Configuring Splash Page Authentication with an LDAP Server

Cisco Meraki access points support authentication through an externally hosted LDAP server. After the server is configured, the dashboard will require a minimal amount of setup to allow for LDAP authentication.

Please use the steps below to successfully configure Dashboard to use your LDAP server for user authentication:

1. Log into Dashboard.
2. Navigate to Configure>Access control.
3. Set the Association requirement to Open

Network access

Association requirements

- Open (no encryption)
  - Any user can associate
- Pre-shared key with WPA2
  - Users must enter a passphrase to associate
- MAC-based access control (no encryption)
  - RADIUS server is queried at association time
- WPA2-Enterprise with Meraki authentication
  - User credentials are validated with 802.1X at association time

4. Set the Network sign-on method to Sign-on Splash page and from the Authentication server drop down select Use my LDAP server.
5. Click **Add a server** for LDAP servers.

6. Enter the IP address of your LDAP server in the **Host** field and the LDAP listening port which is normally 389 in the **Port** field.

7. For **LDAP admin**, enter the distinguished name of the administrative account to be used by the AP to bind to your LDAP server, for example `cn=admin,dc=example,dc=com`, and the password.

8. Click the **Save Changes** button

This completes the configuration that is necessary in Dashboard. Further difficulties will need to be addressed either at the LDAP server or at the client.

**Note:** Client credentials will be passed along to the server by the access point. As such, ensure that firewall rules are in place to allow communication from your access points to the LDAP server IPs and ports.
When using splash page authentication, captive portal strength settings take precedence over configured traffic shaping and firewall rules. This means traffic shaping and firewall rules will only apply after Splash page authentication has occurred successfully. If firewall or traffic shaping rules are configured on an SSID, use the "Block all access until sign-on is complete" captive portal strength setting to apply the principle of least privilege to the SSID. This captive portal strength will ensure all traffic is blocked until the desired firewall and traffic shaping rules can be applied.