Configure LUA Script for DAP Certificate Parameters Evaluation

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configuration

Verify

Introduction

This document describes how to configure an LUA script to detect certificate parameters that users must have when they try to connect to the VPN.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firewall Management Center (FMC)
- Remote Access VPN configuration (RAVPN)
- Basic LUA script coding
- Basic SSL certificates
- Dynamic Access Policy (DAP)

Components Used

The information in this document is based on these software versions:

- Secure Firewall version 7.7.0
- Secure Firewall Management Center version 7.7.0

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

DAP is a powerful feature that allows network administrators to define granular access control policies based on various attributes of users and devices attempting to connect to the network. One of the key capabilities of DAP is the ability to create policies that evaluate digital certificates installed on client

devices. These certificates serve as a secure method to authenticate users and verify device compliance.

Within the Cisco Secure FMC interface, administrators can configure DAP policies to assess specific certificate parameters such as:

- Subject
- Issuer
- Subject Alternate Name
- Serial Number
- Certificate Store

However, the certificate evaluation options available through the FMC GUI are limited to these predefined attributes. This limitation means that if an administrator wants to enforce policies based on more detailed or custom certificate information, such as specific fields within the certificate or custom extensions, this cannot be achieved using the standard DAP configuration alone.

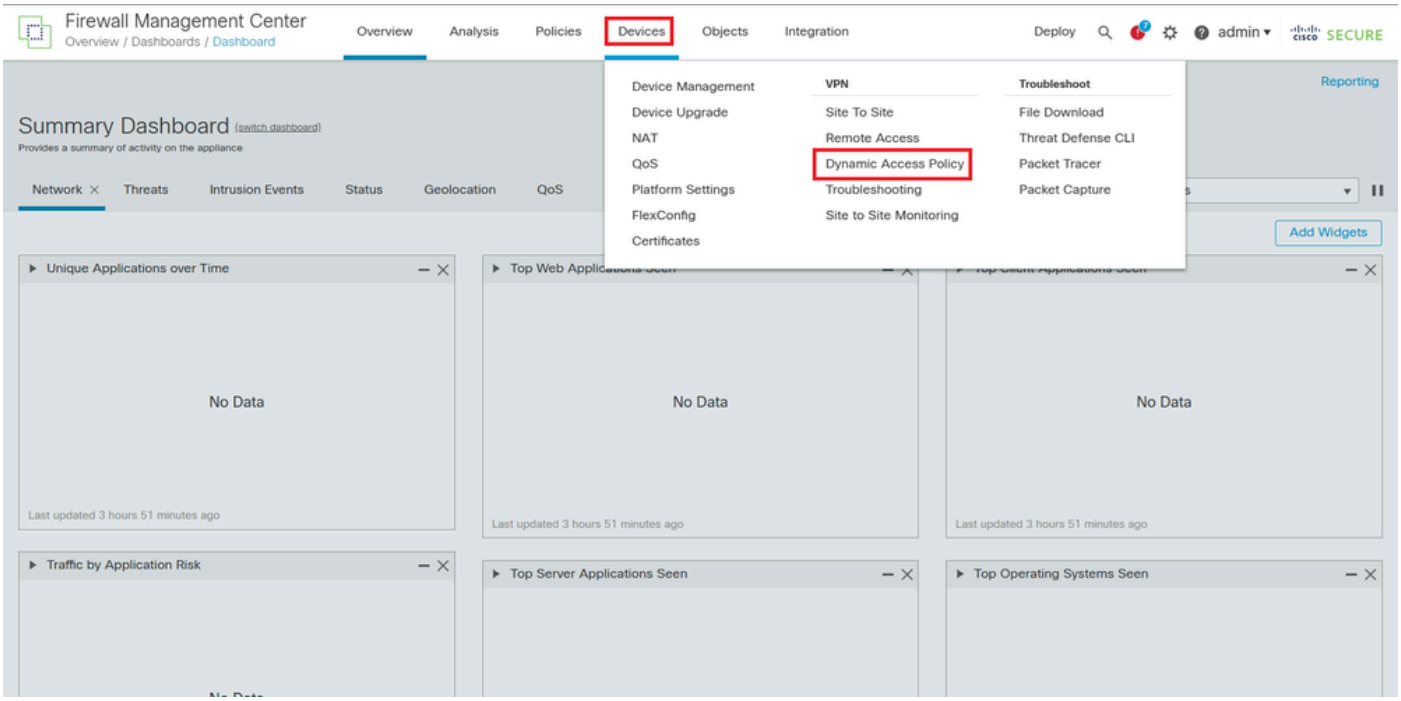
To overcome this limitation, Cisco Secure Firewall supports the integration of LUA scripting within DAP. LUA scripts provide the flexibility to access and evaluate additional certificate attributes that are not exposed through the FMC interface. This capability enables administrators to implement more sophisticated and customized access policies based on detailed certificate data.

By leveraging LUA scripting, it becomes possible to analyze certificate fields beyond the default parameters, such as organization names, custom extensions, or other certificate metadata. This extended evaluation capability enhances security by allowing policies to be tailored precisely to the requirements of the organization, ensuring that only clients with certificates meeting specific, detailed criteria are granted access.

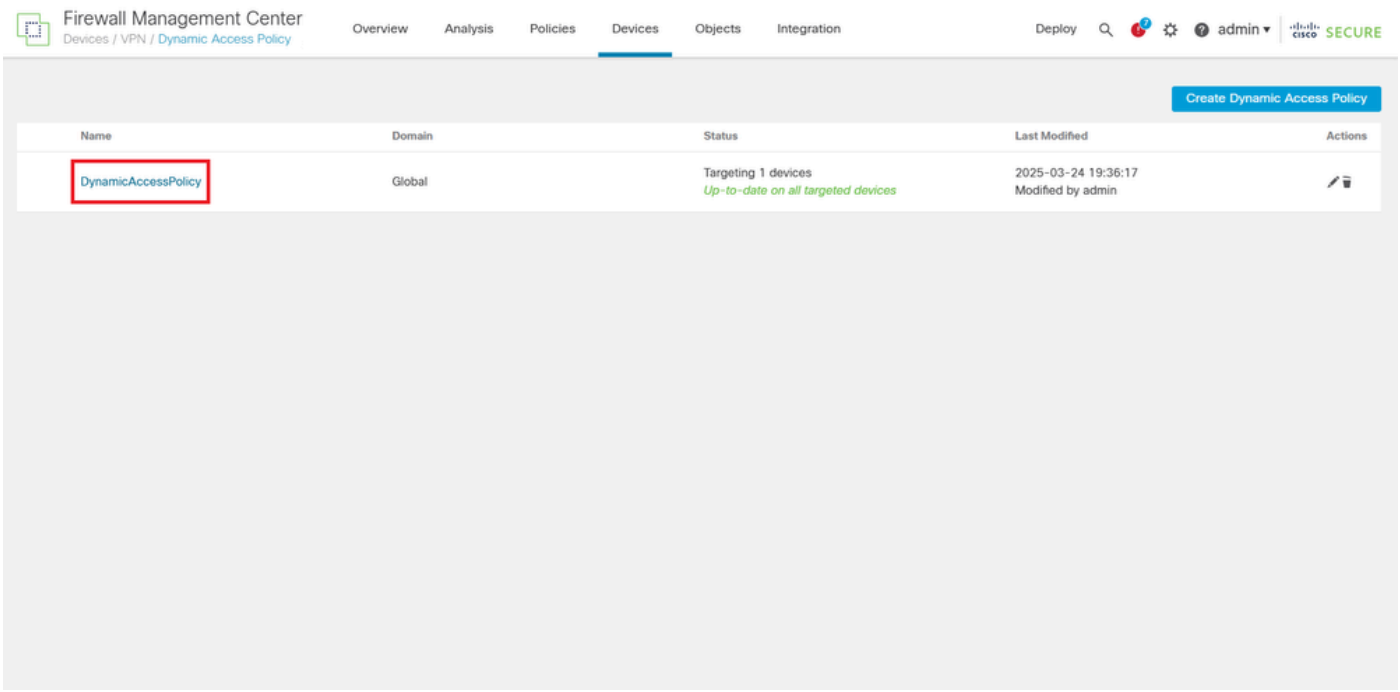
Therefore, in this document, a LUA script is configured to evaluate the Organization parameter within a client certificate by leveraging LUA scripting capabilities.

Configuration

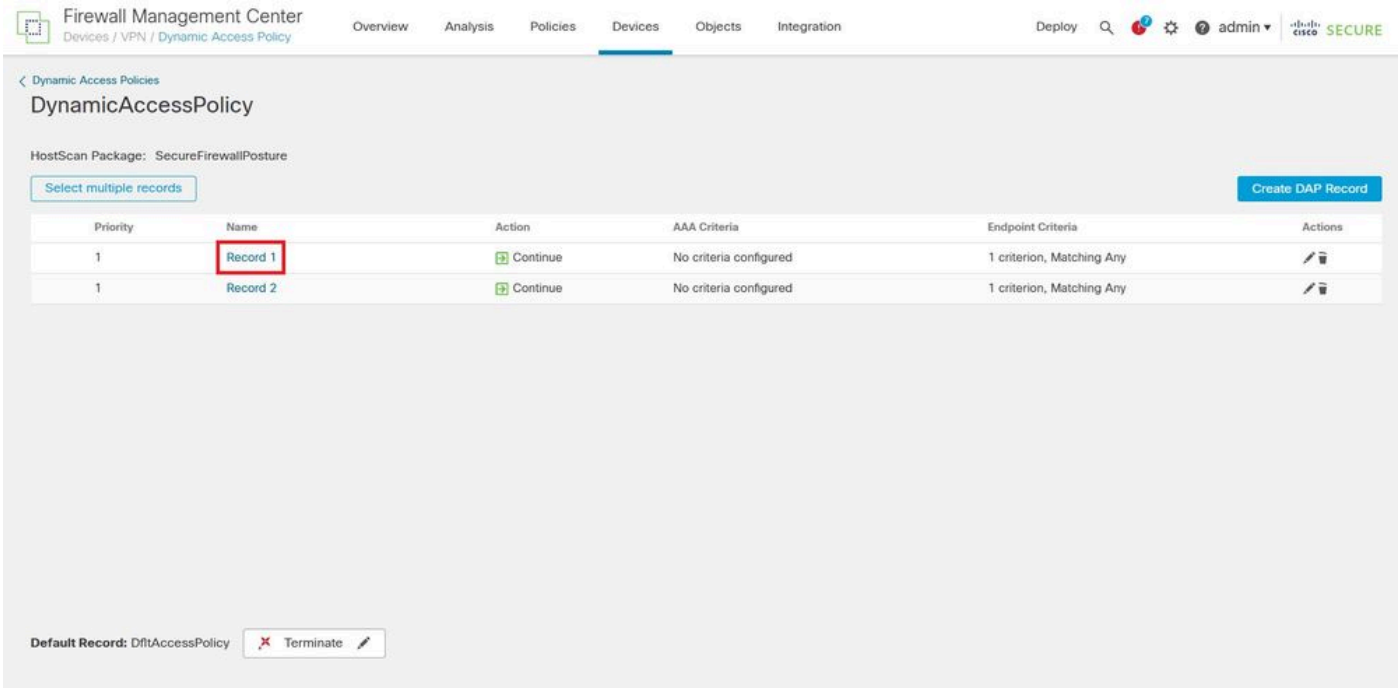
1.Log in to the FMC GUI, then, from the dashboard, navigate to **Devices >Dynamic Access Policy** in the menu.



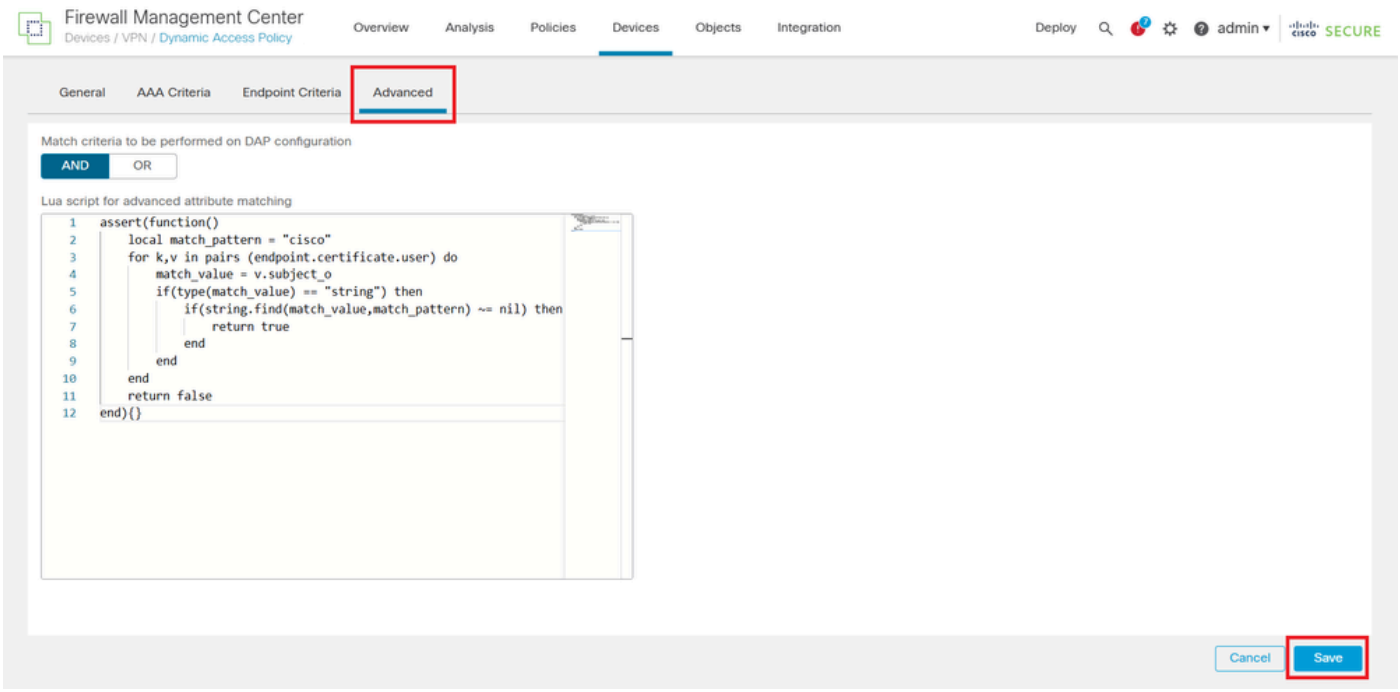
2.Open the **DAP policy** applied to the RAVPN configuration.



3. Edit the desired **record** to configure the LUA script by clicking the **record name**.



4. Within the selected record, navigate to the **Advanced** tab to enter the **LUA script** that evaluates the required certificate parameters. After configuring the script, click **Save** to apply the changes. Once the changes are saved in the **DAP Record**, deploy the **policy** to push the updated configuration to the FTD device.



Note: The code presented in this article is designed to evaluate the certificates installed on the client device, specifically verifying that there is a certificate whose Organization parameter within the Subject field matches the value cisco.

<#root>

```
assert(function()
    local match_pattern = "
```

```
cisco

"
    for k,v in pairs (

endpoint.certificate.user

) do
        match_value =

v.subject_o

        if(type(match_value) == "string") then
            if(string.find(match_value,match_pattern) ~= nil) then


return true

            end
        end
    end
    return false
end){}
```

- The script defines a match_pattern variable set to **cisco**, which is the target organization name to find.
- It iterates over all user certificates available on the endpoint using a for loop.
- For each certificate, it extracts the Organization field (subject_o).
- It checks if the Organization field is a string and then searches for the match_pattern within it.
- If a match is found, the script returns true, indicating the certificate meets the policy criteria.
- If no matching certificate is found after checking all certificates, the script returns false, causing the policy to deny access.

This approach allows administrators to implement customized certificate validation logic beyond the standard parameters exposed by the FMC GUI.

Verify

Run the command **more dap.xml** to verify that the code is present in the DAP configuration on the FTD.

```
<#root>

firepower#

more dap.xml


<?xml version="1.0" encoding="UTF-8"?>
<dapRecordList>
  <dapRecord>
    <dapName>
      <value>Record 1</value>
    </dapName>
    <dapViewsRelation>
      <value>and</value>
    </dapViewsRelation>
    <advancedView>
      <value>

assert(function()
```

```
        local match_pattern = "cisco"
        for k,v in pairs (endpoint.certificate.user) do
                match_value = v.subject_o
                if(type(match_value) == "string") then
                        if(string.find(match_value,match_pattern) ~= nil) then
                                return true
                        end
                end
        end
        return false
end) {}
```

```
</value>
    </advancedView>
  </dapRecord>
</dapRecordList>
```