Active Directory Issue Resolution Guide

Overview

Active Directory (AD) is a component that is used by administrators to grant access to resources and also enforce group policies to a set of members in the Active Directory domain. Cisco Meraki devices can integrate with an AD server in multiple ways. This article will outline AD integration configuration steps and troubleshooting techniques that you can adapt to resolve an issue related to AD.

Ways to Integrate Active Directory with Meraki

Most issues can be resolved by verifying that the configurations match on the AD server and/or Meraki dashboard. Following the configuration steps again for integrating AD can be the best way to ensure configurations are correct on both sides. Listed below are the ways which AD can be integrated with Meraki devices and a comprehensive configuration guide for the same.

MR - Sign-On splash page with MR access points

MR access points support the use of sign-on splash page for authenticating clients. This splash page can be integrated with an AD server to ensure that only clients with valid user credentials are allowed to access network resources.

- To configure: Integrating Active Directory with Sign-On Splash Page for MR Access Points
- To limit which users can get through authentication: Scoping Active Directory per SSID

MX - Applying group policies using AD groups

Meraki policies for bandwidth limits, traffic shaping and firewall rules, security filtering and content filtering settings can be applied to certain AD groups when the server is integrated with an MX security appliance.

- To configure: Configuring Active Directory with MX Security Appliance

MX - Applying group policies using AD groups over MPLS

Meraki group policies can be applied to certain AD groups. This MPLS method can be helpful when the AD server is located upstream or across an MPLS link and AD based content filtering is required.

- To configure: Integrating MX Group Policies with MPLS

MX - Authenticating client VPN users using AD

You can authenticate users connecting to client VPN on MX security appliances using AD credentials.

- To configure: Integrating with Client VPN

SM - System Manager installation using AD GPO

Administrators can push software out to a large number of devices using Active Directory Group Policy Objects
Troubleshooting Active Directory Integration Issues

Troubleshooting Issues Where AD is Used for Authentication

AD can be used for authentication with sign-on splash pages or client VPN. The logic behind both the authentication methods is the same.

Overview

When using AD authentication, your MR/MX needs to perform a secure LDAP bind using SSL/TLS via the starttls command. The LDAP bind authenticates the user logging into the splash page as illustrated below:

1. A secure connection is established using TLS. After the handshake, a secure channel is established. LDAP calls are encrypted preventing outsiders from snooping the portion of the exchange shown below the handshake.
2. The MX/MR binds to the domain controller using the Active Directory admin credentials specified in the Meraki dashboard.
3. If the bind is successful, the MX/MR searches the directory for the user logging in by their sAMAccountName attribute. If a match is found, the DN of the user is returned to the MX/MR.
4. The MX/MR then attempts to bind with the DN of the user and password entered in the dashboard. If the credentials are OK then the user is authenticated.
AD authentication issues fall under two categories

- Failure to Connect to the AD Server
- Failure to Authenticate

**Failure to Connect to the AD Server**

When a connection failure occurs, the test widget on **Configure > Access control** provides a link to the APs that "failed to connect."
The root causes of connection failures are:

- APs in the dashboard are incorrectly configured to use an Active Directory server that is unreachable over TCP port 3268 or is not a Global Catalog
- The Active Directory server does not have a digital certificate installed for LDAP using TLS

Below are the steps that you can follow to troubleshoot a connection failure issue

1. Check the IP connectivity between the reported APs and the configured AD server. Ping the AD server from the AP in question using Live Tools, then try pinging the AP from the AD server. Successful ping tests verify IP connectivity between endpoints.

2. Run the test widget while taking simultaneous packet captures from the AD server using Wireshark and the wired interface of the AP using the Meraki dashboard. These captures are analyzed in Wireshark and can be used to verify if the AD server is receiving TCP packets from the AP on TCP port 3268 and whether the server is responding appropriately.
3. Analyze the capture taken on the AD server using the following Wireshark filter:

   tcp.port==3268 and ip.addr==X.X.X.X

   Where X.X.X.X is the IP address of the AP. If the AD server replies to TCP SYN packet on port 3268 with a TCP RST, it is likely the AD server is not a Global Catalog. In this instance enable the Global Catalog role on the AD server.

   AD server 10.0.0.116 replies to the AP 10.0.0.117 with a TCP RST because it is not listening on TCP port 3268

4. If the packet capture shows the AD server sending an "Error initializing SSL/TLS" in response to the AP's StartTLS packet, then the AD server does not have a valid digital certificate installed. In this case you will need to install a valid digital certificate on the AD server.

   AP 10.0.0.2 sends a StartTLS packet, but the AD server 10.0.0.117 sends a LDAPError: Error Initializing SSL/TLS.
5. Firewalls can also cause connection failures. If the server is a Global Catalog but a TCP RST or ICMP "Destination Unreachable Communication administratively prohibited" is returned by the AD server, make sure TCP port 3268 is opened inbound on the local firewall. If either of these messages shows up on a capture taken from the AP but not on the AD server, there could be an intermediate firewall blocking access to the AD server. If there are no packets from the AP when analyzing the packet capture taken from the AD server, check the packet capture taken from the AP. If you see packets being sent from the AP to the AD server on TCP 3268 but no response, then there may be an intermediate firewall silently blocking communication.

### Failure to Authenticate

1. If you are receiving a "Bad admin password" error, verify that the AD admin account exists and the password is correct.
2. If you are receiving a "Bad user password" error, verify that the user account exists and the password is correct. Also verify that the AD admin has read access to the OU containing user objects.
3. Monitor Windows event view logs to further troubleshoot authentication errors.

### Troubleshooting Issues where AD is Integrated with MX Security Appliances for Applying Policies

Before applying a group policy to a particular client using AD integration, you need to check whether the AD server has a successful connection with the MX security appliance. You can check the status of the AD integration connection on the Security & SD-WAN > Configure > Active Directory page. If AD has connected with the MX without any issue then you should be able to see a green check mark on the status. If the server has failed to integrate with the MX, the following are the most common errors.

- ldap_bind: Invalid credentials
- Could not reach Domain Controller
- ldap_bind: Can't Contact LDAP Server
- ldap_start_tls: Server is Unavailable
- WMI Error
- LDAP Connection error

### ldap_bind: Invalid credentials

**Error Description:** Short domain, Domain admin or Password values are incorrectly configured for the AD server in the Meraki dashboard

**Error Solution:** The following steps describe how to find the correct info to enter in the dashboard under Security & SD-WAN > Configure > Active Directory > Active Directory servers:

**Short domain:** Use the pre-Windows 2000 (NetBIOS) domain name format. Mistakenly using FQDN (fully qualified domain name) is the most common reason for this issue. Find the pre-Windows 2000 domain name by doing either of the following on the domain controller:

- Run the set command from command prompt and locate the USERDOMAIN value:
• In the Active Directory Users and Computers console, locate the pre-Windows 2000 domain name value on the Account Properties tab of the domain administrator or any user in the domain. **Note:** Do not include the backslash when entering the short domain in Dashboard.

• Domain admin: Use the User logon name of the Domain administrator without a NetBIOS domain name prefix or UPN suffix. This can be found on the Account Properties tab of the domain administrator in the Active Directory Users and Computers console of the domain controller.

• Password: The password for the Domain admin account is incorrect or the user is locked out in Active Directory. To determine if the account is locked, check the Account Properties tab of the domain administrator in the Active Directory Users and Computers console of the domain controller.

---

**Could not Reach the Domain Controller**

**Error Description:** You are likely to see this error when the MX is unable to establish a connection with the AD server.

**Error Solution:** Follow the instructions in the Failure to Connect to the AD Server section of this document.
Idap_bind: Can't Contact LDAP Server

Error Description: This error indicates the MX can connect to the WMI service on the domain controller but cannot connect to the LDAP service. Note that this is different from the Could not reach domain controller error (described above) which indicates that both the WMI and LDAP services are unreachable.

Error Solution: To resolve LDAP connection failures, please verify that the domain controller is a Global Catalog listening on TCP port 3268.

Idap_start_tls: Server is Unavailable

Error Description: The MX uses TLS to secure the LDAP connection to the domain controller. This error indicates the MX received an Error initializing TLS response from the domain controller when attempting to establish TLS.

Error Solution: To resolve issues with TLS, please verify the following:

- The domain controller has a valid certificate installed.
- The domain controller supports STARTTLS. The MX does not support LDAP over SSL and uses STARTTLS instead.

WMI Error

Error Description: This error means the WMI service on the domain controller is returning an NT error code when the MX tries to pull security logs. These events are necessary for the MX to learn which user accounts are logged into which computers.

Error Solution: There are two reasons for this error. The applicable error can be identified based on how the dashboard reports it.

If the WMI error is constant then it is an invalid credentials issue. To resolve this error, you need to make sure that the domain admin account is a member of the Domain Admins group in Active Directory.

If the WMI error goes ON and OFF then the issue is related to Quota violation. In order to apply Group Policies to clients in real-time, the MX connects to the WMI service every 5 seconds to pull the most recent logon events. The WMI Provider Service may require increased memory and handle quotas and a smaller Security Event log size to handle the requests.

Follow the steps below to increase WMI Provider Service memory and handle quotas and decrease the size of the Security Event logs:

- Increase the WMI MemoryPerHost value (see Increase WMI Quota properties to maximum values)

Follow the steps below to reduce the Security Log size limit to 1MB:

1. Open the Event Viewer
2. Navigate to Event Viewer > Windows Logs > Security
3. Right click Security and click Properties
4. Set the Maximum log size (KB) to 1024
5. When maximum event log size is reached select Overwrite events as needed (oldest events first) or Archive the log when full, do not overwrite events.
6. Click OK

LDAP Connection Error

Error Description: This error commonly occurs when the domain controller does not support TLS v1.0

Error Solution: Verify the domain controller supports TLS v1.0

After you have successfully linked the AD server with the MX security appliance, if you are still having the issue with the group policy, try the following.

• Try to apply the group policy manually to the test client. Check whether the group policy is working when applied manually. If not then follow the Troubleshooting Group Policy guide to resolve the issue.
• Make sure that the user in question is a member of only one group that has a group policy assigned in the dashboard.

Note: It is recommended to have the MX configured for tracking clients by MAC address in order for the Group policy integration to work as expected. You can check the configuration by navigating to the Security & SD-WAN > Configure > Addressing & VLANs page.