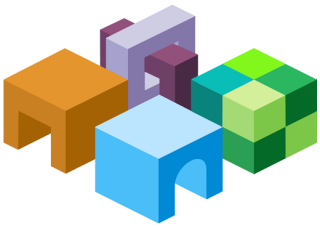


HYPERION® SYSTEM™ 9

SHARED SERVICES™

RELEASE 9.2.0.3

SECURITY AND PROVISIONING BEST PRACTICES WHITEPAPER

Hyperion™

CONTENTS IN BRIEF

About This Document

Overview

This whitepaper provides strategies and tips on setting up the security environment for Hyperion System 9 products. It presents a checklist to help you configure external user directories and a list of best practices to ensure good performance.

Audience

This document is targeted at implementation specialists who need to establish the security environment for Hyperion System 9 products by configuring user directories.

Assumptions

- Knowledge about user directories and their structures
- Expertise in configuring user directories

Information Sources

- *Hyperion System 9 Installation Start Here*
- *Hyperion System 9 Shared Services Installation Guide*
- *Hyperion System 9 User Management Guide*
- *Hyperion System 9 Documentation Addendum 9.2.0.3*
- Documentation from the vendors of your user directory

User Directories and Hyperion System 9 Products

Hyperion System 9 products are supported on a large number of user and identity management systems, which are collectively referred to as user directories. These include Lightweight Directory Access Protocol (LDAP) enabled user directories such as Sun Java System Directory Server (formerly SunONE Directory Server) and Microsoft Active Directory, Windows NT LAN Manager (NTLM), SAP Provider, and custom-built user directories that support LDAP version 3. See *Hyperion System 9 Installation Start Here* for a complete list of supported user directories.

Role of User Directories

By default, Hyperion installs and configures OpenLDAP to support Hyperion System 9 products. Additional external user directories can be configured as the source of user and group information for Hyperion System 9 products.

Hyperion System 9 products require a user directory account for each user who accesses the products. These users may be assigned to one or more user directory groups to facilitate provisioning. Information about the user and the user's groups is used to provide role-based access to Hyperion System 9 products and data.

Users

User directories contain accounts for each user who can access Hyperion System 9 products. Each user directory that stores user information must be configured on Shared Services to support the authorization processes, which is referred to as provisioning. Users from all configured user directories are visible from Hyperion® System™ 9 Shared Services™ User Management Console™.

OpenLDAP is automatically installed and configured with Shared Services. Refer to *Hyperion System 9 Shared Services Installation Guide* for detailed information on working with OpenLDAP and configuring external user directories.

In most deployment scenarios, existing user directories containing users and groups are used to support the Hyperion System 9 provisioning process. For information on working with these user directories, see vendor documentation.

Users can be individually provisioned to grant access rights on the Hyperion System 9 applications registered with Shared Services. Hyperion does not recommend the provisioning of individual users since it imposes administrative overhead.

Groups

Groups are containers for users or other groups. Groups from all configured user directories are displayed in User Management Console.

The procedures to create groups and assign group membership vary depending on the user directory being used. For information on creating OpenLDAP groups, see *Hyperion System 9 User Management Guide*. For information on creating and managing groups in external use directories, see the vendor documentation.

To reduce administrative overhead in the provisioning process, Hyperion recommends that you provision groups rather than users.

OpenLDAP (Native Directory)

OpenLDAP, an open source LDAP-enabled user directory, is configured with Shared Services. It is a standards-based hierarchical directory that is typically used to store user and group hierarchical data. OpenLDAP uses Berkeley DB (BDB) as its repository to provide fast reads. OpenLDAP is used in two ways:

- As the central storage for all Hyperion provisioning information, it stores the relationships among users, groups, and Hyperion System 9 application roles.
- To maintain and manage the default Shared Services user accounts required by Hyperion products.

OpenLDAP is accessed and managed using the User Management Console. Refer to *Hyperion System 9 User Management Guide* for OpenLDAP administrative procedures.

Migrating Users and Groups from Pre-System 9 Releases

If you are upgrading Hyperion products to Hyperion System 9 from a release that did not support provisioning, you must externalize users and groups from the products to Shared Services. You can externalize users who were authenticated through native product security or through an external directory in that release. Each product has a tool that enables you to externalize users, groups, and role information to Shared Services. After completing the externalization process, you can provision users or groups from Shared Services as needed.

See *Hyperion System 9 User Management Guide* and the provisioning appendix in Hyperion System 9 product documentation for detailed procedures.

User Directory Terminology

This section presents commonly used LDAP terminology.

Table 1

Term	Definition
cn	Common Name. The default attribute for users/groups in MSAD.
dc	Domain Component. A partition on a user directory.
DN	Distinguished Name. The DN uniquely identifies each entry in the directory.
BaseDN	The DN of a node in the user directory where the search for users and groups should begin. All the users and groups used by Hyperion products must be available within the BaseDN.
UserDN	A fully qualified user entry that uniquely identifies a user on the user directory.
RDN	Relative Distinguished Name. The entry of an object that is unique relative to its siblings.
User RDN	The Relative Distinguished Name of a user.
Group RDN	The Relative Distinguished Name of a group.
sAMAccountName	Security Account Manager Name Entry that uniquely identifies an object. Available only on NTLM and MSAD.
uid	User ID, the default user attribute in LDAP.
Object Class	Structures attached to entries that define allowed attributes. For example, object class `A` may be defined to take the attributes `name`, `address`, and `phone`.
ou	Organization Unit. OU is a directory partition.
Login Attribute	A user directory attribute that identifies the user during authentication. The user enters the value of this attribute as the user name at login.

Term	Definition
Identity Attribute	The entry that uniquely identifies an object; for example, a DN like `cn=joe,ou=People,DC=Hyperion,DC=com`

User Directory Design Considerations

In a typical deployment scenario, the users of Hyperion System 9 applications are already defined in one or more user directories. The Hyperion System 9 deployment expert has to reconcile the user and group definitions available in existing user directories to ensure good performance benchmarks during login and during any process that involves querying the user directories.

Supported User Directories

Hyperion System 9 products are tested on SunONE LDAP 5.2, Novell eDirectory 8.73, IBM LDAP server, and MSAD. In addition to these, Hyperion System 9 applications work with LDAP Version 3 compliant user directories, although these are not tested. Using untested user directories may raise integration issues, because the values required by Shared Services user directory configuration settings may not match those supported by the user directory. In such scenarios, use the vendor documentation to identify the configuration settings that are equivalent to the required Shared Services configuration settings.

Understand the Existing User Directory Structure

Before making decisions about provisioning Hyperion System 9 applications, use a standard LDAP Browser to explore the user directories that store user credentials. The settings that the LDAP Browser uses to connect to the user directory are identical to those that Hyperion System 9 applications use to connect to the user directories.

You can download a free LDAP Browser from `http://www-unix.mcs.anl.gov/~gawor/ldap/dwld/bin-dwld.cgi?fileid=282b2zip`.

Use the LDAP Browser to determine the following:

- Whether you can connect to the user directory from the server you are using
- The response time
- The starting point (base DN) for any search of the user directory
- A count of the users and groups under the starting point

A user directory is used by multiple corporate applications, including Hyperion System 9 applications. Typically, only a subset of the users and groups available on the user directory are used by Hyperion System 9 applications. You must identify these users and groups and assess whether they are organized in an optimal manner to support Hyperion System 9 applications.

Access to Hyperion System 9 applications is restricted to provisioned users. Users can be provisioned directly by assigning roles to the user or indirectly by assigning roles to the groups

to which the user belongs. To facilitate the administration of the provisioning process, Hyperion recommends that users be provisioned indirectly.

Well-Organized User Directories

A user directory comprises multiple nodes, each with its own DN, which is the unique address of the node. In a well-organized user directory, each node contains a set of logical groups that are used for a specific business function. When a user directory is well-organized, identify the lowest node that contains all the groups that need to be provisioned and use it as the starting point for searches (base DN).

The following illustration shows a well-organized user directory where all users that belong to the Sales department are organized into groups based on their geographical location. This organization allows Shared Services to search a very specific hierarchy within the user directory.

In the illustrated example, all groups containing the sales personnel belonging to the Western region can be accessed by connecting to the DN of `Sales_West` node (`ou=Sales_west,ou=Sales,ou=NorthAmerica,ou=corporate_Global,dc=example,dc=com`). Similarly, all groups containing the sales personnel belonging to the North America organizational unit can be accessed by connecting to the DN of `NorthAmerica` node (`ou=NorthAmerica,ou=corporate_Global,dc=example,dc=com`).

Poorly-Organized User Directories

In a poorly organized user directory, groups are scattered across nodes or groups contain users who have distinctly different business roles. Poorly organized user directories lead to performance degradation because they are not conducive to limiting searches to a specific

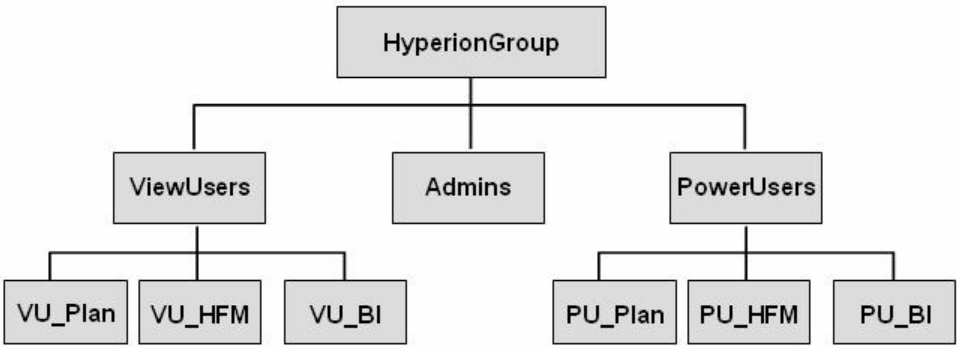
hierarchy within the user directory. In such cases, work with the User Directory Administrator to evaluate options:

- Creating a custom hierarchy of groups in the user directory to support Hyperion System 9 applications, if the security policy of your company allow. See "Creating a Custom Group Hierarchy" on page 7.
- Creating an OpenLDAP group hierarchy with members from external user directories to support Hyperion System 9 applications. See "Creating a Custom Group Hierarchy" on page 7.
- Using group object classifiers to identify the groups that need to be provisioned with Hyperion System 9 application roles.

Creating a Custom Group Hierarchy

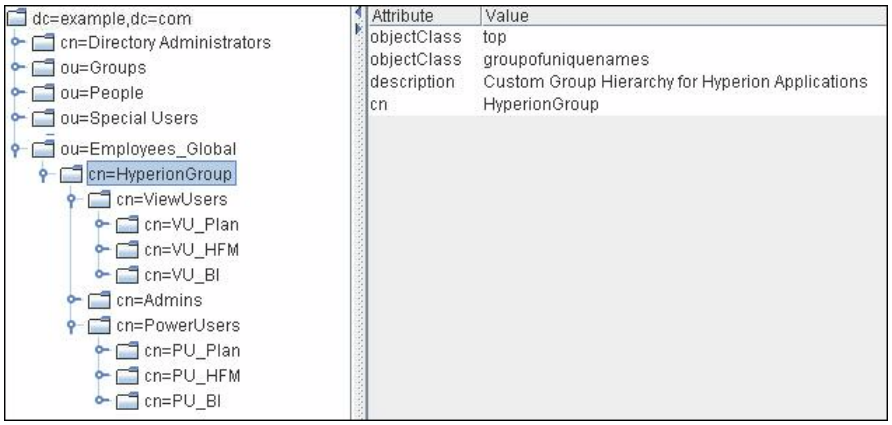
Creating a custom group hierarchy for Hyperion System 9 products alleviates the performance problems imposed by a poorly organized user directory.

The option to create a custom group hierarchy in an external user directory is governed by the security policies of the organization. Investigate whether changes to user directories are permitted. A sample custom hierarchy is depicted.



The location of the top-level group is not an important consideration, because the node where it resides is used as the starting point for searches (base DN). It is recommended that groups that do not belong within the custom hierarchy be excluded from the node containing the top-level group. Users assigned to the groups in the custom hierarchy can be anywhere in the user directory. The location of user accounts does not impact performance.

An LDAP Browser view of the illustrated sample hierarchy is depicted in the following graphic.



The starting point in the sample hierarchy is `HyperionGroup`, which nests all the subgroups used to provision Hyperion System 9 applications. All Hyperion System 9 application users are members of one or more of these groups. Specifying the URL of `HyperionGroup` (`cn=HyperionGroup,ou-Employees_Global,dc=example,dc=com`) as the base DN for searches allows Hyperion System 9 applications to restrict all searches to this custom hierarchy, thereby improving performance.

If you cannot create custom groups within the corporate user directory, create the necessary group hierarchy in OpenLDAP to organize users belonging to the corporate user directories.

Use of Custom Object Classes

Use of custom object attributes with groups that should be provisioned with Hyperion System 9 application roles can improve performance. Shared Services allows you to specify a group filter (an LDAP query) that can limit searches to only the groups that contain a specific value, for example, `Hyp_`, as the value of the custom object attribute. For example, the group filter `(custn=Hyp_*)` retrieves only groups whose custom object attribute `custn` carries the value `Hyp_`.

Note:

Some organizations do not allow the implementation of custom object attributes. Contact the user directory Administrator to identify available custom object attributes that you can use or to create new object attributes.

Considerations for Configuring User Directories

User directories are identified to Hyperion System 9 applications by configuring them on Shared Services. Several factors affect the speed at which Hyperion System 9 applications interact with configured user directories:

- “Login and Search Performance” on page 9
- “Number of User Directories” on page 9
- “Geographic Location of Servers” on page 9
- “Use of Hardware Load Balancers with User Directories” on page 9

- "Secure Connections to User Directories" on page 10
- "Single Sign-On from Security Agents" on page 10

Login and Search Performance

When a provisioned user logs on to a Hyperion System 9 application, the system verifies the identity of the user and then authorizes the user by verifying the provisioning data of the user. Typical response time for the provisioning portion of the login is one second, which increases if Hyperion System 9 applications have to search through a large number of groups (more than 10,000). To ensure acceptable login performance:

- Minimize the number of groups and users for Hyperion System 9 applications.
- Ensure that the server machines that host Hyperion System 9 applications are in the same geographical location as the server machines that host the user directories used in the provisioning process.
- Find an optimal starting point for searches or create a custom group hierarchy. See "Understand the Existing User Directory Structure" on page 5.

Number of User Directories

Hyperion System 9 application users and groups can be stored in multiple user directories. Each user directory that contains Hyperion System 9 application users and groups must be configured separately on Shared Services. An exception to this general rule is where a global catalog is used to accumulate users and groups from MSAD domains and servers into one collection. See "MSAD Global Catalog" on page 10.

Geographic Location of Servers

Geographical proximity of Hyperion System 9 application host machines and the user directory host machines is important to ensure good performance. If the server machines are not in the same geographical location, investigate the network connection speed between the servers to verify that acceptable logon and search performance can be achieved using existing network connections. If the network does not allow for fast connections, investigate whether it is possible to co-locate the servers in a geographic location or to replicate the user directory.

If you need to configure multiple Hyperion System 9 applications in different geographic locations, you must configure user directories so that Shared Services can access the nearest physical user directory.

Use of Hardware Load Balancers with User Directories

If a load balancer front-ends the user directory, the load balancer should be considered the de facto user directory server. In this scenario, use the DNS name or the IP address of the load balancer in place of the user directory host name while configuring user directories in Shared Services.

Secure Connections to User Directories

If you are connecting to a user directory that is set up to use Secure Socket Layer (SSL) for communication, you must establish secure connection communication between Hyperion System 9 and the user directory.

SSL connections require the use of signed certificates. Certificates may be self-signed or digitally signed by a Certificate Authority (CA). Before configuring user directories to use SSL, you must import the root certificate of the CA into the keystore that is used by the JRE of each Hyperion System 9 application. If this step is not completed, you cannot configure a user directory in Shared Services to use SSL communication. See *Configuring Hyperion System 9 in SSL-Enabled Environment* for detailed information on SSL-enabling Hyperion System 9 products.

Single Sign-On from Security Agents

You must already have configured the identity management system or policy server (for example, Oracle Access Manager, SiteMinder, IBM WebSEAL, SunONE Identity Server, or RSA ClearTrust) to work with Hyperion System 9 applications. See *Setting up Authentication* in *Hyperion System 9 Shared Services Installation Guide* for instructions.

After configuring user directories, you must instruct Shared Services to support security agents for single sign-on. See *Hyperion System 9 Shared Services Installation Guide* for detailed procedures.

Working with Microsoft Active Directory

MSAD Global Catalog

If you are using multiple MSAD domains the global catalog may be used to accumulate users and groups across MSAD domains and server into one collection. Using the global catalog server as the user directory server allows you to treat multiple MSAD domains as a single user directory and eliminates the need to configure them individually. You can use the global catalog server to treat multiple domains as a single directory for these domain models:

- Single domain model
- Multiple subdomain model
- Federated forests design model (at least two global catalogs are needed for this model)
- Placeholder domain model
- Special-purpose domains (depending on how the domain is set up)

Note:

You cannot use the global catalog server to consolidate multiple domains into a single directory if you use the multiple trees in a single forest model and peer-root model.

If a global catalog is not used, you must configure each MSAD domain individually so that Hyperion System 9 applications can access users and groups.

If you are using a global catalog, it is essential to define the user and group URLs at the lowest level possible to ensure good performance.

If you are using a global catalog, use the DNS name of the global catalog server machine as the host name of the MSAD user directory. The default global catalog port is 3268 (non-SSL) and 3269 (SSL).

MSAD: Deployment Mode

Hyperion supports MSAD deployed in mixed mode or native mode. MSAD in mixed mode does not support group hierarchy but yields faster response time than native mode.

User Directory Configuration Settings

User directory configuration on Shared Services requires that you specify a number of parameters. Some of these parameters, and their significance, are explained in this section.

Base DN

Base DN identifies the distinguished name (DN) of a node in the user directory hierarchy where the search for users and groups could begin. Shared Services uses this value to bind to the user directory to perform searches.

The Base DN value is extremely important in ensuring acceptable performance because it establishes the default starting point for all user and group searches. To improve performance, you must limit the search results to only the users and groups that Hyperion System 9 applications use.

The Base DN should identify the lowest-level user directory node that contains all the groups and users that you want to provision with Hyperion System 9 application roles. Identifying the lowest level base DN ensures that Hyperion System 9 applications do not have to search through the myriad objects defined elsewhere in the user directory. See "User Directory Design Considerations" on page 5 for design considerations.

The number of users and groups available within the Base DN determines the time that Hyperion System 9 applications take to complete the search. Typical response time for the provisioning portion of the login is one second, which increases if Hyperion System 9 applications must search through a large number of groups (more than 10,000).

In the illustrated LDAP Browser display, assume that only users and groups belonging to the North American Sales organizational unit need to access Hyperion System 9 applications. In this scenario, you can specify many possible Base DN values. Of these, the Base DN `ou=Sales,ou=NorthAmerica,ou=Corporate_Global,dc=example,dc=com` ensures the best search start point because it limits all searches to the North American Sales organizational unit.

Caution!

All users and groups defined within a user directory are stored under the root node (`dc=example,dc=com` in the preceding illustration). Do not use the root node as the Base DN because it causes searches to cycle through the entire user directory.

See *Hyperion System 9 Shared Services Installation Guide* for detailed information on configuring user directories.

Hyperion System 9 applications can bind with the Base DN using anonymous bind or by using the credentials of a user.

Anonymous Binds with Base DN

Anonymous binds do not require Hyperion System 9 applications to supply credentials of a valid user to bind with the Base DN. For security purposes, most organizations do not permit anonymous binds.

User Credentials for Binding with Base DN

The account that Hyperion System 9 applications use to bind with the user directory must have read privileges on the entire user directory.

Typically `sAMAccountName` of the user is used for MSAD and `Directory Manger` account is used for LDAP directories other than MSAD.

User URL

The user URL identifies a node within the Base DN, where the search for users begins. When selecting a user URL, be sure to specify the address of the lowest user directory node within which all the Hyperion System 9 users are available. Identifying the lowest possible node enhances performance, because it limits the search to a subset of the nodes available within the Base DN.

In the preceding illustration, `cn=Sales_West, ou=Sales,ou=NorthAmerica,ou=Corporate_Global,dc=example,dc=com` is the ideal user URL if you plan to provision only the users belonging to the `Sales_West` node of the user directory.

Group URL

The group URL identifies a node within the Base DN where the search for groups begins. The Group URL you select must contain all the groups you want to provision with Hyperion System 9 application roles.

The Group URL has a significant impact on login and search performance. Because it is the starting point for all group searches, you must identify the lowest possible node within which all groups for Hyperion System 9 applications are available. To ensure optimum performance, the number of groups present within the Group URL should not exceed 10,000. If more groups are present, use an appropriate group filter to retrieve only the groups you want to provision. For a discussion about selecting the Group URL, see:

- "Well-Organized User Directories" on page 6
- "Poorly-Organized User Directories" on page 6

Group Filter

Group filters are LDAP queries that help retrieve only the groups that match the filter criteria from the Group URL. Well-designed group filters improve search performance by limiting group searches to only the groups that meet the filter criteria.

Group filters are especially important if the node identified by the Group URL contains groups that need not be provisioned. Filters can be designed to exclude the groups that are not to be provisioned, thereby improving performance. Groups that do not match the filter conditions are not included in search results.

See "Use of Custom Object Classes" on page 8 for a discussion about how object classes can be used in filters.

Login Attribute

The login attribute identifies an attribute on the user directory. The value of this attribute, which is expected to be unique across the user directory, is used as the user ID when a user logs on to Hyperion System 9 applications.

By default, Hyperion System 9 uses `uid` (for user directories other than MSAD) and `cn` (for MSAD) as the login attribute. Typically, this value is set to `sAMAccountName` for MSAD.

ID Attribute

The value of ID attribute uniquely identifies a user in the user directory during a search.

The default ID attribute supported by a product is automatically selected if you are configuring SunOne (`nsuniqueid`), IBM Directory Server (`Ibm-entryUuid`), Novell eDirectory (`GUID`), and MSAD (`ObjectGUID`). You may change the default attribute, if necessary.

If you are using a custom user directory, contact the user directory Administrator to identify the ID attribute appropriate for the user directory.

Tuning Configuration Settings for Performance

Group Settings

If you are provisioning groups, always specify a Group URL. An ideal group URL identifies a node that contains fewer than 10,000 groups. See "Group URL" on page 13.

Set a group filter to limit the number of groups returned during searches. See "Group Filter" on page 13.

User Settings

Always specify a user URL, although this setting is optional.

Search Results

Depending on the data size, set the Maximum Size parameter to an optimal value. Set the value of Maximum Size parameter to 1000 if you need to retrieve only the first 1000 users; set it to 0 if you need to retrieve all matching users.

Search Order

Define the search order of the external user directories so that the most frequently queried user directory is at the top of the search order.

Refresh Interval

The value of `cacheRefreshInterval` in `CSS.xml` determines how often the group cache is refreshed. Set the `cacheRefreshInterval` for MSAD and other LDAP-based user directories to an appropriate value. By default, this value is set to 60 minutes. It can be set to a higher value to reduce requests to the server that hosts the user directory.

Java Heap Size Setting

If a large number of users and groups are present in the user directory, set the Java Heap Size in all Hyperion System 9 products to 1 GB. See your application server documentation for detailed information on setting the Java heap size.

User Directory Configuration Checklist

Use the following checklist to gather the information required to configure a user directory. If you must configure multiple user directories, you should gather information for each user directory before beginning the configuration process.

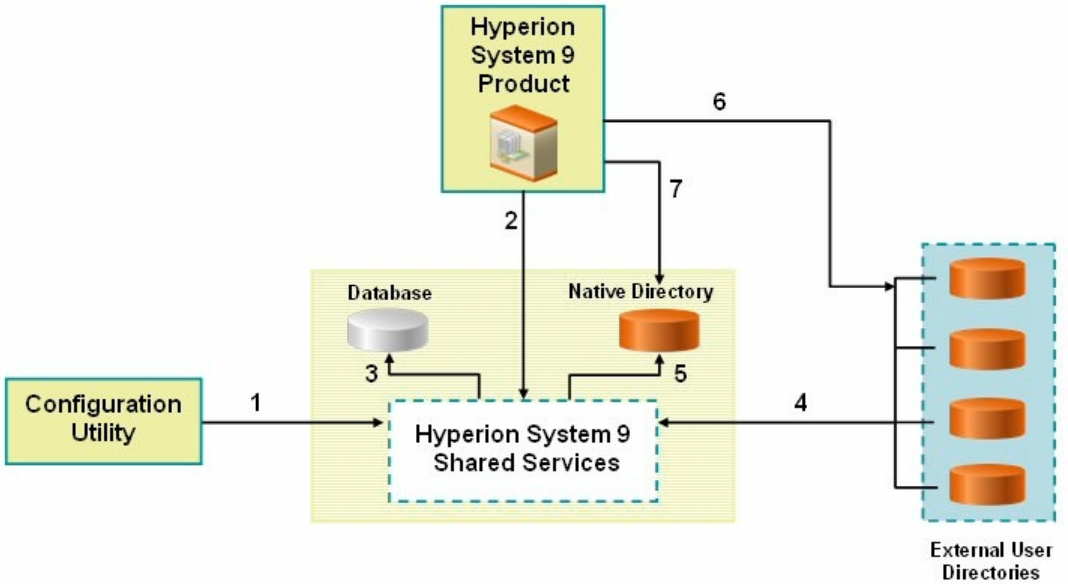
Table 2 User Directory Configuration Checklist

	Configuration Setting	Value
1	Name and version of the user directory See "Supported User Directories" on page 5.	
2	The DNS name of the machine that hosts the user directory. See: ● "Number of User Directories" on page 9 ● "MSAD Global Catalog" on page 10 ● "Use of Hardware Load Balancers with User Directories" on page 9 See *Hyperion System 9 Shared Services Installation Guide* for restrictions on the use of special characters.	
3	User directory port	
4	Is SSL communication required? See "Secure Connections to User Directories" on page 10.	
5	The Base DN to which Hyperion System 9 applications should bind. See "Base DN" on page 11.	
6	The User DN that should be used to bind with the Base DN. See "User Credentials for Binding with Base DN" on page 13.	
7	The password of the user whose DN is used to bind with the Base DN of the user directory. See "User Credentials for Binding with Base DN" on page 13.	

	Configuration Setting	Value
8	The user directory node within which user accounts are defined. See "User URL" on page 13.	
9	If you are provisioning groups, the user directory node under which groups are defined. See "Group URL" on page 13.	
10	**Optional:** Group filter to identify only the groups that are to be provisioned with Hyperion System 9 application roles. See "Group Filter" on page 13.	
11	Login attribute that uniquely identifies a user on the user directory. See "Login Attribute" on page 14.	
12	The ID Attribute to use. See "ID Attribute" on page 14.	
13	The attribute that stores the email ID of users.	
14	Is single sign-on enabled between Hyperion System 9 applications and a security agent? See "Single Sign-On from Security Agents" on page 10.	

Provisioning Sequence

The provisioning sequence for Hyperion System 9 applications is depicted in the illustration.



The numbered sequence:

1. Using Hyperion® Configuration Utility™, deploy Shared Services. The deployment process involves application server and database deployment. OpenLDAP is configured when you deploy Shared Services.

   After deploying Shared Services, using the External Authentication Configuration Console, configure the external user directories that store user and group information for Hyperion System 9 applications. See *Hyperion System 9 Shared Services Installation Guide* for information on configuring user directories. For an overview of the procedures, see "Configuring MSAD and Other LDAP-Enabled User Directories" on page 17.

2. Using Hyperion Configuration Utility, register Hyperion System 9 products with Shared Services.
3. Shared Services stores product registration information in the database.
4. During the provisioning process, Shared Services assigns Hyperion System 9 application roles to users and groups defined in OpenLDAP and external user directories.
5. Shared Services stores provisioning information in OpenLDAP.
6. When users log into a Hyperion System 9 application, the application authenticates the user against the external user directory or OpenLDAP.
7. If the user is authenticated, the Hyperion System 9 application queries OpenLDAP to get the provisioning information of the user. This information is used to authorize Hyperion System 9 application users.

Configuring MSAD and Other LDAP-Enabled User Directories

Use the procedures in this section to configure any LDAP-enabled corporate user directory, such as MSAD, Sun Java System Directory Server, IBM Tivoli Directory Server, or a custom user directory. Before starting these procedures, make sure that Shared Services is running.

➤ To configure MSAD and other LDAP-enabled user directories:

1 **Launch External Authentication Configuration Console.**

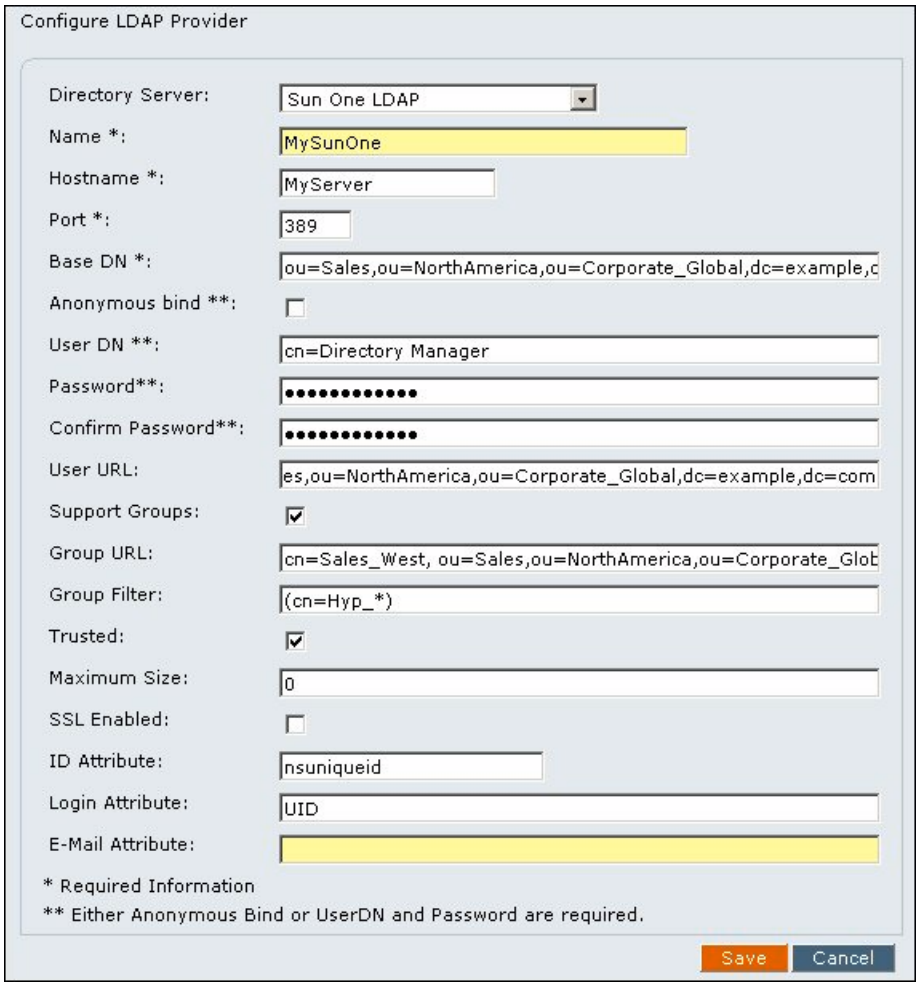
2 **In Defined Providers, select Add.**

3 **From Choose the Provider Type select:**

- **LDAP** to configure LDAP-enabled user directories other than MSAD.
- **MSAD** to configure MSAD.

4 **Click Next.**

The Configure Provider screen for the selected user directory type opens.



5 **Enter the required parameters in the Configure Provider screen.**

Table 3 Configure Provider Screen

Label	Description
Directory Server	Select the directory server name from *checklist item 1* in Table 2. Select `Other` if you are using an LDAP Version 2 (and above) product other than those listed. **Example:** `Sun One LDAP`
Name	A unique descriptive name for the user directory. This name is used to identify a configured user directory. **Example:** `MySunOne`
Hostname	Enter value from *checklist item 2* in Table 2 on page 15. **Example:** `MyServer`
Port	Enter value from *checklist item 3* in Table 2 on page 15. **Example:** `389`
Base DN	Enter value from *checklist item 5* in Table 2 on page 15.

Label	Description
	Example: `ou=Sales,ou=NorthAmerica,ou=Corporate_Global,dc=example,dc=com`
Anonymous bind	Select this option if Shared Services can bind anonymously to the user directory. Most customers do not allow anonymous binds. See "Anonymous Binds with Base DN" on page 12.
User DN	Enter value from *checklist item 6* in Table 2. This field is disabled if the Anonymous bind option is selected. **Example:** ● `cn=Directory Manager` (user directories other than MSAD) ● `sAMAccountName=pturner` (MSAD)
Password	Enter the password from *checklist item 7* in Table 2 on page 15. **Example:** `UserDNpassword`
Confirm Password	Re-enter the password from *checklist item 7* in Table 2 on page 15.
User URL	Enter the URL from *checklist item 8* in Table 2 on page 15. **Example:** `ou=Hyp_users, ou=Hyp_groups, ou=sales,dc=example,dc=com`
Support Groups	Clear this option if you do not plan to provision groups or if users are not categorized into groups on the user directory. Deselecting this option disables the Group URL and Group Filter fields.
Group URL	Enter value from *checklist item 9* in Table 2 on page 15.
Group Filter	Enter value from *checklist item 10* in Table 2 on page 15.
Trusted	Select this option to indicate that this provider is a trusted source. User credentials from trusted sources are not validated during single sign-on (SSO) to Hyperion System 9 product. If this option is not selected, the user credentials are validated every time users request SSO to another Hyperion System 9 product.
Maximum Size	For LDAP-enabled user directories other than MSAD, leave this field blank to retrieve all users and groups that meet the search criterion. The maximum size entered in this screen is constrained by the user directory settings. For MSAD, set this value to `0` to retrieve all users and groups that meet the search criterion. **Note:** This value must not exceed 10,000,000.
SSL Enabled	Select this check box if the answer to *checklist item 4* in Table 2 on page 15 is `Yes`.
ID Attribute	Enter value from *checklist item 12* in Table 2 on page 15.
ID Attribute Type	Enter value from *checklist item 13* in Table 2.
Login Attribute	Enter value from *checklist item 11* in Table 2 on page 15.
Email Attribute	Enter value from *checklist item 14* in Table 2 on page 15.

6 Click **Save**.

7 Add the user directory to the search order used by Shared Services. See *Hyperion System 9 Shared Services Installation Guide* for detailed procedures.

8 Select the **Support for Security Agent for Single Sign-on** option if the answer to *checklist item 15* in Table 2 is `Yes`.

9 Specify other global parameters as if needed. See *Setting Global Parameters* in *Hyperion System 9 Shared Services Installation Guide*.

Shared Services Tools and Utilities

Import/Export Utility

Shared Services administrators can use the Import/Export utility (a standalone, command-line utility) to export, import, and validate data related to entities such as user, groups, roles, group relationships, role relationships, and user and group provisioning relationships.

The Import/Export utility can be used to export data from all user directories configured with Shared Services but not to import data into external user directories.

The Import/Export utility is installed in `<Hyperion_Home>/common/utilities/CSSImportExportUtility`.

For detailed information on this utility, see *Hyperion System 9 Shared Services Installation Guide*.

Update Native Directory Utility

Changes to users and groups in an external user directory that is configured with Shared Services lead to stale data within OpenLDAP, because the Hyperion security system is not synchronized to be aware of such changes. Use the Update Native Directory utility to synchronize OpenLDAP with the changes that have taken place within external user directories.

The `UpdateNativeDir.zip` archive containing the Update Native Directory utility is installed in `<Hyperion_Home>/common/utilities/nativedirectoryupdateutility`.

For detailed information on this utility, see *Hyperion System 9 Shared Services Documentation Addendum for 9.2.0.3*.

CSSSpy

CSSSpy is used to validate connections to external user directories and user login. It can also be used to retrieve user role information and to assess performance. CSSSpy can connect to any user directory and authenticate a user and perform various Shared Services calls, bypassing Hyperion System 9 products.

CSSSpy is deployed with Shared Services. To launch CSSSpy, use the following URL:

`http://<HSS_hostname>:<port>/interop/cssSpy`; for example, `http://myServer:58080/interop/cssSpy` where `myServer` indicates the DNS name of the Shared Services host machine.

WebDAV Browser

The WebDAV browser helps to view and validate the metadata contained in `.product` and `.instance` files, which are created when an application is registered with Shared Services.

Use the WebDAV browser to diagnose:

- A failed product registration
- A failed application launch from Shared Services

The WebDAV browser is a part of Shared Services installation. To launch WebDAV browser, use the following URL:

`http://<HSS_hostname>:<port>/interop/content`; for example, `http://myServer:58080/interop/content` where `myServer` indicates the DNS name of the Shared Services host machine.

Use Shared Services Administrator credentials to log on to the WebDAV browser.

Synchronizing OpenLDAP Database with Shared Services Repository

The database configured with Shared Services stores product registration information, and the OpenLDAP database contains provisioning data for Hyperion System 9 products. These databases work in tandem to support Hyperion System 9 products.

Data inconsistencies between the databases impact normal operations. Inconsistencies could occur during manual database update, database upgrades, or in replicated OpenLDAP environments in which the OpenLDAP slave has taken over for a failed OpenLDAP master. To remove inconsistencies, the OpenLDAP database must be synchronized with Shared Services database. The synchronization process uses the Shared Services database as the master database to resolve data inconsistencies.

Use the OpenLDAP Sync utility in the following situations:

- Product registration fails after the application was deleted from Shared Services
- Shared Services database is recreated manually without recreating OpenLDAP, and Shared Services backup is not available
- OpenLDAP database is recreated manually without recreating Shared Services database, and Shared Services backup is not available

Note:

The Sync OpenLDAP utility does not synchronize user and group provisioning data on Hyperion System 9 products.

➤ To synchronize OpenLDAP database with Shared Services repository:

1. **Log on to External Authentication Configuration Console as Shared Services Administrator.**
2. Select **Configuration > Sync OpenLDAP**.
3. **Optional:** Click **Refresh** to update the status.
4. **Optional:** Click **View Log** to display `Sync OpenLDAP Log` that details the operations that were performed during the synchronization process.
5. Click **Close**.

Working with OpenLDAP

Shared Services and OpenLDAP

Shared Services uses OpenLDAP to store the user provisioning data and a relational database to store product registration data.

After the initial logon to a Hyperion System 9 products, the products directly query OpenLDAP for user provisioning information. Hyperion System 9 products can function normally only if OpenLDAP is running.

Install Location

The default install location of OpenLDAP is `<HSS_Home>/OpenLDAP`; for example, `C:\hyperion\SharedServices9\9.2\openLDAP` (Windows) and `app/hyperion/SharedServices9/9.2/openLDAP` (UNIX). `<HSS_Home>/OpenLDAP` is referred to as `<openLDAP_Home>` throughout this document.

OpenLDAP data is stored in `<openLDAP_Home>/var/openldap-data` and utilities are stored in `<openLDAP_Home>/bdb/bin`.

Starting OpenLDAP

By default, OpenLDAP is installed as a Windows service or UNIX process.

On Windows, you can start OpenLDAP by starting `Hyperion SharedServices9 OpenLDAP` service from the **Services** window, or by executing `<openLDAP_Home>startService.bat`.

On UNIX systems, run `<openLDAP_Home>/startOpenLDAP` script to start the process.

Starting OpenLDAP in Debug Mode

➤ To start OpenLDAP in debug mode:

1. **Using a command prompt window, navigate to** `<openLDAP_Home>`.
2. **Execute the following command:**

   `slapd –d 1`.

Stopping OpenLDAP

On Windows, you can stop OpenLDAP by stopping `Hyperion SharedServices9 OpenLDAP` service from the **Services** window, or by executing `<openLDAP_Home>stopService.bat`.

On UNIX systems, run `<openLDAP_Home>/stopOpenLDAP` script to stop the OpenLDAP process.

Recovering OpenLDAP Database

If OpenLDAP service (Windows) or process (UNIX) fails, causing OpenLDAP to crash, you must recover the provisioning data contained in the OpenLDAP database before users can access Hyperion System 9 products, including Shared Services.

➤ To recover OpenLDAP database:

1. **Stop OpenLDAP service or process. See** **"Stopping OpenLDAP" on page 23**.
2. **Using a command prompt window, navigate to:**
   - `<openLDAP_Home>\bdb\bin` (Windows)
   - `<openLDAP_Home>/usr/local/bdb/bin` (UNIX)
3. **Execute the following command:**

   `db_recover –h <Path_Native_Directory_data_file>` . For example, `db_recover –h ../../var/openldap-data`.
4. **Monitor the utility to ensure that it runs successfully.**
5. **Start OpenLDAP. See** **"Starting OpenLDAP" on page 23**.

6 Restart Shared Services.

Backing Up OpenLDAP Database

The OpenLDAP database must be backed up periodically to recover from loss of provisioning data due to media failures, user errors, and unforeseen circumstances. Hyperion recommends that you regularly back up this database.

Best Practices

Hyperion recommends monthly cold backups of the OpenLDAP database and Shared Services repository. Perform hot backups daily to supplement the cold backups.

- Schedule hot backups when the database usage is at its lowest.
- Back up Shared Services repository and OpenLDAP database at the same time so that backup is in sync.
- Store backup for disaster recovery.
- Test backup and recovery procedures to ensure that the process works.

Hot Backup

Regular incremental backups of OpenLDAP database can be performed without shutting down OpenLDAP. Known as hot backups, they do not interfere with the availability of Shared Services.

Use `backup.bat` (Windows) or `backup.sh` (UNIX) to schedule daily hot backups. This Hyperion-supplied backup file is stored in `<HSS_Home>/server/scripts`; for example `C:\Hyperion\SharedServices9\9.2\server\scripts` (Windows) or `/apps/Hyperion/SharedServices9/9.2/server/scripts` (UNIX).

See *Hyperion System 9 Shared Services Installation Guide* for information on the files and directories that are backed up.

Note:

This procedure backs up Shared Services configuration files and OpenLDAP.

➤ To run a hot backup:

1 Using a command prompt window, navigate to `<HSS_Home>/server/scripts`.

2 Execute the following command.

- **Windows:** `backup.bat <backup_directory>`
- **UNIX:** `backup.sh <backup_directory>`

  where *backup_directory* indicates the path of the directory where the backup is to be stored.

3 Monitor the backup process to ensure that it runs successfully.

Cold Backup

Cold backups are taken after shutting down OpenLDAP.

Note:

Data in the OpenLDAP database is synchronized with the data available in the Shared Services repository. Hyperion recommends that you back up the Shared Services repository along with the OpenLDAP database.

➤ To back up OpenLDAP database:

1. **Stop OpenLDAP service or process. See "Stopping OpenLDAP" on page 23.**
2. **Copy `<openLDAP_Home>` into a secure location.**

Restoring Data from Backups

Attempt to recover provisioning data before restoring it from the latest backup. See "Recovering OpenLDAP Database" on page 23.

➤ To restore data from backup:

1. **Stop OpenLDAP service or process. See "Stopping OpenLDAP" on page 23.**
2. **Using a command prompt window, navigate to `<HSS_Home>/server/scripts` and execute the following command.**
   - **Windows:** `recover.bat <Path_backup_directory>`
   - **UNIX:** `recover.sh <Path_backup_directory>`

     In this command, *`Path_backup_directory`* indicates the path of the directory where the backup is stored.
3. **Monitor the utility to ensure that it runs successfully.**
4. **Start OpenLDAP. See "Starting OpenLDAP" on page 23.**
5. **Restart Shared Services.**

Shared Services Log File Location

Shared Services log files are created in `<Hyperion_Home>/logs/SharedServices9`.

Runtime errors and messages are recorded in log files stored in these log files.

Log File	Contains
`SharedServices_Security.log`	Messages related to external authentication and single sign on. Includes messages concerning users, groups, roles, and provisioning operations

Log File	Contains
SharedServices_Admin.log	Messages related to user management
SharedServices_Metadata.log	Metadata management and registration errors and messages
SharedServices_Taskflow.log	Taskflow-related errors and messages from Common Event Services
SharedServices_Taskflow_CMDExecute.log	Taskflow scheduling errors and messages from Common Event Services
SharedServices_Taskflow_Optimize.log	Taskflow optimization errors and messages from Common Event Services
SharedServices_SyncOpenLDAP.log	Messages from the synchronization of OpenLDAP with Shared Services database
SharedServices_Security_Client.log	Product-specific messages and errors generated by Hyperion products during external authentication. Available in servers that host Hyperion System 9 products.