Configuring Active Directory with MX Security Appliances

Active Directory (AD) integration allows you to restrict access to the network and enforce Group Policies based on membership in Active Directory groups.

Currently, Active Directory-based authentication works only if one of the following is true:

- The Domain Controller is in a VLAN configured on the appliance
- The Domain Controller is in a subnet for which a static route is configured on the appliance
- The Domain Controller is accessible through the VPN.

If there are multiple Domain Controllers in the domain, all of them must meet one of these criteria in order for Active Directory integration to function properly.

**Note:** The information listed here should be used as a general operating system configuration guideline. Your specific options and menus may differ depending on the version of Windows Server deployed.

Integrating with Group Policies

A Group Policy in the Dashboard is a set of bandwidth limits, traffic shaping and firewall rules, security filtering, and content filtering settings that can be applied on a per client basis.

**Note:** Cisco Meraki Active Directory-Based Group Policy on the MX should not be confused with Microsoft Active Directory Group Policy as they are in no way related.

Traffic Flow

The MX utilizes Microsoft's Windows Management Instrumentation (WMI) service to pull a continuous stream of Logon Security Events from specified Domain Controllers in the Active Directory domain. These security events have critical information that tells the MX which user accounts are logged into which computers. Specifically, the events contain the IP address of the computer and the Windows username of the logged on user.

The MX will run through the following steps to identify AD group members and apply associated group policies:

1. MX securely contacts the specified Domain Controllers for the AD domain, using TLS
2. MX reads WMI logon events from the DC's security events, to determine which users are logged into which devices.
3. MX binds to DCs using LDAP/TLS to gather each user's AD group membership.
4. Group membership is added to a database on the MX.
5. If a domain user's group membership matches an AD group policy mapping in Dashboard, the MX can apply the associated group policy to the user's computer.

Because the MX is continuously gathering this information from the domain controllers, it is able to accurately apply the policy in real-time whenever a new user logs in.
Benefits of Active Directory Integration

By using Microsoft WMI and standards-based LDAP to interact with the Active Directory network infrastructure, the MX can do real-time Active Directory-based Group Policy assignment without the need to install or maintain any agent software on local Active Directory Domain Controllers.

Configuration Overview

The following steps outline the required configuration (both in Dashboard and Active Directory) to allow for AD-based group policy application. Please be sure to follow each step as accurately as possible, errors can be difficult to diagnose and resolve.

1. Create an Active Directory site for the MX so users authenticate against the correct Domain Controllers.
2. Enable security auditing on Active Directory Domain Controllers so the MX can obtain all relevant logon events.
3. Enable the Global Catalog role on each Domain Controller because the MX uses LDAP/TLS over TCP port 3268.
4. Install a digital certificate on each Domain Controller for LDAP/TLS.
5. Certificate Requirements for TLS
6. Create groups in Active Directory which will be mapped to Group Policies in Dashboard.
7. Add users to groups in Active Directory.
8. Configure Group Policies in Dashboard.
10. Create LDAP group to Group Policy mappings in Dashboard.

Create an Active Directory Site

In Active Directory, Domain Controllers are placed into sites. Sites are assigned IP subnets. Domain users and computers authenticate with Domain Controllers located in the site (IP subnet) for which they reside. Each authentication generates a logon entry within the Domain Controllers Security Event Log. Because the MX uses these Security Events to determine which users are logged onto which computers, all of the Domain Controllers that service logons in an Active Directory site whose IP subnets also correspond to the subnets configured on the MX must be added to Dashboard.

In the example below, the MX has the following IP subnets 10.0.0.0/24 and 192.168.0.0/24 configured under Addressing & VLANs. Active Directory sites need to be applied to both subnets.

Both IP subnets on the MX, are members of the Active Directory site named "Default-First-Site-Name" (shown below). Therefore, the IP addresses of servers DC1, DC1-UK, DC2, SE-Test, and WIN-K7346GNLZ29 located in this site must be added to Dashboard on the Active Directory page in Dashboard.

Note: At this time, the MX does not support mapping group policies via Active Directory for users connecting through the Client VPN.
Enable Security Auditing on Active Directory Domain Controllers

Explanation

When Active Directory Group Policy is enabled, the MX pulls a continuous stream of Security Events from Windows Active Directory Domain Controllers. Using Logon Events (540 and 4624) and Account Logon Events (672 and 4768) specifically, the MX can determine which domain users are logged into which domain computers and what the IP address of those computers are. This information is then coupled with the users Group Membership retrieved from an LDAP/TLS lookup and the IP address or MAC address of the computer learned via Cisco / Meraki client detection. By combining these pieces of information, the appropriate filtering policy can be applied transparently in real-time to each computer based on the currently logged on user. If Domain Controllers specified in Dashboard do not have Security Auditing enabled, the MX will not be able to associate users to computers transparently. To ensure that a Domain Controller is configured to audit successful Logon and Account Logon Events, enable this logging using the Default Domain Controller Policy or Local Computer Policy for Domain Controllers in your domain.

Configuration

3. Confirm that ‘Audit Account Logon Events’ and ‘Audit Logon Events’ is set to ‘Success’ as shown in this image:
Enable the Global Catalog Role on Each Domain Controller

In order for a Domain Controller to maintain the logon events used by the MX for user/group identification, it must be running the Global Catalog Role. As such, a required configuration step is to enable the Global Catalog Role for each Domain Controller that the MX will be polling.

Please refer to official Microsoft documentation for specific configuration steps.

Install a Digital Certificate on Each Domain Controller

In order to communicate with a Domain Controller, the MX security appliance will need to establish Transport-Layer Security (TLS) so all communication between the MX and Active Directory will be encrypted. As a prerequisite to TLS, the MX will need to verify the identity of the Domain Controller. This is done with certificate validation.

An existing certificate can be used on the Domain Controller (so long as it meets the requisite requirements for TLS), or a self-signed certificate can be created on the server.

Certificate Requirements for TLS

The following notes describe certificate parameters used in Windows Server, but can be generalized for any certificate's parameters.

Under the General tab, check for the following attributes:

- The server must have the corresponding private key. To verify that the private key exists, view the General tab of the certificate and verify that you see the following message: "You have a private key that corresponds to this certificate".
- Verify that the following statement appears: "This certificate is intended for the following purpose(s): Proves your identity to a remote computer".
- Check that the certificate is still valid, based on the "Valid from" values.

Note: If these auditing entries are not set to log Success events and the option to edit it is greyed out, then this setting is defined by Domain Group Policy, and you will need to modify this at the Domain level instead. This setting can be found by opening the applicable Group Policy in the server's Group Policy Management Editor and navigating to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy. If further issues are encountered, please refer to Microsoft's documentation for assistance:

- Security Auditing Settings Not Applied by Domain-based Policy
Under the Details tab:

- The **Version** value must contain "v3", indicating that it is an X.509 Version 3 certificate.
- The **Enhanced Key Usage** value must contain the Server Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.1").

- The **Subject** value must contain the Fully Qualified Domain Name of the RADIUS server or Active Directory server, e.g. myserver.mydomain.com.

- The **Public key** value should be set to "RSA (2048 Bits)".

![Certificate Details Image]
• The "Subject Alternative Name" value must contain the syntax "DNS Name=myserver.mydomain.com" where the DNS name is the Fully Qualified Domain Name of your server. This is especially important when using an Active Directory-based PKI.
• The **Key usage** must contain the "Digital Signature" and "Key Encipherment" values.

  *Note: In Server 2012, this option may be available as "Data Encipherment."*
Create Groups in Active Directory

Since the MX will be mapping Active Directory groups to its own group policies, the appropriate groups will have to be created in Active Directory.

Please refer to official Microsoft documentation for specific configuration steps.

Add Users to Groups in Active Directory

When a user logs on to a domain, the logon event will include both user information and group membership. Since this group membership defines which Dashboard group policy will be applied, it is important to ensure that users are added to the appropriate groups in Active Directory.

Please refer to official Microsoft documentation for specific configuration steps.

Configure Group Policies in Dashboard

A group policy in Dashboard will determine the custom network rules and regulations that will apply to users with that policy. This can include custom bandwidth limits, more or less restrictive content filtering rules, custom access to subnets, etc.

Please refer to our documentation for more information about configuring Dashboard group policies.

Configure Active Directory Authentication in Dashboard

The following instructions explain how to add Active Directory servers to Dashboard and enable AD authentication for network clients.

1. Log into Dashboard and navigate to Security & SD-WAN > Configure > Active Directory.
2. From the Active Directory drop-down, select Authenticate users with Active Directory.
3. For Per-VLAN settings choose to Require logon via splash or Default to network-wide settings (Use global settings). Enabling logon via splash will prompt network users with a splash page where they will log in with their domain credentials, but is not a prerequisite to group policy integration. In our example below, we are requiring splash logon for the data VLAN and network defaults for the server VLAN.

   ![Note: The MX AD splash page authorization expires after 2 days or if AD detects a new logon event on the client. The clear authorization button on the client list does not clear the AD splash page authorization on the MX.]

4. For Active Directory Servers, click Add an Active Directory domain server. Remember to add all Domain Controllers that are responsible for the sites/subnets that the MX handles. In our example below, we added all 5 Domain Controllers located in our Active Directory site.
5. To add an Active Directory server, enter the following information:
   a. **Short Domain**: Short name of the domain (a.k.a., NetBIOS name), as opposed to the fully qualified domain name (FQDN). Typically if the FQDN is "mx.meraki.com", the short domain is "mx".
   b. **Server IP**: The IP address of the domain controller.
   c. **Domain admin**: A domain administrator account that the MX can use to query the AD server.
   d. **Password**: The password of the domain administrator account.

   ![Note: Unicode characters in usernames and passwords are not currently supported.]

---

9
Create LDAP Group to Group Policy Mappings in Dashboard

Once Active Directory has been successfully integrated on the MX, the following steps outline how to map Dashboard group policies to groups in AD:

1. In Dashboard, navigate to **Security & SD-WAN > Configure > Active Directory > LDAP policies**.
2. Click the **Refresh LDAP Groups** button to pull LDAP groups from the configured Active Directory servers based on the domain credentials provided in the dashboard.

**Note:** Policy mappings in Dashboard are done based on the FQDN of the group policy object in Active Directory. If the OU of any object in the FQDN path changes, the group policy mapping will need to be re-added in Dashboard.

3. Under **Groups**, select the LDAP group, and under **Policy** select the appropriate group policy for that LDAP group.
4. Click **Save Changes** at the bottom of the page.

If a user is part of more than one group specified in a Group Policy mapping the first group in the list is applied, they will not receive a combination of both policies. For example, in the screenshot below, if a user was part of both staff and executives they would be mapped to staff and only receive the policy configured as the staff policy:
The best practice for deploying Active Directory-based group policy is to add users to a single AD group which is mapped to a single group policy. In the example below, a company has different security levels for its executives and staff. A user Bob is a staff member and Billy is an executive. In this case, the company creates two AD groups, staff and executives. Bob is added to the staff group and Billy the executives group. Therefore Bob receives the policy applied by staff and Billy the policy from executives:

**Integrating Group Policies with MPLS**

An MX appliance must be configured in *Passthrough mode* when Active Directory-based content filtering is desired and the Active Directory domain controllers are located upstream or across an MPLS. Additional information on the traffic flow and the reason for this required configuration is explained below.

**Passthrough Mode Configuration**

To support Active Directory Group Policy mappings when Active Directory servers are located across an MPLS, the MX Security Appliance must be placed in *Passthrough* mode. This can be accomplished by going to **Security & SD-WAN > Configure > Addressing & VLANs** on the Cisco Meraki Dashboard and selecting the option for *Passthrough or VPN Concentrator*. 

---

**Note:** Active Directory group policy does not support group nesting or policy overlapping. If a domain user is a member of an AD group (e.g. staff), and that group is contained within another group that has a Group Policy mapping (e.g. executives), the mapped policy (executives) will not be applied to the user.
Deployment Settings

Mode

- Routed
  In this mode, the MX will act as a layer 3 gateway between the subnets configured below. Unless otherwise configured (see below), client traffic to the internet is translated (NATed) so that its source IP becomes the uplink IP of the security appliance. Configure DHCP on the [DHCP settings page](#).

- Passthrough or VPN Concentrator
  This option can be used for two deployment models: in-line passthrough or one-arm concentrator. In a passthrough deployment, the security appliance acts as a Layer 2 bridge, and does not route or translate client traffic.

In this mode, the MX Security Appliance acts as a layer 2 bridge and does not modify the source address of traffic that traverses the WAN uplink. This configuration allows the MX to query the security logs, obtain an end-user’s account name and associated device IP address, and apply the corresponding group policy.

Routed Mode Configuration

When an MX Security Appliance is configured for Routed mode and Active Directory Domain Controllers are located across an MPLS, authentication requests will traverse the MX WAN uplink. When this uplink traversal occurs, a NAT translation takes place and the source IP will be modified from the user's client device IP address to the WAN IP address of the MX Security Appliance.

In this scenario, the Active Directory security logs will contain the IP address of the MX Security Appliance, rather than the IP address of the end-user's device. This prevents the MX from knowing which device to apply the identity-based content filtering policies. Because of this, a Routed mode configuration will not.
Integrating with Client VPN

The Cisco Meraki MX Security Appliance supports Active Directory authentication with Client VPN, so a client will be required to provide domain credentials in order to connect via VPN.

Traffic Flow

When a user attempts to connect to Client VPN, the following process occurs:

1. The user's device attempts to establish a VPN tunnel using L2TP over IP.
2. The user provides their valid domain credentials.
3. The MX, from its LAN IP, queries the Global Catalog over TCP port 3268 (encrypted using TLS) to the AD server configured in Dashboard.
4. If the user's credentials are valid, the AD server will send its response to the MX, completing authentication.
5. The MX offers the client an IP configuration on the Client VPN subnet, and the client can start communicating on the network.

Note: At this time, the MX does not support mapping group policies via Active Directory for users connecting through the Client VPN.

Configuration Overview

In order to configure Active Directory authentication for Client VPN, configuration steps must be completed on both Dashboard and Active Directory, outlined below:

Active Directory Configuration

The following requirements must be configured on each AD server being used for authentication:

- Every AD server specified in Dashboard must hold the Global Catalog role.
- Since communication between the MX and AD server will be encrypted using TLS, a valid certificate with the appropriate parameters must be configured on the server.
  - If no certificate is present, it will be necessary to install a Self-Signed certificate.
  - If a certificate already exists, please ensure that it has been configured with the necessary parameters for TLS.
- The MX will communicate from its LAN IP with each AD server over TCP port 3268, ensure that no firewalls or ACLs on the network or server will block that communication.

When Active Directory authentication is configured, the MX queries the Global Catalog over TCP port 3268. Therefore the Active Directory server (Domain Controller) specified in Dashboard must also hold the Global Catalog role.

Dashboard Configuration

Once the AD servers have been primed with the configuration requirements outlined above, the following steps outline how to set up AD authentication for Client VPN:

1. In Dashboard, navigate to Security & SD-WAN > Configure > Client VPN
2. If Client VPN has not yet been enabled, please refer to our Client VPN documentation for info on initial configuration.

   Note: In order for Client VPN users to be able to resolve internal DNS entries, the Custom nameservers option should be configured with an internal DNS server. The server's firewall may need to be adjusted to allow queries from the Client VPN subnet, and best practices dictate that a public DNS server should be listed as a secondary option.

3. Set Authentication to Active Directory.

4. Under Active Directory server, provide the short domain name and server IP, as well as the credentials for an AD domain admin.

   Note: If the credentials provided do not have domain admin permissions, the MX will be unable to query the AD server.

5. Click Save Changes.

Client Configuration

Clients can use their native VPN client to connect to Client VPN, with or without Active Directory.

Please refer to our Client VPN documentation for OS-specific configuration steps.

(Optional) Client Scoping

Due to the nature of Active Directory authentication for Client VPN, all domain users will be able to authenticate and connect to Client VPN. There is no Dashboard-native way to limit which users can authenticate, however, there is a workaround in Active Directory that allows the scope of users to be limited by specifying a domain administrator with limited group visibility.

The following article outlines how to configure this workaround for wireless networks, but the same principles can be applied to Client VPN: Scoping Active Directory per SSID

   Note: This configuration is entirely reliant on Active Directory. Depending on how domain groups are managed, this may not work some environments - please refer to Microsoft documentation and support for assistance with Active Directory configuration.

User permissions for AD integration

While the AD integration account does not have to be a domain admin, it is usually the easiest way to implement this feature. If using a domain admin account is not possible or not preferable, ensure that the account has the necessary permissions to perform the following actions:

- Query the user database via LDAP
- Query group membership via LDAP
- Query the domain controller via WMI

Testing

Once the configuration above has been completed, the Meraki device should be able to communicate with the Active Directory server using TLS. If this fails,
Microsoft offers the Ldp.exe tool to ensure that the LDAP service is running and compatible with the current certificate.

Please reference Microsoft documentation for error code details and troubleshooting assistance.

**Additional Resources**

For more information about both Client VPN and Active Directory integration, please refer to the following articles:

- [Troubleshooting Client VPN](#)
- [Resolving NetBIOS Names over Client VPN](#)