Configure Duo Multi Factor Authentication to Work with UCS Manager

Contents

Introduction

This document describes the configuration and best practices to implement Cisco Duo Multi-Factor Authentication (MFA) with UCS Manager.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- UCS Manager
- Cisco Duo

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco UCS Manager uses two-factor authentication for remote user logins. Two-factor authentication login requires a username, a token, and a password combination in the password field.

Two-factor authentication is supported when you use Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System +(TACACS+) provider groups with designated authentication domains with two-factor authentication for those domains. Two-factor authentication does not support Internetwork Performance Monitor (IPM) and is not supported when the authentication realm is set to Lightweight Directory Access Protocol (LDAP), local, or none.

With the Duo implementation, the Multi-Factor Authentication is performed via The Duo Authentication Proxy which is an on-premises software service that receives authentication requests from your local devices and applications via RADIUS or LDAP, optionally performs primary authentication against your LDAP directory or RADIUS authentication server, and then contacts Duo to perform secondary authentication. Once the user approves the two-factor request, which is received as a push notification from Duo Mobile, or as a phone call, etc, the Duo proxy returns access approval to the device or application who requested authentication.

Configure

This configuration covers the requirements for a successful Duo implementation with UCS Manager through LDAP and Radius.

> **Note**: For basic Duo Authentication Proxy configuration please check the Duo Proxy guidelines: Duo Proxy Document

LDAP Integration

UCS Manager

Navigate to **UCS Manager > Admin Section > User Management > LDAP** and enable **LDAP Providers SSL**, this means encryption is required for communications with the LDAP database. LDAP uses STARTTLS. This allows encrypted communication by the use port 389. Cisco UCS negotiates a Transport Layer Security (TLS) session on port 636 for SSL, but the initial connection starts unencrypted on port 389.

```
Bind DN: Full DN path, it must be the same DN that is entered in the Duo Authentication Proxy
for exempt_ou_1= below
Base DN: Specify DN path
Port: 389 or whatever your preference is for STARTTLS traffic.
Timeout: 60 seconds
Vendor: MS AD
```

> **Note**: STARTTLS operates on a standard LDAP port, so unlike LDAPS, STARTTLS integrations use the **port=** field not **ssl_port=** field on the Duo Authentication Proxy.

On the Duo Authentication Proxy

```
[ldap_server_auto]
ikey=
skey_protected= ==
api_host=api.XXXXXX.duosecurity.com
client=ad_client1
failmode=secure
port=389 or the port of your LDAP or STARTTLS traffic.
ssl_port=636 or the port of your LDAPS traffic.
allow_unlimited_binds=true
exempt_primary_bind=false
ssl_key_path=YOURPRIVATE.key
ssl_cert_path=YOURCERT.pem
exempt_primary_bind=false
exempt_ou_1=full DN path
```

Radius Integration

UCS Manager

Navigate to **UCS Manager > Admin > User Management > Radius** and click on **Radius Providers:**

```
Key and Authorization Port: Must match the Radius/ Authentication Proxy configuration.
Timeout: 60 seconds
Retries: 3
```

Duo Authentication Proxy

```
[radius_server_auto]
ikey=DIXXXXXXXXXXXXXXXXX
skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
api_host=api-XXXXXXXX.duosecurity.com
radius_ip_1=5.6.7.8
radius_secret_1=radiussecret1
client=ad_client
port=18121
failmode=safe
```

Best Practices to Install and Configure Duo Authentication Proxy

Deploy the Authentication Proxy in a firewalled internal network that:

- Allows outbound communication from the Authentication Proxy to the general Internet on TCP/443. If further restrictions are required, please see Duo's List of IP ranges to Allowed List.
- The Duo Authentication Proxy can also be configured to reach Duo's service through a previously configured web proxy that supports the CONNECT protocol.
- Can connect to the appropriate IDPs, typically over TCP/636, TCP/389, or UDP/1812
- Allows communication to the proxy on the appropriate RADIUS, LDAP, or LDAPS ports.

These rules allow appliances/applications to authenticate users against the proxies.

- If any SSL inspection appliances exist in the environment, disable/Allow List SSL inspection for Auth Proxy IPs.
- Configure each **[radius_server_METHOD(X)]** and **[ldap_server_auto(X)]** sections to listen on a unique port.
  Read more on how to use the Duo Authentication Proxy to power multiple applications on the Duo site Duo Proxy for Multiple Applications.
- Use unique RADIUS secrets and passwords for every appliance.
- Use protected/encrypted passwords in the proxy configuration file.
- While the Authentication Proxy can co-exist on multi-purpose servers with other services, it is recommended to use a dedicated server(s).
- Ensure the Authentication Proxy points to a reliable NTP server to ensure accurate date and time.
- Before the upgrade of the Authentication Proxy, always make a backup copy of the configuration file.
- For Windows-based Authentication Proxy servers, configure the Duo Security Authentication Proxy Service to include some recovery options in case of power or network failures:

  Step 1. Within **Services** on your server, right-click the **Duo Security Authentication Proxy** service, and then click **Preferences.**
  Step 2. Click **Recovery**, then configure options to restart the service after failures.
- For Linux-based Authentication Proxy servers, click **yes** to the prompt visible on the installation that asks if you want an init script created. Then, when you start the Authentication Proxy, use a command such as **sudo service duoauthproxy start**, that the command for the init script may differ based on what system you are on.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshoot information available for this configuration.

Related Information

- **Technical Support & Documentation - Cisco Systems**