# Secure Client Machine Tunnel Authentication Popup Causes Disconnections on Untrusted Networks

## Contents

## Issue

Cisco Secure Client (AnyConnect) repeatedly prompts for username and password while a machine tunnel is connected, particularly when users connect from untrusted networks. The authentication popup interrupts the machine tunnel connectivity and causes disconnections, affecting the ability of users to maintain stable remote access. This issue occurs despite the machine tunnel being properly established and authenticated, with the popup appearing unexpectedly and disrupting the VPN session continuity.

## Environment

- Cisco Secure Client (AnyConnect) with machine tunnel configuration
- Remote Access VPN profile with Trust Network Detection (TND) feature enabled
- User machine connected to Machine Tunnel
- Group Policy Objects (GPO) used for client profile distribution
- Both user tunnel and machine tunnel profiles configured with TND settings

## Resolution

The issue was resolved by modifying the Trust Network Detection (TND) configuration settings for both machine tunnel and user tunnel profiles. The solution involves configuring the TND action behavior to prevent unnecessary authentication prompts on untrusted networks.

### Step 1: Configure TND Settings for Untrusted Networks

Set the Trust Network Detection action to **Do nothing** for untrusted networks on both machine tunnel and user tunnel profiles. This configuration prevents the client from prompting for additional credentials when connected to untrusted networks.

### Step 2: Configure TND Settings for Trusted Networks

Set the Trust Network Detection action to **Disconnect** for trusted networks, maintaining the intended security behavior for known secure network environments.

### Step 3: Deploy Configuration Changes

Deploy the updated TND settings through Group Policy Object (GPO) push to distribute the configuration changes to all affected client machines.

### Step 4: Restart Client Machines

Reboot the client machines after the profile update to ensure the new TND settings take effect properly.

### Step 5: Validation Testing

Test the machine tunnel connectivity across multiple untrusted networks to verify that:

- The authentication popup no longer appears
- The machine tunnel remains connected consistently
- No credential prompts interrupt the VPN session
- Users can maintain stable remote access without disconnections

The user confirmed successful resolution after implementing these changes, with multiple user tests validating stable VPN session continuity across various network conditions.

## Cause

The root cause was misconfigured Trust Network Detection (TND) settings on the Cisco Secure Client profiles. The TND feature was triggering authentication prompts when users connected from untrusted networks, even though the machine tunnel was already properly authenticated and established. The TND actions for both user tunnel and machine tunnel profiles were not optimally configured for the network environment, causing the client to request additional credentials unnecessarily and disrupting the machine tunnel connectivity.

## Related Content