CA Identity Manager - 14.2

Manage Authentication

Module Properties

Date: 31-May-2018

Table of Contents

Manage Authentication Module Properties

By default, CA Identity Manager comes with an out-of-the-box, Default authentication module. The Default module authenticates the user against the directory that is configured for their environment. Two other authentication module choices exist: The Active Directory or a custom module. Administrators can view, set, and add authentication properties to modules. The Active Directory module has a set of required properties. The custom, Other authentication module allows administrators to create authentication module properties.

Follow these steps:

1. In the **Management Console**, select **Environment**, select the environment that you want to manage, and then click **Advanced Settings**. The **Advanced Settings** page appears.

2. Select **User Console**.

3. In the **Authentication Properties** section, select the radio button for the desired authentication module class:

- **Default**: This module uses the default authentication module that authenticates the user against the directory configured for their environment.
  To use this option, select it, click **Save**, and then **Restart the Environment** to apply these changes.

- **Active Directory**: This module authenticates the user against to an external Active Directory. See **Using the Active Directory Authentication Module** in the following section.

- **Other**: The Other authentication module configures a custom authentication module created using Java. A custom authentication module coded in Java must implement the CA Identity Manager Authentication Module interface and a custom JSP (if needed). See How To Customize Identity Manager Authentication (https://docops.ca.com/display/CIM142/How+To+Customize+Identity+Manager+Authentication) in the Programming Guide for Java (https://docops.ca.com/display/CIM142/Programming+Guide+for+Java). To configure custom modules, see **Using the Other Authentication Module** in the following section.

Note: The **authentication attribute to use** and the **login page to use** properties are common properties for any configured authentication module.

Using the Active Directory Authentication Module

Note: The Active Directory endpoint must be provisioned by CA Identity Manager so the Active Directory accounts are synchronized with the CA Identity Manager user store. This procedure also assumes that the administrator is proficient with Active Directory.

The Active Directory Authentication module can be configured to authenticate to an external Active Directory. You can make task-based password changes directly to Active Directory.

Note: If you are upgrading from CA Identity Manager 14.1 and have configured the Active Directory Adapter, be aware that the **ad_auth_settings.properties** file no longer uses the Active Directory Server settings. In 14.2, when a CA Identity Manager environment is started and the Active Directory Adapter is configured, properties defined in the **ad_auth_settings.properties** file are read and stored with the Active Directory Authentication adapter configuration. You can now manage the configuration in the **Authentication Properties** section of the **Management Console**, **Environment**, **<** ***Environment*****>**, **User Console** screen. The values are persisted with the environment in the CA Identity Manager object store.

Also note that the **PWDKEY** and **KEYSTOREPWD** properties are no longer required.

If you configure the Active Directory authentication model, user password sets from the Forgotten Password or Reset Password tasks automatically propagate to both the CA Identity Manager User Store and the Active Directory server. Password status changes are detected during authentication. This requires an LDAPS connection between the CA Identity Manager Server and the Active Directory server. Specifically, the SSL property must be set to true. The Active Directory certificates must then be imported into the keystore of Java running CA Identity Manager.

Before you attempt authentication with this module, the login name that is entered in the login screen must uniquely identify the same user in both the CA Identity Manager User Store and in Active Directory.

Specifically, CA Identity Manager searches for the user name entered in the login screen in the CA Identity Manager User Console by the attribute that is defined in the **Management Console, Environments, <Environment Name>, Advanced Settings, Authentication Properties, Authentication attribute to use** property. Typically, this attribute is defined as **%USER_ID%** or **%LOGIN_ID%**. Deployments can use some other attribute that uniquely identifies the user. The search filter property of the Active Directory Authentication module must define an attribute whose value can uniquely identify the Active Directory user. CA recommends either **sAMAccount** or **userPrincipalName**.

Defining a configuration or entering a login ID value that fails to find both the CA Identity Manager user and the Active Directory results in an authentication failure.

The following table shows some common scenarios and the associated required configurations.

CA Identity Manager Configuration		**User Data**	
Authentication attribute	AD Authentication provider filter	CA Identity Manager User	Active Directory User
%USER_ID%	sAMAccountName=%s	userId=smithjo01	sAMAccountName = smithjo01
%LOGIN _ID%	sAMAccountName=%s	loginId=smithjo01	sAMAccountName = smithjo01
%LOGIN _ID%	userPrincipalName=%s	loginId=john.smith@mycompany.com	userPrincipalName = john.smith@mycompany.com
%EMAIL%	userPrincipalName=%s	email= john.smith@mycompany.com	userPrincipalName = john.smith@mycompany.com

Use the following procedure to use the Active Directory authentication module class.

Follow these steps:

1. In the **Management Console**, select **Environment**, <Environment_Name>, and then click **Advanced Settings**.

2. In the **Authentication Properties** section, select **Active Directory**.

3. Select **Module Properties** to display the **Active Directory Authentication Properties** page. The following list of default properties appears; select the property and then enter a corresponding value:

   - **SERVERS**: Specifies the IP address of the Active Directory server(s). Use the following format (no spaces):
     IP1:PORT,IP2:PORT
     For example: 192.168.152.152:10261,192.168.154.127:10261

   - **ADMINDN:** Specifies the DN of the Administrator ID used to connect to Active Directory. This property is required. For example:
     cn=Administrator,cn=Users,dc=companyX,dc=com

- **ADMINPWD**: Specifies the Administrator Password for Active Directory. Enter and then confirm this password. This value is required.
- **BASEDN:** Specifies the Base DN for the User Search in Active Directory**.** This property is required. For example: cn=Users,ca=companyX,dc=com
- **SSL**: Determines whether to use SSL. Values are TRUE or FALSE.
- **SEARCHFILTER**: Specifies a valid LDAP search filter with a variable substitution for an AD User. "%s" must be part of the filter, as it is replaced with the user name in authentication. This property is required. For example, to define a filter when using the default Active Directory User Schema, enter SEARCHFILTER=sAMAccountName=%s

  Note: When using a custom Active Directory User schema, the objectCategory and ObjectClass filters clauses must both be defined in the filter and match the LDAP object classes of the custom schema. For example, enter: SEARCHFILTER=(& (objectCategory=person)(objectClass=CompanyXUser)(sAMAccountName=%s))

4. To add new authentication module properties, enter a new **Property** and **Value** in the corresponding fields, and then click **Add**.

   Note: Currently no additional properties are supported for the Active Directory module. Additional properties may be added in the future. Additional property values are not validated.

5. To apply these changes, click **Save**, and then **Restart the Environment**.

Using the Other Authentication Module

The Other authentication module configures a custom authentication module created using Java. A custom authentication module coded in Java must implement the CA Identity Manager Authentication Module interface and a custom JSP (if needed). See How To Customize Identity Manager Authentication (https://docops.ca.com/display/CIM142/How+To+Customize+Identity+Manager+Authentication) in the Programming Guide for Java (https://docops.ca.com/display/CIM142/Programming+Guide+for+Java).

Use the following procedure to use a custom Authentication module class.

Follow these steps:

1. In the **Management Console**, select **Environment**, select the environment that you want to manage, and then click **Advanced Settings**.
2. In the **Authentication Properties** section, select **Other**.

3. In the text box, enter the full Java class name (including the package) of the custom module class in the provided text box.

4. Select **Module Properties** to display the **Other Properties** page.

5. To add new authentication module properties, enter a new **Property** and **Value** in the corresponding fields, and then click **Add**.

> **Note**: These values are not validated. It is assumed the custom module developer will provide documentation for any properties needed by the custom module.

6. To apply these changes, click **Save**, and then **Restart the Environment**.