Cisco TrustSec Critical Authentication

The Cisco TrustSec Critical Authentication feature ensures that the Network Device Admission Control (NDAC)-authenticated 802.1X links between Cisco TrustSec devices are in an open state even when the Authentication, Authorization, and Accounting (AAA) server is not reachable.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Cisco TrustSec Critical Authentication

- The Cisco TrustSec Network Device Admission Control feature must be configured on the device. For more information, see the "Cisco TrustSec Network Device Admission Control" chapter in the *Cisco TrustSec Configuration Guide*.
- Ensure that the RADIUS server is marked as dead before configuring the Cisco TrustSec Critical Authentication feature.

Restrictions for Cisco TrustSec Critical Authentication

- All Cisco TrustSec 802.1X links must be part of a single port channel or must be on different VLANs. If multiple links are on the same VLAN, authentication fails because Spanning Tree Protocol (STP) drops all the packets on a blocked interface.

Note All STP forwarding ports are maintained in the open state when Cisco TrustSec critical authentication mode is enabled.

- If the authenticating device (authenticator) is down or if connectivity between the authenticator and Cisco Identity Services Engine (ISE) is lost, the Cisco TrustSec 802.1X links move to the critical authentication mode until connectivity is regained or until the links are reconfigured.
- The default peer security group tag (SGT) value used to configure the Cisco TrustSec 802.1X links for critical authentication must be defined in the ISE server. If the default peer-SGT value is not defined in the ISE server, the policies related to the default peer SGT are not downloaded and are not applied on the Cisco TrustSec 802.1X links. In such a situation, the default policy is applied when the links are in critical authentication mode.
- You must not refresh the environment data when connectivity to the ISE server is lost and when the Cisco TrustSec 802.1X links are in critical authentication mode. If the environment data is refreshed and fails to download, the policies on the device may get cleared.

Information About Cisco TrustSec Critical Authentication

Critical Authentication Overview

The Cisco TrustSec solution provides end-to-end security that is centrally managed using an Authentication, Authorization, and Accounting (AAA) server. The AAA server authenticates and authorizes each device coming into the network, and encryption is done on a per-link basis. The authentication information is downloaded to both the authenticating device (authenticator) and to the incoming device (supplicant) that are added to the CTS network. Another key component of Cisco TrustSec is the Cisco Identity Services Engine (ISE). The ISE server is the policy control point for Cisco TrustSec. The authenticator must be connected to the ISE server to ensure that the Cisco TrustSec 802.1X links are active. After authentication, the supplicant is connected to the ISE server through the authenticator.

Cisco TrustSec Network Device Admission Control helps to add network devices into trusted networks.

When the AAA server is down, Cisco TrustSec can neither add any new device into the network nor maintain the currently authenticated devices in the trusted network. This situation results in the Cisco TrustSec links going into the disconnect state.

The Cisco TrustSec Critical Authentication feature aims to prevent the Cisco TrustSec 802.1X links from going down if the AAA server is not reachable. For devices that are already in the trusted network, previously obtained (cached) security group access control list (SGACL) policies, peer security group tag (SGT) values, and pairwise master key (PMK) values are used until the AAA server is reachable again. For new devices coming into the network, the default peer-SGT value (trusted or untrusted), default PMK value, and default

SGACL policy are used until the AAA server is reachable and the full authentication and authorization policy is received from the AAA server.

All three values—SGACL policy, peer-SGT value, and PMK value—are configurable.

If a user does not want to configure the PMK value, critical authentication brings up 802.1X links without link encryption, and the Security Association Protocol (SAP) negotiation does not occur between interfaces. The default PMK value is used for all SAP negotiations.

In critical authentication mode, preference is given to cached data because it is the last valid set of values received from the AAA server. However, this is a configurable option, and the user can decide if default values should be preferred over cached values.

Note The Cisco TrustSec Critical Authentication feature is triggered only when the AAA server is unreachable. It is not triggered if the AAA server responds to an authenticator request from a device with a failure message (Access-Reject).

Consider this example: If the entry for Device A is deleted from the AAA server and the AAA server is thus unreachable, a Device A link in authenticator state will trigger the critical authentication feature . If Device B is connected to this link, Device B will also enter into critical authentication mode, and Device B will become the authenticator. Now, if Device B has one or more other links in supplicant state that are connected to Device A, then these supplicant links will attemp to to reauthenticate with the AAA server. However, the AAA server will reject Device B's request for authentication (by sending the Access-Reject message). As a result, critical authentication feature on both devices will be terminated. The other interfaces connected to both devices (with SAP negotiation on one end and 802.1x authentication on the other) will now start flapping.

This is a security mechanism to prevent unauthorized devices from assuming the role of authenticator.

How to Configure Cisco TrustSec Critical Authentication

Configuring Critical Authentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*]
4. **radius-server deadtime** *minutes*
5. **radius server** *server-name*
6. **address ipv4** {*hostname* | *ipv4address*} [**acct-port** *port* | **alias** {*hostname* | *ipv4address*} | **auth-port** *port* [**acct-port** *port*]]
7. **automate-tester username** *user* [**ignore-auth-port**] [**ignore-acct-port**] [**idle-time** *minutes*]
8. **pac key** *encryption-key*
9. **exit**
10. **cts server test** {*ipv4-address* | **all**} {**deadtime** *seconds* | **enable** | **idle-time** *minutes*}
11. **cts critical-authentication default peer-sgt** *peer-sgt-value* [**trusted**]
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*] **Example:** `Device(config)# radius-server dead-criteria time 15 tries 3`	Configures the conditions that determine when a RADIUS server is considered unavailable or dead. • **time** *seconds* - Sets the time, in seconds, during which the device does not need to get a valid response from the RADIUS server. The range is from one to 120 seconds. • **tries** *number-of-tries* - Sets the number of times that the device does not get a valid response from the RADIUS server before the server is considered unavailable.
Step 4	**radius-server deadtime** *minutes* **Example:** `Device(config)# radius-server deadtime 10`	Defines time, in minutes (up to a maximum of 1440 minutes or 24 hours), a server marked as DEAD is held in that state. This command improves RADIUS response times when some servers might be unavailable, and causes the unavailable servers to be skipped immediately. Once the deadtime expires, the device marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the DEAD criteria is met, then server is marked as DEAD again for the deadtime interval.
Step 5	**radius server** *server-name* **Example:** `Device(config)# radius server RASERV-1`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode.
Step 6	**address ipv4** {*hostname* | *ipv4address*} [**acct-port** *port* | **alias** {*hostname* | *ipv4address*} | **auth-port** *port* [**acct-port** *port*]] **Example:** `Device(config-radius-server)# address ipv4 172.20.254.4 auth-port 1812 acct-port 1813`	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.

	Command or Action	Purpose
Step 7	**automate-tester username** *user* [**ignore-auth-port**] [**ignore-acct-port**] [**idle-time** *minutes*] **Example:** `Device(config-radius-server)# automate-tester username dummy`	Enables the automated testing feature for the RADIUS server. With this practice, the device sends periodic test authentication messages to the RADIUS server. It looks for a RADIUS response from the server. A success message is not necessary - a failed authentication suffices, because it shows that the server is alive.
Step 8	**pac key** *encryption-key* **Example:** `Device(config-radius-server)# pac key 7 mypackey`	Specifies the Protected Access Credential (PAC) encryption key. The *encryption-key* argument can be **0** (specifies that an unencrypted key follows), **6** (specifies that an advanced encryption scheme [AES] encrypted key follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.
Step 9	**exit** **Example:** `Device(config)# exit`	Exits RADIUS server configuration mode and returns to global configuration mode.
Step 10	**cts server test** {*ipv4-address* | **all**} {**deadtime** *seconds* | **enable** | **idle-time** *minutes*} **Example:** `Device(config)# cts server test all idle-time 3`	Configures the server-liveliness test for a specified RADIUS server or for all servers on the dynamic server list. By default, the test is enabled for all servers. The default **deadtime** is 20 seconds; the range is 1 to 864000 seconds. The default **idle-time** is 60 seconds; the range is from 1 to 14400 seconds.
Step 11	**cts critical-authentication default peer-sgt** *peer-sgt-value* [**trusted**] **Example:** `Device(config)# cts critical-authentication default peer-sgt 5`	Configures the default peer security group tag (SGT) value. • The peer-SGT value is used to tag new devices coming into the Cisco TrustSec network. This value must be configured before the Cisco TrustSec critical authentication mode is enabled. Use the **trusted** keyword to mark a device as trustworthy. • The range for the *peer-SGT-value* argument is from 2 to 65519.
Step 12	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

- Use the **debug cts critical-auth events** and **debug cts critical-auth errors** commands in user EXEC or privileged EXEC mode to help troubleshoot issues with the critical authentication mode.

- Troubleshooting can also be done using the log messages that notify users when an interface enters critical authentication mode and when it reauthenticates.

Verifying Critical Authentication

SUMMARY STEPS

1. **enable**
2. **show running-config | section critical**
3. **show cts interface summary**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show running-config | section critical**

Displays the critical authentication configuration and the configured values.

Example:

```
Device# show running-config | section critical

cts critical-authentication default pmk 4444000000000000000000000000000000000000000000000000000000000000
cts critical-authentication default peer-sgt 10
cts critical-authentication fallback default
cts critical-authentication
```

Step 3 **show cts interface summary**

Displays summary information about the configured Cisco TrustSec interfaces, including the Cisco TrustSec 802.1X links in critical authentication mode and their status.

Example:

```
Device# show cts interface summary

Global Dot1x feature is Enabled


CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical-Authentication
------------------------------------------------------------------------------
Gi3/0/2    DOT1X   OPEN      Authent    3k_3       valid    Cached
```

```
CTS Layer3 Interfaces
---------------------
Interface   IPv4 encap       IPv6 encap       IPv4 policy      IPv6 policy
-------------------------------------------------------------------------
```

Configuration Examples for Cisco TrustSec Critical Authentication

Example: Configuring Critical Authentication

```
Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 15 tries 3
Device(config)# radius-server deadtime 10
Device(config)# radius server RASERV-1
Device(config-radius-server)# address ipv4 172.20.254.4 auth-port 1812 acct-port 1813
Device(config-radius-server)# automate-tester username dummy
Device(config-radius-server)# pac key 7 mypackey
Device(config-radius-server)# exit
Device(config)# radius server RASERV-2
Device(config-radius-server)# address ipv4 172.20.254.8 auth-port 1645 acct-port 1646
Device(config-radius-server)# automate-tester username dummy
Device(config-radius-server)# pac key 7 mypackey
Device(config-radius-server)# exit
Device(config)# cts dot1x-server-timeout 30
Device(config)# cts dot1x-supp-timeout 30
Device(config)# cts server test all idle-time 3
Device(config)# cts critical-authentication default peer-sgt 5
Device(config)# cts critical-authentication
Device(config)# cts critical-authentication default pmk password123
Device(config)# cts cache nv-storage bootdisk:cache
Device(config)# cts critical-authentication fallback cached
Device(config)# exit
```

Additional References for Cisco TrustSec Critical Authentication

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Cisco TrustSec configuration	"Cisco TrustSec Support for IOS" chapter in the *Cisco TrustSec Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco TrustSec Critical Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Cisco TrustSec Critical Authentication

Feature Name	Releases	Feature Information
Cisco TrustSec Critical Authentication	Cisco IOS 15.2(1)SY	The Cisco TrustSec Critical Authentication feature ensures that the Network Device Admission Control (NDAC)-authenticated 802.1X links between Cisco TrustSec devices are in an open state even when the Authentication, Authorization, and Accounting (AAA) server is not reachable. The following command was introduced by this feature: **cts critical-authentication**.