Whitepaper

LDAP configuration tool

MICRO FOCUS

Contents

Overview

The LDAP Configuration Tool is a command line tool for HPE Cloud Service Automation (CSA) that creates or updates the LDAP configuration of an organization.

LDAP (Lightweight Directory Access Protocol) used by CSA is used to:

Authenticate a user's login to the Cloud Service Management Console or Marketplace Portal

Authenticate a user's access to information

Authorize a user's access to information

The LDAP Configuration Tool provides the same actions available in the Cloud Service Management Console: configure LDAP for authentication to log in to CSA and configure LDAP to access information in CSA. To completely configure access to CSA, using the Cloud Service Management Console, you must also configure access control for an organization to authorize a user's access to information. Refer to the Cloud Service Management Console online help for more information about configuring access control.

Configuration

The LDAP Configuration Tool is located in `<csa_home>\Tools\LdapTool\` where `<csa_home>` is the directory in which CSA is installed.

Configuration Details

IdM and LDAP Configuration Properties File

IdM and LDAP configuration properties files are required by the LDAP Configuration Tool when creating or updating the LDAP configuration of an organization. These configuration properties files must be located in the same folder as the `ldap-tool.jar` file (`<csa_home>\Tools\LdapTool\`). Sample configuration properties files can be generated using the LDAP Configuration Tool (see Generating Sample Configuration Properties Files" for more information).

IdM configuration properties file – Required information used to communicate with the HP CSA Identity Management. In the examples used in this document, this file is named config.properties.idm, but you can use a different name. To specify the file in the command line, use the –c or –-config option.

If you use the sample IdM configuration properties file, you must provide or update the property values. See "IdM Configuration Properties File Parameters" for more information about the contents of this file. See "Sample config.properties.idm Contents" for examples of this file.

LDAP configuration properties file – Required information used to specify the LDAP configuration to be created or updated. In the examples used in this document, this file is named `config.properties.ldap`, but you can use a different name. To specify the file in the command line, use the `-l` or `--ldapconfig` option.

All required properties (Hostname, Port, User Email, Group Membership, Manager Identifier, Manager Identifier Value, User Name Attribute and User Search Filter) must be provided in this file. If you use the sample LDAP configuration properties file, you must uncomment and provide values for the required properties. See "LDAP Configuration Properties File Parameters" for more information about the contents of this file. See "Sample config.properties.ldap Contents" for examples of this file.

Generating Sample Configuration Properties Files

The `ldap-tool.jar` produces sample configuration properties files by executing the following at the command prompt:

```
"<csa_jre>\bin\java" –jar ldap-tool.jar –g
```

where <csa_jre> is the directory in which the JRE that is used by CSA is installed.

The following sample configuration properties files are generated:

config.properties.ldap

config.properties.idm

Update the contents of config.properties.idm as needed, as described in the table below.

In the current directory, make a copy of the sample LDAP configuration properties file as a backup file. Then, edit the config.properties.ldap file, as necessary (you must uncomment and provide values for the required properties). See “LDAP Configuration Properties File Parameters” for more information about the properties.

IdM Configuration Properties File Parameters

This table lists the parameters found in the IdM configuration file.

Table 1. IdM Configuration Properties File Parameters

Property Name	Description
idmConfig.Url	The system on which CSA is installed. Default: https://127.0.0.1:8444
securityIdmTransport UserName	The user used to authenticate CSA Consumption REST API calls. Default: idmTransportUser
securityIdmTransport Password	The password for the user used to authenticate CSA Consumption REST API calls. The password should be encrypted (see "Encrypt a Password" in the CSA Configuration Guide for instructions on encrypting passwords). An encrypted password is preceded by ENC without any separating spaces and is enclosed in parentheses. If you have configured CSA to be FIPS 140-2 compliant, encrypt this password after you have configured CSA to be FIPS 140-2 compliant (that is, you should use the updated encryption tools to encrypt the password). Example securityIdmTransportPassword=ENC(rlbE840uFDlert5441fe70jkY)

LDAP Configuration Properties File Parameters

This table lists the parameters found in the LDAP configuration file.

Table 2. LDAP Configuration Properties File Parameters

Property	Name
csa.ldap.hostname	**Required**. The fully-qualified LDAP server domain name (server.domain.com) or IP address.

	Example `ldap.xyz.com`
csa.ldap.port	**Required**. The port used to connect to the LDAP server. 389 for ldap and 636 for ldaps.
csa.ldap.ssl	Connection Security. If the LDAP server is configured to require ldaps (LDAP over SSL), set this property to `true`. If the LDAP server does not require ldaps, set this property to `false`.
csa.ldap.basedn	Base distinguished name. The Base DN is the top level of the LDAP directory that is used as the basis of a search. Example `DC=cirrus,DC=com`
csa.ldap.userid	The fully distinguished name of any user with authentication rights to the LDAP server. If the LDAP server does not require a User ID or password for authentication, this value can be omitted. Example `CN=csaldap,CN=Users,DC=cirrus,DC=com`
csa.ldap.password	Password of the User ID. If the LDAP server does not require a User ID or password for authentication, this value can be omitted. The password should be encrypted (see "Encrypt a Password" in the CSA Configuration Guide for instructions on encrypting passwords). An encrypted password is preceded by ENC without any separating spaces and is enclosed in parentheses. If you have configured CSA to be FIPS 140-2 compliant, encrypt this password after you have configured CSA to be FIPS 140-2 compliant (that is, you should use the updated encryption tools to encrypt the password). Example `ENC(A0Ell2PmN6ajnhlInJAnEumDDvCBvQLV)`
csa.ldap.useremail	**Required**. Designates the email address of the user to which to send email notifications. Common LDAP attribute names for email include `mail` and `email`. If the value for this attribute in the user object in LDAP is empty or not valid, the user for whom the value is empty or not valid does not receive email notifications. Example `mail`

csa.ldap.groupmembership	**Required**. Identifies a user as belonging to the group. Common LDAP attribute names that convey group membership include `member` and `uniqueMember`.
	Examples
	`member`
	`member,uniqueMember`

csa.ldap.managerIdentifier	**Required**. Identifies the manager of the user. A common LDAP attribute name for a user's manager is `manager`. If the value for this attribute in the user object in LDAP is empty or not valid, approval policies that use the User Context Template will fail. Example `manager`
csa.ldap.managerIdentifierValue	**Required**. Describes the value of the manager identifier. A common value for the manager identifier in LDAP is the dn (distinguished name) of the manager's user object. If the manager's user object cannot be located based on the values for manager identifier and manager identifier value, approval policies that use the User Context Template will fail. Example `dn`
csa.ldap.userAvatar	LDAP attribute whose value is the URL to a user avatar image that will display for the logged in user in the Marketplace Portal. If no avatar is specified, a default avatar will be used. Example `avatar`
csa.ldap.userNameAttribute	**Required**. The name of the attribute of a user object that contains the username that will be used to log into the Cloud Service Management Console or Marketplace Portal. The value for this field can be determined by looking at one or more user objects in the LDAP directory to determine which attribute consistently contains a unique user name. Example `sAMAccountName`
csa.ldap.userSearchBase	LDAP container that contains the users. This value must be relative to the Base DN. Example `cn=Users`
csa.ldap.userSearchFilter	**Required**. Specifies the general form of the LDAP query used to identify users during login. It must include the pattern {0}, which represents the user name entered by the user when logging in to the Cloud Service Management Console or Marketplace Portal. The filter is generally of the form `<attribute>= {0}`, with `<attribute>` typically corresponding to the value entered for User Name Attribute. Example `sAMAccountName={0}`
csa.ldap.searchSubtree	When a user logs in to the Cloud Service Management Console or Marketplace Portal, the LDAP directory is queried to find the user's account. The Search Subtree setting controls the depth of the search under User Search Base. If you want to search for a matching user in the User Search Base and all subtrees

	under the User Search Base, set this property to `yes`. If you want to restrict the search for a matching user to only the User Search Base, excluding any subtrees, set this property to no. Examples `yes` no

Usage

Command Line Options

The command options and sub-options for the LDAP Configuration Tool are shown in the following table.

Option	Option Description	Sub-options Associated with the Option	Sub-option Description
`-h, --help`	Display syntax and usage information.	none	
`-g, --generate`	Generate sample input config properties file	none	
`-o, --organization <organization Identifier>`	Name of the organization for which the LDAP configuration information needs to be created or modified	`-c, --config <config_filename>`	**Required**. The configuration property filename. This file must be located in the same folder as the ldap-tool.jar file (`<csa_home>\Tools\LdapTool\`).
		`-l, --ldapconfig`	**Required**. The LDAP configuration property filename. This file must be located in the same folder as the `ldap-tool.jar` file (`<csa_home>\Tools\LdapTool\`).
		`-j, --jars <jar filenames>`	Ignored, just for backward compatibility.

To list the supported options, invoke the LDAP Configuration Tool from the command line as follows:

```
java.exe -jar ldap-tool.jar –h
usage: java -jar ldap-tool.jar
       java -jar ldap-tool.jar -o [organization Identifier][-c [Configuration properties file
      name]] -l [ldap configuration properties file name]]
       java -jar ldap-tool.jar -h
       java -jar ldap-tool.jar -g

LDAP tool - The LDAP tool can be used to create or update LDAP configuration for an organization.
```

```
Only a user with CSA administrator role will be able to run this tool.
 -c,--config <config property file>       The config property file name.
    --dbconfig <config property file>     The same as --config, just for backward compatibility.
 -g,--generate                            Generate sample input config properties file
 -h,--help                                Print the usage information.
 -j,--jars <Oracle JARs>                  Ignored, just for backward compatibility
 -l,--ldapconfig <config property file>   The LDAP config property file name.
 -o,--organizationIdentifier              Name of the organization for which LDAP configuration
                                         needs to be created or updated.
```

For more information on the LDAP configuration information that needs to be provided in the config properties file, please refer to the LDAP Configuration Tool Guide.

Example Usage

> **Note:**
>
> When running the LDAP Configuration Tool to create or update the LDAP configuration for an organization, you are prompted for a username and password. This user MUST be assigned to the CSA Administrator role. Users who are not assigned to this role cannot create or update the LDAP configuration for an organization.

Display the LDAP Configuration Tool help:

```
"<csa_jre>\bin\java" -jar ldap-tool.jar –h
```

Generate sample configuration properties files:

```
"<csa_jre>\bin\java" -jar ldap-tool.jar –g
```

Create/update LDAP configuration for an organization:

"<csa_jre>\bin\java" -jar ldap-tool.jar –o orgIdentifier –c config.properties.idm –l config.properties.ldap

Sample config.properties.idm Contents

```
# A sample config properties file for CSA running locally
idmConfig.Url=https://127.0.0.1:8444
# IDM Transport User Name.
securityIdmTransportUserName=idmTransportUser
# IDM Transport User Password.
securityIdmTransportUserPassword=ENC(AR3r0wcMNgOVZ/cFv//Y60r1pYQ9BshH/mSb6VSaVj8=)
```

Sample config.properties.ldap Contents

```
csa.ldap.hostname=172.16.200.50
csa.ldap.port=389
csa.ldap.ssl=false
csa.ldap.basedn=DC=cirrus,DC=com
csa.ldap.userid=CN=csaldap,CN=Users,DC=cirrus,DC=com
csa.ldap.password=ENC(A0Ell2PmN6ajnhlInJAnEumDDvCBvQLV)
csa.ldap.useremail=mail
csa.ldap.groupmembership=member
csa.ldap.managerIdentifier=manager
```

```
csa.ldap.managerIdentifierValue=dn
csa.ldap.userAvatar=avatar
csa.ldap.userNameAttribute=sAMAccountName
csa.ldap.userSearchBase=
csa.ldap.userSearchFilter=sAMAccountName={0}
csa.ldap.searchSubtree=no
```

Generated Sample LDAP Configuration Properties File

```
# Sample properties file for LDAP configuration in CSA.
# Required. The fully-qualified LDAP server domain name (server.domain.com) or IP address.
# Example: ldap.xyz.com
# csa.ldap.hostname=

# Required. The port used to connect to the LDAP server. 389 for ldap and 636 for ldaps.


# Example: 389

# csa.ldap.port=

# Required. This LDAP attribute designates the email address of the user to which to send email
  notifications. Common LDAP attribute names for email include mail and email.
# If the value for this attribute in the user object in LDAP is empty or not valid, the user for
  whom the value is empty or not valid does not receive email notifications.

# Example: mail

#csa.ldap.useremail=

# Required. This LDAP attribute identifies a user as belonging to the group. Common LDAP attribute
  names that convey group membership include member and uniqueMember.
# Example: member,uniqueMember
#csa.ldap.groupmembership=

# Required. This LDAP attribute identifies the manager of the user. A common LDAP attribute name
  for a user's manager is manager. If the value for this
# attribute in the user object in LDAP is empty or not valid, approval policies that use the User
  Context Template will fail.
# Example: manager
#csa.ldap.managerIdentifier=

# Required. This LDAP attribute describes the value of the manager identifier.
# A common value for the manager identifier in LDAP is the dn (distinguished name) of the
  manager's user object.
# If the manager's user object cannot be located based on the values for manager identifier and
  manager identifier value, approval policies that use the User Context Template will fail.
# Example: dn
#csa.ldap.managerIdentifierValue=

# Required. The name of the attribute of a user object that contains the username that will be
  used to log into the Cloud Service Management Console or Marketplace Portal.
# The value for this field can be determined by looking at one or more user objects in the LDAP
  directory to determine which attribute consistently contains a unique user name.
# Example: sAMAccountName
```

```
#csa.ldap.userNameAttribute=

# Required. Specifies the general form of the LDAP query used to identify users during login.
# It must include the pattern {0}, which represents the user name entered by the user when logging
  in to the Cloud Service Management Console or Marketplace Portal. The filter is generally of the
  form <attribute>= 0}, with <attribute> typically corresponding to the value entered for User
  Name Attribute.
# Example: sAMAccountName={0}
#csa.ldap.userSearchFilter=

# Connection Security. If the LDAP server is configured to require ldaps (LDAP over SSL), set this
  attribute to true.
# Example: false
#csa.ldap.ssl=

# Base distinguished name. The Base DN is the top level of the LDAP directory that is used as the
  basis of a search.
# Example: DC=dom,DC=com
#csa.ldap.basedn=

# The fully distinguished name of any user with authentication rights to the LDAP server. If the
  LDAP server does not require a User ID or password for authentication, this value can be
  omitted.
# Example: CN=ldap,CN=Users,DC=dom,DC=com
#csa.ldap.userid=

# Password of the User ID. If the LDAP server does not require a User ID or password for
  authentication, this value can be omitted.
# Example: password
#csa.ldap.password=

# LDAP attribute whose value is the URL to a user avatar image that will display for the logged in
  user in the Marketplace Portal. If no avatar is specified, a default avatar will be used.
# Example: avatar
#csa.ldap.userAvatar=

# The LDAP container that contains users. This value must be relative to the Base DN.
# Example:ou=People
#csa.ldap.userSearchBase=

# When a user logs in to the Cloud Service Management Console or Marketplace Portal, the LDAP
  directory is queried to find the user's account.
# The Search Subtree setting controls the depth of the search under User Search Base.
# If you want to search for a matching user in the User Search Base and all subtrees under the
  User Search Base, set the value of this attribute to yes.
# If you want to restrict the search for a matching user to only the User Search Base, excluding
  any subtrees, set the value of this attribute to no.
# Example: yes
#csa.ldap.searchSubtree=
```

Known Issues

None.

Document Change Notes

Date	Description
Aug 2016	Original release of document
Oct 2016	Updated for QCCR1D227711

Send documentation feedback

If you have comments about this document, you can send them to docs.feedback@microfocus.com.

Legal notices

Warranty

The only warranties for Seattle SpinCo, Inc. and its subsidiaries ("Seattle") products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Seattle shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Except as specifically indicated, valid license from Seattle required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notice

Trademark notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.softwaregrp.com.

This website provides contact information and details about the products, services, and support that Micro Focus offers.

Micro Focus online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Access the Software Licenses and Downloads portal
- Download software patches
- Access product documentation

- Manage support contracts
- Look up Micro Focus support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require you to register as a Passport user and sign in. Many also require a support contract.

You can register for a Software Passport through a link on the Software Support Online site.

To find more information about access levels, go to https://softwaresupport.softwaregrp.com/web/softwaresupport/access-levels.

To check for recent updates or to verify that you are using the most recent edition of a document, contact your Client Director.