

# Troubleshoot TETRA definitions update failures

## Contents

[Introduction](#)

[Troubleshooting](#)

[Checking Endpoint Reported Connectivity on the Secure Endpoint Console](#)

[Checking Connectivity on the Endpoint](#)

[Checking TETRA definitions on the Endpoint](#)

[Forcing a TETRA definitions update on the Endpoint](#)

[Checking TETRA Definition Server Connectivity on the Endpoint](#)

[Direct connection validation](#)

[Proxy validation](#)

[Additional Information](#)

## Introduction

This document describes the steps that should be followed in order to investigate the reason as to why are endpoints failing to update the TETRA definitions from Cisco TETRA definitions update servers.

Definitions Last Updated failure seen on the Secure Endpoint Console appears under the Computer details as seen below.

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	1f8bfbff00906ea	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

## Troubleshooting

The Cisco Secure Endpoint for Windows requires a sustained connection to the TETRA definition server in order to download updates.

Common errors in downloading the TETRA definitions includes:

- Failure to resolve server address
- Failure to validate the SSL Certificate (including Certificate Revocation List check)
- Interruption during the download

- Failure to connect to the proxy server
- Failure to authenticate to the proxy server

If a failure occurs while attempting to download the TETRA definitions, the next attempt will occur on the next update interval or if a manual update initiated by the user.

## Checking Endpoint Reported Connectivity on the Secure Endpoint Console

The Secure Endpoint Console shows if the endpoint is connecting regularly. Ensure that your endpoints are active, and have a recent "Last Seen" status. If the endpoints are not checking in with the Secure Endpoint Console, then this indicates that the endpoint is not active or has some connectivity issues.

Cisco releases an average of 4 definition updates daily, and if it at any point during the day, if the endpoint fails to download the update, then the connector posts a failure error. Considering this frequency, only if the endpoints are constantly connected, and have a stable network connection to the TETRA server throughout, then, the endpoints will report as "Within Policy".

The "Last Seen" status is on the Computer details page as circled below:

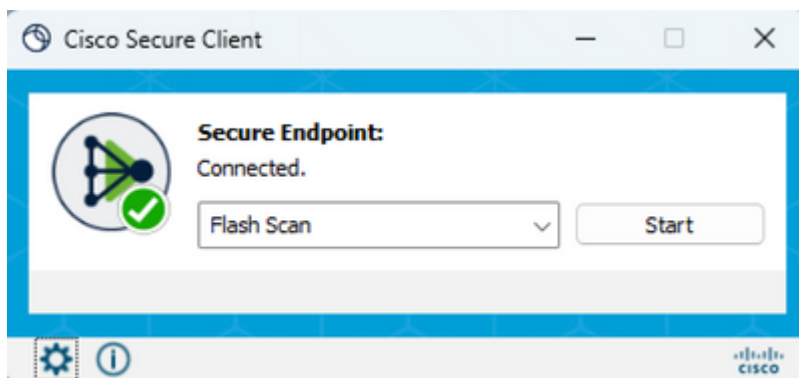
DESKTOP-QFC3PVT in group Protect		Definition Update Failed 0	
Hostname	DESKTOP-QFC3PVT	Group	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1702)	Policy	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138, 172.23.0.1, 172.30.144.1
Install Date	2023-05-17 01:58:07 UTC	External 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.

If the endpoint is connecting and an error is reported that the definitions are not downloaded but is being seen by the console, then the issue might be intermittent. Further investigation can be conducted if the time differences is large between "Last Seen" and "Definitions Last Updated".

## Checking Connectivity on the Endpoint

End users can check the connectivity using the UI interface.

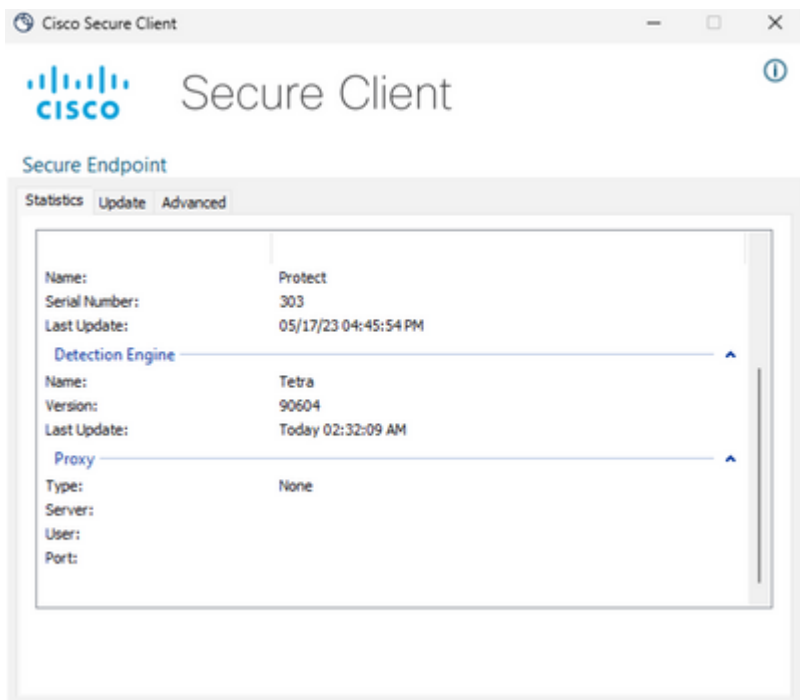
Opening the Cisco Secure Client displays the connectivity status.



The ConnectivityTool can be used when the endpoint is not connected and reports connection problems. This is included in the IPSupportTool that generates the support package.

## Checking TETRA definitions on the Endpoint

Cisco Secure Client provides information on the current TETRA definitions loaded by the endpoint connector. The end user can open the client and check the settings for Secure Endpoint. On the Statistics tab, the current definition for TETRA is available.



â€f

Also, current TETRA definition details are reported by the AmpCLI tool on the endpoint. An example of the command is as follows:

```
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", "engi
```

The definition versions are displayed for each of the engines including TETRA. In this output above, it is version 90604. This can be compared with the Secure Endpoint Console under: **Management > AV Definition Summary**. An example of the page is as below.

## 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>

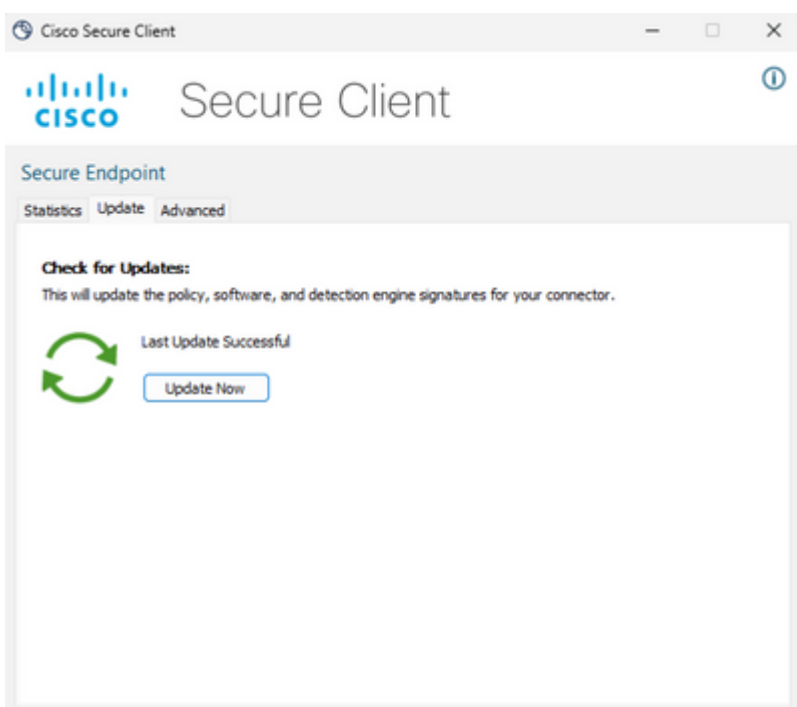
â€f

If the version is still behind and connector status is connected, then either an update of the definitions or checking the endpoint connectivity to the TETRA server can be conducted.

### Forcing a TETRA definitions update on the Endpoint

End users can initiate and check the TETRA download progress. For the user to trigger the update, the option needs to be set in the policy. Under **Advanced Settings > Client User Interface** policy settings page, the settings **Allow user to update TETRA definitions** needs to be enabled for the definitions to be triggered by the user.

In the Cisco Secure Client, the end user can open the client and check the settings for Secure Endpoint. The user can click on "Update Now" to trigger the TETRA definition update as showned below:



If you are running AMP for Endpoints Connector version 7.2.7 and above, you may use a new switch "-forceupdate" to force the connector to download the TETRA definitions.

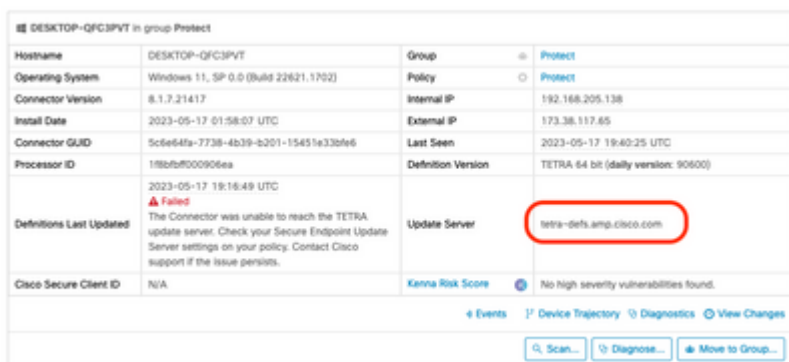
```
C:\Program Files\Cisco\AMP\8.1.7.21417\sfc.exe -forceupdate
```

After the update is forced, the TETRA definition can be checked again to see if an update occurs. If an update still is not occurring, then connection to the TETRA server needs to be checked.

## Checking TETRA Definition Server Connectivity on the Endpoint

Endpoint policy includes the definition server that the endpoint contacts to download the definitions.

The computer details page includes the update server. Image below shows where the update server is shown:



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	173.38.117.65
Connector GUID	5c6e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-17 19:40:25 UTC
Processor ID	198bf0000906ea	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.

â€f

On Public Cloud, the required server name that the endpoint can connect to are listed under: [Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations](#)

## Direct connection validation

From the endpoint, the following command can be run to check DNS lookup to the update server:

```
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
```

If the IP is resolved, the connection connection to the server can be tested. A valid response will look like the following:

<#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

```

If the connection can't be made to validate the certificate with the CRL server (such as commercial.ocsp.identrust.com or validation.identrust.com), then an error will be seen as follows:

```
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

```

## Proxy validation

If the endpoint is configured to use a proxy, the last error status can be checked. Running the PowerShell below can return the last error from TETRA update attempt.

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

Last Error Code	Issue	Actions
-----------------	-------	---------

4294965193	Could not be established connection to the proxy	Check network connectivity to the proxy
4294965196	Could not authenticate with proxy	Check authentication credentials for the proxy
4294965187	Connected with the proxy and download failed	Check proxy logs for download issues

## Additional Information

- If you're seeing endpoints that are constantly failing to download the TETRA definitions, despite completing the above checks, then please enable the Connector in debug mode for a time interval equal to the update interval as defined in your policy and generate the support bundle. When the connector is in debug mode, please note to take the Wireshark packet captures as well. The packet capture must also be run for a time interval equal to the update interval defined in your policy. Once this information has been collected, please open a Cisco TAC case along with this information for further investigation.

[Collection of Diagnostic Data from AMP for Windows Connector](#)