LDAP Authentication and Authorization

What is LDAP Authentication?

Today, the network can include elements such as LANs, WANs, an intranet, and the Internet. Many enterprises have turned to centralized directory-enabled applications to provide their users with seamless access to all of the applications, devices, and appliances they are authorized to use.

Directory services simplify administration: additions and changes to permissions are made once in the directory and are then immediately available to all authorized users, directory-enabled applications, devices, and appliances. Blue Coat ProxySG supports the use of an external LDAP-enabled directory for authentication and authorization of users on a per-group basis. Authentication determines that the user is who they say they are; authorization determines what the user is allowed to do. LDAP authentication for Blue Coat ProxySG can be configured to support any LDAP-compliant directory including:

- Microsoft Active Directory Server
- Novell NDS/eDirectory Server
- Netscape/Sun iPlanet Directory Server

Blue Coat ProxySG also provides the ability to locate a group or a single user in a single root of an LDAP directory information tree (DIT) through its VPM search functionality. Once located, the user or group can be selected for inclusion in authentication and authorization.

Why Enable LDAP Authentication and Authorization?

Blue Coat ProxySG makes use of your existing directory-based authentication by passing login requests to the directory service. There is no need to define an additional authentication database when using ProxySG. By keeping authentication centralized on your directory, a security administrator always knows who is accessing network resources and can easily define user and/or group-based policies to control access (authorize) and provide auditable logs. Group authentication provides the additional advantage of being able to create more granular rules such as: Security Group can download .zip and .exe files and Finance Group is guaranteed bandwidth for end of month/end of quarter.

Implementing LDAP Authentication and Authorization

There are four parts to implementing LDAP authentication and authorization services on the ProxySG:

1. **Create an LDAP Realm on the ProxySG**
2. **Configure LDAP properties on the ProxySG**
3. **Configure an LDAP Authentication Policy on the ProxySG**
4. **Configure an Authorization Policy on the ProxySG**
5. **Test your LDAP Authentication and Authorization Policy**

**Note:** This document describes setting up a Microsoft Active Directory LDAP authentication; the same steps apply to any other LDAP compliant directory.
About the Default Proxy Policy

On the Management Console Configuration > Policy > Policy Options page you can set the default policy option to Deny or Allow. The two options provide two different approaches:

- A default proxy transaction policy of Deny prohibits proxy-type access through the ProxySG appliance; instead, you must create policies to explicitly grant access on a case-by-case basis.
- A default proxy transaction policy of Allow permits most proxy transactions. If your policy is set to Allow, you must create policies to explicitly deny access on a case-by-case basis. Please note: if protocol detection is enabled (the default), HTTP CONNECT transactions are only allowed if they are tunneling SSL; if protocol detection is disabled, HTTP CONNECT is only allowed on port 443.

Note: This document assumes the Deny default proxy policy and that HTTP traffic is set to intercept [General > Services > Proxy Services]. If your default proxy policy is Allow, you would need to add a Web Access Layer denying particular users/groups access. For more information on developing effective policies, see the Policy Best Practices tech brief.

Part 1 – Create an LDAP Realm on the ProxySG

Using the Blue Coat Management Console, create an authentication realm:

1. Go to General > Authentication > LDAP. The LDAP Realms tab displays.
2. Click New. The Add Realm dialog displays.
3. Name the realm appropriately. NOTE: To help maintain scalability, Blue Coat recommends giving relevant names to layers and objects. Select Microsoft Active Directory for the Type of LDAP server option, type an IP address for the Primary server host option, and a port number, if needed. Click OK to add the realm; click Apply to finish and OK to dismiss the confirmation.

Note: The default port is 389 (for plaintext LDAP; if you are configuring secure LDAP, a port that supports SSL would be needed) and the default user attribute type (for Active Directory) is sAMAccountName. You may have to change these defaults for your particular LDAP configuration. Only an experienced LDAP administrator should make configuration changes.
Part 2 – Configure LDAP Properties on the ProxySG

If needed, configure any additional needed LDAP properties on the ProxySG; you may need to use the arrow keys in the upper right corner in order to see all of the tabs. This section describes the available LDAP configuration tabs and their options.

**Note:** ProxySG attempts to retrieve configured information from the database; however, some changes may need to be made and should only be done by an experienced LDAP administrator.

**LDAP Servers** tab: Select a realm and set server options.

- **Server type:** Other, Microsoft Active Directory, Netscape/Sun iPlanet, Novell NDS/eDirectory
- **LDAP Protocol Version:** Default is 3; 2 can be selected
- **Follow referrals** [LDAP v3 only]: Allows the client to follow referrals to other LDAP servers
- **Primary server host** and **Port**
- **Alternate server host** and **Port** (optional)
- **Enable SSL** [LDAP v3 only]: Makes the LDAP server connection use SSL and, if selected, activates Verify server certificate: Causes a server certificate check before LDAP queries
- **Timeout request after:** Default is 60 seconds
- **Case sensitive:** If the LDAP server is configured to be case-sensitive, check this box
LDAP DN tab: Select a realm and specify base Distinguished Names (DNs) to search per realm.

- **User attribute type**: Varies based on LDAP server type
- **Base DN**: The base DN identifies the entry for searching such as DC=example, DC=com. At least one non-null base DN must be specified. Use the Promote entry and Demote entry buttons to re-order the Base DNs you add.

LDAP Search & Groups tab: Select a realm and specify search parameters.
• **Search:**
  - **Anonymous search allowed:**
    - If selected (default): Use anonymous as the search name.
    - If deselected: Set the bind credentials, **Search user DN**.

  **NOTE:** Some directories (for example, Active Directory) require a valid user to perform LDAP search and do not allow anonymous bind. LDAP directory attributes for an anonymous search typically only provide a subset of available information.

  - **Dereference aliases:** Choose when to search for a specific object rather than the object’s alias.

• **Group information:** the ProxySG enters these defaults:
  - For Microsoft AD
    - **Membership type:** user
    - **Membership attribute:** memberof
  - For Netscape/Sun iPlanet
    - **Membership type:** group
    - **Membership attribute type:** uniquemember
  - For Novell eDirectory
    - **Membership type:** user
    - **Membership attribute type:** member

**LDAP Objectclasses** tab: Select a realm and define the starting **Object Type** used when a search is made by the ProxySG, if needed. For example, a user entry may have the attribute `objectclass=user`. 
Please note for Object Classes:

- Objectclass attribute values can vary among LDAP servers
- Objectclass attribute values are used by the Visual Policy Manager to browse the content of an LDAP server
- The objectclass list is customizable

**LDAP General** tab (enlarge window to see all options): Select a realm and do the following, if needed:

- **Display name**: The name of the LDAP realm that users see
- **Refresh Times**: Specify length of time to cache user credentials (default 900 seconds), including surrogate credentials and authorization. To make changes, de-select the **Use the same refresh time for all** option. See the online help for details.
- **Inactivity timeout**: The amount of time an authenticated session can be inactive before being logged out (default is 900 seconds)
- **Rejected credentials time**: Set how long a rejected credential stays in cache
- **Cookies**: Select **Use persistent cookies** to disable the default of browser cookies
- **Verify the IP address in the cookie**: De-select to disable cookie verification
- **Virtual URL**: Change the virtual URL if needed; see the online help for details
- **Challenge user after logout**: De-select to allow authenticated users to re-login without another challenge

*Note*: See the online help for details on these settings. Blue Coat recommends using the defaults for most situations. Policy settings override these settings.
Part 3 – Configure an Authentication Policy on the ProxySG

The authentication policy specifies which configured LDAP database to use to authenticate users and groups. You use the Visual Policy Manager to do this: go to Policy > Visual Policy Manager and click Launch.

1. Click Policy > Add Web Authentication Layer; name the layer appropriately.

2. Right-click the Action setting and select Set. The Set Action Object dialog displays.

3. Click New and select Authenticate. The Add Authenticate Object dialog displays.

4. Name the object appropriately. Select your LDAP realm for the Realm option. Click OK to add the object and dismiss the dialog. The Set Action Object dialog re-displays with the new object selected. Click OK to set the object.

5. Click Install Policy to finish.
Part 4 – Configure an Authorization Policy on the ProxySG

The authorization policy uses a Web Access Layer to set rules for authenticated users and groups. Without the Web Access Layer rules, all users and groups must be authenticated for any Web access. You use the Visual Policy Manager to do this: go to Policy > Visual Policy Manager and click Launch. This procedure configures a Web Access Layer that limits the traffic source to an authenticate-able group [technical marketing in the example]. You can select User in step 3 to limit the policy to a particular user instead.

1. Add the Web Access Layer to apply rules to users or groups. Click Policy > Add Web Access Layer and name the layer appropriately.

2. Right-click the Source setting and select Set. The Set Source Object dialog displays.

3. Click New and select Group. The Add Group Object dialog displays. If you know the LDAP name of the group, enter it in the Group option and proceed to step 6; otherwise, continue with step 4.
If you’re not sure what name to enter, click Browse to open an LDAP Browser and see a list of all configured LDAP groups in the database selected for this authentication policy.

Select a group and click OK to set the group and dismiss the dialog. The Add Group Object dialog re-displays with the selected group name.
Click OK to add the Source object and dismiss the dialog. The Set Source Object dialog re-displays with the new object selected. Click OK to set the object and dismiss the dialog.

Next, right-click the Action setting and select Allow.

Click Install Policy to finish.

Note: Use the Time setting to limit the policy to a certain schedule.
Part 5 – Test Your LDAP Authorization Policy

Test the LDAP authentication and authorization policy by opening up a Web Browser (explicitly configured to go through the proxy). You are prompted for your user name and password credentials as shown; type in a valid user name (if your policy authenticates groups, the user must be a valid member of that group) and password from your Active Directory domain. If the credentials are valid, the URL proceeds. If the credentials are not valid, the following exception page displays (you can customize the exception page; for details see the ProxySG technical brief Creating Exception Pages).

Conclusion

The ProxySG is designed to take advantage of existing authentication environments including LDAP directory servers. Utilizing existing authentication services saves time and money simplifying the deployment of the ProxySG. Most LDAP parameters are automatically configured to default settings on the ProxySG for easy deployment. Authentication and authorization policies allow you to set granular control over Web access on a per-user or per-group basis.