



Cisco TrustSec How-To Guide: Failed Authentications and Authorizations

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 27, 2012

Table of Contents

Table of Contents	1
Introduction	3
What Is the Cisco TrustSec System?	3
About the TrustSec How-To Guides	3
<i>What does it mean to be "TrustSec Certified"?</i>	4
Troubleshooting Failed Authentications and Authorizations	5
Overview	5
TrustSec Components	10
5411 No response received during 120 seconds on last EAP message sent to the client	22
12520 EAP-TLS failed SSL/TLS handshake because the client rejected the ISE local-certificate	22
22044 Identity policy result is configured for certificate based authentication methods but received password based	22
22045 Identity policy result is configured for password based authentication methods but received certificate based authentication request	22
22056 Subject not found in the applicable identity store(s)	22
24408 User authentication against Active Directory failed since user has entered the wrong password	23
15039 Rejected per authorization profile	23
22040 Wrong password or invalid shared secret	23
11036 The Message-Authenticator RADIUS attribute is invalid	23
11007 Could not locate Network Device or AAA Client	23
5417 Dynamic Authorization failed	23
Appendix A: References	24
Cisco TrustSec System:	24
Device Configuration Guides:	24

Introduction

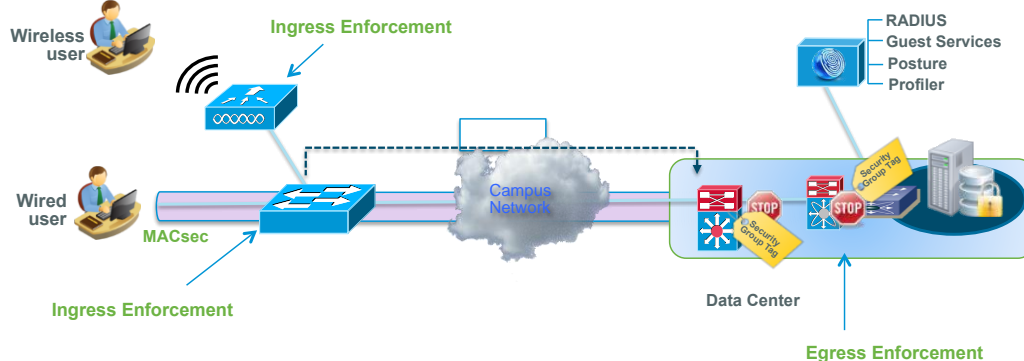
What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

Figure 1: TrustSec Architecture Overview

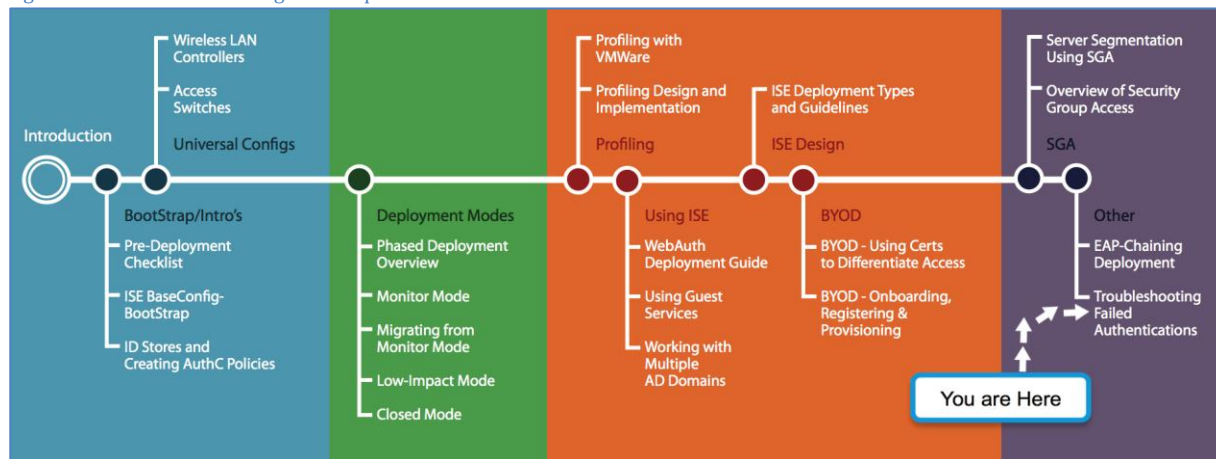


About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide in this series comes with a subway-style “You Are Here” map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).

Figure 2: How-To Guide Navigation Map



What does it mean to be ‘TrustSec Certified’?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked “TrustSec certified,” all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as “TrustSec certified”. The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

Troubleshooting Failed Authentications and Authorizations

Overview

Cisco TrustSec relies on multiple components. When authentication fails in the TrustSec environment, it may be challenging to find out root cause of the issue because you may need to look at different components. TrustSec 2.1 components include:

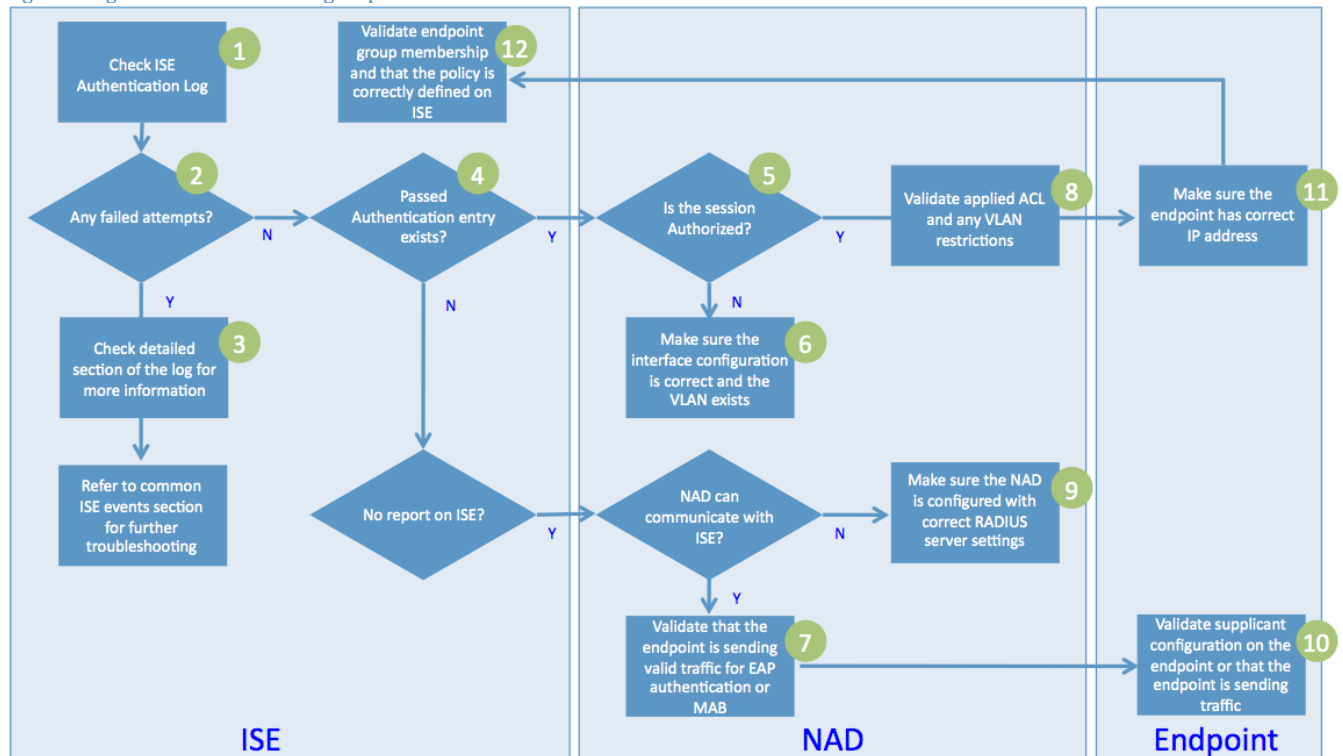
- Cisco ISE nodes
- Network access devices (NADs): Cisco Catalyst® Switches, Cisco Wireless LAN Controllers (WLC), Cisco ASA Adaptive Security Appliances
- Supplicants
- External identity stores

With recent enhancements, Cisco has put effort into providing a single point of view for troubleshooting by correlating switch syslog events to internal ISE events, as well as by providing interfaces on the ISE to poll for different authentication-related information on demand. Other enhancements on the ISE include a configuration validator, a TCP dump utility, and the ability to provide details about supplicant issues when the client is running Cisco AnyConnect® Network Access Manager with a certificate-based EAP type.

High-level Troubleshooting Steps

Figure 3 shows a high-level view of the troubleshooting flow.

Figure 3 High-level Troubleshooting Steps



Procedure 1 Check ISE Authentication Log

Step 1 Log in to the primary ISE Policy Administration Node (PAN).

Step 2 Go to Operations → Authentications.



Step 3 (Optional) If the event is not present in the Live Authentications log, go to Operations → Reports → Catalog → AAA Protocol → RADIUS Authentication.

Procedure 2 Check for Any Failed Authentication Attempts in the Log

Step 1 If the MAC address or username is known, use filters to view the events only from the specific endpoint.

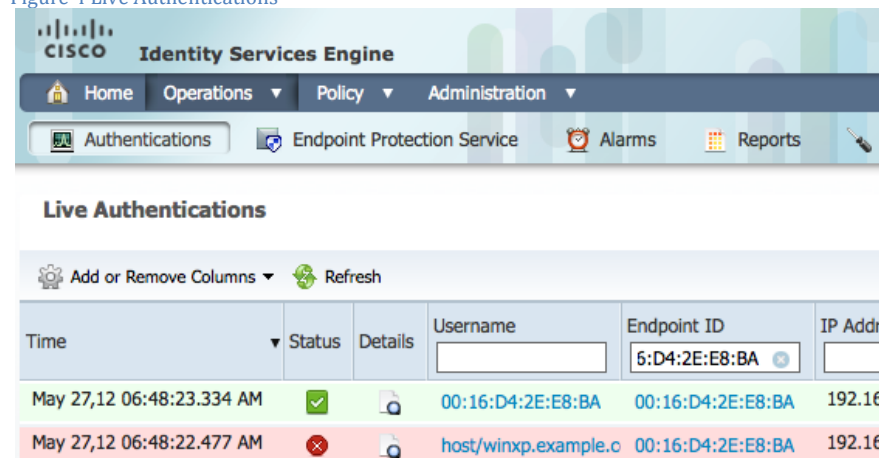
Note: Even for 802.1X authentications, it is helpful to filter with MAC address instead because: depending on where in the process the failure occurred, the endpoint user or computer name may not be known to ISE.





Step 2 The Live Authentications log (Figure 4) shows events up to past 24 hours, so make sure to look at the latest events.

Step 3 Successful events have status of  with green background. A failed event will have  with red background to clearly identify the status.

Step 4 Note the network device and device port before proceeding. Figure 4 Live Authentications Log: Failed Authentication Events

Figure 4 Live Authentications



Time	Status	Details	Username	Endpoint ID	IP Address
May 27,12 06:48:23.334 AM			00:16:D4:2E:E8:BA	00:16:D4:2E:E8:BA	192.168.1.1
May 27,12 06:48:22.477 AM			host/winxp.example.c	00:16:D4:2E:E8:BA	192.168.1.1

Procedure 3 Check the Log for More Information

Step 1 In the Live Authentications log, check Failure Reason column.

Step 2 Click the  button (Details button) for more information.

Step 3 Click the Authentication failed message for additional detail (Figure 5).

Figure 5 Failed Authentication Detail




AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID : C0A8013C0000066396C159E6
 AAA session ID : ise11/126948118/9137
 Date : May 27,2012

Generated on May 28, 2012 7:43:41 AM UTC

Authentication Summary	
Logged At:	May 27,2012 6:48:22.477 AM
RADIUS Status:	Authentication failed : 12520 EAP-TLS failed SSL/TLS handshake because the client rejected the ISE local-certificate
NAS Failure:	
Username:	host/winxp.example.com
MAC/IP Address:	00:16:D4:2E:E8:BA

Actions

[Troubleshoot Authentication](#) 
[View Diagnostic Messages](#)
[Audit Network Device Configuration](#) 
[View Network Device Configuration](#) 
[View Server Configuration Changes](#)

Step 4 Perform the remediation action per the Resolution Steps (Figure 6).

Remediation is described in more detail later in this document.

Figure 6 Authentication Failure Code Lookup

Failure Reason > Authentication Failure Code Lookup

Failure Reason : 12520 EAP-TLS failed SSL/TLS handshake because the client rejected the ISE local-certificate

Generated on: May 28, 2012 7:46:11 AM UTC

Description
EAP-TLS failed SSL/TLS handshake because the client rejected the ISE local-certificate

Resolution Steps
Check whether the proper server certificate is installed and configured for EAP in the Local Certificates page (Admin) . Check the previous : handshake failed. Check the OpenSSLErrorMessage and OpenSSLErrorStack for more information.

Procedure 4 Check for Passed Authentication Entry or the MAC Address in the Log

Step 1 Check to see if latest event for that endpoint was a passed authentication.

Step 2 Since even after the passed authentication, the endpoint is still having issues, there may be configuration mismatch between the ISE and the network access device (NAD).

Step 3 If there are no events for that endpoint, follow the flow chart shown in Figure 3 for further troubleshooting on the NAD and the endpoint.

Procedure 5 Check the NAD Interface Status or the ISE Detailed Reports

Step 1 If this is a Cisco Catalyst switch, log in using Telnet or Secure Shell (SSH) and run following command in enabled mode:

```
show authentication sessions interface Gig x/y/z
```


Step 2 (Optional) If the switch is configured for ISE to poll information via SNMP, open detailed reports by selecting Operations → Authentications. Then click on the  button. Figure 7 shows the results:

Figure 7 Authentication Detail: Interface Status

AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID : C0A8013C000006679C3F253D
AAA session ID : ise11/126948118/9150
Date : May 28, 2012

Generated on May 28, 2012 8:11:02 AM UTC

Act
Tro
Vie
Aug
Vie
Vie

Authentication Summary

Logged At:	May 28, 2012 8:10:49.516 AM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	winxp.example.com
MAC/IP Address:	00:16:D4:2E:E8:BA
Network Device:	switch : 192.168.1.60 FastEthernet0/1
Allowed Protocol:	Default Network Access
Identity Store:	
Authorization Profiles:	Whitelist
SGA Security Group:	
Authentication Protocol :	EAP-TLS

Authentication Result

User-Name=winxp.example.com
State=ReauthSession:C0A8013C000006679C3F253D
Class=CACS:C0A8013C000006679C3F253D:ise11/126948118/9150

Step 3 (Optional) In Detailed Reports, click the interface name (for example, Gigabit Ethernet x/y/z).

Step 4 This will do a SNMP poll that is the equivalent of the **show authentication** command in step 1 without your having to log in to the individual switch.

Procedure 6 Validate the WLC or Switch Configuration

Step 1 Check that the Cisco Wireless LAN Controller (WLC) configuration or the switch OS platform and/or version is supported by the TrustSec version you are implementing.

Step 2 For the NAD to be able to authorize, it needs to have following entry in the configuration:

```
aaa authorization network radius
```

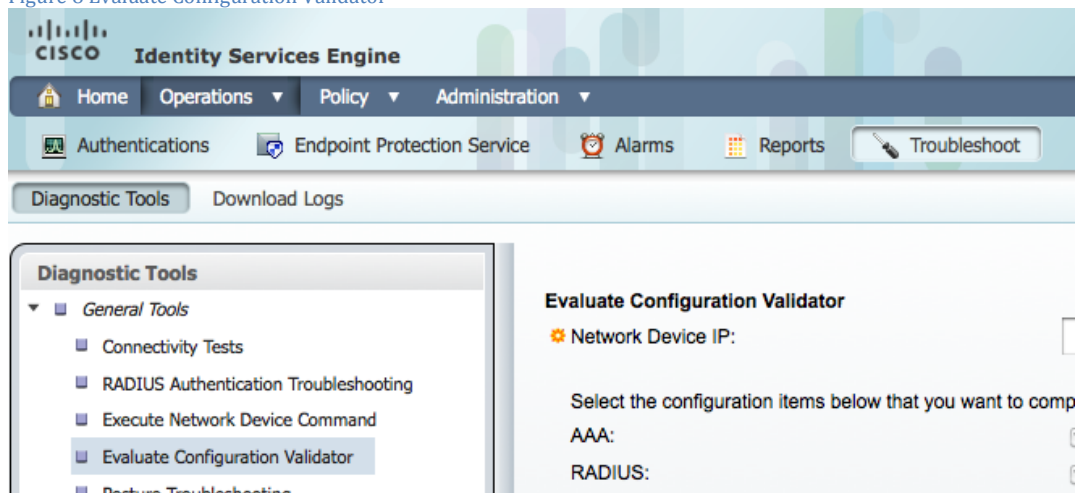
Step 3 For the dynamic VLAN (dVLAN), run the following from exec mode to check that the WLC or the switch VLAN database includes the VLAN that the ISE is trying to assign:

```
show vlan
```

Step 4 For dACL, validate that the ISE ACL syntax is correct by going to Policy → Policy Elements → Results → Authorization → Downloadable ACLs.

Step 5 For Catalyst switches, you can verify the configuration using the ISE Evaluate Configuration Validator tool. Go to Operations → Troubleshooting → Diagnostic Tools → General Tools (Figure 8).

Figure 8 Evaluate Configuration Validator



Procedure 7 Validate Endpoint-to-NAD Communication

Step 1 For Catalyst switches, enable 802.1X debugging by running the following in exec mode:

```
debug dot1x
```

Step 2 Validate that client is sending EAP over LAN (EAPoL) Start message by checking the debug log.

Step 3 For devices using MAC Authentication Bypass (MAB), validate that the device is sending traffic.

If the interface is configured with the settings for order and timers that are recommended for Cisco TrustSec 2.1, it will take 30 seconds before the switch will accept and use the traffic from the endpoint to send a MAB request. This is typically not an issue for chatty devices, such as Windows PC devices; however, some printers may take a while to go through the MAB. If you are experiencing long delays to successfully MAB a device, like a printer, consider running the interface-specific command **authentication control-direction in** to allow traffic from the network to the endpoint prior to authentication, which could accelerate the MAB process.

Procedure 8 Check the ACL Applied to the VLAN and to the Session

Step 1 For the dVLAN, validate that the ACL applied to the VLAN is not too restrictive. You can do this by looking at the VLAN interface ACL or manually assigning an interface to a non-802.1X-enabled interface and validating the endpoint experience.

Step 2 For the dACL, validate that the ACL applied to the session is not too restrictive. A few useful commands include the following:

```
show authentication sessions interface <int_name>
show ip access-list interface <int_name>
show running-config interface <int_name>
show access-list <int_name>
```

Procedure 9 Validate the RADIUS Configuration on the NAD

Step 1 For Catalyst switches, run the Evaluate Configuration Validator (as described in Procedure 6) to validate the RADIUS configuration.

Step 2 From the NAD, try to ping the ISE Policy Services Nodes (PSN).

Step 3 If there are any filtering devices between the NAD and the ISE PSN, verify that the device is allowing RADIUS authentication, authorization, and accounting (UDP 1645/1656 or 1812/1813).

Step 4 You can use the Cisco IOS® Software test feature to run a test authentication. Enter the following command from exec mode:

```
test aaa group radius {test_user} {test_password} new-code
```

Procedure 10 Validate That the Endpoint Has Correct IP Address

Step 1 Next, we need to verify that the supplicant is configured properly and running. First we'll validate that the endpoint has the correct IP address.

Step 2 For Windows devices, run the following from the command prompt:

```
ipconfig /all
```

Step 3 For Mac OS X and Linux devices, run following from the command prompt:

```
ifconfig
```

Step 4 For clientless devices, please refer to the device user guide to find out the IP address.

Procedure 11 Validate ISE Endpoint Group and AuthZ Policy

Step 1 If troubleshooting a MAB authentication, validate that the endpoint MAC address is in correct endpoint group by going to Administration → Identity Management → Endpoints.

Step 2 The detailed endpoint screen will show the current endpoint group in the Identity Group assignment. If the assignment is incorrect, update the group with correct one.

Step 3 Validate the authorization rule by going to Policy → Authorization.

TrustSec Components

Supplicant

As discussed earlier, the ISE Policy Administration Node (PAN) should be the first stop when troubleshooting authentication failures. Some failures will require additional diagnostic work at the NAD level. In most cases, the logs and debugs from the ISE and the NAD should be enough to determine the root cause of the problem.

The diagnostic work that can be performed on a supplicant is largely dependent on the troubleshooting tools that a particular supplicant provides. The native Windows supplicant has almost no debugging tools. Cisco AnyConnect Network Access Manager has a diagnostic and reporting tool (DART) that can be deployed to clients and used to generate a detailed report file. However, the report file is primarily for use by Cisco support staff and not generally recommended for the end user.

Sniffer traces provide vital troubleshooting information, but they are also of limited use on the end client. In general, using the Cisco Switched Port Analyzer (SPAN) to sniff the traffic at the switch is a more reliable and effective way to gather EAP packet traces.

Some of the common supplicant failures arise in situations where the client sends an EAPoL Start request, but fails to respond to an Identity Request message from the switch. Usually this happens because the supplicant is unable to find valid credentials. When the client “goes silent,” there is no way for the switch or Cisco ISE to understand the failure.

Unlike Windows native supplicants or other supplicants available on other operating systems, Cisco AnyConnect Network Access Manager includes an enhanced feature for notifying the ISE of the failure reason. As an example, take the situation in which the client is misconfigured and does not trust the ISE certificate in an EAP Transport Layer Security (EAP-TLS) or Protected EAP (PEAP) authentication (Figure 9).

AAA Protocol > RADIUS Authentication Detail

AAA session ID : ise11/126948118/9118

Date : May 27, 2012

Generated on May 28, 2012 10:08:05 AM UTC

Actions
Troubleshoot Authentication
View Diagnostic Messages
Audit Network Device Configuration
View Network Device Configuration
View Server Configuration Changes

Authentication Summary	
Logged At:	May 27, 2012 5:08:15.274 AM
RADIUS Status:	No response received during 120 seconds on last EAP message sent to the client : 5411 No response
NAS Failure:	
Username:	host/winxp.example.com
MAC/IP Address:	00:16:D4:2E:E8:BA

Figure 10 shows an example in which the PC is running Cisco AnyConnect Network Access Manager. The Failure Reason clearly indicates what the issue is on the supplicant settings.

AAA Protocol > RADIUS Authentication Detail	
RADIUS Audit Session ID :	C0A8013C0000066396C159E6
AAA session ID :	ise11/126948118/9136
Date :	May 27,2012
Generated on May 28, 2012 10:07:42 AM UTC	
<div> <div>Actions</div> <div> Troubleshoot Authentication View Diagnostic Messages Audit Network Device Configuration View Network Device Configuration View Server Configuration Changes </div> </div>	
Authentication Summary	
Logged At:	May 27,2012 6:48:14.762 AM
RADIUS Status:	Authentication failed : 12520 EAP-TLS failed SSL/TLS handshake because the client rejected the ISE local-certificate
NAS Failure:	
Username:	host/winxp.example.com
MAC/IP Address:	00:16:D4:2E:E8:BA

Most of the information needed to troubleshoot Cisco TrustSec authentication issues can be gathered from the ISE itself. In some situations, however, the ISE cannot provide sufficient information to troubleshoot a failed authentication. It is therefore necessary to examine the troubleshooting capabilities of the NAD.

Useful Cisco IOS show Commands

One of the most useful show commands on the Cisco Catalyst switch is **show authentication sessions interface**. The command output shows the current authentication status of the specified port. Other useful commands include `show dot1x interface` and `show running-config interface`.

```
Switch#show authentication sessions interface fastEthernet 0/1
```

```
      Interface:  FastEthernet0/1
      MAC Address:  0016.d42e.e8ba
      IP Address:   192.168.1.78
      User-Name:    winxp.example.com
      Status:       Authz Success
      Domain:       DATA
      Security Policy: Should Secure
      Security Status: Unsecure
      Oper host mode: multi-domain
      Oper control dir: both
      Authorized By: Authentication Server
      Vlan Policy:   100
      Session timeout: N/A
      Idle timeout:  N/A
      Common Session ID: C0A8013C000006679C3F253D
      Acct Session ID:  0x00000C51
      Handle:          0x68000667
```

```
Runnable methods list:
```

```
      Method  State
      dot1x    Authc Success
      mab       Not run
```

```
Switch#
```

```
Switch#
```

```
Switch#show dot1x interface fastEthernet 0/1
```

```
Dot1x Info for FastEthernet0/1
```

```
-----
```

```
PAE                                = AUTHENTICATOR
PortControl                        = AUTO
ControlDirection                  = Both
HostMode                          = MULTI_DOMAIN
QuietPeriod                       = 60
ServerTimeout                     = 0
SuppTimeout                       = 30
ReAuthMax                        = 2
MaxReq                           = 2
TxPeriod                         = 10
```

```
Switch#
```

```
Switch#
```

```
Switch#show running-config interface fastEthernet 0/1
```

```
Building configuration...
```

```

Current configuration : 599 bytes
!
interface FastEthernet0/1
  description 802.1x Enabled
  switchport access vlan 2
  switchport mode access
  switchport voice vlan 110
  authentication event fail action next-method
  authentication event no-response action authorize vlan 100
  authentication event server alive action reinitialize
  authentication host-mode multi-domain
  authentication port-control auto
  authentication periodic
  authentication timer reauthenticate server
  authentication timer inactivity server
  authentication violation restrict
  mab
  dot1x pae authenticator
  dot1x timeout tx-period 10
  spanning-tree portfast
end

Switch#
Switch#

```

SPAN

One of the most useful tools for debugging 802.1X failures on the authenticator is the Switched Port Analyzer (SPAN). SPAN allows you to mirror all the EAP traffic sent and received on one port to a different port where it can be analyzed by a sniffer. By sniffing the actual EAP packets that are exchanged between the authenticator and the client, you can diagnose some failures that are not visible from the Cisco ISE.

To configure a Cisco Catalyst 3000 Series Switch to mirror all the traffic from one port (the source port) to another (the destination port), use the following Cisco IOS commands in configuration mode:

```

(config)# monitor session 1 source interface Gigabit 0/1
(config)# monitor session 1 destination interface Gigabit 0/2 encapsulation replicate

```

To configure a Cisco Catalyst 4500 Series Switch to mirror all the traffic from one port (the source port) to another (the destination port), use the following Cisco IOS commands in configuration mode:

```

(config)# monitor session 1 source interface Gigabit 1/1
(config)# monitor session 1 destination interface Gigabit 1/2

```

No special configuration options are required to use SPAN on Layer 2 frames on the Cisco Catalyst 4500 Series switch, since the Cisco Catalyst 4500 monitors all Layer 2 frames with the default SPAN configuration shown above.

Communication with ISE PSN

There are three common reasons why the switch does not or cannot send RADIUS messages to the AAA server when a client attempts to authenticate:

- Lack of proper network connectivity
- RADIUS configuration on the switch
- Lack of response from the client

To verify network connectivity, ping the AAA server from the switch. Here is an example `ping` command:

```
Switch#
Switch#ping 192.168.1.60

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.60, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#
```

If the ping is not successful, or some packets are dropped, use standard routing and switching debugging techniques to establish reliable connectivity between the switch and the AAA server.

If the ISE PSN is pingable, it can be useful to use the `test aaa` diagnostic command in this situation. The following example illustrates this command:

```
Switch#test aaa group radius testuser cisco123 new-code
User successfully authenticated

Switch#
```

The `test aaa` command causes the switch to send an Access Request to the AAA server for a PAP (clear-text) authentication for (in this example) the user `testuser` with password `cisco123`. The switch will attempt to authenticate to the server configured in the `radius-server host` command. Optionally, if you are using AAA groups instead of the default RADIUS group, you can specify a specific RADIUS group to test a specific server configured as part of the group.

If the result of the `test aaa` command is `User successfully authenticated`, as shown in the preceding code snippet, it means that three things are true: the switch is properly configured to communicate with the AAA server (correct shared key); the switch has network connectivity to the AAA server; and the username and password specified in the `test` command are valid. The ISE Live Authentication event will show this authentication:

```
Switch#test aaa group radius testuser cisco123 new-code
User rejected

Switch#
```

If the result of the `test aaa` command is `User authentication request was rejected by server`, you know that the switch configuration is working and network connectivity is validated, but the username and/or password provided in the `test` command are not valid. This failed authentication will show up in the ISE Live Authentication event. Another possibility is that the switch is not able to authenticate to the AAA server. Either the shared key does not match or there is no network connectivity to the AAA server. This could be the reason that no RADIUS messages are received by the AAA server. Revalidating the configuration and/or verifying network connectivity will allow the switch to communicate with the AAA server during 802.1X authentications.

Policy Mismatch

If the ISE Live Authentications shows successful authentication for the endpoint, but the result of `show authentication sessions interface Gigabit x/y/z` indicates that the port unauthorized, there may be policy mismatch between the ISE policy and the switch. This means although the ISE was able to authenticate and authorize the session, the attribute value pair (AVP) sent from the ISE to the NAD was invalid. Common reasons for this are:

- The VLAN does not exist.
- There was an ACL syntax error.
- There was an AVP syntax error.

If the AAA server has attempted to assign a VLAN that is not defined on the switch, the switch will not be able to authorize the port. In the following example, the AAA server tries to assign the VLAN named EMPLOYEE. The switch returns the follow syslog message:

```
Switch#
Switch#
May 28 07:06:11.156 UTC: %AUTHMGR-5-START: Starting 'dot1x' for client (0016.d42e.e8ba)
on Interface Fa0/1 AuditSessionID C0A8013C0000066D9D16ABF7
May 28 07:06:11.592 UTC: %DOT1X-5-SUCCESS: Authentication successful for client
(0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID
May 28 07:06:11.592 UTC: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x'
for client (0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C0000066D9D16ABF7
May 28 07:06:11.592 UTC: %DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-
existent or shutdown VLAN EMPLOYEE to 802.1x port FastEthernet0/1 AuditSessionID
C0A8013C0000066D9D16ABF7
May 28 07:06:11.592 UTC: %AUTHMGR-5-FAIL: Authorization failed for client
(0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C0000066D9D16ABF7
May 28 07:06:11.592 UTC: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0016.d42e.e8ba|
AuditSessionID C0A8013C0000066D9D16ABF7| AUTHTYPE DOT1X| EVENT APPLY
May 28 07:06:11.592 UTC: %EPM-6-IPEVENT: IP 0.0.0.0| MAC 0016.d42e.e8ba| AuditSessionID
C0A8013C0000066D9D16ABF7| AUTHTYPE DOT1X| EVENT IP-WAIT
May 28 07:06:11.592 UTC: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0016.d42e.e8ba|
AuditSessionID C0A8013C0000066D9D16ABF7| AUTHTYPE DOT1X| EVENT REMOVE
May 28 07:06:11.592 UTC: %DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for
client (0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C0000066D9D16ABF7
Switch#
Switch#
```

As you can see from the following output, the switch's employee VLAN is named EMP, not EMPLOYEE:

```
Switch#sh vlan | i EMP
100 EMP      active      Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22,
```

Because the switch does not have an exact match for the VLAN name EMPLOYEE, it sends an EAP-Failure message to the endpoint. To remedy this problem, either rename the VLAN on the switch or define the correct name in the ISE authorization profile.

In the following example, the dACL uses a wrong syntax. ISE sent `allow ip any any` instead of `permit ip any any`.

```
Switch#
May 28 07:11:59.395 UTC: %AUTHMGR-5-START: Starting 'dot1x' for client (0016.d42e.e8ba)
on Interface Fa0/1 AuditSessionID C0A8013C000006719D1BFAB1
May 28 07:11:59.815 UTC: %DOT1X-5-SUCCESS: Authentication successful for client
(0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID
May 28 07:11:59.815 UTC: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x'
for client (0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C000006719D1BFAB1
```

```

May 28 07:11:59.823 UTC: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0016.d42e.e8ba|
AuditSessionID C0A8013C000006719D1BFAB1| AUTHTYPE DOT1X| EVENT APPLY
May 28 07:11:59.823 UTC: %EPM-6-AUTH_ACL: POLICY Auth-Default-ACL| EVENT Auth-Default-ACL
Attached Successfully
May 28 07:11:59.823 UTC: %EPM-6-AAA: POLICY xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fc368f7|
EVENT DOWNLOAD-REQUEST
May 28 07:11:59.840 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed
state to up
May 28 07:11:59.890 UTC: %EPM-6-AAA: POLICY xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fc368f7|
EVENT DOWNLOAD-FAIL
May 28 07:11:59.890 UTC: %EPM-4-POLICY_APP_FAILURE: IP 0.0.0.0| MAC 0016.d42e.e8ba|
AuditSessionID C0A8013C000006719D1BFAB1| AUTHTYPE DOT1X| POLICY_TYPE dACL| POLICY_NAME
xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fc368f7| RESULT FAILURE| REASON AAA download failure
May 28 07:11:59.890 UTC: %EPM-6-IPEVENT: IP 0.0.0.0| MAC 0016.d42e.e8ba| AuditSessionID
C0A8013C000006719D1BFAB1| AUTHTYPE DOT1X| EVENT IP-WAIT
May 28 07:11:59.890 UTC: %AUTHMGR-5-FAIL: Authorization failed for client
(0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C000006719D1BFAB1
May 28 07:11:59.890 UTC: %DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for
client (0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C000006719D1BFAB1
May 28 07:11:59.890 UTC: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0016.d42e.e8ba|
AuditSessionID C0A8013C000006719D1BFAB1| AUTHTYPE DOT1X| EVENT REMOVE
May 28 07:11:59.899 UTC: %EPM-6-AUTH_ACL: POLICY Auth-Default-ACL| EVENT DETACH-SUCCESS
May 28 07:11:59.899 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed
state to down
May 28 07:12:00.846 UTC: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C000006719D1BFAB1
Switch#
Switch#

```

Because the switch was not able to process the dACL, it sends an EAP-Failure response to the endpoint. To remedy this problem, correct the syntax error on the dACL on ISE, as follows:

```
Switch#show authentication sessions interface FastEthernet 0/1
```

```

Interface: FastEthernet0/1
MAC Address: 0016.d42e.e8ba
IP Address: 192.168.2.100
User-Name: winxp.example.com
Status: Authz Failed
Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-domain
Oper control dir: both
Authorized By: Authentication Server
Vlan Group: N/A
Session timeout: N/A
Idle timeout: N/A
Common Session ID: C0A8013C000006719D1BFAB1
Acct Session ID: 0x00000C5D
Handle: 0xB2000671

```

```
Runnable methods list:
```

```

Method State
dot1x   Authc Success
mab     Not run

```

```
Switch#
```


Identity Services Engine (ISE)

Before looking at the symptoms and causes of specific failures, it is instructive to review what a successful authentication looks like from the ISE perspective. This section will also serve to review the tools that can be used to troubleshoot authentication failures.

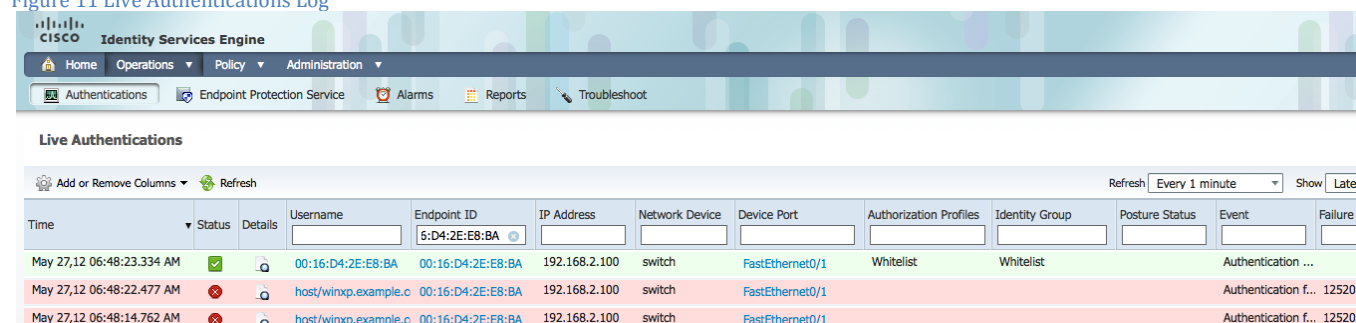
Procedure 1 Live Authentications Log

The Live Authentications log in ISE lists all the authentications that have reached ISE. If there is no entry for the user in this screen, the authentication request has not been received by ISE.

You can look at the Live Authentications log by logging in to ISE primary PAN and going to Operations → Authentications. Doing so will bring up a screen similar to the one shown in Figure 11.

Note: The Live Authentications log screen is provided by Primary MnT node. The same information is also available on backup MnT node. Access to the Live Authentications log is also available by logging in to the secondary PAN and also logging in directly to either MnT node.

Figure 11 Live Authentications Log



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure Reason
May 27, 12 06:48:23.334 AM	✓	🔍	00:16:D4:2E:E8:BA	00:16:D4:2E:E8:BA	192.168.2.100	switch	FastEthernet0/1	Whitelist	Whitelist		Authentication ...	
May 27, 12 06:48:22.477 AM	✗	🔍	host/winxp.example.c	00:16:D4:2E:E8:BA	192.168.2.100	switch	FastEthernet0/1				Authentication f... 12520	
May 27, 12 06:48:14.762 AM	✗	🔍	host/winxp.example.c	00:16:D4:2E:E8:BA	192.168.2.100	switch	FastEthernet0/1				Authentication f... 12520	

The Live Authentications log has several important pieces of information that are critical to determining who is on the network, when and where they connected, and how they were authenticated.

Note: Some of the columns listed described here are visible only by using the Add/Remove Columns feature. To make these columns visible, right-click on the header row.

Time—Shows the time that the log was received by the collection agent. This column is required and cannot be deselected.

Status—Shows if the authentication was successful or failed. This column is required and cannot be deselected.

Details—Brings up a report when you click the magnifying glass icon, allowing you to drill down to view more detailed information on the selected authentication scenario. This column is required and cannot be deselected.

Username—Shows the username that is associated with the authentication.

Endpoint ID—Shows the unique identifier for an endpoint, usually a MAC or IP address.

IP Address—Shows the IP address of the endpoint device.

Network Device—Shows the IP address of the network access device.

Device Port—Shows the port number at which the endpoint is connected.

Authorization Profiles—Shows an authorization profile that was used for authentication.

Identity Group—Shows the identity group that is assigned to the user or endpoint, for which the log was generated.

Posture Status—Shows the status of the posture validation and details on the authentication.

Event—Shows the event status.

Failure Reason—Shows a detailed reason for failure, if the authentication failed.

Optionally, you can choose to show the following categories:

Session ID—Shows the session ID.

In Figure 14, the Authentication Details section shows other information produced during authentication. In Figure 15, the Steps section shows the detailed process that the session went through within ISE.

Figure 14 RADIUS Authentication Detail 3

Authentication Details	
Logged At:	May 27, 2012 4:28:26.812 AM
Occurred At:	May 27, 2012 4:28:26.804 AM
Server:	ise11
Authentication Method:	dot1x
EAP Authentication Method :	EAP-TLS
EAP Tunnel Method :	
Username:	winxp.example.com
RADIUS Username :	host/winxp.example.com
Calling Station ID:	00:16:D4:2E:E8:BA
Framed IP Address:	192.168.2.100
Use Case:	
Network Device:	switch
Network Device Groups:	Device Type#All Device Types,Location#All Locations
NAS IP Address:	192.168.1.60
NAS Identifier:	
NAS Port:	50001
NAS Port ID:	FastEthernet0/1
NAS Port Type:	Ethernet
Allowed Protocol:	Default Network Access
Service Type:	Framed

Figure 15 RADIUS Authentication Detail 4

Steps	
11001	Received RADIUS Access-Request
11017	RADIUS created a new session
	Evaluating Service Selection Policy
15048	Queried PIP
15048	Queried PIP
15004	Matched rule
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12502	Extracted EAP-Response containing EAP-TLS challenge-response and accepting EAP-TLS as negotiated
12800	Extracted first TLS record; TLS handshake started
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12807	Prepared TLS Certificate message
12809	Prepared TLS CertificateRequest message
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing EAP-TLS challenge-response
12505	Prepared EAP-Request with another EAP-TLS challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request

Reports

If the event happened more than 24 hours ago, it's a historical event can be viewed by going to Operations → Reports → Catalog → AAA Protocol → RADIUS Authentication.

Procedure 3 Configuration Validator

You can use the diagnostic tool to evaluate the configuration of a network device and identify any configuration problems. The Expert Troubleshooter compares the configuration of the device with the standard configuration. Figure 16 shows the Evaluate Configuration Validator options.

Figure 16 Evaluate Configuration Validator Options

Diagnostic Tools

- General Tools
 - Connectivity Tests
 - RADIUS Authentication Troubleshooting
 - Execute Network Device Command
 - Evaluate Configuration Validator**
 - Posture Troubleshooting
 - TCP Dump
- Security Group Access Tools

Evaluate Configuration Validator

Network Device IP: [Clear](#)

Select the configuration items below that you want to compare against the recommended template.

AAA: ☒

RADIUS: ☒

Device Discovery: ☒

Logging: ☒

Web Authentication: ☒

Profiler Configuration: ☒

CTS: ☒

802.1X ☒

Open Mode: ☒

Low Impact Mode (Open Mode + ACL): ☐

High Security Mode (Closed Mode): ☐

[Run](#)

Step 1 Go to Operations → Troubleshoot → Diagnostic Tools → Evaluate Configuration Validator.

Step 2 Enter the Network Device IP address of the device whose configuration you want to evaluate, and specify other options as necessary.

Step 3 Select configuration options to compare against the recommended template. A green check mark means the option is selected. Click the option again to deselect. Choose from the following:

Step 4 Web Authentication—Select this check box to compare the Web Authentication configuration for the device with the standard configuration.

Step 5 Profiler Configuration—Select this check box to compare the Profiler configuration for the device with the standard configuration.

Step 6 CTS—Select this check box if you want to compare Security Group Access configuration for the device with the standard configuration.

Step 7 802.1X—Select this check box if you want to compare the 802.1X configuration for the device with the standard configuration. Then choose one of the following options:

Step 8 Open Authentication Mode

Step 9 Low-Impact Mode (Open Mode + ACL)

Step 10 High Security Mode (Closed Mode)

Step 11 Click Run. The Progress Details page appears, prompting you for additional input.

Step 12 Click User Input Required, and modify the fields as necessary. A new window appears, prompting you to select the interfaces for the configuration analysis.

Step 13 Check the check boxes next to the interfaces that you want to analyze, and click Submit. The Progress Details page is displayed again.

Step 14 Click Show Results Summary.

The TCP Dump utility monitors the contents of packets on a network interface that match a given Boolean expression. You can use this utility to troubleshoot problems on your network. Cisco ISE troubleshooting diagnostic tools provide an intuitive user interface (Figure 17).

Figure 17 TCP Dump Options

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentications', 'Endpoint Protection Service', 'Alarms', 'Reports', and 'Troubleshoot'. The 'Diagnostic Tools' section is active, showing a list of tools on the left: 'General Tools' (Connectivity Tests, RADIUS Authentication Troubleshooting, Execute Network Device Command, Evaluate Configuration Validator, Posture Troubleshooting, TCP Dump) and 'Security Group Access Tools'. The 'TCP Dump' tool is selected, showing its configuration page. The page title is 'TCP Dump' with a subtitle 'Monitor the packet headers on the network and save to a file (up to 500,000 packets)'. The configuration options are: Status (Stopped, with a 'Start' button), Host Name (ise11), Network Interface (GigabitEthernet 0), Promiscuous Mode (On, with radio buttons for On and Off), Filter (ip host 192.168.1.60, with an example 'ip host helios and not iceberg'), and Format (Raw Packet Data). A 'Dump File' section shows details of the last created dump file: 'Last created on Fri Apr 13 04:41:50 UTC 2012 by admin', 'File size: 12,625 bytes', 'Format: Raw Packet Data', 'Host Name: ise11', 'Network Interface: GigabitEthernet 0', 'Promiscuous Mode: On', and 'Filter: ip host 192.168.1.60'. There are 'Download' and 'Delete' buttons for the dump file.

Step 1 Go to Operations → Troubleshoot → Diagnostic Tools → TCP Dump.

Step 2 Select a Network Interface to monitor from the drop-down menu. This is the interface upon which the network traffic is monitored, or sniffed.

Step 3 Set Promiscuous Mode to On or Off by clicking the radio button. The default is On.

Step 4 Promiscuous Mode is the default packet sniffing mode. It is recommended that you leave it set to On. In this mode, the network interface is passing all traffic to the system's CPU.

Step 5 In the Filter field, enter a Boolean expression on which to filter. Standard TCP Dump filter expressions are supported, such as the following: `host 10.0.2.1` and `port 1812`

Step 6 Click Start to begin monitoring the network.

Step 7 Click Stop when you have collected a sufficient amount of data, or wait for the process to conclude automatically after accumulating the maximum number of packets (500,000).

TrustSec authentications can fail for many reasons. These include an unknown user, bad credentials, expired credentials, missing certificates, misconfiguration, and so on. Many of these failures can be diagnosed using careful examination of the ISE logs. Common failures and their symptoms are explained below.

5411 No response received during 120 seconds on last EAP message sent to the client

Applies to	All EAP types
Possible Causes	NAD or supplicant: Timeout for EAP may be too aggressive. Supplicant: Configured with certificate base authentication and the supplicant either does not have valid credentials or does not trust ISE certificate. Supplicant and user: Configured with password-based authentication and the user did not provide valid credentials.
Resolution	Verify that supplicant is configured properly to conduct a full EAP conversation with ISE. Verify that NAS is configured properly to transfer EAP messages to or from supplicant. Verify that supplicant or network access server (NAS) does not have a short timeout for EAP conversations. Check the network that connects the NAS to ISE. If the external ID store is used for the authentication, it may be not responding fast enough for current timeouts.

12520 EAP-TLS failed SSL/TLS handshake because the client rejected the ISE local-certificate

Applies to	EAP-TLS (AnyConnect Network Access Manager)
Possible Causes	The supplicant does not trust the ISE PSN certificate.
Resolution	Check whether the proper server certificate is installed and configured for EAP by going to the Local Certificates page (Administration > System > Certificates > Local Certificates). Also ensure that the certificate authority that signed this server certificate is correctly installed in client's supplicant. Check the previous steps in the log for this EAP-TLS conversation for a message indicating why the handshake failed. Check <code>OpenSSLErrorMessage</code> and <code>OpenSSLStack</code> for more information.

22044 Identity policy result is configured for certificate based authentication methods but received password based

Applies to	EAP-TLS, PEAP-TLS
Possible Causes	ISE authentication policy is configured for password-based authentication, but the supplicant is sending certificate credentials.
Resolution	Check the appropriate configuration in Policy > Authentication. This error happens when the identity source is configured for certificate-based authentication and received a password based authentication request.

22045 Identity policy result is configured for password based authentication methods but received certificate based authentication request

Applies to	EAP-FAST, PEAP-MSCHAPv2
Possible Causes	ISE authentication policy is configured for certificate-based authentication, but the supplicant is sending password-based credentials.
Resolution	Check the appropriate configuration in Policy > Authentication. This error happens when the identity source is configured for password-based authentication and received a certificate-based authentication request.

22056 Subject not found in the applicable identity store(s)

Applies to	EAP-FAST, PEAP-MSCHAPv2, MAB
Possible Causes	User or device was not found in the configured identity store
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped if they do not support the current authentication protocol. Make sure the authentication policy points to correct identity store.

	For authentication in a Microsoft Windows network with multiple domains, make sure that the supplicant is appending the domain suffix (For users: administrator@example.com , for machines: winxp.example.com).
--	--

24408 User authentication against Active Directory failed since user has entered the wrong password

Applies to	EAP-FAST, PEAP-MSCHAPv2
Possible Causes	User entered wrong password.
Resolution	Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the shared secret configured for the network device.

15039 Rejected per authorization profile

Applies to	All EAP types
Possible Causes	The default AuthZ rule is to deny access, and there are no specific AuthZ rules for this session.
Resolution	The authorization profile with the ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate authorization policy rule-results.

22040 Wrong password or invalid shared secret

Applies to	Password-based EAP types
Possible Causes	Check the password of the user in internal identity store. The shared RADIUS key does not match between ISE and NAD.
Resolution	Check the user credentials and device shared secret in Administration > Network Resources > Network Devices.

11036 The Message-Authenticator RADIUS attribute is invalid

Applies to	All EAP types and MAB
Possible Causes	The shared RADIUS key does not match between ISE and NAD
Resolution	Check whether the shared secrets on the AAA client and ISE server match. Ensure that the AAA client and the network device have no hardware problems or problems with RADIUS compatibility. Also ensure that the network that connects the device to the ISE has no hardware problems.

11007 Could not locate Network Device or AAA Client

Applies to	All EAP types and MAB
Possible Causes	NAD may not be in the network device list on ISE
Resolution	Verify whether the network device or AAA client is configured in Administration > Network Resources > Network Devices.

5417 Dynamic Authorization failed

Applies to	All EAP types and MAB
Possible Causes	NAD is not configured with change of authorization (CoA) from ISE PSN.
Resolution	Check the connectivity between ISE and the NAD. Ensure that ISE is defined as the dynamic authorization client on NAD and that CoA is supported on device.

Appendix A: References

Cisco TrustSec System:

- <http://www.cisco.com/go/trustsec>
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Device Configuration Guides:

Cisco Identity Services Engine User Guides:

http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

For Cisco Wireless LAN Controllers: <http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html>