Meraki Local Authentication - MR 802.1X

Overview

In large-scale deployments RADIUS servers are typically located in remote data centers (DCs) or otherwise off-site, requiring a working WAN uplink in order to reach these servers for authentication purposes and connect to 802.1X-protected SSID. This is especially true for retail environments where wireless point-of-sale (POS) devices require both the high security of the data transferred over the air provided by 802.1X authentication and high availability in the case of inability to reach RADIUS server(s).

The Meraki Local Auth feature provides an alternative authentication method to allow connection to 802.1X-protected SSIDs that does not rely on the reachability of the RADIUS server(s). This is done by running a built-in RADIUS server on MR access points and allowing MRs to act not only as Authenticator but also an Authentication Server – the role typically played by a RADIUS server.
When relevant servers are reachable, MR access points cache wireless clients’ authentication information. If wireless clients try to connect when servers are unreachable, the MR access point consults its cache to accept or reject the authentication.

**Note:** [Alternative Management Interface](#) can be used to communicate with the LDAP server only. It cannot be used to communicate with the OCSP server.

### Username/Password Caching (Password Auth)

When enabled, the MR access point connects to the configured LDAP server to ensure the user exists and is authorized for WiFi access. It will then check the credentials presented by the user either against a password attribute received from the LDAP server or through an LDAP bind using the user credentials provided. It then caches a hash of the credentials used if the authentication is successful. This cache is referenced whenever a user tries to connect via 802.1x and the LDAP server is unreachable.

![Diagram of Username/Password Caching](#)

### Certificate Caching (Certificate Auth)

The MR and client mutually authenticate each other using SSL certificates. MR uses the certificate signed by QuoVadis CA and the client uses the certificate signed by their own CA.

To check the revocation status of the client certificate, you can (optionally) add a URL for the OCSP responder that will indicate if the certificate is revoked or not. To (optionally) check if the certificate belongs to a user or device that can use WiFi, you can add an LDAP server.

Instead of caching a password, MR will cache a hash of the client certificate if all configured checks pass, and the authentication is successful. When a wireless client tries to authenticate again but either the OCSP or LDAP servers are unreachable, the client certificate will again be verified against the configured CA certificate (in case it has changed), then the hash of the certificate will be compared against the "known good" certificate hash for that user in the cache. If the hashes match, the user will be authenticated. If neither OCSP nor LDAP verification is enabled, the MR never needs to consult any external servers, so no information is cached in this scenario.
Requirements

- All MR access points in the Network must be running MR27.1+ firmware
- An admin account credential for the LDAP server with read-only permissions has to be input as part of dashboard configuration
- If an Active Directory-based LDAP server is used, it must support an LDAP bind operation
- The LDAP server must support STARTTLS
- CA certificate used to sign the LDAP server's private key must be uploaded to the dashboard. This certificate is used by an MR to verify the authenticity of the LDAP server.

**Note:** An external RADIUS server is not involved in this process and is not needed. The RADIUS server on the MR will handle 802.1X authentication instead.

**Note:** For password-based authentication, and for certificate authentication (if enabled), the MR will perform an ldapsearch using the username provided by the wireless client (supplicant) in the inner EAP tunnel, limiting the search to the base DN provided in the dashboard configuration. The search will look for accounts that have one of the following attributes equal to the username: sAMAccountName, uid, cn, or userPrincipalName. If certificate-based authentication is used, the MR will additionally check that the provided username matches either the CN or userPrincipalName in the certificate, since the username would otherwise be unauthenticated.
The LDAP server’s certificate must have a subjectAltName field that matches the Host address configured on the dashboard (either IP address or FQDN).

Wireless clients must trust the certificate presented by the MR which is signed by a well-known Certification Authority QuoVadis for the purposes of validation of the MR for certificate-based authentication.

* MR27+ firmware is not supported on all MR models. Please refer to the to Product Firmware Version Restrictions.

---

**Supported Authentication Types**

**Password-based**

- EAP-TTLS/PAP
- PEAP-GTC

In both cases, communication between the MR and the wireless clients is protected by TLS. The default method is EAP-TTLS/PAP, as this is the most widely supported authentication method. Windows 10 and iOS require special configuration to use PEAP-GTC.

**Note:** EAP-MSCHAPv2 is not supported with Meraki Local Auth.

**Certificate-based**

- EAP-TLS

**Note:** Currently we cannot check if a user’s account is locked or disabled in the Active Directory. In addition, it’s not possible to “pre-cache” specific clients only. By default, all clients will be cached.

---

**Configuration**

Please complete your LDAP server configuration first. Refer to your vendor documentation for detailed configuration steps.

At a minimum, the following tasks need to be completed and the following information should be gathered on your LDAP server:

- LDAP server IP or FQDN and port number the server is listening to for LDAP queries
- Create an Admin account with read-only permissions
- Note the LDAP search base DN. In the example below Microsoft Active Directory is shown. In this example, “dc=ballena,dc=local” is the LDAP search base DN.
Create users accounts

Export the CA certificate used to sign the LDAP server's private key. PEM and DER formats are supported.

Password Authentication

Navigate to Wireless > Access Control and select the desired SSID from the dropdown on the top of the page.

Under Association Requirements select Enterprise with Local Auth
Under **Authentication Configuration** set **Password Auth** to **Allow password authentication**

Select the **"Caching timeout"** in seconds. By default, the timeout is set to 86400 seconds (24 hours). Please note that 24 hours is the maximum timeout that can be set.

Add LDAP server IP or FQDN and port number the server is listening to for LDAP queries.

Note: The maximum of one LDAP server is currently supported. You can have different LDAP servers for different SSIDs. Secure LDAP (LDAPS) is not currently supported.

Next, provide the admin credentials for your LDAP server. This admin account only requires read access to your LDAP server.

Enter the LDAP search base DN that will be used as a point in the LDAP directory below which the user accounts will be searched for.

Note: The MR access point uses the configured LDAP server to authenticate supplicants (wireless clients), either using the password attribute read from the LDAP server, or by using the provided credentials to do an LDAP bind for the user and checking that it is successful.

When a wireless client successfully authenticates, the MR access stores a hash of the password used to authenticate, so if the connection to the LDAP server is
lost, the MR can still authenticate wireless clients based on their last known good password. This hash is also accessible by other APs in the Network because the client may connect to a different AP than where its last known password is stored.

Please upload the CA certificate used to sign the LDAP server's private key in the LDAP Server CA section so the AP can verify the LDAP server before sending the admin credentials to it. This is also important if we have to bind against the LDAP server to verify user credentials.

**Certificate authentication**

Under Authentication Configuration set Certificate Auth to Allow certificate authentication

Select the Caching timeout in seconds. By default, the timeout is set to 86400 seconds (24 hours). Please note that 24 hours is the maximum timeout that can be set.

Ensure that the wireless devices are set to trust the certificate presented by the MR which is signed by a well-known QuoVadis Certification Authority. Note that
users might get prompted to trust the QuoVadis CA when connecting to the SSID.

If you wish to check if the certificate presented to the MR belongs to a user or device that is authorized to use Wi-Fi, set LDAP to **Verify Certificate CN with LDAP** and set the same settings noted in the previous section.

**Note:** If the **Verify Certificate CN with LDAP** option is set only clients that previously successfully authenticated and verified with the LDAP server to be authorized for wireless access will be able to connect to the SSID. Any clients that have not been successfully authenticated and, therefore, not cached will be denied access to the SSID if the LDAP server is down. Secure LDAP (LDAPS) is not currently supported.

Otherwise, leave the LDAP option set to **Do not verify certificate with LDAP**. Note that in this case, any wireless device that presents a valid certificate will be able to connect to the SSID regardless of the permissions set for that device/user.

If you wish to check if the certificate presented to the MR is revoked, set OCSP to **Verify Certificate with OCSP** and set the OCSP Responder URL the MR can use to check the certificate against.

Please upload the **Client Certificate CA** certificate used to sign the client certificate in a form of PEM or DER file.

### Authentication Configuration

- **Password Auth**: Do not allow password authentication
- **Certificate Auth**: Allow certificate authentication
- **Caching timeout (seconds)**: 3600
- **RADIUS Client Trust Settings**:
  - **Root CA**: QuoVadis Root CA 2
  - **Current network**
  - **Current organization**

### Certificate Verification Options

- **LDAP**: Do not verify certificate with LDAP
- **OCSP**: Verify Certificate with OCSP
- **OCSP Responder**: http://example.com/ocsp
- **Client Certificate CA**: [Upload a file with PEM or DER encoded certificates]