Verify Domain in Security Cloud Control - CUI Update

Contents

Introduction

This document describes how the new domain verification in Security Clould Control (SCC) after the Cisco Unified Identity (CUI) update.

Background

When claiming and verifying a domain in Cisco Security Cloud Control (SCC), administrators are required to publish a DNS TXT record to prove ownership of the domain.

Problem

There is a change in the DNS record placement required for successful verification. The previous instructions referenced in the Cisco documentation use a dedicated verification subdomain:

_cisco-sxso-verification.example.com

However, the current verification process requires publishing the Cisco-provided TXT verification token directly under the root domain, rather than the dedicated verification subdomain.

What has changed?

Previous configuration (no longer applicable to the current verification workflow):

DNS Field	Value
Record Type	TXT
Host / Name	_cisco-sxso-verification.example.com
Value	Cisco verification token

New configuration (required):

DNS Field	Value
Record Type	TXT
Host / Name	@
Value	Cisco verification token

Solution

Implementation steps

1. Log in to your domain DNS provider (GoDaddy, Cloudflare, Route 53, Azure DNS, and so on.).
2. Navigate to DNS management for the domain.
3. Create a new TXT record.
4. Configure the record as follows:
   Type: TXT
   Host / Name: @
   Value: Paste the verification token generated by Cisco SCC.
   TTL: Default value.
5. Save the DNS record and allow time for DNS propagation.
6. Return to Cisco SCC and click Verify.

Verification

You can confirm that the TXT record is published correctly using this command:

```
dig TXT example.com
```

The response must include the Cisco verification token.

Once the record is visible in DNS, return to SCC and retry the domain verification.