Description of authentication windows and dialog boxes

Active IQ Unified Manager 9.9

NetApp
February 20, 2023

Table of Contents

Description of authentication windows and dialog boxes

You can enable LDAP authentication from the Setup/Authentication page.

Remote Authentication page

You can use the Remote Authentication page to configure Unified Manager to communicate with your authentication server to authenticate remote users who attempt to log into the Unified Manager web UI.

You must have the Application Administrator or Storage Administrator role.

After you select the Enable remote authentication checkbox, you can enable remote authentication using an authentication server.

- **Authentication Service**

  Enables you to configure the management server to authenticate users in directory service providers, such as Active Directory, OpenLDAP, or specify your own authentication mechanism. You can specify an authentication service only if you have enabled remote authentication.

  - **Active Directory**
    - Administrator Name

      Specifies the administrator name of the authentication server.

    - Password

      Specifies the password to access the authentication server.

    - Base Distinguished Name

      Specifies the location of the remote users in the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is `cn=ou,dc=domain,dc=com`.

    - Disable Nested Group Lookup

      Specifies whether to enable or disable the nested group lookup option. By default this option is disabled. If you use Active Directory, you can speed up authentication by disabling support for nested groups.

    - Use Secure Connection

      Specifies the authentication service used for communicating with authentication servers.

  - **OpenLDAP**
    - Bind Distinguished Name

      Specifies the bind distinguished name that is used along with the base distinguished name to find

remote users in the authentication server.

- Bind Password

  Specifies the password to access the authentication server.

- Base Distinguished Name

  Specifies the location of the remote users in the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is `cn=ou,dc=domain,dc=com`.

- Use Secure Connection

  Specifies that Secure LDAP is used for communicating with LDAPS authentication servers.

◦ **Others**

- Bind Distinguished Name

  Specifies the bind distinguished name that is used along with the base distinguished name to find remote users in the authentication server that you have configured.

- Bind Password

  Specifies the password to access the authentication server.

- Base Distinguished Name

  Specifies the location of the remote users in the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is `cn=ou,dc=domain,dc=com`.

- Protocol Version

  Specifies the Lightweight Directory Access Protocol (LDAP) version that is supported by your authentication server. You can specify whether the protocol version must be automatically detected or set the version to 2 or 3.

- User Name Attribute

  Specifies the name of the attribute in the authentication server that contains user login names to be authenticated by the management server.

- Group Membership Attribute

  Specifies a value that assigns the management server group membership to remote users based on an attribute and value specified in the user's authentication server.

- UGID

  If the remote users are included as members of a GroupOfUniqueNames object in the authentication server, this option enables you to assign the management server group membership to the remote users based on a specified attribute in that GroupOfUniqueNames object.

- Disable Nested Group Lookup

Specifies whether to enable or disable the nested group lookup option. By default this option is disabled. If you use Active Directory, you can speed up authentication by disabling support for nested groups.

- Member

  Specifies the attribute name that your authentication server uses to store information about the individual members of a group.

- User Object Class

  Specifies the object class of a user in the remote authentication server.

- Group Object Class

  Specifies the object class of all groups in the remote authentication server.

- Use Secure Connection

  Specifies the authentication service used for communicating with authentication servers.

If you want to modify the authentication service, ensure that you delete any existing authentication servers and add new authentication servers.

Authentication Servers area

The Authentication Servers area displays the authentication servers that the management server communicates with to find and authenticate remote users. The credentials for remote users or groups are maintained by the authentication server.

- **Command buttons**

  Enables you to add, edit, or delete authentication servers.

  - Add

    Enables you to add an authentication server.

    If the authentication server that you are adding is part of a high-availability pair (using the same database), you can also add the partner authentication server. This enables the management server to communicate with the partner when one of the authentication servers is unreachable.

  - Edit

    Enables you to edit the settings for a selected authentication server.

  - Delete

    Deletes the selected authentication servers.

- **Name or IP Address**

  Displays the host name or IP address of the authentication server that is used to authenticate the user on the management server.

- **Port**

  Displays the port number of the authentication server.

- **Test Authentication**

  This button validates the configuration of your authentication server by authenticating a remote user or group.

  While testing, if you specify only the user name, the management server searches for the remote user in the authentication server, but does not authenticate the user. If you specify both the user name and password, the management server searches and authenticates the remote user.

  You cannot test the authentication if remote authentication is disabled.

SAML Authentication page

You can use the SAML Authentication page to configure Unified Manager to authenticate remote users using SAML though a secure identity provider (IdP) before they can to log in to the Unified Manager web UI.

- You must have the Application Administrator role to create or modify the SAML configuration.
- You must have configured remote authentication.
- You must have configured at least one remote user or remote group.

After remote authentication and remote users have been configured, you can select the Enable SAML authentication checkbox to enable authentication using a secure identity provider.

- **IdP URI**

  The URI to access the IdP from the Unified Manager server. Example URIs are listed below.

  ADFS example URI:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Shibboleth example URI:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **IdP Metadata**

  The IdP metadata in XML format.

  If the IdP URL is accessible from the Unified Manager server, you can click the **Fetch IdP Metadata** button to populate this field.

- **Host System (FQDN)**

  The FQDN of the Unified Manager host system as defined during installation. You can change this value if necessary.

- **Host URI**

  The URI to access the Unified Manager host system from the IdP.

- **Host Metadata**

  The host system metadata in XML format.

Copyright information

Trademark information