# Error de sincronización de configuración de ZTNA de Secure Access con descifrado SSL y túneles de red

## Contenido

## Problema

Cisco Secure Client Zero Trust Access (ZTA) se inscribe correctamente, pero falla durante la sincronización de la configuración con las respuestas HTTP 502 y el estado de conectividad del servidor "BadResponse". Los registros DART del extremo de Windows 11 muestran una inscripción correcta pero errores repetidos de sincronización de la configuración. El problema solo se produce cuando el terminal está conectado a la ruta de red corporativa mediante Secure Access/Umbrella proxy con túneles Meraki AutoVPN, mientras que el mismo terminal completa correctamente la sincronización de la configuración en una red doméstica sin proxy ni infraestructura de túnel.

## Entorno

- Cisco Secure Client ZTA versión 5.1.16.4434
- terminal Windows 11 Enterprise
- Dispositivos Meraki MX con integración AutoVPN
- Secure Access (SSE) con Network Tunnels Gateway (NTG)
- Umbrella DNS y Secure Access Web Security
- Descifrado SSL e inspección de HTTPS habilitados en la ruta de red corporativa
- La lista de no descifrado (DND) proporcionada por el sistema no está configurada inicialmente

# Resolución

El error de sincronización de la configuración se resolvió implementando las derivaciones de descifrado SSL adecuadas para los dominios relacionados con ZTA cuando se utilizan túneles de red con acceso seguro.

## Paso 1: Identificar el impacto del descifrado SSL

Verifique que el descifrado SSL esté causando errores de sincronización de la configuración mediante la revisión de los registros de Búsqueda de actividad en Secure Access para los eventos de descifrado relacionados con los dominios ZTA.

## Paso 2: Configuración de la lista DND proporcionada por el sistema

Cuando se utiliza Network Tunnels Gateway (NTG) con Secure Access, debe activarse la función NoMIsta proporcionada por el sistema para omitir correctamente el tráfico relacionado con ZTA de la inspección SSL.

Navegue hasta Panel de acceso seguro > Seguro > No descifrar listas y modifique la lista No descifrar proporcionada por el sistema.

## Paso 3: Crear perfil de seguridad para dominios ZTA

Agregue los dominios relacionados con ZTA requeridos a un nuevo perfil de seguridad mediante la lista DND proporcionada por el sistema:

- zpc.sse.cisco.com
- *.zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com

- devices.api.umbrella.com

### Paso 4: Aplicar perfil de seguridad a regla de prueba

Asigne el perfil de seguridad recién creado que contiene los desvíos de dominio ZTA a una regla de prueba para validar la configuración.

### Paso 5: Validar sincronización de configuración

Pruebe la inscripción ZTA y la sincronización de la configuración desde la red corporativa. La sincronización puede completarse correctamente sin errores de HTTP 502.

### Paso 6: Coordinación con el equipo de Meraki

Para obtener una cobertura completa, coordine con el soporte de Meraki la validación de las URL y dominios oficiales relacionados con ZTA que se pueden omitir en la inspección de acceso seguro. Consulte la siguiente documentación de Meraki:

- Reglas de firewall ascendentes para la conectividad a la nube
- Actualización de URL del panel de Meraki - Cumplimiento de PCI

## Causa

La falla de sincronización de la configuración fue causada por el descifrado SSL y el proxy del tráfico de acceso de confianza cero en la red corporativa. Cuando se utiliza Network Tunnels Gateway (NTG) con Secure Access, se deben omitir los dominios relacionados con ZTA mediante la lista No descifrar (DND) proporcionada por el sistema. Sin esta configuración de omisión, la inspección SSL modifica las cadenas de certificados e interfiere con la comunicación del plano de control ZTA, lo que hace que el cliente reciba respuestas HTTP 502 durante los intentos de sincronización de la configuración.

# Contenido relacionado

- Solución de problemas de SSL y descifrado de acceso seguro
- Acceso seguro Zero Trust Client-Based Enrollment Services
- Requisitos del dominio ZTA para el acceso seguro
- Solucionar problemas de inscripción de errores de acceso seguro
- Troubleshooting de Error de Sincronización de Configuración de Secure Client
- Recopilar registros detallados de ZTNA para la resolución de problemas
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).