Configuring Authorization Rules

An authorization rule is used to perform an access check for a particular Broker instance against an (authenticated) user ID and list of rules. Checks are performed on a UNIX or Windows Broker kernel, using standard EntireX Security on these platforms. Authorization rules can be stored within a repository. When an authorization call occurs, the security exit performs checks based on the values of Broker attributes `AUTHORIZATIONDEFAULT` and `AUTHORIZATIONRULE`.

This chapter covers the following topics:

- Configuration of LDAP (Lightweight Directory Access Protocol) Server
- Configuration of Authorization Rule Agent using System Management Hub

See also *Administering Authorization Rules using System Management Hub*

Configuration of LDAP (Lightweight Directory Access Protocol) Server

General Considerations for all LDAP Server Products

An LDAP server is a prerequisite (based on LDAPv3); it is not installed with EntireX.

Tested LDAP servers include IBM Secureway Directory, Microsoft Active Directory. For the installation of the LDAP server, see the respective product documentation. All servers have to support the attribute types `sag-key`, `sag-value` and the object-class `sag-xds`. They are defined in the following schema.

```
attributetypes:
      ( 1.2.276.0.12.2.1.1
      NAME ’sag-key’
      DESC ’User Defined Attribute’
      SYNTAX ’1.3.6.1.4.1.1466.115.121.1.26’)
attributetypes:
      ( 1.2.276.0.12.2.1.2
      NAME ’sag-value’
      DESC ’User Defined Attribute’
      SYNTAX ’1.3.6.1.4.1.1466.115.121.1.5’)
objectclasses:
      ( 1.2.276.0.12.2.3.1
      NAME ’sag-xds’
      DESC ’User Defined ObjectClass’
      SUP ’top’
      MUST ( objectclass $ sag-key )
      MAY ( aci $ sag-value ) )
```

We recommend setting up a separate branch in the directory for authorization rules. The distinguished name of this branch is the value of the configuration setting baseDN. See *Configuration of Authorization Rule Agent using System Management Hub* below.

Configuration of Authorization Rule Agent using System Management Hub

- Configuration File xds.ini
- xds.ini with the LDAP Server
- xds.ini with a Flat File Directory

Configuration File *xds.ini*

Edit file *xds.ini* to configure the EntireX authorization rule agent, which is a plug-in of the System Management Hub. *xds.ini* is the configuration of the directory access for authorization rules. This file is needed on each computer that is a managed host for the System Management Hub or where authorization rules are used.

The syntax of this file is the syntax of Windows .ini files. For authorization rules, all lines in the section `[Authorization Rules]` are used. Each line has the format <*key*>=<*value*>, where <*value*> is the contents of the line after the first ’=’. The keys are not case-sensitive. Lines starting with ’;’ are comments.

Under UNIX, *xds.ini* is located in */opt/softwareag/EntireX/config*.

Note:
If you use read access, an LDAP server with authentication, and only one LDAP user (account), the *xds.ini* is the same on all computers accessing the same directory. Then you can deploy xds.ini with a deployment tool.

xds.ini with the LDAP Server

The section for authorization rules looks as follows:

```
[Authorization Rules]
dirService=LDAPDIR
baseDN=<DN>
host=<host>
port=<port>
protocol=<protocol>
authDN=<user>
authPass=<ldap_password>
```

where	*<DN>*	is the base distinguished name of the directory object that is the root of all objects for authorization rules; <*DN*> must not be empty
	<host>	is the host of the LDAP server.
	<port>	is the port of the LDAP server. Default is 389 for TCP communication; default port for SSL is 636
	<protocol>	is is either "`ldap`" (default) for TCP communication, or "`ldaps`" for SSL

For authenticated access to the LDAP server, use the keywords `authDN` and `authPass`,

where *`<user>`* is the DN of the user

`<ldap_password>` is the password of this user

⚠ **Warning:**
The password is not encrypted in *xds.ini*

For unauthenticated access to the LDAP server, do not include these keywords `authDN` and `authPass` in the *xds.ini*.

Example

```
dirService=LDAPDIR
host=myHost.myDomain
baseDN=dc=myCompany,dc=de
port=389
protocol=ldap
authDN=cn=admin,dc=myCompany,dc=de
authPass=myLdapPassword
```

xds.ini with a Flat File Directory

If a flat file directory is used, the section for authorization rules looks as follows:

```
[Authorization Rules]
dirservice=FLATDIR
file=C:\SoftwareAG\EntireX\config\flat
```

Under UNIX, the file is created by the System Management Hub if it does not exist. The file must have at least write permission. The folder for the file must exist. It is not recommended sharing this file over the network for writing.