be effective.

***organization*** ***Group***

When a personnel record is unassigned from an organization group, all organizations in the group will also be unassigned from the personnel record, unless they are associated to another organization group that is still assigned to the personnel. It will be read-only field and data will be displayed during account aggregation.

***confidentiality******Level***

A coded value representing the confidentiality code that applies to the relationship.

***personnel******Alias***

Personnel alias information.

***personnel******Group***

It contains personnel group information.

***credential***

Credentials are used to highlight the level of education and specialty of a care provider.

***Additional Account Schema Attribute***

The **organization** attribute can be added to account schema as follows:

***Through UI***

Add the following schema attribute manually to support aggregation and provisioning for **organization** attribute:

- **Name:** organization
- **Type:** string
- **Value:** true for entitlement, managed and multi
- **Description:** It contains organization information

***Through debug page:***

Add the following entry in the application debug page to support aggregation and provisioning for **organization** attribute:

```
<AttributeDefinition entitlement="true" managed="true" multi="true" name="organization"
type="string">
<Description>It contains organization information</Description>
</AttributeDefinition>
```

**Group Attributes**

The following table lists the group attributes:

***Id***

The Id of the group.



**Display**

Display name of the group.

**Organization Group Attributes**

The following table lists the organization group attributes:

**Id**

Unique identifier of the organization group.

**Display**

Display value of the organization group.

**Provisioning Policy Attributes**

This section describes the provisioning policy attributes for Create and Update Account.

The 'confidentialityLevel' attribute must be configured in the new application provisioning policy with the following details:

- Type as String
- Review required

For better governance, ensure that the value of the 'confidentialityLevel' attribute is same as the managed system.

**Create Account**

The following table lists the provisioning policy attributes for Create Account:

**username**

The user name associated with the account. The value of the user name field must be unique within target Cerner Millennium domain [1- 48 characters]

**password**

The password for the user account. Any value, assuming that value meets all criteria defined in the Cerner Millennium password policy maintained in AuthView. The password is only required when the user being provisioned is a non-LDAP user (when the user will authenticate against the Cerner Millennium user directory).

**first name**

Given (first) name for the personnel.

**lastname**

Surname (last name) for the personnel.

**confidentialityLevel**

The confidentiality level set for organization or organization groups.

**Update Account**

The following table lists the provisioning policy attributes for Update Account:

**confidentialityLevel**

The confidentiality level set for organization or organization groups.

## Dormant Account Support

IdentityIQ for Cerner Healthcare now provides support for an additional functionality of removing an username or disassociating an account which can be achieved by adding a new checkbox with name as **removeUserName** (of type boolean) in Provisioning Policy.

If the newly added 'removeUserName' checkbox is checked, then the Cerner Connector would by default remove the Username and disassociate the account from Personnel. This disassociated Username can be assigned to any other account.

If user wants to only remove the Username and not disassociate an account, then add the **disassociateAccount** attribute in the application debug page as follows:

```
<entry key="disassociateAccount" value="false"/>
```

## Additional Information

This section describes the additional information related to the Cerner Healthcare.

### Upgrade Considerations

- After upgrading Cerner application, ensure that account and group aggregation are performed again.
- After upgrading Cerner application, if:

Parameter	Before upgrade	Option selected after upgrade
Include end-dated Personnel Records	Selected	Active and Suspended
	Not Selected	Active

### Aggregating Additional Attributes

- To aggregate all the user accounts based on the status, add the following entry in the application debug page:

```
<entryKey="userStatus" value="All"/>
```

- To aggregate all the user accounts with active and disabled status (Inactive users will not be aggregated), add the following entry in the application debug page:

```
<entryKey="userStatus" value="Active and Suspended"/>
```

- To aggregate all the active user accounts, add the following entry in the application debug page:

```
<entryKey="userStatus" value="Active only"/>
```

### Provisioning Additional Attributes

- **personnelAlias:** To provision **personnelAlias** through update account provisioning policy, enter the input format for attribute as follows:

```
beginEffectiveDateTime=#~#2010/09/13#~#endEffectiveDateTime=2100/12/30#~#alias=677001#~#type=DOCDEA#~#aliasPool=DEA
```

- **credential:** To provision **credential** through update account provisioning policy, enter the input format for attribute as shown in the following example:

```
name=BLS#~#type=Certificate#~#renewalDateTime=2035/01/01#~#state=NY#~#beginEffectiveDateTime=#~#2010/09/13#~#endEffectiveDateTime=2100/12/30#~#addToNameIndicator=true
```

- **address:** To provision **address** through update account provisioning policy, enter the input format for attribute as shown in the following example:

```
streetAddr=1200 Northside Forsyth Dr#~#streetAddr2=Times Square#~#addressTypeCd=Business#~#state=NY#~#city=Cumming#~#zipCode=30041#~#beginEffectiveDateTime=#~#2010/09/13endEffectiveDateTime=2100/12/30
```

- **phone:** To provision **phone** through update account provisioning policy, enter the input format for attribute as shown in the following example:

```
phoneNumber=0001112222#~#phoneType=Business#~#phoneFormat=FreeText#~#extension=09#~#description=A phone number#~#beginEffectiveDateTime=#~#2010/09/13#~#endEffectiveDateTime=2100/12/30
```

## Troubleshooting

### 1 - An error message is displayed while performing the operations

The following error message is displayed while performing the operations:

```
xml.soap.SOAPException: Read timed out" OR "call: Connection Refused: connect
```

**Resolution:** Ensure that the Cerner server is up and running.

### 2 - Aggregation task fails with an error message

The Aggregation task fails with the following error message even when the test connection is successful:

```
An error has occurred retrieving user: XXXXXXXX
```

**Resolution:** Verify the read and write privileges for the Cerner Administrator account provided in application configuration.

### 3 - Insufficient privileges displayed in the Managed System due to authorize server not running in the domain

If insufficient privileges are displayed in the Managed System for a particular account and the domain server is not available, then the permissions of the account are disabled.

This issue is related to the Authorize server not running in the domain. This is caused by an issue with the server controller service.

**Resolution:** Perform the following to cycle the Millennium domain and resolve the issue:

- Run an **mbt -ctrl**, to verify if there were no orphaned processes
- Run an **mbs -ctrl** to restart

#### ***4 - An error message appears during aggregation***

During group aggregation the following error message may appear:

```
"Exception during aggregation of Object Type Group on Application CernerOLD.  
Reason: sailpoint.connector.ConnectorException: Group Aggregation failed :  
[Unable to unmarshall request, error: Unexpected end of element  
{urn:cerner:xmlns:security-provisioning:refData}:refData]"
```

**Resolution:** Ensure that the **position** account schema attribute must be **group** instead of **string**.