

# Red Hat Directory Server DSML Gateway

Directory Server provides a Java gateway application based on Directory Service Markup Language (DSML) version 2.0. The following sections contain background on DSML, information on how to use the DSML gateway with Directory Server and Web servers, and how to configure your DSML gateway:

- Introduction to DSML Gateway
- DSML Gateway with Directory Server
- Activating the Gateway
- Configuring the DSML Gateway

For information on implementing and configuring the Default and Directory Express LDAP gateways that come with Directory Server, refer to the *Red Hat Directory Server Gateway Customization Guide*.

## Introduction to DSML Gateway

- Introduction to DSML
- DSML Authentication Mapping
- Java Implementation

## Introduction to DSML

Directory Service Markup Language (DSML) is an open, extensible format that allows directories to exchange information across directory server types. The flexibility of DSML enables clients to interact with customers, partners, and remote locations, regardless of the type of directory service used.

DSML version 2.0, the basis for Directory Server's DSML Gateway, allows directory contents to be accessed, modified, and controlled through XML (eXtensible Markup Language), a more flexible language than HTML that allows customized markup languages to be created for different uses.

As a Web services protocol, DSML closely mirrors Lightweight Directory Access Protocol (LDAP). DSML is designed to allow arbitrary Web services clients to access directory services using the client's native protocols (`http://soap`), which allows content stored in a directory service to be easily accessed by standard Web service applications and development tools. DSML is useful in Web applications because it can access directories when a firewall would normally screen out an LDAP request.

Simple Object Access Protocol (SOAP) is an XML-based protocol used in combination with Hypertext Transfer Protocol (HTTP) to access information in a distributed database. DSMLv2 uses SOAP to bind to a Directory Server over the Web in such a way that LDAP directories, such as Directory Server, can be faithfully rendered in XML.

## DSML Authentication Mapping

The DSML authentication mechanism is native to `http://soap`, but the gateway interacts cleanly with LDAP. Client credentials presented via `HTTP Client Authentication` or SSL connections are mapped to a distinguished name (DN) and then proceed as if an LDAP client had bound with that DN.

The gateway mapping is implemented essentially as follows:

1. The client's authentication credentials are obtained from the servlet container (username/password from `http://soap` or client certification DN from SSL).
2. A mapping function is applied to yield a target DN in the host Directory Server's directory information tree.
3. The gateway attempts to verify the presented credentials by binding as the mapped DN against the host Directory Server.
4. If the gateway binds successfully, the session is marked as "authenticated."
5. For authenticated sessions, LDAP proxy authorization controls are sent with every operation to the Directory Server. This ensures that operations are done in the security context of the presented credentials (as mapped).

---

**NOTE** Since the bindDN and password for a user in the DSML gateway is the same bindDN and password used to access the Directory Server, proxy authorization is the same proxy right that is determined by access control rules. This is an extremely powerful right, and there is not way to limit as whom a user with proxy rights may bind. Proxy rights should be limited to privileged users, such as `root`.

---

## Java Implementation

The DSML gateway is implemented as a Java application. Implementation as a gateway, as opposed to natively within the Directory Server, offers the following benefits:

- Improved throughput since XML-parsing, which is CPU-intensive, can be done on a different CPU than the server uses.
- Integration with emerging Web services protocols can be added without affecting Directory Server performance.

The gateway architecture does increase response times slightly in relation to a native Directory Server implementation because each request must be forwarded through the gateway.

Implementation in Java offers the following benefits:

- Execution in a wide range of operating system and hardware environments, including those that do not support Directory Server.
- Leverage of existing Java Web services implementations.
- Deployment within the execution environment of your choice. Installation will be easy even without experience using Java Web services.

## DSML Gateway with Directory Server

To use the DSML Gateway application as part of your Directory Server deployment, you must:

1. Ensure prerequisites are met.

Since the DSML gateway natively runs via `http://soap`, the machine or application that uses the gateway must be SOAP compatible.

2. Install Directory Server.

The DSML gateway is installed with Directory Server. It must be activated separately; see step 3. The DSML Gateway can run simultaneously with the other two gateways that are installed with Directory Server; however, it does not interact with them.

3. Enable the the gateway.

See “Activating the Gateway” for instructions on how to enable the gateway and for the command-line utilities available.

4. Modify the configuration files.

During installation, the files relevant to the DSML gateway are placed in *serverRoot/clients/dsmlgw*. The configuration information is stored in *dsmlgw.cfg*. You can modify desired settings in the file and customize the application to suit your organization.

The gateway connects to the default port (389) of Directory Server. The gateway can also point to a different server and port; you can configure this at installation or when moving or creating instances of the gateway. This is addressed in “Configuring the DSML Gateway.”

DSML gateway can be configured to point to the Directory Server or the Admin Server, to run from a different port, and to allow read-write access. The default settings allow read-only access to the directory with the server set as the Directory Server. See “Configuring the DSML Gateway” for detailed information on configuration parameters. It is recommended that you not change the default settings.

## Activating the Gateway

The DSML gateway is installed with Directory Server. To enable it, do the following:

1. Stop the server with the `./stop-admin` command.
2. Run the activation script to enable the gateway:

```
./slapd-serverID/dsml-activate.extension -i
```

where *extension* is either `.bat`, for Windows systems, or `.pl`, for all others. `-i` initializes the gateway.

Running this script changes the `jvm12.conf`, `obj.conf`, and `server.xml` files in the `/admin-serv/config` directory.

3. Restart the Admin Server with the `./start-admin` command.

---

**NOTE** Any changes made to files in the `/admin-serv/config` directory will be lost if the gateway is deactivated and restarted.

---

## Gateway Utilities

The DSML gateway comes with three command-line utilities, listed in Table DSML-1.

**Table DSML-1** Gateway Command-Line Utilities

---

<code>-i</code>	Initializes the gateway.
<code>-p</code>	<i>Optional.</i> Sets the port number. The <code>-p</code> utility is only used with <code>-i</code> .
<code>-u</code>	Restores edited files and disables the gateway the next time the server is restarted.

---

When activating the gateway, you can use the `-p` utility to specify a port number other than the default (389 for the Directory Server, 8080 for the Admin Server). This parameter can also be edited manually; see “Changing the Port.”

The `-u` utility will restore edited files when the server is restarted. Any changes made to the configuration files are normally lost when the gateway is deactivated and restarted; using this utility will save those changes and restore them when the host server is stopped and started:

```
./slapd-serverID/dsml-activate.{pl|bat} -u
```

You must run the `-u` utility after `-i`. If you were to run the commands

```
dsml-activate.{pl|bat} -i -p 3033
```

```
dsml-activate.{pl|bat} -i -p 3222
```

back-to-back, the Admin Server and the gateway will not start, with an error message, such as:

```
-u required at ./dsml-activate.pl line 30
```

Any changes in configuration or restarts must occur in a `-i -u -i` order, as follows, to ensure that both the server and the gateway will start:

```
dsml-activate.{pl|bat} -i -p 3033
```

```
dsml-activate.{pl|bat} -u
```

```
dsml-activate.{pl|bat} -i -p 3222
```

## Configuring the DSML Gateway

The gateway is already configured at installation. With the default settings, the gateway is running using the Admin Server as the host. The default URL is *host:port/axis/services/dsmlgw*, where the *host* and *port* are the Admin Server's hostname and DSML gateway port as determined by `dsml-activate`.

The configuration settings are stored in a Java properties text file in the following location:

```
serverRoot/clients/dsmlgw/dsmlgw.cfg
```

Table DSML-2 lists the DSML gateway default configuration settings:

**Table DSML-2** Configuration Settings

Parameter	Description	Default Setting
ServerHost	Host name for its peer Directory Server.	localhost
ServerPort	Port number for its peer Directory Server.	389
BindDN	Bind DN.	anonymous
BindPW	Bind password.	(empty)
MinimumConnectionPool	Minimum connections the DSML gateway will make to the Directory Server for operations.	3
MaximumConnectionPool	Maximum connections the DSML gateway will make to the Directory Server for operations.	15
MinimumLoginPool	Minimum connections the DSML gateway will make to the Directory Server for user authentication.	1
MaximumLoginPool	Maximum connections the DSML gateway will make to the Directory Server for user authentication.	2
UseAuth	true false expression. If the expression is true, it requires the user to authenticate in order to bind; if it is false, it accepts the userID and password offered.	false

## Configuring the Gateway

The DSML gateway is configured when it is installed; no additional configuration is necessary. However, some clients may want to move a gateway or create multiple gateway instances. This may be recommended for high traffic gateways that may require a separate HTTP server.

## Changing the Host and BindDN

### *Changing the Host*

1. Stop the gateway.

If the gateway is configured with the default parameters, this is done by stopping the server:

```
./stop-admin
```

2. Open the `dsmlgw.cfg` file in the `/clients/dsmlgw` directory.
3. Edit the value of the `ServerHost` attribute to reflect the server you wish to use.

For example, to change the default server `localhost` to `ds-internal.example.com`, edit `ServerHost=localhost` to `ServerHost=ds-internal.example.com`.

4. Restart the gateway.

If the gateway is configured with the default parameters, this is done by restarting the server:

```
./start-admin
```

### *Changing the Bind DN and Password*

The default setting allows read-only access since the default bind DN is `anonymous`. Changing the bind DN will allow read-write access for the directory if you reset the bind DN to a DN that has read-write permissions.

---

**NOTE**      Everyone can read from the DSML gateway in its default configuration. To restrict access further, set the `UseAuth` value to `true`.

---

If the `UseAuth` attribute value is set to `true`, the gateway requires standard HTTP headers, consisting of the user's full distinguished name and password. Any operations done over the gateway will be done with proxy authorization and will require a distinguished name with proxy rights. For more about proxy authorization, refer to the *Red Hat Directory Server Administrator's Guide*.

1. Stop the gateway.

If the gateway is configured with the default parameters, this is done by stopping the server:

```
./stop-admin
```

2. Open the `dsmlgw.cfg` file in the `/clients/dsmlgw` directory.

3. Edit the value of the `BindDN` attribute to reflect the user for whom you are allowing access.

For example, to change the default `bindDN` `anonymous` to `uid=fred,ou=people,dc=example,dc=com`, change the line that reads `BindDN=anonymous` to `BindDN=uid=fred,ou=people,dc=example,dc=com`.

4. Edit the value of the `BindPW` attribute. The password must be the same as the password for authentication to the directory to keep access controls functioning.

Change the line which reads `BindPW=` to `BindPW=foo`.

5. Restart the gateway.

If the gateway is configured with the default parameters, this is done by restarting the server:

```
./start-admin
```

## Changing the Port

Edit the value of the `ServerPort` attribute to reflect the server you wish to use. Be sure that this port number is not used by another application.

1. Stop the gateway.

If the gateway is configured with the default parameters, this is done by stopping the server:

```
./stop-admin
```

2. Open the `server.xml` file in the `/clients/dsmlgw/conf` directory.
3. The recommended way to change the port number is by running the `-u` utility with the activation script to save changes and then the `-i -p portNumber` utilities to change the port number. Any typos or errors caused by manually changing this parameter will prevent the gateway and/or Admin Server from restarting; running the activation script avoids this problem.

However, to change the port number manually, edit the value of the line that reads `ServerPort="4456"` to reflect the port you wish to use. Remember to select a port that is not in use by any other application.

For example, to change the port from 4456 to port 5564, edit `ServerPort="4456"` to `ServerPort="5564"`.

4. Restart the gateway.

If the gateway is configured with the default parameters, this is done by restarting the server:

```
./start-admin
```

## Example Configuration

Parameters not in the file are set to the default value. All of the configuration options that are currently in the document are correct and exist. The following is an example gateway configuration for `example.com` Corporation:

```
# DSMLGW configuration for example.com Corporation
ServerHost=ds-internal.example.com
ServerPort=8080
BindDN=uid=fred,ou=people,dc=example,dc=com
BindPW=foo
UseAuth=false
```

