LDAP Guide

Version 2023.1
2024-07-11

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

LDAP Guide
InterSystems IRIS Data Platform Version 2023.1 2024-07-11

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

1

LDAP and InterSystems IRIS®

InterSystems IRIS® provides support for authentication and authorization using LDAP, the Lightweight Directory Access Protocol. LDAP systems have a central repository of user information, from which InterSystems IRIS retrieves information. For example, on Windows, a domain controller using Active Directory is an LDAP server.

Support includes:

- LDAP authentication — InterSystems IRIS prompts users for a username and password. The instance is associated with an LDAP server, which performs authentication and retrieves the user's roles and other authorization information. The instance can also be configured to use cached credentials to authenticate users, in cases where it cannot connect to the LDAP server.
- LDAP authorization — InterSystems supports LDAP groups for specifying roles as part of authorization. LDAP authorization with OS-based authentication is used for the local InterSystems IRIS terminal. (Access to the Terminal is managed by **%Service_Console** on Windows and **%Service_Terminal** on all other operating systems.)

InterSystems IRIS can also provide authentication and authorization for multiple LDAP domains simultaneously.

You can also use LDAP with the InterSystems IRIS delegated authentication feature, which allows you to implement custom mechanisms to replace the authentication and role-management activities that are part of InterSystems security.

InterSystems IRIS provides LDAP support for:

- Active Directory
- OpenLDAP
- LDAP version 3 protocols (earlier LDAP protocols are not supported)

2

LDAP Authentication

2.1 Overview of Setting Up LDAP Authentication

To configure an InterSystems IRIS service or application to use an LDAP server for authentication:

1. Configure InterSystems IRIS to use the LDAP server:
   a. Enable LDAP and related features for the instance.
   b. Create an LDAP configuration for the instance of InterSystems IRIS. This includes specifying the names of LDAP user properties to be used for setting the values of properties of InterSystems IRIS users.
   c. Optionally, test the LDAP configuration.
   d. Optionally, configure the instance to support multiple LDAP domains.
   e. Set up a role that is required for logging in to the instance.
   f. Enable LDAP for the instance's relevant services and applications. This involves enabling LDAP for the entire instance of InterSystems IRIS and then enabling it for the relevant services or applications.

Note: To perform LDAP authentication programmatically, use InterSystems IRIS delegated authentication.

2.2 Enable LDAP for an Instance

The first step in configuring an instance of InterSystems IRIS to use LDAP is to enable the features you wish to use:

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. On the **Authentication/Web Session Options** page:
   - To enable LDAP authentication, select **Allow LDAP authentication**.
   - To enable authentication using LDAP cached credentials, select **Allow LDAP cache credentials authentication**. For more information on this topic, see LDAP Cached Credentials.
3. Click **Save** to apply the changes.

2.2.1 LDAP Cached Credentials

If you configure an instance to use *LDAP cached credentials*, it stores (caches) a copy of the credentials that it most recently used to authenticate each user. If an instance supports cached credentials and it cannot connect to the LDAP server, then it uses the cached LDAP credentials to authenticate users. This can be caused by an issue with the LDAP server itself or with the connection to the server.

To secure cached credentials, InterSystems IRIS stores all LDAP passwords in the security database as a one-way hash. If the instance cannot use the LDAP server to validate the user, it then attempts to confirm that:

- The hash of the entered password matches the hash of the stored password
- The cached expiration date from the last LDAP login has not been reached

If both conditions are true, the instance authenticates the user and login proceeds; otherwise, login fails.

2.3 Create or Modify an LDAP Configuration

To perform LDAP authentication, InterSystems IRIS uses an *LDAP configuration*. An LDAP configuration specifies a connection to an LDAP server for a particular security domain and has information required to:

- Connect to and query the LDAP server
- Retrieve the required information about the user being authenticated

Note: If Kerberos is enabled for an instance, all menu items and other labels for LDAP configurations refer to LDAP/Kerberos configurations. The following procedure does not note this in each individual situation.

To create or modify an LDAP configuration:

1. Go to the Management Portal **Security LDAP Configurations** page (**System Administration** > **Security** > **System Security** > **LDAP Configurations**).

   During installation, if you are installing InterSystems IRIS onto a machine that is currently using an LDAP server, InterSystems IRIS creates an LDAP configuration based on that LDAP server's domain and other configuration information.

2. Create or modify a configuration:

   - To modify an existing configuration, click its name. For example, if you are using the configuration associated with the local LDAP server, then you may simply wish to check this configuration's attributes and modify any as needed.
   - To create a configuration, click the **Create New LDAP Configuration** button. This displays the **Edit LDAP configuration** page.

     Note: When creating a configuration, on the **Edit LDAP configuration** page, select the **LDAP configuration** check box if it is available. This displays the fields that define the LDAP configuration.

3. Modify or complete the fields to define the configuration (listed below).
4. If you create multiple configurations, you must specify which one is the default on the **System-wide Security Parameters** page (**Security Administration** > **Security** > **System Security** > **System-wide Security Parameters**), using the **Default security domain** drop-down.

2.3.1 LDAP Configuration Fields

An LDAP configuration includes the following fields:

- **Login Domain Name** — *Required.* The name of the LDAP configuration. This is typically in the form of example.com or example.org.

  If you enter a value that does not include a period, the system appends .com to it, so that example becomes example.com. If you enter a value in uppercase, the system puts in lowercase, so that EXAMPLE.COM becomes example.com. The system performs both transformations, if appropriate.

  The system uses the transformed value of the **Name** field to populate the **LDAP Base DN to use for searches** field.

- **Description** — Any text to describe the configuration.

- **Copy from** — *Available only when creating a configuration.* Whether or not InterSystems IRIS copies attributes from an existing LDAP configuration to specify initial values for this one.

- **LDAP Enabled** — Whether or not InterSystems IRIS can use the configuration to connect to an LDAP server.

- **LDAP server is a Windows Active Directory server** — *Windows only.* Whether or not the LDAP server is a Windows Active Directory server.

- **LDAP hostnames** — *Required.* The name(s) of the host(s) on which the LDAP server is running. Separate multiple hostnames using spaces as a delimiter. The complexity of each hostname can range from an unqualified hostname to fully-qualified hostname with a port number; the required form of the hostname(s) depends on the particular configuration.

  If the LDAP server is configured to use a particular port, you can specify it by appending "`:`*portname*" to the hostname; typical usage is not to specify a port and to let the LDAP functions use the default port. You can specify the domain `example.com` as your hostname if you have multiple replicated domain servers on your network like:

  ```
  ldapserver.example.com
  ldapserver1.example.com
  ldapserver2.example.com
  ldapserver3.example.com
  ```

  LDAP performs a DNS query for the addresses of all the matching LDAP servers and then automatically selects one to connect to.

  Important: Including a port number in the value of **LDAP hostnames** affects the TLS behavior when establishing a connection:

  – If the value specified contains a port number *other than 636*, such as `ldapserver.example.com:389` and the **Use TLS/SSL encryption for LDAP sessions** check box is selected, then the instance attempts to establish a plaintext connection to the LDAP server and then issue a StartTLS command to encrypt the connection.

  – If the value specified for LDAP hostnames contains the port number *636*, such as `ldapserver.example.com:636`, then the instance attempts to establish a TLS connection with the LDAP server directly—whether or not the **Use TLS/SSL encryption for LDAP sessions** check box is selected. Note, however, that connecting directly to port 636 from UNIX® client instances is not supported.

  For background, see the class reference for the **%SYS.LDAP.Init()** method.

- LDAP search information — varies by circumstances:

– **LDAP username to use for searches** — *For Windows Active Directory servers only. Required if available.* The user name provided to the LDAP server to establish an initial connection and which is used to perform LDAP searches and lookups. This user is also known as the *search user*.

  The search user must have permission to read the entire LDAP database. It is important to ensure that the search user has uninterrupted access to the LDAP database. For example, the user's LDAP account should be set so that:

  - The user cannot change the account's password
  - The password never expires
  - The account never expires

  For more information on searching the LDAP database, see How LDAP Looks Up the Target User in Its Database.

– **LDAP search user DN** — *For all non-Windows platforms and Windows non-Active Directory servers. Required if available.* The Distinguished Name (DN) of the user provided to the LDAP server to establish an initial connection and which is used to perform LDAP searches and lookups. This user is also known as the *search user*.

  The search user must have permission to read the entire LDAP database. It is also important to ensure that the search user has uninterrupted access to the LDAP database. For example, the user's LDAP account should be set so that:

  - The user cannot change the account's password
  - The password never expires
  - The account never expires

  For example, if the search user is "ldapsearchuser", the LDAP DN (distinguished name) might be as follows:

  ```
  uid=ldapsearchuser,ou=People,dc=example,dc=com
  ```

  For more information on searching the LDAP database, see How LDAP Looks Up the Target User in Its Database.

- **LDAP username password** — *Available only when creating or modifying a configuration.* The password associated with the account used for the initial connection.
- **LDAP Base DN to use for searches** — *Required.* The point in the directory tree from which searches begin. This typically consists of domain components, such as `DC=example,DC=com`.
- **LDAP Base DN for Groups to use for searches** — *Required.* The point in the directory tree from which searches for nested groups begin. This typically consists of organizational units and domain components, such as `OU=IRIS,OU=Groups,DC=test,DC=com`. By default, this is set to the same value as **LDAP Base DN to use for searches**.
- **LDAP Unique search attribute** — *Required.* A unique identifying element of each record, which therefore makes it appropriate for searches. For more information on searching the LDAP database, see How LDAP Looks Up the Target User in Its Database.
- **Use TLS/SSL encryption for LDAP sessions** — Whether or not the InterSystems IRIS instance and the LDAP server encrypt their communications using TLS (disabled by default).

  Important: InterSystems recommends that you enable TLS encryption for LDAP.

  For connections to Active Directory servers, note the following:

  – When enabled for an LDAP connection from an instance on Windows to an Active Directory server, the connection uses port 636 (which is a TLS-encrypted port).

  - When enabled for an LDAP connection from an instance on UNIX® to an Active Directory server, InterSystems IRIS first establishes the connection on port 389 (the unencrypted LDAP port); encryption is then turned on by a **StartTLS** call.

  InterSystems also recommends setting the *LDAP server signing requirements* parameter to `Require signature` on the Active Directory Server. This prevents any LDAP **bind** command on the server on port 389 to be executed unless the channel is encrypted with StartTLS. For more information, see Domain Controller: LDAP Server Signing Requirements article on the Microsoft web site.

- **File with Certificate Authority certificate(s) to authenticate the LDAP server** — *UNIX® only.* The location of the file containing any TLS certificates (in PEM format) being used to authenticate the server.

  On Windows, to specify the location of a file containing any TLS certificates (in PEM format) being used to authenticate the server certificate to establish a secure LDAP connection, use Microsoft Certificate Services. Certificates must be installed in the Certificates (Local Computer)\Trusted Root Certification Authorities certificate store.

- **Allow ISC_LDAP_CONFIGURATION environment variable** — If you are using OS-based LDAP and multiple domains, specifies whether or not to use the *ISC_LDAP_CONFIGURATION* environment variable. If the environment variable is defined, then OS-based LDAP uses it to determine which LDAP configuration to use for authentication.

- **Use LDAP Groups for Roles/Routine/Namespace** — Whether or not the user's roles, routine, and namespace come from the user's group memberships (true by default); if not, then they come from the attribute fields of the user's LDAP record. If you select this field, the system enables and disables other fields (see each subsequent field for details).

  Note: InterSystems recommends the use of LDAP groups for authorization, rather than LDAP attributes (including InterSystems registered LDAP properties). If you have existing code or are otherwise required to use registered properties, see Configure Authorization with LDAP Attributes for details.

- **Search Nested Groups for Roles/Routine/Namespace** — *Only active if* **LDAP server is a Windows Active Directory server** *and* **Use LDAP Groups for Roles/Routine/Namespace** *are selected.* Whether or not search returns all of a user's nested groups. See Nested Groups for more information on nested groups.

- **Organization ID prefix for group names** — *Only active if* **Use LDAP Groups for Roles/Routine/Namespace** *is selected.* See LDAP Group Name Configuration for more information.

- **Allow Universal group Authorization** — *Only active if* **Use LDAP Groups for Roles/Routine/Namespace** *is selected.* Whether or not searches use the attributes on the LDAP server that are relevant for all InterSystems IRIS instances. See Create Universal LDAP Authorization Groups for more information.

- **Authorization Group ID** — *Only active if* **Use LDAP Groups for Roles/Routine/Namespace** *is selected.* The multiple-instance group to which this instance belongs. See Create LDAP Authorization Groups for Multiple Instances (Multiple-Instance Groups) for more information.

- **Authorization Instance ID** — *Only active if* **Use LDAP Groups for Roles/Routine/Namespace** *is selected.* The single-instance group to which this instance belongs. See Create LDAP Authorization Groups for a Single Instance (Single-Instance Groups) for more information.

- **User attribute to retrieve default namespace** (not active if LDAP groups are selected) — The attribute whose value is the source for the *Startup namespace* property for a user. This property of an InterSystems IRIS user is described in User Account Properties; this LDAP property is described in Configure Authorization with LDAP Attributes.

- **User attribute to retrieve default routine** (not active if LDAP groups are selected) — The attribute whose value is the source for the *Tag^Routine* property for a user. This property of an InterSystems IRIS user is described in User Account Properties; this LDAP property is described in Configure Authorization with LDAP Attributes.

- **User attribute to retrieve roles** (not active if LDAP groups are selected) — The attribute whose value determines the roles to which a user is assigned. When creating this attribute, it must be specified as an LDAP multivalued attribute.

For information about an InterSystems IRIS user's roles, see the **Roles** tab of a user's **Edit User** page; this LDAP property is described in Configure Authorization with LDAP Attributes.

- **User attribute to retrieve comment attribute** — The attribute whose value is the source for the *Comment* property for a user. This property is described in User Account Properties. Once a user has logged in, you can retrieve the value of this property using the **Security.Users.Get()** method.
- **User attribute to retrieve full name from** — The attribute whose value is the source for the *Full name* property for a user. This property is described in User Account Properties. Once a user has logged in, you can retrieve the value of this property using the **Security.Users.Get()** method.
- **User attribute to retrieve mail address** — The attribute whose value is the source for the *Email address* property for a user. This property is described in User Account Properties. Once a user has logged in, you can retrieve the value of this property using the **Security.Users.Get()** method.
- **User attribute to retrieve mobile phone** — The attribute whose value is the source for the *Mobile Phone Number* property for a user. This property is described in User Account Properties. Once a user has logged in, you can retrieve the value of this property using the **Security.Users.Get()** method.
- **User attribute to retrieve mobile provider from** — The attribute whose value is the source for the *Mobile Phone Service Provider* property for a user. This property is described in User Account Properties. Once a user has logged in, you can retrieve the value of this property using the **Security.Users.Get()** method.
- **LDAP attributes to retrieve for each user** — Any attributes whose values are the source for any application-specific variables. Application code can then use the **Get** method of the Security.Users class to return this information.

The values of the fields of an LDAP configuration are stored in an instance of the Security.LDAPConfigs class.

2.3.2 Note on LDAP/Kerberos Configuration Fields

If Kerberos authentication is enabled for an instance, then the page for creating an LDAP configuration is **Edit LDAP/Kerberos configurations** page. It has the same fields as the **Edit LDAP configurations** page, as described in LDAP Configuration Fields.

2.4 Test an LDAP Configuration

Once you have created an LDAP configuration, you can test it. This allows you to confirm that it properly connects to the LDAP server or troubleshoot any issues that arise. To test a configuration:

1. In the Management Portal, go to the **Security LDAP Configurations** page (**System Administration** > **Security** > **System Security** > **LDAP Configurations**).
2. Click **Test LDAP Authentication**.
3. In the **Username** and **Password** fields, enter a valid username and password defined on the LDAP server. If the instance is configured to use multiple domains, you must provide a fully qualified username, such as `EndUser@example.com`; if the instance is using only a single domain, simply enter the unqualified username (without the @ symbol or the domain name), such as `EndUser`.
4. Click **Test**.

The **Test Results** field displays output from the LDAP server.

Note: This feature only tests if an instance can connect to an LDAP server and perform authentication checks for the entered user. It does not perform any authorization or permission checks to determine if the user can successfully log in to the system.

If the test succeeds for the entered user, but the user cannot log in, then check the audit record for the login failure. To ensure successful login, you may need to give additional permissions to the user.

2.5 Use Multiple LDAP Domains

InterSystems IRIS supports LDAP authentication with multiple domains. This allows the instance to have user accounts that include the same username from more than one domain, such as EndUser@example.com and EndUser@otherexample.com. This feature can be useful in multiple scenarios. For example:

- It allows merging distinct sets of users from multiple domains into one larger group while preserving unique identifiers for each user.
- It allows the same individual to have accounts on multiple domains with varying privileges for each.

To use multiple domains:

1. Create additional LDAP configurations according to the instructions in Create or Modify an LDAP Configuration.
2. Configure the instance to use multiple domains and then specify a default domain:
   a. Enable the use of multiple domains for the instance. In the Management Portal, on the **System-wide Security Parameters** page (**System Administration** > **Security** > **System Security** > **System-wide Security Parameters**), select the **Allow multiple security domains** check box.
   b. Specify a default domain. In the Management Portal, on the **System-wide Security Parameters** page (**System Administration** > **Security** > **System Security** > **System-wide Security Parameters**), select a default domain using the **Default security domain** drop-down.
   c. Click **Save**.

   For more information about this page, see System-Wide Security Parameters.

Note: Even if you are using multiple domains, the name for each user must be unique, even if they are of different types. Hence, if you create a user such as EndUser@example.com that is a password user, you cannot then log in to InterSystems IRIS through LDAP as the user EndUser@example.com, as InterSystems IRIS cannot create the account for EndUser@example.com as an LDAP user.

2.6 Set Up a Required Login Role

If you have multiple instances of InterSystems IRIS and are using LDAP authentication or OS-based authentication with LDAP authorization, then InterSystems *strongly* recommends that each instance have a role that is required for the users who are connecting to it. This mechanism prevents users from accessing instances where they are insufficiently privileged; otherwise, a user who holds various roles on one instance may then have those same roles on an instance where this is not intended.

To set up a required login role:

1. For each instance, if the role to be required does not already exist, create it according to the instructions in Create Roles.
2. For each instance, specify the required role in the **Role required to connect to this system** field on the **System Security Settings** page (**System Administration** > **Security** > **System Security** > **System-wide Security Parameters**).
3. Add an LDAP group with a name that includes the name of the required role. The name of the group is of the form:

   `intersystems-Instance-`*instanceID*`-Role-`*rolename*

   where:

   - *instanceID* is the unique identifier for the instance on the LDAP server
   - *rolename* is the name of the role required to connect

Note: In certain circumstances, such as with mirroring, you may prefer to have a single required login role among multiple instances.

For example, suppose there are two systems, *TEST* and *PRODUCTION*. To secure each of these systems, create a role on **TEST** called **TESTACCESS** and a role on **PRODUCTION** called **PRODUCTIONACCESS**. On **TEST**, set the value of the **Role required to connect to this system** field to **TESTACCESS**; on **PRODUCTION**, set it to **PRODUCTIONACCESS**. Then, if a user is only allowed to access the **TEST** system, assign that user the **TESTACCESS** role *only* and do not assign the **PRODUCTIONACCESS** role to the user. For users who can access either system, assign them both **PRODUCTIONACCESS** and **TESTACCESS** roles.

2.7 Enable LDAP for Services and Applications

After enabling LDAP authentication for the instance, enable it for the instance's relevant services or applications:

1. Because LDAP authentication is enabled for the instance, an **LDAP** check box appears on the **Edit Service** page for the services that support LDAP authentication and the **Edit Web Application** page for web applications.
2. Enable LDAP authentication for services and applications as appropriate.

The following services support LDAP authentication:

- **%Service_Bindings**
- **%Service_CallIn**
- **%Service_ComPort**
- **%Service_Console**
- **%Service_Login**
- **%Service_Terminal**
- **%Service_Telnet**
- **%Service_WebGateway**

These fall into several categories of access modes:

- Local Access —

  %Service_CallIn, **%Service_ComPort**, **%Service_Console**, **%Service_Login**, **%Service_Terminal**, **%Service_Telnet**

To use LDAP authentication with local connections, enable it for the service.

- Client-Server Access —

  %Service_Bindings

  To use LDAP authentication with client-server connections, enable it for the service.

- Web Access —

  %Service_WebGateway

  To allow named users to log in to web applications using LDAP authentication, you will have to enable the relevant web applications to use LDAP. See Security Settings in "Defining Applications" for more information about adding authentication mechanisms to a web application. Enabling LDAP authentication for the service also allows the Web Gateway itself to authenticate using LDAP authentication.

2.8 The State of an Instance After LDAP Authentication

Any user who is initially authenticated using LDAP authentication is listed in the table of users on the **Users** page (**System Administration** > **Security** > **Users**) as having a Type of "LDAP user". If a system administrator has explicitly created a user through the Management Portal (or using any other native InterSystems IRIS facility), that user has a type of "InterSystems IRIS password user". If a user attempts to log in using LDAP authentication and is successfully authenticated, InterSystems IRIS determines that this user already exists as an InterSystems IRIS user — not an LDAP user — and so login fails.

2.9 View an LDAP Configuration in the Portal As %Operator

If you are logged in to the Management Portal as a user who has the **%Operator** role or the **%Admin_Operate:Use** privilege, you can view (but not edit) the instance's LDAP configurations:

1. In the Portal, go to the **LDAP Configurations** page (**System Operation** > **LDAP Configurations**).
2. On that page, click on the name of the configuration you wish to view, which displays the **Display LDAP Configuration** for that configuration.

To edit an LDAP configuration, go to the **Security LDAP Configurations** page (**System Administration** > **Security** > **System Security** > **LDAP Configurations**); you must have the **%Admin_Secure:Use** privilege.

2.9.1 The Security LDAP Configurations Page

The Portal's **Security LDAP Configurations** page (**System Operation** > **LDAP Configurations**) displays a list of the instance's LDAP configurations. Click the name of a configuration to view its properties. If Kerberos authentication is enabled for the instance, this is called the **Security LDAP/Kerberos configurations** page (**System Operation** > **LDAP/Kerberos configurations**).

3

LDAP Authorization

In addition to performing authentication with LDAP, InterSystems IRIS supports LDAP authorization. InterSystems recommends the use of LDAP groups rather than LDAP attributes for managing role, routine, and namespace definitions.

3.1 Overview of Configuring LDAP Authorization

To configure an InterSystems service or application to use LDAP for authorization:

1. Configure the instance for LDAP or OS-based authentication
2. For LDAP authorization:
   a. Design the groups for LDAP authorization on InterSystems IRIS instances
   b. Configure the LDAP server to use those groups

3.2 Configure Authorization with LDAP Groups

- LDAP Groups and InterSystems IRIS
- LDAP Authorization Group Models:
  - Create LDAP Authorization Groups for a Single Instance (Single-Instance Groups)
  - Create LDAP Authorization Groups for Multiple Instances (Multiple-Instance Groups), including Authorization for Mirroring
  - Create Universal LDAP Authorization Groups
- Other Topics for LDAP Authorization with LDAP Groups

3.2.1 LDAP Groups and InterSystems IRIS

LDAP groups allow you to assign privileges to users using an LDAP server:

- The schema on the LDAP server specifies the names of groups. Typically, the LDAP administrator defines these names; InterSystems IRIS uses one of three predefined name structures described below.

- Each group has a distinguished name (DN) that uniquely identifies it.
- Each group specifies access to an InterSystems IRIS role, routine, or namespace

InterSystems IRIS supports LDAP groups that provide authorization for:

- A single instance
- Multiple instances
- All instances

To set up groups for InterSystems IRIS:

1. Determine if you are going to use groups for a single instance, for multiple instances, or for all instances.
2. Create one or more groups with names that follow the appropriate naming convention. Each group specifies a user's role, default namespace, or default routine; since a user can have multiple roles, it is valid to belong to multiple groups that specify roles.

   Note: Note that when defining these groups on your LDAP server, they should be created as *security* groups, and not *distribution* groups.

3. Configure your LDAP users to specify which ones belong to which groups. This requires that, for each user's LDAP account, you assign the user to multiple groups to specify one or more roles, a default namespace, and a default routine. This determines which roles each user has after logging in, the user's default namespace, and the user's default routine.
4. Configure the local InterSystems IRIS instance so that there are definitions for all the roles that are specified on the LDAP server.

3.2.2 LDAP Authorization Group Models

InterSystems IRIS supports for three kinds of group authorization using LDAP.

- Create LDAP authorization groups for a single instance (single-instance groups)
- Create LDAP authorization groups for multiple instances (multiple-instance groups), including mirroring
- Create universal LDAP authorization groups

3.2.2.1 Create LDAP Authorization Groups for a Single Instance (Single-Instance Groups)

InterSystems IRIS allows you to create LDAP groups that provide authorization for only a single instance; hence, each of these is known as a *single-instance group*. To create this kind of authorization group:

1. On the InterSystems IRIS instance, confirm or modify the value of the LDAP parameter **Authorization Instance ID**. By default, its value is *NodeName_InstanceName*, where *NodeName* is the machine on which the InterSystems IRIS instance is running and *InstanceName* is the name of that instance.

   To set the parameter's value manually:

   a. In the Management Portal, go to the **Security LDAP Configurations** page (**Management Portal** > **System Administration** > **Security** > **System Security** > **LDAP Configurations**).

   b. On that page, select the configuration to edit by clicking on its name.

   c. On the page for editing the configuration that appears, select **Use LDAP Groups for Roles/Routine/Namespace**.

   d. Next, in the **Authorization Instance ID** field, enter the value for the parameter and click **Save**.

2. On the LDAP server, define role, namespace, and routine groups with names that conform to the required InterSystems structure and that use the `Instance` keyword, followed by the value of the **Authorization Instance ID**. Note that these strings are not case sensitive. These group names are of the form:

   `intersystems-Instance-`*AuthorizationInstanceIDValue*`-Role-`*RoleName*

   `intersystems-Instance-`*AuthorizationInstanceIDValue*`-Routine-`*RoutineName*

   `intersystems-Instance-`*AuthorizationInstanceIDValue*`-Namespace-`*NamespaceName*

   where:

   - *AuthorizationInstanceIDValue* is the value specified for the **Authorization Instance ID** field
   - *RoleName*, *RoutineName*, and *NamespaceName* are each the name of the role, default routine, or default namespace.

     Note: A user can have any number of roles; typically, access to the system requires at least one role. A user can have only one default routine and one default namespace; however, these are not required, so a user may have no default routine and no default namespace.

   - *RoleName* can include multiple roles, delimited by a "^". For example, "%All^Admin^Application4" includes the "%All", "Admin", and "Application4" roles.

3. On the InterSystems IRIS instance, configure a role associated with each group.

For example, suppose you are running an application on an instance called Test that is on a machine called Node1. You wish to set up three categories of users:

- Application users — Can only run the application
- Administrative users — Can run various administrative tools and the application
- Superusers — Have full access

To set up this authorization model, create the following groups on the LDAP server:

```
intersystems-Instance-Node1_Test-Role-Administrator
intersystems-Instance-Node1_Test-Role-LocalApplication
intersystems-Instance-Node1_Test-Role-%All
intersystems-Instance-Node1_Test-Routine-LocalApplication
intersystems-Instance-Node1_Test-Routine-%SS
intersystems-Instance-Node1_Test-Routine-%pmode
intersystems-Instance-Node1_Test-Namespace-%SYS
intersystems-Instance-Node1_Test-Namespace-USER
```

Next, create the roles that corresponds to each category of user:

- Administrator
- LocalApplication

Note: You do not need to create a **`%All`** role, because it already exists.

Finally, create the three categories of users:

- Application users — Can run only the application, LocalApplication; are assigned to the following LDAP groups:
  - `intersystems-Instance-Node1_Test-Role-LocalApplication`
  - `intersystems-Instance-Node1_Test-Routine-LocalApplication`
  - `intersystems-Instance-Node1_Test-Namespace-USER`

- Administrative users — Can run various administrative tools and the application; are assigned to the following LDAP groups:
  - `intersystems-Instance-Node1_Test-Role-LocalApplication`
  - `intersystems-Instance-Node1_Test1-Role-Administrator`
  - `intersystems-Instance-Node1_Test-Routine-%SS`
  - `intersystems-Instance-Node1_Test-Namepace-%SYS`
- Superusers — Have **`%All`** access; are assigned to the following LDAP groups:
  - `intersystems-Instance-Node1_Test-Role-%All`
  - `intersystems-Instance-Node1_Test-Namespace-%SYS`
  - `intersystems-Instance-Node1_Test-Routine-%pmode`

3.2.2.2 Create LDAP Authorization Groups for Multiple Instances (Multiple-Instance Groups)

InterSystems IRIS allows you to create LDAP groups that provide authorization for multiple instances; hence, each of these is known as a *multiple-instance group*. To create this kind of authorization group:

1. Determine how the various instances are sharing information among groups. This determines the group for each instance and the information to which users have access.
2. For each instance in the group, modify the value of the LDAP parameter **Authorization Group ID** to be the same as the other instances in the group.

   To set the parameter's value manually:

   a. In the Management Portal, go to the **Security LDAP Configurations** page (**Management Portal** > **System Administration** > **Security** > **System Security** > **LDAP Configurations**).

   b. On that page, select the configuration to edit by clicking on its name.

   c. On the page for editing the configuration that appears, select **Use LDAP Groups for Roles/Routine/Namespace**.

   d. Next, in the **Authorization Group ID** field, enter the value for the parameter and click **Save**.

3. On the LDAP server, set up role, namespace, and routine groups that conform to the required InterSystems structure and that use the `Group` keyword, followed by the value of the **Authorization Group ID**. Note that these strings are not case sensitive. These group names are of the form:

   `intersystems-Group-`*AuthorizationGroupIDValue*`-Role-`*RoleName*

   `intersystems-Group-`*AuthorizationGroupIDValue*`-Routine-`*RoutineName*

   `intersystems-Group-`*AuthorizationGroupIDValue*`-Namespace-`*NamespaceName*

   where:

   - *AuthorizationGroupIDValue* is the value specified for the Authorization Group ID field
   - *RoleName*, *RoutineName*, and *NamespaceName* are each the name of the role, default routine, or default namespace.

     Note: A user can have any number of roles; typically, access to the system requires at least one role. A user can have only one default routine and one default namespace; however, these are not required, so a user may have no default routine and no default namespace.

   - *RoleName* can include multiple roles, delimited by a "^". For example, "%All^Admin^Application4" includes the "%All", "Admin", and "Application4" roles.

4. Configure the required roles on all the instances that are using them.

For example, suppose you have seven ECP application servers attached to five database servers. Two of the database servers are a failover pair, and the other three are async reporting members. All these servers (both the application servers and the database servers) run the SALES application. The application's end users need a more limited set of privileges and its administrative users need greater privileges. Hence, you set up three categories of users:

- Application users — Can only run the application
- Application server administrators — Can run the application; have full access to the application servers and no access to the database servers
- Database administrators — Have full access to the application servers and administrative access to the database servers

To configure LDAP authorization to support these requirements:

- Set the **Authorization Group ID** on the applications servers to SALESAPP
- Set the **Authorization Group ID** on the database servers to SALESDB

On the LDAP server, define the groups as follows:

```
intersystems-Group-SALESAPP-Role-%All
intersystems-Group-SALESAPP-Role-LocalApplication
intersystems-Group-SALESAPP-Routine-LocalApplication
intersystems-Group-SALESAPP-Routine-%pmode
intersystems-Group-SALESAPP-Namespace-USER
intersystems-Group-SALESAPP-Namespace-%SYS
intersystems-Group-SALESDB-Role-Administrator
intersystems-Group-SALESDB-Routine-INTEGRIT
intersystems-Group-SALESDB-Namespace-%SYS
```

Next, create the roles that corresponds to each category of user:

- Administrator
- LocalApplication

Note: You do not need to create a **`%All`** role, because it already exists.

Finally, create the three categories of users:

- Application users – Can only run the application, LocalApplication; are assigned to the following LDAP groups:
  - `intersystems-Group-SALESAPP-Role-LocalApplication`
  - `intersystems-Group-SALESAPP-Routine-LocalApplication`
  - `intersystems-Group-SALESAPP-Namespace-USER`
- Application server administrators — Can run the application, have full access to the application servers, and have no access to the database servers; are assigned to the following LDAP groups:
  - `intersystems-Group-SALESAPP-Role-LocalApplication`
  - `intersystems-Group-SALESAPP-Namespace-USER`
  - `intersystems-Group-SALESAPP-Role-%All`
  - `intersystems-Group-SALESAPP-Routine-%pmode`
- Database administrators — Have full access to the application servers and administrative access to the database servers; are assigned to the following LDAP groups:
  - `intersystems-Group-SALESAPP-Role-%All`

- intersystems-Group-SALESAPP-Routine-%pmode
- intersystems-Group-SALESAPP-Namespace-%SYS
- intersystems-Group-SALESDB-Role-Administrator
- intersystems-Group-SALESDB-Routine-INTEGRIT
- intersystems-Group-SALESDB-Namespace-%SYS

At this point, there is a fully functioning authorization model, but it does not include any superuser access to the database servers (that is, with **%All**). To add such access, create and add users to the following new group:

intersystems-Group-SALESDB-Role-%All

3.2.2.3 Configure LDAP Authorization Groups with Mirroring

In you are using LDAP and mirroring, InterSystems recommends using multiple-instance LDAP groups to configure authorization. Create the required multiple-instance groups and configure all the users on all members (including any async members) to use these groups.

Consider the following example, which is based on the group structure defined in the example above. Suppose, additionally:

- There is a mirror called SALESDBMIR which is a failover pair and three reporting async members
- You wish to have users with **%All**, but only on the failover pair

To configure authorization for this mirror:

1. To provide full access to the failover pair, create the group

   intersystems-Group-SALESDBMIRFAILOVER-Role-%All

2. To provide full access to the asynchronous members, create the group

   intersystems-Group-SALESDBMIRASYNC-Role-%All

3. Set the LDAP parameter **Authorization Instance ID** on each member in the failover pair to SALESDBMIRFAILOVER.

   Important: Because a disaster recovery (DR) async member may be promoted to failover member, the **Authorization Instance ID** for any DR async should also be set to SALESDBMIRFAILOVER

4. Set the LDAP parameter **Authorization Group ID** on the mirror's asynchronous members to SALESDBMIRASYNC.
5. Next, create the mirror administrators, who have **%All** access to the application servers; administrative access to the nonmirrored database servers; and **%All** access to the failover pair only. These users are assigned to the following LDAP groups:
   - intersystems-Group-SALESAPP-Role-%All
   - intersystems-Group-SALESAPP-Routine-%pmode
   - intersystems-Group-SALESAPP-Namespace-%SYS
   - intersystems-Group-SALESDB-Role-Administrator
   - intersystems-Group-SALESDB-Routine-INTEGRIT
   - intersystems-Group-SALESDB-Namespace-%SYS
   - intersystems-Group-SALESDBMIRFAILOVER-Role-%All
6. Finally, create the full administrators, who have **%All** access to all the members (the application servers, the database servers, the failover pair, and the asynchronous members). These users are assigned to the following LDAP groups:

- `intersystems-Group-SALESAPP-Role-%All`
- `intersystems-Group-SALESDB-Role-%All`
- `intersystems-Group-SALESDBMIRFAILOVER-Role-%All`
- `intersystems-Group-SALESDBMIRASYNC-Role-%All`

3.2.2.4 Create Universal LDAP Authorization Groups

InterSystems IRIS allows you to create LDAP groups that provide authorization for all its instances that use a single LDAP server; these are known as *universal authorization groups*. To create this kind of authorization group:

1. Enable the use of universal authorization groups for the current instance:
   a. In the Management Portal, go to the **Security LDAP Configurations** page (**Management Portal** > **System Administration** > **Security** > **System Security** > **LDAP Configurations**).
   b. On that page, select the configuration to edit by clicking on its name, which displays the page for editing that configuration.
   c. On the page for editing the configuration, select **Use LDAP Groups for Roles/Routine/Namespace**.
   d. Select **Allow Universal group Authorization**.
   e. Click **Save**.
2. On the LDAP server, set up role, namespace, and routine groups that conform to the required InterSystems structure. Note that these strings are not case sensitive. These group names are of the form:

   `intersystems-Role-`*RoleName*

   `intersystems-Routine-`*RoutineName*

   `intersystems-Namespace-`*NamespaceName*

   where *RoleName*, *RoutineName*, and *NamespaceName* are each the name of the role, default routine, or default namespace. *RoleName* can include multiple roles, delimited by a "^". For example, "%All^Admin^Application4" includes the "%All", "Admin", and "Application4" roles.

   Note: A user can have any number of roles; typically, access to the system requires at least one role. A user can have only one default routine and one default namespace; however, these are not required, so a user may have no default routine and no default namespace.
3. Configure the required roles on all the instances that are using the LDAP server.

For example, suppose you have an application called LocalApplication and you wish to grant various levels of access to it for users on all the InterSystems IRIS instances that use your LDAP server. Define the following LDAP groups:

```
intersystems-Role-%All
intersystems-Role-Administrator
intersystems-Role-LocalApplication
intersystems-Routine-%SS
intersystems-Routine-LocalApplication
intersystems-Namespace-USER
intersystems-Namespace-%SYS
```

Next, create the roles that corresponds to each category of user:

- Admin
- LocalApplication

Note: You do not need to create a **%All** role, because it already exists.

Finally, create the three categories of users:

- Application users – Have access to the application on all servers; are assigned to the following LDAP groups:
  - `intersystems-Role-LocalApplication`
  - `intersystems-Routine-LocalApplication`
  - `intersystems-Namespace-USER`
- Administrators — Have administrative access to all servers; are assigned to the following LDAP groups:
  - `intersystems-Role-Administrator`
  - `intersystems-Routine-%SS`
  - `intersystems-Namespace-%SYS`
- Superusers — Have full access to all servers; are assigned to the following LDAP groups:
  - `intersystems-Role-%All`

3.2.3 Other Topics for LDAP Authorization with LDAP Groups

Topics include:

- LDAP Group Definition Structure
- LDAP Group Name Configuration
- Mix Different Kinds of Groups
- Nested Groups
- How LDAP Groups Regulate Access to InterSystems IRIS

3.2.3.1 LDAP Group Definition Structure

Group definitions typically include:

- The group name
- A declaration of the group's organizational unit: `OU=Groups`
- A declaration of the domain component (DC) such as `DC=example,DC=com`
- Any other required information

For example, some possible group definitions might be:

```
CN=intersystems-Role-Administrator,OU=Groups,DC=intersystems,DC=com
CN=intersystems-Group-MyGroup-Namespace-USER,OU=Groups,DC=intersystems,DC=com
CN=intersystems-Instance-MyNode:MyInstance-Routine-INTEGRIT,OU=Groups,DC=intersystems,DC=com
```

3.2.3.2 LDAP Group Name Configuration

InterSystems IRIS allows you to further configure LDAP group names. The following sections describe the default configuration, the configurable properties, and the procedure to change them.

- Default Group Name Configuration

Default Group Name Configuration

By default, LDAP group names use the following syntax:

`intersystems-Role-`*RoleName*

`intersystems-Routine-`*RoutineName*

`intersystems-Namespace-`*NamespaceName*

`intersystems-Group-`*GroupName*`-Role-`*RoleName*

`intersystems-Group-`*GroupName*`-Routine-`*RoutineName*

`intersystems-Group-`*GroupName*`-Namespace-`*NamespaceName*

`intersystems-Instance-`*InstanceName*`-Role-`*RoleName*

`intersystems-Instance-`*InstanceName*`-Routine-`*RoutineName*

`intersystems-Instance-`*InstanceName*`-Namespace-`*NamespaceName*

Group Name Properties

Group names consist of the following configurable properties:

- *OrganizationID* — Default `intersystems`. Replace the `intersystems` segment of the group name with a user-defined or empty string. For example, if set to `OrgABC`, then the group name becomes:

  `OrgABC-Role-`*RoleName*

  `OrgABC-Group-`*GroupName*`-Routine-`*RoutineName*

  `OrgABC-Instance`*InstanceName*`-Namespace-`*NamespaceName*

  If set to the empty string, then the group name becomes:

  `Role-`*RoleName*

  `Group-`*GroupName*`-Routine-`*RoutineName*

  `Instance-`*InstanceName*`-Namespace-`*NamespaceName*

- *DelimiterID* — Default hyphen (-). This is the delimiter between segments in the group name. For example, if set to underscore (_), then the group name becomes:

  `intersystems_Role_`*RoleName*

  `intersystems_Group_`*GroupName*`_Routine_`*RoutineName*

  `intersystems_Instance_`*InstanceName*`_Namespace_`*NamespaceName*

- *GroupID* — Default `Group`. For example, if set to `SystemGrouping`, then the group name becomes:

  `intersystems-SystemGrouping-`*GroupName*`-Role-`*RoleName*

  `intersystems-SystemGrouping-`*GroupName*`-Routine-`*RoutineName*

  `intersystems-SystemGrouping-`*GroupName*`-Namespace-`*NamespaceName*

- *InstanceID* — Default `Instance`. For example, if set to `SystemInstance`, then the group name becomes:

  `intersystems-SystemInstance-`*InstanceName*`-Role-`*RoleName*

  `intersystems-SystemInstance-`*InstanceName*`-Routine-`*RoutineName*

`intersystems-SystemInstance-`*InstanceName*`-Namespace-`*NamespaceName*

- *RoleID* — Default `Role`. For example, if set to `SystemRole`, then the group name becomes:

  `intersystems-SystemRole-`*RoleName*

  `intersystems-Group-`*GroupName*`-SystemRole-`*RoleName*

  `intersystems-Instance-`*InstanceName*`-SystemRole-`*RoleName*

- *NamespaceID* — Default `Namespace`. For example, if set to `SystemNamespace`, then the group name becomes:

  `intersystems-SystemNamespace-`*NamespaceName*

  `intersystems-Group-`*GroupName*`-SystemNamespace-`*NamespaceName*

  `intersystems-Instance-`*InstanceName*`-SystemNamespace-`*NamespaceName*

- *RoutineID* — Default `Routine`. For example, if set to `SystemRoutine`, then the group name becomes:

  `intersystems-SystemRoutine-`*RoutineName*

  `intersystems-Group-`*GroupName*`-SystemRoutine-`*RoutineName*

  `intersystems-Instance-`*InstanceName*`-SystemRoutine-`*RoutineName*

Procedure for Changing Properties

To change these properties:

1. In the Management Portal, go to the **Security LDAP Configurations** page (**Management Portal** > **System Administration** > **Security** > **System Security** > **LDAP Configuration**).
2. To edit a configuration, click on its name.
3. On this page, you can edit the *OrganizationID* property. Click on **Advanced Settings** to view and edit the rest of the properties.
4. Click **Save** at the top of the page to save your changes.

3.2.3.3 Mix Different Kinds of Groups

You can use universal groups in conjunction with single-instance or multiple-instance roles.

For example, suppose you:

- Have an application on multiple instances
- Are using universal groups
- Have a user named UserOne who can run the application on all instances, but cannot use it as an administrator on any machine

You would like for UserOne to:

- Continue to be able to run the application on all instance
- Additionally, to be able to administer the application on a particular instance, called APPTEST, on a particular machine, called Test

To do this:

1. Set the authorization instance ID on the APPTEST instance on the Test machine to Test:APPTEST
2. Create the following group on the LDAP server:

```
intersystems-Instance-Test_APPTEST-Role-Administrator
```

3. Assign this group to UserOne on the LDAP server
4. Create the Administrator role on the APPTEST instance on the Test machine and grant it administrative access

You can also mix authorization groups in other ways. For example, if UserTwo has **%All** permission on all the instances authenticating to the LDAP server, you can give UserTwo exclusive administrative permission on an instance called SECRET on a machine called Server10. To do this, disable **Allow universal groups access** and then go through the process of assigning an `intersystems-Instance-Server10_SECRET-Role-Administrator` to that user.

3.2.3.4 Nested Groups

On an Active Directory LDAP server, LDAP groups include support for what are known as *nested groups*. A nested group is a group that is a member of a parent group, which means that all the users who are members of the nested group are implicitly members of the parent group. For example, suppose that there are two LDAP groups defined, known as *ABC* and *DEF*. You can make *ABC* a nested group within *DEF*; this means that, if a user is a member of *ABC*, then they are also a member of *DEF* without explicitly assigning the user to that group.

When searching for a user's nested groups, InterSystem IRIS returns only groups that are defined as Security Groups on the LDAP server. If you are using nested groups, ensure that any group used as a role for an InterSystems IRIS system is created as a Security Group.

Note: Systems which do not use nested groups will return both Security and Distribution groups.

3.2.3.5 How LDAP Groups Regulate Access to InterSystems IRIS

Through their LDAP groups, users receive roles along with a default namespace and a default routine. If the user's granted roles lack sufficient privilege for any required point of access for an instance, the user then is denied access to that instance; for example, if a user lacks sufficient privilege to use their default routine, that user is denied access.

The following rules also apply:

- If a user is assigned to a group for a role, but that role is not defined on the instance where the user is logging in, then the user does not have that role on that instance.
- If a user is assigned to a group for a default routine, but that routine is not defined on the instance where the user are logging in, then the user cannot connect to the instance.
- If a user is assigned to a group for a default namespace, but that namespace is not defined on the instance where the user are logging in, then the user cannot connect to the instance.

3.3 Configure LDAP Authorization with Operating System–Based Authentication

Topics include:

- Operating System LDAP Authentication
- Enable OS/LDAP for an InterSystems IRIS Instance
- Enable OS/LDAP for the %Service_Console and %Service_Terminal Services
- OS/LDAP with a Single Domain and Multiple Domains

- Configure OS/LDAP with Multiple Domains for Simplified Prompting

3.3.1 Operating System LDAP Authentication

InterSystems IRIS allows you to configure your system to support operating system–based authentication, and then to perform authorization via LDAP. This is known as *Operating System LDAP authorization* or *OS/LDAP*. It allows a user to authenticate to InterSystems IRIS using credentials from the operating system login and then to have their authorization information retrieved from an LDAP server. Operating system LDAP authorization is available in the Console on Windows and in the Terminal and on UNIX®, Linux, and macOS.

To configure OS/LDAP:

1. Enable OS-based authentication with LDAP authorization for an InterSystems IRIS instance.
2. As with standard LDAP authentication, set up a role that is required in order to be able to log in to the instance.
3. Enable OS/LDAP for the %Service_Console and %Service_Terminal services.
4. Configure authorization. This occurs in the same manner as that which accompanies LDAP authentication, as described in Configure LDAP Authorization for InterSystems IRIS.
5. If you are using multiple domains, optionally configure OS/LDAP for simplified prompting.

3.3.2 Enable OS/LDAP for an InterSystems IRIS Instance

To use OS/LDAP, first enable it for the instance:

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. On the **Authentication/Web Session Options** page, select **Allow Operating Systems LDAP authentication**.
3. Click **Save** to apply the changes.

3.3.3 Enable OS/LDAP for the %Service_Console and %Service_Terminal Services

To enable OS/LDAP for the instance's relevant services or applications:

1. With LDAP authentication enabled for the instance, an **Operating System LDAP Authorization** check box appears on the **Edit Service** page for **`%Service_Console`** and **`%Service_Terminal`**, which are the services that support OS/LDAP.
2. Enable LDAP authentication for those services, as appropriate.

3.3.4 OS/LDAP with a Single Domain and Multiple Domains

OS/LDAP supports the use of a single domain or multiple domains.

When InterSystems IRIS is configured to support only a single domain:

1. The system prompts the user for a username and password for the first login.
2. For subsequent logins, there is no prompt because the operating system has already authenticated the user.

When InterSystems IRIS is configured to support multiple domains:

1. The system prompts the user for a username and password for the first login.
2. For subsequent logins, the operating system prompts for a username and password by default. You can configure InterSystems IRIS to prevent this prompting; see the next section.

3.3.5 Configure OS/LDAP with Multiple Domains for Simplified Prompting

If you are using OS/LDAP and multiple domains, you can configure the instance for simplified prompting. By default, users are prompted for a username and password at every login. You can configure InterSystems IRIS so that there is only a username/password prompt when a user first logs in, and that subsequent connections are authenticated without prompting.

To configure InterSystems IRIS for this behavior:

1. For each user, create the environment variable *ISC_LDAP_CONFIGURATION* with a value of the domain in which the user is authenticating.
2. For each domain in which users are authenticating:
   a. Ensure that there is an LDAP configuration or create one.
   b. For that LDAP configuration, select the **Allow ISC_LDAP_CONFIGURATION environment variable** check box, which enables use of the environment variable.

3.4 Configure Authorization with LDAP Attributes

For LDAP authorization, InterSystems recommends the use of LDAP groups. However, InterSystems also supports authorization using LDAP attributes. There are three registered OIDs that are available for use with an LDAP schema to store authorization information. Each has its own dedicated purpose:

- *intersystems-Namespace* — The name of the user's default namespace (OID 1.2.840.113556.1.8000.2448.2.1).
- *intersystems-Routine* — The name of the user's default routine (OID 1.2.840.113556.1.8000.2448.2.2).
- *intersystems-Roles* — The name of the user's login roles (OID 1.2.840.113556.1.8000.2448.2.3).

To use these attributes, the procedure on the LDAP server is:

1. Enable the attributes for use. To do this, modify the value of *objectClass* field in the LDAP schema by appending the `intersystemsAccount` value to its list of values. (`intersystemsAccount` has an LDAP OID of 1.2.840.113556.1.8000.2448.1.1.)
2. Add the fields (as few or as many as required) to the schema.
3. Populate their values for the entries in the LDAP database.

Note: It is not required to use the registered LDAP schema names. In fact, you may use existing attributes from your LDAP schema.

For example, with a UNIX® LDAP server, to define the schema for using LDAP authentication with InterSystems IRIS, use the content that appears in the following definitions:

```
# Attribute Type Definitions

attributetype ( 1.2.840.113556.1.8000.2448.2.1 NAME 'intersystems-Namespace'
       DESC 'InterSystems Namespace'
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE )
```

```
attributetype ( 1.2.840.113556.1.8000.2448.2.2 NAME 'intersystems-Routine'
        DESC 'InterSystems Routine'
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128} SINGLE-VALUE )

attributetype ( 1.2.840.113556.1.8000.2448.2.3 NAME 'intersystems-Roles'
        DESC 'InterSystems Roles'
        EQUALITY caseIgnoreMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# Object Class Definitions

objectclass ( 1.2.840.113556.1.8000.2448.1.1
        NAME 'intersystemsAccount'
        SUP top
        AUXILIARY
        DESC 'Abstraction of an account with InterSystems attributes'
        MAY (
                intersystems-Routine $
                intersystems-Namespace $
                intersystems-Roles
        )
)
```

This content goes to two locations:

- Place it in the intersystems.schema file in the /etc/openldap/schema/ directory.
- Include it, along with any other content, in the /etc/openldap/slapd.conf file.

4

Other LDAP Topics

4.1 Create a Secure Outbound LDAP Connection

While this document primarily concerns using LDAP for authentication and authorization when connecting to InterSystems IRIS, you may also connect from InterSystems IRIS to an LDAP server. To establish a secure outbound connection to an LDAP server, InterSystems IRIS includes support for TLS. For more information on this topic, see the class documentation for %SYS.LDAP, in the content for the Init method.

4.2 Use the LDAP APIs

The %SYS.LDAP class supports LDAP programmatically.

If you are using the InterSystems IRIS LDAP APIs with certificates on UNIX® and need detailed debugging information, you may wish to use the ldapsearch program that is part of the OpenLDAP package. Once you have corrected any problems with certificates, you can use the test configuration tool to verify that the connection is functioning. The ldapsearch program may also be useful for debugging other LDAP connection problems.

4.3 How Various LDAP Actions Occur

This section describes what occurs during certain processes associated with LDAP authentication and authorization:

- How LDAP Performs Authentication and Authorization
- How LDAP Looks Up the Target User in Its Database
- How an Instance Checks and Removes Local Accounts Based on LDAP Account Conditions

4.3.1 How LDAP Performs Authentication and Authorization

When a user attempts to authenticate to an instance of InterSystems IRIS that uses LDAP authentication, the process is:

1. The user is prompted for a user name and password. This user, who is trying to authenticate, is known as the *target user.*

2. InterSystems IRIS establishes a connection to the LDAP server using the values specified for the **LDAP username to use for searches** and **LDAP username password**. This user, who has privileges to search the LDAP database so that InterSystems IRIS can retrieve information, is known as the *search user.*
3. Once the connection is established, the next step is to look up the target user in the LDAP database using the **LDAP Unique search attribute**.
4. If the target user is found in the LDAP database, it retrieves the attributes associated with the user, such as the user's roles, namespace, and routine.
5. InterSystems IRIS then attempts to authenticate the user to the LDAP database, using the user name and password provided in step 1.
6. If authentication succeeds, authorization occurs on the LDAP server (either via group assignment or attributes). The user can then interact with InterSystems IRIS based on the privileges associated with their roles and any publicly available resources. The user's properties are displayed read-only in the Management Portal and are not editable from within InterSystems IRIS.

4.3.2 How LDAP Looks Up the Target User in Its Database

Once InterSystems IRIS has established a connection to the LDAP server as the search user, it next retrieves information about the target user. To do this, InterSystems IRIS checks the username provided at login against values in the LDAP database for the *LDAP Unique search attribute*. The name of this attribute is often "sAMAccountName" for an Active Directory LDAP server and "uid" for an OpenLDAP server.

Once InterSystems IRIS has located the user, it retrieves attribute information. It retrieves information about every named attribute in the InterSystems IRIS LDAP configuration fields (described in Create or Modify an LDAP Configuration), and it retrieves all values associated with each attribute. Note that InterSystems IRIS retrieves all values associated with all attributes specified for the user in the InterSystems IRIS LDAP configuration fields; it is not possible to configure it to retrieve only a subset of these.

4.3.3 How an Instance Checks and Removes Local Accounts Based on LDAP Account Conditions

InterSystems IRIS removes a user account on the local instance when the account meets any of the following conditions:

- The LDAP account no longer exists
- The LDAP account is disabled
- On Active Directory only, the LDAP account has the flag set to require a password change
- On Active Directory only, the LDAP account is expired

InterSystems IRIS checks for these conditions and removes accounts under the following circumstances:

- When a user attempts to log in to an InterSystems IRIS instance, the instance checks the user's LDAP account. If any of the specified conditions are true for the LDAP account, InterSystems IRIS removes the local user account.
- As a result of the SecurityScan task. InterSystems IRIS comes with this task; run it to determine if any of these conditions are true for the LDAP account associated with any local user account. If so, InterSystems IRIS removes the local user account.