First Look: LDAP and InterSystems Products

Version 2019.4
2020-01-28

InterSystems Corporation 1 Memorial Drive Cambridge MA 02142 www.intersystems.com

First Look: LDAP and InterSystems Products
InterSystems IRIS Data Platform Version 2019.4 2020-01-28

For Support questions about any InterSystems products, contact:

InterSystems Worldwide Response Center (WRC)
Tel: +1-617-621-0700
Tel: +44 (0) 844 854 2917
Email: support@InterSystems.com

Table of Contents

First Look: LDAP and InterSystems Products

The InterSystems IRIS® data platform can integrate with an LDAP (Lightweight Directory Access Protocol) server to seamlessly authenticate and provide authorization for users based on this widely used technology. When a user attempts to log in to InterSystems IRIS, the username and password are sent to the LDAP server to verify that the user exists. Once the user's identity has been authenticated, the LDAP server sends InterSystems IRIS information about which groups the user belongs to. These groups correspond to the roles in InterSystems IRIS that control what actions the user is authorized to perform and whether they can read or write content. In this way, InterSystems IRIS uses LDAP technology for both authentication and authorization aspects of its security strategy.

By following the steps in this First Look guide, you can connect to an LDAP server and explore how it affects security in InterSystems IRIS. In these exercises, you configure InterSystems IRIS to integrate with a Windows Active Directory server. Though other LDAP servers are supported, this tour of LDAP authentication and authorization focuses on using Active Directory.

To browse all of the First Looks, including others that can be performed on a free Community Edition instance as described below, see InterSystems First Looks.

1 Setting up LDAP authentication

Before logging in as LDAP users and exploring LDAP-based security in InterSystems IRIS, you need to do the following:

- Select InterSystems IRIS Instance
- Define an LDAP configuration
- Select an LDAP domain as the default
- Enable LDAP authentication in InterSystems IRIS
- Install the security certificate for the LDAP server

1.1 Selecting an InterSystems IRIS Instance

Select an InterSystems IRIS instance to use for this procedure from among the following:

- *Deploy InterSystems IRIS in a container*

  You can deploy a free instance of InterSystems IRIS Community Edition in two ways:

  – Provision a cloud node hosting a running InterSystems IRIS Community Edition container on the Google Cloud Platform, Microsoft Azure, or Amazon Web Services public cloud platforms.

  – Pull the container image from the Docker Store and deploy an InterSystems IRIS Community Edition container on the system of your choice.

  For instructions for deploying and using InterSystems IRIS Community Edition, see Getting Started with InterSystems IRIS Community Edition.

- *Deploy InterSystems IRIS on the web*

  The InterSystems Labs web page lets you easily create your own demo instance of InterSystems IRIS Community Edition, accessible on the web. Your InterSystems Labs instance includes an integrated IDE and plenty of samples to work with, and you can connect your own IDE.

- *Install InterSystems IRIS on your system*

  If you are an InterSystems customer, you can install and license a development instance of InterSystems IRIS on your local machine or on another on your network; for instructions, see InterSystems IRIS Basics: Installation. Install with Normal security settings.

1.2 Defining an LDAP Configuration

InterSystems IRIS uses an LDAP configuration to define the information needed to connect to the LDAP server and search for users. To create and define a new LDAP configuration:

1. Open the Management Portal for your instance in your browser. The URL to use depends on the type of instance you selected; for information about determining the correct URL, see InterSystems IRIS Connection Information in *InterSystems IRIS Basics: Connecting an IDE*.
2. Go to the **Security LDAP Configurations** page (**System Administration > Security > System Security > LDAP Configurations**).
3. Click **Create New LDAP configuration**.
4. In the **Name** field, enter `irisldap.com`.
5. Select the **Enabled** checkbox.
6. Select the **LDAP server is a Windows Active Directory server** checkbox.
7. Define the following fields:

Field	Contents
LDAP domain name (Windows only)	`irisldap.intersystems.com`
LDAP host names	`irisldapdc1.irisldap.intersystems.com`
LDAP username to use for searches	• (Windows) `sidLDAPQuery` • (UNIX®) `CN=sidLDAPQuery,CN=Users,DC=irisldap,DC=intersystems,DC=com`
LDAP username password	Select **Enter New Password**, then enter the password as `Cach3L3arning`
LDAP Base DN to use for searches	`DC=irisldap,DC=intersystems,DC=com`
LDAP Unique search attribute	`sAMAccountName`

8. Select the **Use TLS/SSL encryption for LDAP sessions** checkbox.
9. Select the **Use LDAP Groups for Roles/Routine/Namespace** checkbox.
10. Select the **Allow Universal group Authorization** checkbox.
11. Click **Save**.

1.3 Selecting the New LDAP Domain as the Default

Once the LDAP configuration for the LDAP server is defined, you need to set the new LDAP configuration as the default LDAP domain. To set the LDAP server as the default:

1. From the Management Portal home page, go to the **System-wide Security Parameters** page (**System Administration > Security > System Security > System-wide Security Parameters**).
2. Select `irisldap.com` from the **Default security domain** drop-down list.
3. Click **Save**.

1.4 Enabling LDAP Authentication

Using an LDAP server is just one method of authentication available in InterSystems IRIS. Not only must LDAP authentication be enabled for the entire instance of InterSystems IRIS, but each component of InterSystems IRIS that needs to be accessed by an LDAP user must also be enabled for LDAP authentication. The following procedure enables LDAP authentication for the instance and those components needed for this tour of InterSystems IRIS security:

1. From the Management Portal home page, go to the **Authentication/Web Session Options** page (**System Administration > Security > System Security > Authentication/Web Session Options**).
2. Select the **Allow LDAP authentication** checkbox.
3. Click **Save**.
4. From the Management Portal home page, go to the **Web Applications** page (**System Administration > Security > Applications > Web Applications**).

   From this page you will enable LDAP authorization for the sections of the Management Portal that you will be accessing in the tour of InterSystems IRIS. Because other sections of the Management Portal will not have LDAP authorization enabled, you might be asked to log in if you try exploring these other sections.
5. Click **/csp/sys** to display the page used to configure the web application.
6. In the **Security Settings** section, select the **LDAP** checkbox in the **Allowed Authentication Methods** field.
7. Click **Save**.
8. Once the setting is saved, click **Cancel** to return to the **Web Applications** page.
9. Click **/csp/sys/sec**. This web application contains the security pages of the Management Portal.
10. In the **Security Settings** section, select the **LDAP** checkbox in the **Allowed Authentication Methods** field.
11. Click **Save**.
12. Once the setting is saved, click **Cancel** to return to the **Web Applications** page.
13. Click **/csp/sys/op**. This web application contains the operation pages in the Management Portal.
14. In the **Security Settings** section, select the **LDAP** checkbox in the **Allowed Authentication Methods** field.
15. Click **Save**.

1.5 Installing a Security Certificate for the LDAP Server

The LDAP server is secured with TLS/SSL, so you need to install a security certificate to successfully access the server. You will create a .cer file that contains the required certificate content before identifying it as the security certificate.

1.5.1 Creating .cer file

To create the file that will be installed as the security certificate:

1. Open a text editor such as Notepad and create a new file.
2. Copy all of the following content and paste it into the new file in the text editor. The new file should begin with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.

```
-----BEGIN CERTIFICATE-----
MIIDuTCCAqGgAwIBAgIQO5hG2uC7G7ZBxcXt/J+z3TANBgkqhkiG9w0BAQsFADBv
MRMwEQYKCZImiZPyLGQBGRYDY29tMRwwGgYKCZImiZPyLGQBGRYMaW50ZXJzeXN0
ZW1zMRgwFgYKCZImiZPyLGQBGRYIaXJpc2xkYXAxIDAeBgNVBAMTF2lyaXNsZGFw
LUlSSVNMREFQREMxLUNBMB4XDTE4MDQwOTE0MDUzMloXDTIzMDQwOTE0MTUzMlow
bzETMBEGCgmSJomT8ixkARkWA2NvbTEcMBoGCgmSJomT8ixkARkWDGludGVyc3lz
dGVtczEYMBYGCgmSJomT8ixkARkWCGlyaXNsZGFwMSAwHgYDVQQDExdpcmlzbGRh
cC1JUklTTERBUERDMS1DQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AL/aNDJJNbzGh6tXG8+hmEEplb80UQMcIhLvoanz/RKKZXBBY68rO5pkYUwn/24g
pryGy0OUjA997KKol5rdbXWzK7vUMuVSp0atw1m4vF9hmp1bpKBC60OXmV39Fqar
ej1dkRl0ZXOmCexP8JqTyNwhpOLXvazzzvsNRr4ts9u1m6y9kFYecu4PRqtFCgoC
T6rbgqz1Ew3VrhQHi0HWvq1sR2CngxdyG8AnlSo6nz3X/IrTwrw5lauNLfpsRda5
D5YfUpxYeqpONSUB650u9bC0l5eRWe8kS33Xr+u5Odkhy087I/zN+GK7xMGzxYMR
OWNINIGRvlLuDRshKQl4gP0CAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB
/wQFMAMBAf8wHQYDVR0OBBYEFM3Ofv4R/zkEgHkp4ayvTkAvxJikMBAGCSsGAQQB
gjcVAQQDAgEAMA0GCSqGSIb3DQEBCwUAA4IBAQC8hhvc/+WsDeipNezBo+ovum2z
7q0fStr73Tj84cDGSyCmT2Q/h0qFvkfjtRd8AUBdG0qjhIB4VLVyWmrWDl1jAUcr
3AzygfO6UZjNRT+4c8r8R2xOhE3wJEJWibzXD9bPCtCkhYNJT6bi5PSRgUq+r9GU
IHnAUmaQa+K+kNEpAvBfIeQ2ox9NPbtUfj/fswKpubWzZZc2udeU8SQLacl6tZMA
tXgZPT6lQfoZU2WmDG1EnoC4Ji1++Sf6Ho2i6kxg1m6geyOPSsGPdsAVjYCqCjuZ
pxjAsfZXV2juLyTBM51rrmV/Rqfougnikh4zhFRBrOHtMP71ZxCptMVz3RHe
-----END CERTIFICATE-----
```

3. Save the file as irisldap.cer in a directory that you can access.

1.5.2 Installing the Security Certificate on Windows

If you are running InterSystems IRIS on Windows, complete the following steps to finish the process of installing the security certificate that you created.

1. Using Windows Explorer, double-click the security file irisldap.cer in the directory where you saved the file.
2. Click **Install Certificate**.
3. Select **Local Machine** and click **Next**.
4. Click **Yes** to allow changes to be made to your device.
5. Select **Place all certificates in the following store** and click **Browse**.
6. Select **Trusted Root Certification Authorities** and click **OK**.
7. Click **Next**.
8. Click **Finish**.

1.5.3 Installing the Security Certificate on UNIX®

If you are running InterSystems IRIS on UNIX®, complete the following steps to finish the process of installing the security certificate that you created.

1. While logged into the Management Portal as the `_system` user, go to the **Security LDAP Configurations** page (**System Administration > Security > System Security > LDAP Configurations**).
2. Click **irisldap.com** from the list of LDAP configurations.
3. In the **TLS/SSL certificate file** field, enter the path and filename of irisldap.cer, which is the file you created and saved.

2 Exploring LDAP Users and Groups

Now that you have configured your LDAP connection and enabled LDAP authentication, you can use the LDAP server to log into InterSystems IRIS. The LDAP server contains three users: user1, user2, and user3. The user1 belongs to the intersystems-Role-%Operator group, user2 belongs to the intersystems-Role-%Manager group, and user3 belongs to the intersystems-Role-%Developer group. Each group grants privileges belonging to a corresponding role in InterSystems IRIS. For example, when user1 is successfully authenticated by the LDAP server, they are assigned the **%Operator** role.

In this tour, you will log into InterSystems IRIS as all three users and explore what actions are available based on the roles associated with the user. When you log into InterSystems IRIS as a valid LDAP user, InterSystems IRIS automatically creates the user without requiring that you manually add the user beforehand.

2.1 User1: Operator

To log in as user1 and explore InterSystems IRIS:

1. If you are currently logged into InterSystems IRIS, click the **Logout** link at the top left of the Management Portal.
2. Log into InterSystems IRIS using the following credentials:

   User Name: `user1`

   Password: `Password1`

   User1 is a member of the intersystems-Role-%Operator group. Based on this group, when user1 is authenticated, they are automatically granted the privileges associated with the **%Operator** role in InterSystems IRIS.
3. From the Management Portal home page, go to the **Databases** page (**System Operation > Databases**). User1 has access to this page because they have been authorized by the LDAP server to interact with pages associated with the **%Operator** role.
4. On the Management Portal home page, notice that the **System Administration** menu is disabled. User1 cannot access this menu because the **%Operator** role does not include the proper privileges.

2.2 User2: Manager

To log in as user2 and explore InterSystems IRIS:

1. Click the **Logout** link at the top left of the Management Portal.
2. Log into InterSystem IRIS using the following credentials:

   User Name: `user2`

   Password: `Password2`

   User2 is a member of the intersystems-Role-%Manager group. Based on this group, when user2 is authenticated, they are automatically granted the privileges associated with the **%Manager** role. As you will see, these privileges include access to pages that user1 could not see.
3. From the Management Portal home page, go to the **Users** page (**System Administration > Security > Users**). Remember that user1 could not access the **System Administration** menu.
4. Click user1 from the list of users.
5. Click the **Roles** tab.

   Notice that **%Operator** is the only role assigned to user1.

6. Click **Cancel** to return to the **Users** page.
7. Notice that there is no entry for user3 in the list of users. This user will be created automatically when user3 logs in, at which point InterSystems IRIS uses the LDAP server to authenticate the user.

2.3 User3: Developer

To log in as user3 and explore InterSystems IRIS:

1. Click the **Logout** link at the top left of the Management Portal.
2. Log into InterSystem IRIS using the following credentials:

   User Name: `user3`

   Password: `Password3`

   User3 is a member of the intersystems-Role-%Developer group. Based on this group, when user3 is authenticated, they are automatically granted the privileges associated with the **`%Developer`** role.
3. Notice that the user has access to the **System Explorer** menu, but not the **System Operation** and **System Administration** menus. You can tell that the **`%Developer`** role assigned to user3 has different privileges than the roles assigned to user1 and user2. This prevents user3 from seeing their own user profile because the **Users** page is under the **System Administration** menu.

2.4 Automatic User Creation

You have been logging into InterSystems IRIS without creating new users first. InterSystems IRIS automatically creates these users when they are found on the LDAP server. The following procedure demonstrates this process:

1. Click the **Logout** link at the top left of the Management Portal.
2. Log into InterSystem IRIS using the following credentials:

   User Name: `user2`

   Password: `Password2`

   Remember that user2 has the **`%Manager`** role.
3. From the Management Portal home page, go to the **Users** page (**System Administration > Security > Users**).
4. Find user3 in the list and click **Delete** in its row.

   At this point, user3, the user with the **`%Developer`** role, no longer exists in InterSystems IRIS.
5. Click the **Logout** link at the top left of the Management Portal.
6. Log into InterSystem IRIS using the following credentials:

   User Name: `user3`

   Password: `Password3`

   Because user3 still exists on the LDAP server, you are able to log back into InterSystems IRIS as user3 even though you just deleted the user account in InterSystems IRIS.
7. If desired, you can log back into InterSystems IRIS to confirm that user3 is now a user.
   a. Click the **Logout** link at the top left of the Management Portal.
   b. Log into InterSystem IRIS using the following credentials:

      User Name: `user2`

Password: `Password2`

c. From the Management Portal home page, go to **System Administration > Security > Users**. User3 is now in the list even though you previously deleted the user account.

3 Learn More About LDAP and Security

You can use the following resources to learn more about LDAP and other security concepts.

- For detailed information about using LDAP with InterSystems IRIS, see Using LDAP in the *Security Administration Guide*.
- For an introduction to role-based security in InterSystems IRIS, see First Look: Role-Based Access Control.