

# Troubleshooting de Fallas de Actualización de Definiciones TETRA

## Contenido

[Introducción](#)

[Resolución de problemas](#)

[Verificación de la Conectividad Informada de Extremo en la Consola de Extremo Seguro](#)

[Comprobación de la conectividad en el terminal](#)

[Comprobación de las definiciones de TETRA en el terminal](#)

[Cómo forzar una actualización de definiciones de TETRA en el Terminal](#)

[Verificación de la Conectividad del Servidor de Definición TETRA en el Terminal](#)

[Validación de conexión directa](#)

[Validación de proxy](#)

[Additional Information](#)

## Introducción

Este documento describe los pasos que deben seguirse para investigar la razón por la cual los terminales no pueden actualizar las definiciones de TETRA de los servidores de actualización de definiciones de Cisco TETRA.

Definiciones Último error actualizado observado en Secure Endpoint Console aparece en los detalles del equipo como se muestra a continuación.

DESKTOP-QFC3PVT in group Protect			
Hostname	DESKTOP-QFC3PVT	Group	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1702)	Policy	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138
Install Date	2023-05-17 01:58:07 UTC	External IP	173.38.117.65
Connector GUID	5c6e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-17 19:40:25 UTC
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (daily version: 90600)
Definitions Last Updated	2023-05-17 19:16:49 UTC <b>Failed</b> The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

◀ Events ▶ Device Trajectory ↻ Diagnostics 🔍 View Changes

🔍 Scan... 🩺 Diagnose... 📁 Move to Group...

â€f

## Resolución de problemas

El Cisco Secure Endpoint para Windows requiere una conexión sostenida con el servidor de definición de TETRA para descargar las actualizaciones.

Los errores comunes al descargar las definiciones de TETRA incluyen:

- Error al resolver la dirección del servidor
- Error al validar el certificado SSL (incluida la comprobación de la lista de revocación de certificados)
- Interrupción durante la descarga
- Error al conectarse al servidor proxy
- Error al autenticarse en el servidor proxy

Si se produce un error al intentar descargar las definiciones de TETRA, el siguiente intento se producirá en el siguiente intervalo de actualización o si el usuario ha iniciado una actualización manual.

## Verificación de la Conectividad Informada de Extremo en la Consola de Extremo Seguro

Secure Endpoint Console muestra si el terminal se está conectando con regularidad. Asegúrese de que los terminales están activos y de que su estado es "Último visto" (Last Seen). Si los terminales no se están protegiendo con Secure Endpoint Console, esto indica que el terminal no está activo o tiene algunos problemas de conectividad.

Cisco publica una media de 4 actualizaciones de definiciones al día y, si en algún momento del día el terminal no puede descargar la actualización, el conector publica un error de fallo. Teniendo en cuenta esta frecuencia, solo si los terminales están conectados constantemente y tienen una conexión de red estable con el servidor TETRA en todo momento, los terminales se informarán como "Dentro de la política".

El estado "Visto por última vez" se encuentra en la página de detalles del ordenador, como se indica en un círculo a continuación:

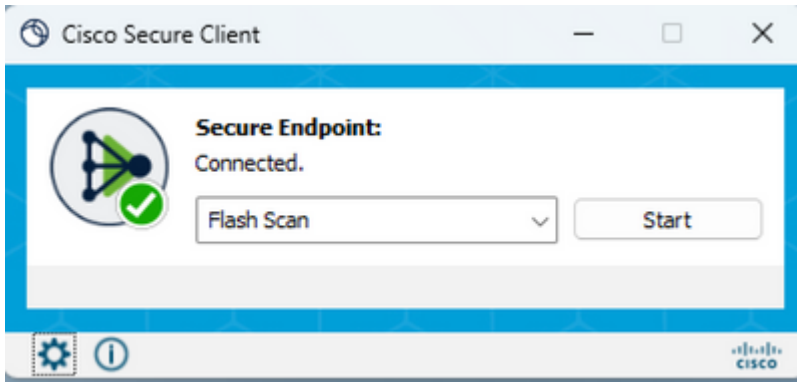
DESKTOP-QFC3PVT in group Protect		Definition Update Failed 0	
Hostname	DESKTOP-QFC3PVT	Group	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1702)	Policy	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138, 172.23.0.1, 172.30.144.1
Install Date	2023-05-17 01:58:07 UTC	External IP	173.38.117.65
Connector GUID	5c6e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-18 21:37:02 UTC
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (daily version: 90604)
Definitions Last Updated	2023-05-18 16:54:33 UTC <b>Failed</b> The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

Si el terminal se está conectando y se informa de un error que indica que las definiciones no se descargan pero que la consola está viendo, el problema puede ser intermitente. Se puede realizar una investigación adicional si las diferencias de tiempo son grandes entre "Última vez visto" y "Definiciones actualizadas por última vez".

## Comprobación de la conectividad en el terminal

Los usuarios finales pueden comprobar la conectividad mediante la interfaz de usuario.

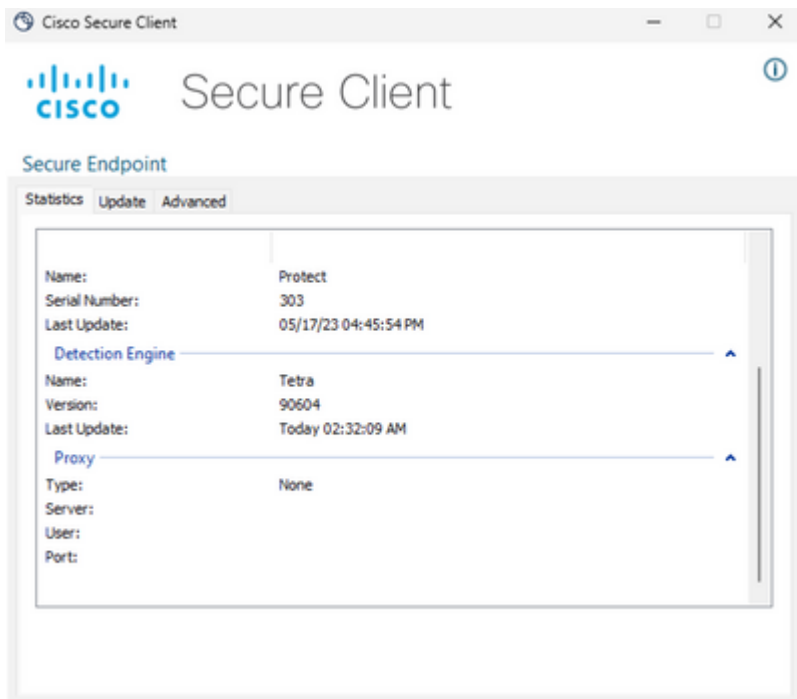
Al abrir Cisco Secure Client, se muestra el estado de la conectividad.



ConnectivityTool se puede utilizar cuando el extremo no está conectado y notifica problemas de conexión. Esto se incluye en la herramienta IPSupportTool que genera el paquete de soporte.

## Comprobación de las definiciones de TETRA en el terminal

Cisco Secure Client proporciona información sobre las definiciones TETRA actuales cargadas por el conector de terminal. El usuario final puede abrir el cliente y comprobar la configuración de Secure Endpoint. En la pestaña Statistics (Estadísticas), está disponible la definición actual de TETRA.






â€f

Además, la herramienta AmpCLI informa de los detalles de la definición de TETRA actual en el terminal. Un ejemplo del comando es el siguiente:

```
PS C:\Program Files\Cisco\AMP\8.1.7.21417> .\AmpCLI.exe posture
{"agent_uuid": "5c6e64fa-7738-4b39-b201-15451e33bfe6", "connected": true, "connector_version": "8.1.7", "engin
```

Las versiones de definición se muestran para cada uno de los motores, incluido TETRA. En este resultado anterior, es la versión 90604. Esto se puede comparar con Secure Endpoint Console en: **Management > AV Definition Summary**. A continuación se muestra un ejemplo de la página.

## AV Definition Summary

 Version 90606 2023-05-18 20:13:58 UTC	 Version 120765 2023-05-18 20:13:57 UTC	 Version 120765 2023-05-18 20:13:57 UTC	
TETRA 64bit	TETRA 32bit	ClamAV Mac	ClamAV Linux-Or
Version	Available		
90606	<a href="#">2023-05-18 20:13:58 UTC</a>		
90605	<a href="#">2023-05-18 16:15:48 UTC</a>		
90604	<a href="#">2023-05-18 12:13:36 UTC</a>		

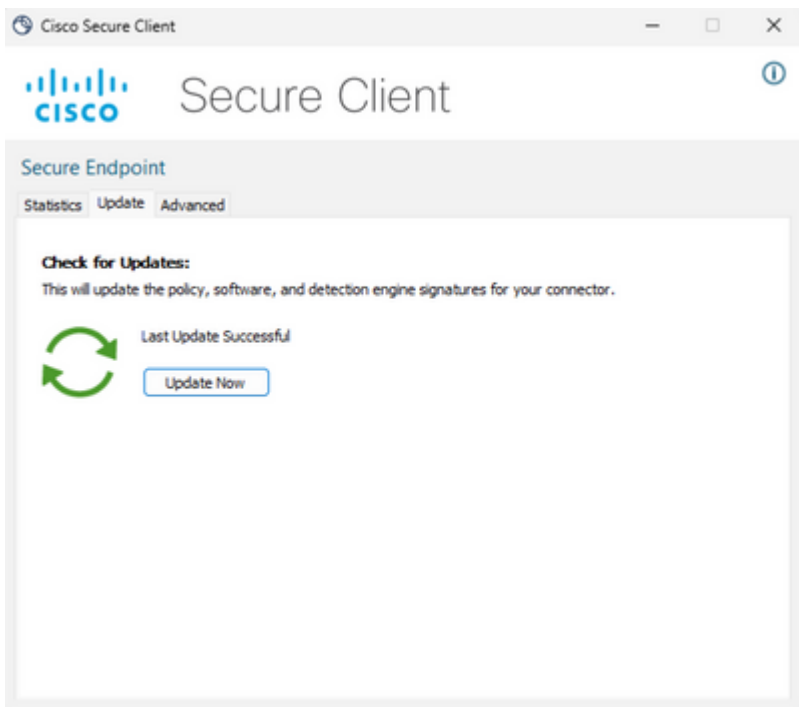
â€f

Si la versión aún está atrasada y el estado del conector está conectado, entonces se puede realizar una actualización de las definiciones o verificar la conectividad del punto final con el servidor TETRA.

### Cómo forzar una actualización de definiciones de TETRA en el Terminal

Los usuarios finales pueden iniciar y verificar el progreso de la descarga de TETRA. Para que el usuario active la actualización, la opción debe establecerse en la directiva. En la página **Configuración avanzada > Configuración de la política de la interfaz de usuario del cliente**, la configuración **Permitir al usuario actualizar las definiciones de TETRA** debe estar habilitada para las definiciones que el usuario desencadenará.

En Cisco Secure Client, el usuario final puede abrir el cliente y comprobar la configuración de Secure Endpoint. El usuario puede hacer clic en "Actualizar ahora" para activar la actualización de la definición de TETRA como se muestra a continuación:



Si ejecuta AMP para terminales Connector versión 7.2.7 y posteriores, puede utilizar un nuevo switch "-forceupdate" para forzar al conector a descargar las definiciones de TETRA.

```
C:\Program Files\Cisco\AMP\8.1.7.21417\sfc.exe -forceupdate
```

Después de forzar la actualización, la definición de TETRA puede ser verificada nuevamente para ver si ocurre una actualización. Si todavía no se está produciendo una actualización, se debe verificar la conexión con el servidor TETRA.

## Verificación de la Conectividad del Servidor de Definición TETRA en el Terminal

La directiva de terminales incluye el servidor de definiciones con el que el terminal se pone en contacto para descargar las definiciones.

La página de detalles del equipo incluye el servidor de actualización. La siguiente imagen muestra dónde se muestra el servidor de actualización:

DESKTOP-QFC3PVT in group Protect			
Hostname	DESKTOP-QFC3PVT	Group	Protect
Operating System	Windows 11, SP 0.0 (Build 22H2.1702)	Policy	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138
Install Date	2023-05-17 01:58:07 UTC	External IP	173.36.117.65
Connector GUID	5c8e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-17 19:40:25 UTC
Processor ID	198bf000906ea	Definition Version	TETRA 64 bit (daily version: 90600)
Definitions Last Updated	2023-05-17 19:16:49 UTC ▲ Failed The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

← Events | Device Trajectory | Diagnostics | View Changes

Scan... Diagnose... Move to Group...

â€f

En la nube pública, el nombre de servidor requerido al que se puede conectar el terminal se muestra en:

## [Direcciones de servidor requeridas para las operaciones adecuadas de Cisco Secure Endpoint y Malware Analytics](#)

### Validación de conexión directa

Desde el punto final, se puede ejecutar el siguiente comando para comprobar la búsqueda de DNS en el servidor de actualización:

```
PS C:\Program Files\Cisco\AMP> Resolve-DnsName -Name tetra-defs.amp.cisco.com
Name                               Type TTL Section IPAddress
----                               -
tetra-defs.amp.cisco.com          A     5   Answer 192.XXX.X.XX
tetra-defs.amp.cisco.com          A     5   Answer 192.XXX.X.X
tetra-defs.amp.cisco.com          A     5   Answer 192.XXX.X.X
```

Si se resuelve la IP, se puede probar la conexión con el servidor. Una respuesta válida tendrá el siguiente aspecto:

```
<#root>
```

```
PS C:\Program Files\Cisco\AMP> curl.exe -v https://tetra-defs.amp.cisco.com
* Trying 192.XXX.X.X:443...
* Connected to tetra-defs.amp.cisco.com (192.XXX.X.X) port 443 (#0)
* schannel: disabled automatic use of client certificate
* ALPN: offers http/1.1
* ALPN: server did not agree on a protocol. Uses default.
* using HTTP/1.x
> GET / HTTP/1.1
> Host: tetra-defs.amp.cisco.com
> User-Agent: curl/8.0.1
> Accept: */*
>
* schannel: server closed the connection
< HTTP/1.1 200 OK

< Date: Fri, 19 May 2023 19:13:35 GMT
< Server:
< Last-Modified: Mon, 17 Apr 2023 15:48:54 GMT
< ETag: "0-5f98a20ced9e3"
< Accept-Ranges: bytes
< Content-Length: 0
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
* Closing connection 0
* schannel: shutting down SSL/TLS connection with tetra-defs.amp.cisco.com port 443
```

Si no se puede establecer la conexión para validar el certificado con el servidor CRL (como [commercial.ocsp.identrust.com](#) o [validation.identrust.com](#)), se mostrará un error como sigue:

```
PS C:\Program Files\Cisco\AMP> curl.exe -v https://tetra-defs.amp.cisco.com
```

```
* Trying 192.XXX.X.XX:443...
* Connected to tetra-defs.amp.cisco.com (192.XXX.X.XX) port 443 (#0)
* schannel: disabled automatic use of client certificate
* ALPN: offers http/1.1
* schannel: next InitializeSecurityContext failed: Unknown error (0x80092013) - The revocation function
* Closing connection 0
* schannel: shutting down SSL/TLS connection with tetra-defs.amp.cisco.com port 443
curl: (35) schannel: next InitializeSecurityContext failed: Unknown error (0x80092013) - The revocation
```

## Validación de proxy

Si el terminal está configurado para utilizar un proxy, se puede comprobar el último estado de error. La ejecución del siguiente PowerShell puede devolver el último error del intento de actualización de TETRA.

```
PS C:\Program Files\Cisco\AMP> (Select-Xml -Path local.xml -XPath '//tetra/lasterror').Node.InnerText
```

Último código de error	Problema	Acciones
4294965193	No se pudo establecer la conexión con el proxy	Comprobar la conexión de red con el proxy
4294965196	No se pudo autenticar con el proxy	Comprobar las credenciales de autenticación para el proxy
4294965187	Se conectó con el proxy y falló la descarga	Comprobar los registros de proxy para problemas de descarga

## Additional Information

- Si observa que los terminales no descargan constantemente las definiciones de TETRA, a pesar de haber completado las comprobaciones anteriores, habilite el conector en modo de depuración durante un intervalo de tiempo igual al intervalo de actualización definido en su política y genere el paquete de soporte. Cuando el conector esté en modo de depuración, tenga en cuenta que también debe tomar las capturas de paquetes de Wireshark. La captura de paquetes también se debe ejecutar durante un intervalo de tiempo igual al intervalo de actualización definido en su política. Una vez recopilada esta información, abra un caso del Cisco TAC junto con esta información para continuar con la investigación.

[Recopilación de datos de diagnóstico de AMP para Windows Connector](#)

## 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).