LDAP/AD User Guide

for 6.5 or later

Catalog No. 11-808-615-01

Rev. 8/8/2018

 Important changes are listed in Document revision history at the end of this document.

Contents

What is the LDAP/AD add-on?

The LDAP/AD add-on is an authentication provider that allows you to log in to the building automation system using LDAP (Lightweight Directory Access Protocol) or AD (Active Directory®) credentials.

Here are some of the benefits this add-on provides:

- Ease of retrieving or resetting a user's building automation system password
- Ability to lock a user out of the building automation system
- A single, central server for managing several building automation system servers' logins

Requirements

- You are running a v6.5 or later system with the latest cumulative patch applied
- You have the Admin privilege on your WebCTRL® system.
- You have purchased and downloaded the LDAP/AD license
- You have downloaded ldap.addon

See "Installing an Add-on User Guide" for the following:

- Installing an add-on
- Applying a license
- Running an add-on
- Upgrading an add-on

Login names and passwords

The building automation system operator login name does not have to match the user's LDAP login name. The add-on uses the building automation system (BAS) operator login name to find the user's LDAP entry and then to discover their LDAP login name from the entry. The exact configuration is determined by the authentication type chosen, but all will require a Search Base where the LDAP add-on will search to find users. The values set in the Search Filters determine how that search is performed.

TIP When logging into a BAS using LDAP/AD as the Authentication Provider, the operator must enter their BAS operator login name with their LDAP password.

Setting up the LDAP/AD add-on

Step 1: *Configure the LDAP/AD add-on* (page 2).
Step 2: *Configure the truststore* (page 4), if needed.
Step 3: *Set up local operators* (page 6), if needed.
Step 4: *Turn on LDAP/AD authentication* (page 6).

NOTE The add-on is not active until Step 4 is complete.

Using the LDAP Questionnaire

An LDAP Worksheet is included in the *Questionnaire* (page 7). We recommend that the customer's network administrator complete this questionnaire to allow you to configure the add-on appropriately.

NOTE The LDAP/AD add-on supports two LDAP authentication methods:

- Simple with TLS
- Digest-MD5 with or without TLS

TIP No other authentication method is supported at this time. If the customer uses a different type of authentication, notify Technical Support to make them aware of the need.

If your LDAP configuration is supported, proceed to *Step 1 To configure the LDAP/AD add-on* (page 2) using the completed worksheet.

Step 1: Configure the LDAP/AD add-on

The LDAP/AD add-on supports two LDAP authentication methods:

- Simple with TLS
- Digest-MD5 with or without TLS

TIP No other authentication method is supported at this time.

Configure the LDAP Host

Using the *LDAP Questionnaire* (page 7), follow the instructions below to configure the add-on for either Simple or Digest-MD5 authentication to configure the add-on.

1. On the **Configuration** tab, select the authentication type (Q1).
2. Enter the host address and the port number from the worksheet (Q2a and 2b).
   NOTE 389 and 636 are standard LDAP ports, but the add-on also supports custom ports.
3. Select whether the LDAP/AD server uses referrals or not (Q3).
4. Select whether TLS is used or not (Q4).
5. Enter the LDAP bind name and password assigned to the building automation system (BAS) server (Q6).
   In order to use LDAP, the BAS server will need to be able to authenticate with the LDAP server.
6. If using Digest-MD5, enter the **Default Realm** and **ID Lookup** from the Questionnaire (5b).
7. Enter the **Search Base** and **Search Filters** as needed (Q5a/Q5b).
8. Click **Update** for the add-on to attempt to authenticate with the LDAP host server.

TIPS

- If TLS is used, you must *configure your truststore* (page 4) now.
- You can verify if the authentication was successful by viewing the **Diagnostic Logs** tab. (See table below for some troubleshooting issues and how to resolve them.)

Error Message	TIP
Bind Failed	Verify the Server Bind Name and Password are correct.
Bind Result: Connection Error (91)	Check the LDAP server Machine Network connection and Active directory service is running.
Error Updating connection settings, see log for details	Check the Truststore configuration.

Digest-MD5 requirements

Digest-MD5 authentication requires the following configuration. Digest-MD5 may be used with or without TLS.

NOTE If TLS is used, a *truststore* (page 4) must be configured.

Default Realm	This is used when attempting to authenticate a user. If no realm is specified in the bind name or found when looking up the user on the server, this value is used to attempt the authentication. It is also used when the add-on creates the initial connection pool. NOTE A default realm may not be required, depending on how your LDAP server is configured.
Quality of Protection	Specify the quality of the protection required by your LDAP server. If TLS is being used, then **Authentication only** is used as the **Quality of Protection** setting.
Search Base	This is the base directory where the LDAP/AD add-on searches for user authentication information. If the user entries are located at the server's base suffix, the **Discover Base Suffix** button can be used to set this value. Otherwise, the Search Base must be entered manually.
ID Lookup Field	This is the name of the field that contains the user's LDAP login name.
Search Filter	The name of the LDAP entry attribute used by the add-on to attempt to match the BAS operator login name in order to discover the operator's LDAP entry. NOTE You must set at least one search filter field, but more can be used if needed. Add additional search filters using the **+** button; remove them by using the **X** button.

Simple requirements

The Simple authentication method requires TLS to be used, so you must configure a truststore as well. Two configuration options are required to use simple authentication: search base and a search filter.

Search Base	This is the base directory where the LDAP/AD add-on searches for user authentication information. If the user entries are located at the server's base suffix, the **Discover Base Suffix** button can be used to set this value. Otherwise, the Search Base must be entered manually.
Search Filter	The name of the LDAP entry attribute used by the add-on to attempt to match the BAS operator login name in order to discover the operator's LDAP entry. NOTE You must set at least one search filter field, but more can be used if needed. Add additional search filters using the **+** button; remove them by using the **X** button.

Step 2: Configure the truststore

Many LDAP configurations will require TLS. To use TLS, a certificate truststore is required.

CAUTION If a truststore has already been configured and you go through this process again, the previous truststore will be replaced. In the case of a truststore managed by the building automation system (BAS), it will be overwritten.

Selecting a truststore type

To use the BAS-managed truststore

1. On the **Configuration** tab, click **Create Truststore**.
2. Select **Create New**.
3. Provide a truststore password.
4. Select **OK** to accept the truststore configuration.

   The add-on creates an empty truststore to which certificates can be added (see *Managing a Truststore* (page 5)).

To use an existing truststore

1. On the **Configuration** tab, select **Existing Truststore**.
2. Enter the path to the truststore file.

   The add-on uses this file at this location. If it is deleted or moved, the configuration will fail.
3. If you want to be able to manage the truststore through the add-on, provide the truststore password.

   If you provide the truststore password, you will be able to view, add and delete the certificates in the truststore just as if the truststore was being managed by the add-on.
4. Select **OK** to accept the truststore configuration.

Managing a truststore

If you are using a BAS-managed truststore, or you provided the password to an existing truststore, you can view and manage the certificates in that truststore. If you have just created a new truststore, you can add certificates to it using this add-on.

There are two methods for adding certificates to the truststore:

- by discovering the LDAP host certificates
- by adding a certificate manually

To view the certificates in the truststore

1 On the **Configuration** tab, click **Manage Truststore** to view a list containing the serial number, validity, and subject name of each certificate for identification.

NOTE Certificates can expire over time, rendering them invalid. Invalid certificates need to be removed and replaced to keep the LDAP connection working.

To discover LDAP host certificates

1 Click **Discover Host Certificates**. A second table of certificates will appear below.

NOTE If it is empty, no certificates were discovered and the LDAP add-on is likely mis-configured.

2 Select the certificates to be added to the truststore by selecting their checkboxes.

3 Click **Add Selected Certificates** to refresh the list, showing the newly added certificates.

To add a certificate manually

1 Click **Add Certificate**.

2 Copy and paste the Base 64 encoded certificate text (including the BEGIN CERTIFICATE and END CERTIFICATE lines).

3 Click **Add Certificate** to refresh the list, showing the newly added certificates.

NOTE If the certificate encoding was invalid, an error will occur.

4 Close the **Manage Truststore** dialog when you are done.

To delete a certificate

1 Check the checkbox of the certificate(s) to be deleted.

2 Click **Delete Selected Certificates** to view the refreshed list.

NOTES

- Deleting a certificate can cause the LDAP connection to fail.
- Deleted certificates cannot be recovered, but you can re-add them to the truststore.

Step 3: Set up local operators

You can configure operators who will use their building automation system (BAS) credentials instead of an LDAP authentication. To add a local operator, you must to know their BAS operator login name.

TIP Be sure to set up at least one Admin level local operator before turning on LDAP/AD authentication in Step 4.

To add a Local Operator

1. On the **Local Operator** tab, enter the operator name in the text field.
2. Click **Add** to allow that operator to be able to log in using their BAS operator login name and password.

To remove a Local Operator

1 On the **Local Operator** tab, select the operator name and click **Remove Selected**.

Step 4: Turn on LDAP/AD authentication

NOTE The add-on is not active until this step is complete.

1. In SiteBuilder, click the **Configure** > **Preferences** > **Web Server** tab.
2. Select **LDAP/AD** in the **Authentication Provider** drop-down list.

TIP To turn off LDAP/AD authentication, select **Default** in the **Authentication Provider** drop-down list.

Troubleshooting

TIPS

- You can view the date and time of each LDAP/AD login on the **Logs** tab in the LDAP/AD add-on, plus any diagnostic messages and errors that occur.
- For more detailed logging, **Verbose Logging** can be enabled; contact Technical Support for more information.
- In the event that users are locked out of building automation system due to issues with the LDAP server, LDAP/AD authentication can be turned off in SiteBuilder until the issue is resolved. See the TIP in section "*Step 4* (page 6): Turn on LDAP/AD authentication" for details.
- In the event that the building automation server loses its connection with the LDAP server, the LDAP/AD add-on will recognize the disconnected state the next time an operator tries to log in using their LDAP credentials. Once the disconnect has been recognized, the LDAP/AD add-on will attempt to reconnect every minute until the connection succeeds. While users are locked out of the building automation system due to issues with the LDAP server, LDAP/AD authentication can be turned off in SiteBuilder until the issue is resolved.
- If experiencing delays when logging in, have your network administrator verify communication between the building automation system and the LDAP servers.

Appendix

LDAP Questionnaire

To be filled out by the system administrator for **each** authentication type supported by your LDAP server.

Q1 What type of authentication does the LDAP/AD host server support?

Simple with TLS ____ (Complete Q2 - Q4, then continue with Q5a)

Digest-MD5 ____ (Complete Q2 - Q4, then continue with Q5b)

Other ____ (Stop here; the add-on will not work. No other type of authentication is supported at this time. If a different type is used, notify Technical Support to make them aware of the need.)

Q2a What is the address of the LDAP/AD host server?

_____

Q2b What is the port number of the LDAP/AD host server?

_____

Q3 Does the LDAP/AD host server use referrals?

Yes ____ No ____

Q4 Does the LDAP/AD host server support TLS?

_____

Q5a **Simple with TLS**

When using Simple authentication, the LDAP add-on attempts to find a user entry under the Search Base directory where the user's building automation system (BAS) username matches the value in one or more of the Search Filter attributes. If one and only one user entry is found, the add-on uses that entry's Distinguished Name (DN) as the bind name when the authentication is attempted.

Search base _____

NOTE Specify 'Default' if the server's base suffix is the search base.

Search filters

_____

_____

_____

Q5b Digest-MD5

To authenticate LDAP users with Digest-MD5, the add-on searches the entries under the directory indicated by the Search Base. It then attempts to match one (and only one) entry where the user's building automation system (BAS) operator login name matches the value of at least one of the values in the search filter. If a match is found, the add-on uses the user's bind name when attempting the authentication.

What is the default realm, if any? _____

Search base _____

NOTE Specify 'Default' if the server's base suffix is the search base.

ID Lookup _____

Search filters

_____

_____

_____

What user entry attribute is used to get the user's LDAP bind name?

_____

Q6 What are the LDAP credentials assigned to the LDAP/AD add-on?

NOTE The LDAP/AD add-on requires an LDAP login. It uses this login to:

- bind to the server.
- establish a small pool of connections that are used for directory searches.
- authenticate BAS users when they log in.

a. Username _____

b. Password _____

Document revision history

Important changes to this document are listed below. Minor changes such as typographical or formatting errors are not listed.

Date	Topic	Change description	Code*
		No changes yet	

* For internal use only