

Configure AnyConnect Secure Mobility Client for Linux with Client Certificate Authentication on an ASA

Contents

[Introduction](#)

[Background](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[ASA CLI Configuration](#)

[Troubleshoot](#)

Introduction

This document describes a configuration example for Adaptive Security Appliance (ASA) Cisco AnyConnect Secure Mobility Client access.

Background

The configuration example described in this document is for Adaptive Security Appliance (ASA) Cisco AnyConnect Secure Mobility Client access that uses client certificate for authentication for a Linux Operating System (OS) for an AnyConnect user to connect successfully to an ASA Headend.

Prerequisites

Requirements

This document assumes that the ASA is fully operational and configured to allow the Cisco Adaptive Security Device Manager (ASDM) or Command Line Interface (CLI) to make configuration changes.

Cisco recommends that you have knowledge of these topics:

Basic knowledge of the ASA CLI and ASDM
SSL VPN configuration on the Cisco ASA Head End
Fundamental knowledge of PKI
Familiarity with Linux OS

Components Used

The information in this document is based on these software and hardware versions:

Cisco Adaptive Security Appliance ASA5585-SSP-20
Cisco Adaptive Security Appliance Software Version 9.9(2)36
Adaptive Security Device Manager Version 7.9(1)
AnyConnect Version 4.6.03049
Ubuntu OS 16.04.1 LTS

Note: Download the AnyConnect VPN Client package (anyconnect-linux*.pkg) from the Cisco [Software Download](#) site. Copy the AnyConnect VPN Client to the ASA flash memory, which is then downloaded to the remote user computers in order to establish the SSL VPN connection with the ASA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

For a successful client certificate authentication on Linux devices, AnyConnect secure mobility client supports these certificate stores:

1. Linux OS (PEM) certificate store
2. Firefox (NSS) certificate store

This document is based on client certificate authentication that uses a Linux OS (PEM) certificate store.

1. To use Linux OS certificate store, PEM file-based certificates are placed in these directories.

Entity	Path	Example
Certificate authority (CA) certificate	/opt/.cisco/certificates/ca	tactest:~\$ ls /opt/.cisco/certificates/ca CACERT.pem VeriSignClass3PublicPrimaryCertificationA y-G5.pem
User certificate	/home/tactest/.cisco/certificates/client	tactest:~\$ ls /home/tactest/.cisco/certificates/client myclient.pem

User private key [Initially used to create CSR] : /home/tactest/.cisco/certificate
s/client/private tactest:~\$ ls
/home/tactest/.cisco/certificates/client/private
myclient.key

Note: By default, the path to install the client certificate and the private key is not present, so it needs to be manually created with this command:

```
mkdir -p .cisco/certificates/client/private/
```

If you use a Windows Certificate Authority:

1. Download the CA Certificate (Base64 encoded) with extension .cer
2. Download the User Identity Certificate (Base64 encoded) with extension .cer
3. Change the extension of certificates from .cer to .pem extension

2. To use the Firefox (NSS) certificate store, users can import their certificate by Firefox. The CA certificate for the ASA can be imported into the NSS certificate store by AnyConnect client automatically if the user clicks the *Always Connect* button on the certificate security message dialog box when navigation to ASA is performed with HTTPS.

AnyConnect Linux uses the Firefox certificate store (NSS) as default. If that fails, then it would next use the Linux OS certificate store.

Note: Currently, AnyConnect on a Linux OS does not support GNOME Key, so AnyConnect is unable to use the certificate imported to the GNOME Keyring.

Please make sure there are no related certificates in the Linux OS certificate store and the Firefox (NSS) certificate store before you import a new user certificate.

Ensure that your files meet these requirements:

- All certificate files must end with the extension .pem.
- All private key files must end with the extension .key.
- A client certificate and its associated private key must have the same filename. For example: client.pem and client.key.

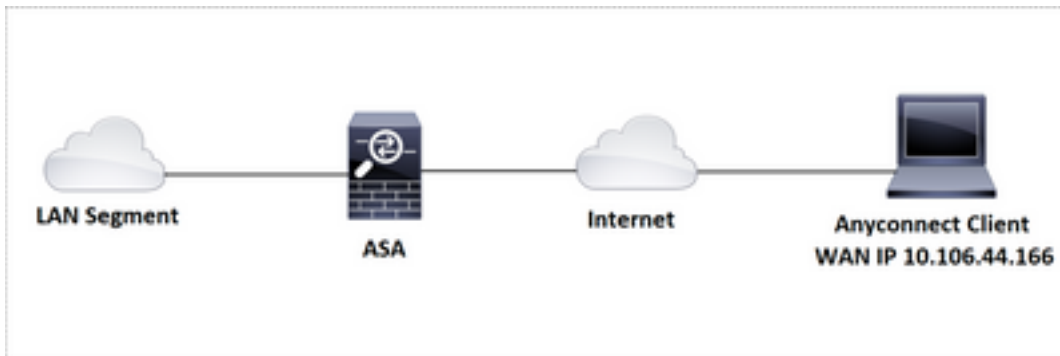
For a clean start, please use this approach:

- Linux OS (PEM) certificate store:
 - A. Remove unnecessary PEM files under /opt/.cisco/certificates, but keep the /opt/.cisco/certificates/ca/VeriSignClass3PublicPrimaryCertificationAuthority-G5.pem certificate intact. This is the CA certificate AnyConnect relies on to perform the code signature verification.
 - B. Remove the user certificates that are not required from the path ~/.cisco/certificates.

- Firefox (NSS) certificate store:
Use Firefox settings to inspect and delete related certificates imported by the user or by AnyConnect.

Configure

Network Diagram



Configurations

Linux Client Setup

1. Download the AnyConnect package, extract the contents and install the AnyConnect application on the Linux client.

```
tactest:Documents$ pwd
/home/tactest/Documents
tactest:Documents$ ls
anyconnect-linux64-4.6.03049-predeploy-k9.tar.gz
tactest:Documents$ tar -xvf anyconnect-linux64-4.6.03049-predeploy-k9.tar.gz
tactest:Documents$ ls
anyconnect-linux64-4.6.03049  anyconnect-linux64-4.6.03049-predeploy-k9.tar.gz
tactest:Documents$ cd anyconnect-linux64-4.6.03049/vpn/
tactest:vpn$ sudo su
[sudo] password for tactest:
root:vpn# pwd
/home/tactest/Documents/anyconnect-linux64-4.6.03049/vpn
root:vpn# ./vpn_install.sh
Installing Cisco AnyConnect Secure Mobility Client...
```

2. Create a certificate signature request for the identity certificate on Linux client with the use of OpenSSL.

```
[dime@localhost ~]$ openssl genrsa -des3 -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for server.key:
```

```

Verifying - Enter pass phrase for server.key:
[dime@localhost ~]$
[dime@localhost ~]$ openssl rsa -in server.key -out server.key.insecure
Enter pass phrase for server.key:
writing RSA key
[dime@localhost ~]$ mv server.key server.key.secure
[dime@localhost ~]$
[dime@localhost ~]$ mv server.key.insecure server.key
[dime@localhost ~]$
[dime@localhost ~]$ ! The insecure key is now named server.key, and you can use this file to
generate the CSR without passphrase.
[dime@localhost ~]$
[dime@localhost ~]$ openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:SJ
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:HTTS
Common Name (eg, your name or your server's hostname) []:dimenet
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[dime@localhost ~]$
[dime@localhost ~]$ ls | grep -i server
server.csr server.key server.key.secure
[dime@localhost ~]$
[dime@localhost ~]$ cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICvTCCAaUCAQAwYTELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAkNBMQswCQYDVQQL
DAJTSjEOMAwGA1UECgwFQ2l2Y28xDTALBgNVBAsMBEhUVFmXGTAxBGNVBAMMEGRp
bWViCG5lCAgICAgICAgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC/
0e5PF09y45/+vlfZbuWRawlvUiJPxy8OdXZhKT7VmDsitdTnPs2Q7cfzVaM1GdIw
c/HoHTL+rmmCn2Ccc9NGoWok3damhhu19xAt2Vxz8jS6mV5bqTeBLYEWJ2Tgh7wA
4/0aPGILZCkQNNn3PruTLe8dqfEhFU6nGp7iJKNjlvvd34Di5YL1NhEQGdZ9q7aK
5VE3nBhgELmPOle53Pt/ZYWwjil38QN8Qo9bXOzmQmRXgRucFaeN0VJVF+0EnnAJ
Y58+yiImEvgKe8h1OCxT2H/TH+5+XRHmggee/zZvis7JMWWcKACOUjQ9scTrjp+z
TW4CM2Cmox3AEcOJ9yg/AgMBAAGgFzAVBgkqhkiG9w0BCQcxCAwGy2l2Y28IMA0G
CSqGSIb3DQEBCwUAA4IBAQC7uRbj+0JxUw7REXc41Ma30WIxhhzvn6QGax8+EP1L
c7wpsMtCSvV7B0gFLKqI7h+dcME+CfBYlcPre2/5LMYo336i9i0tsodV/+EU3NBg
L/RSoH099wBIEo7Xxx30xi38PvnCPnbZZEL2IWrgTy04ohEOUjEOYnD16kUJvISy
Ky8z/3gGDRuhks2Yv4CTTRcvQAvljsLCOZiyaVVrp2xmsPtHxrd6vLrupoxdNpJy
xG1P/67JMLS3qppTuvAqXT5uT2OBAC2hBgMGuKZCOC3mR4WlmoED9woFPESUUMQf
mKOksgQfrrxOZKPyhV8J4jByAjLSw6vh41dJHY9qKaGo
-----END CERTIFICATE REQUEST-----
[dime@localhost ~]$

```

3. The CSR generated previously can be used to request CA to issue a user identity certificate.

4. Once the certificate is issued by CA, copy the certificate to the Linux client.

- a. Create a .pem file at `/home/tactest/.cisco/certificates/client` by use of the command `touch myclient.pem`

- b. Copy the Base64 encoded certificate content from the client identity certificate issued by the CA.
- c. Edit the file by the use of
`Vi myclientcert.pem` Or **nano myclientcert.pem**
- d. Press "i" to insert text in the file.
- e. Paste the Base64 encoded certificate.
- f. Press **Escape** and then enter `:wq!` to save and stop the file edit function.

5. Similarly, place the CA certificate in the path `/opt/cisco/certificates/ca`

ASA CLI Configuration

This section provides the CLI configuration for the Cisco AnyConnect Secure Mobility Client for reference purposes.

```
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 10.106.63.179 255.255.255.0
!
interface GigabitEthernet0/2
 nameif inside
 security-level 100
 ip address 192.168.30.1 255.255.255.0

asdm image disk0:/asdm-791.bin
route outside 0.0.0.0 0.0.0.0 10.106.63.1 1

!-----Client pool configuration-----

ip local pool ANYCONNECT-POOL 192.168.100.1-192.168.100.254 mask 255.255.255.0

!-----Split ACL configuration-----

access-list SPLIT-TUNNEL standard permit 10.0.0.0 255.255.255.0

!-----Configure Trustpoint containing ASA Identity Certificate -----

crypto ca trustpoint IDENTITY
 enrollment terminal
 subject-name CN=bglanyconnect.cisco.com
 keypair ID_CERT
 crl configure

!-----Apply trustpoint on outside interface-----

ssl trust-point IDENTITY outside

!-----Enable AnyConnect and setup AnyConnect Image-----

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-linux64-4.6.03049-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
```

!-----Group Policy configuration-----

```
group-policy GroupPolicy_ANYCONNECT-PROFILE internal
group-policy GroupPolicy_ANYCONNECT-PROFILE attributes
  dns-server value 10.10.10.99
  vpn-tunnel-protocol ssl-client ssl-clientless
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value SPLIT-TUNNEL
  default-domain value cisco.com
```

!-----Tunnel-Group (Connection Profile) Configuraiton-----

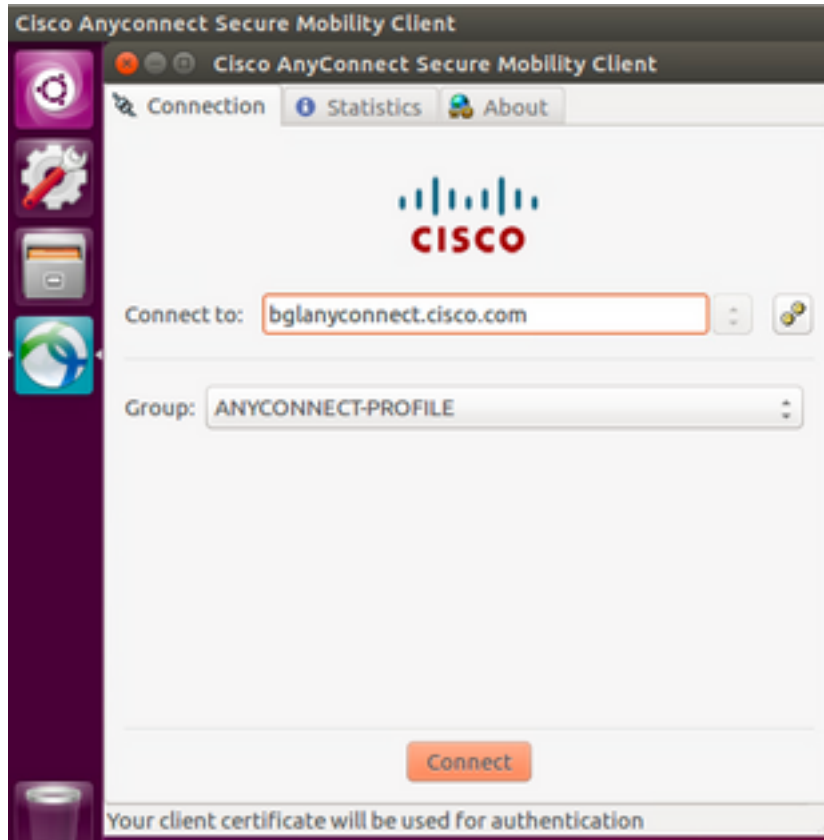
```
tunnel-group ANYCONNECT_PROFILE type remote-access
tunnel-group ANYCONNECT_PROFILE general-attributes
  address-pool ANYCONNECT-POOL
  default-group-policy GroupPolicy_ANYCONNECT-PROFILE
tunnel-group ANYCONNECT_PROFILE webvpn-attributes
  authentication certificate
  group-alias ANYCONNECT-PROFILE enable
```

: end

Verify

Use this section in order to confirm that your configuration works properly.

1. On an Ubuntu OS 16.04.1 LTS, connect AnyConnect by the GUI.



2. If you want to connect AnyConnect by the command line on a Linux client, navigate to this path:

```
tactest:vpn$ cd /opt/cisco/anyconnect/bin
tactest:vpn$
tactest:bin$ ./vpn
Cisco AnyConnect Secure Mobility Client (version 4.6.03049) .

Copyright (c) 2004 - 2018 Cisco Systems, Inc. All Rights Reserved.
```

```
>> state: Disconnected
>> state: Disconnected
>> notice: Ready to connect.
>> registered with local VPN subsystem.
```

VPN>

3. Verify the AnyConnect client is able to establish the connection:

```
VPN> connect bglanyconnect.cisco.com
connect bglanyconnect.cisco.com
>> contacting host (bglanyconnect.cisco.com) for login information...
>> notice: Contacting bglanyconnect.cisco.com.

>> Your client certificate will be used for authentication
Group: ANYCONNECT-PROFILE
>> state: Connecting
>> notice: Establishing VPN session...
The AnyConnect Downloader is analyzing this computer. Please wait...
The AnyConnect Downloader is performing update checks...
>> notice: The AnyConnect Downloader is performing update checks...
>> notice: Checking for profile updates...
The AnyConnect Downloader updates have been completed.
Please wait while the VPN connection is established...
>> state: Connecting
>> notice: Checking for product updates...
>> notice: Checking for customization updates...
>> notice: Performing any required updates...
>> notice: The AnyConnect Downloader updates have been completed.
>> notice: Establishing VPN session...
>> notice: Establishing VPN - Initiating connection...
>> notice: Establishing VPN - Examining system...
>> notice: Establishing VPN - Activating VPN adapter...
>> notice: Establishing VPN - Configuring system...
>> notice: Establishing VPN...
>> state: Connected
>> notice: Connected to bglanyconnect.cisco.com.
>> state: Connected
>> notice: Connected to bglanyconnect.cisco.com.
```

VPN> **disconnect**

```
disconnect
>> state: Disconnecting
>> notice: Disconnect in progress, please wait...
>> state: Disconnecting
>> notice: Disconnect in progress, please wait...
>> state: Disconnecting
>> state: Disconnected
>> notice: Ready to connect.
>> state: Disconnected
>> notice: Ready to connect.
```

VPN>

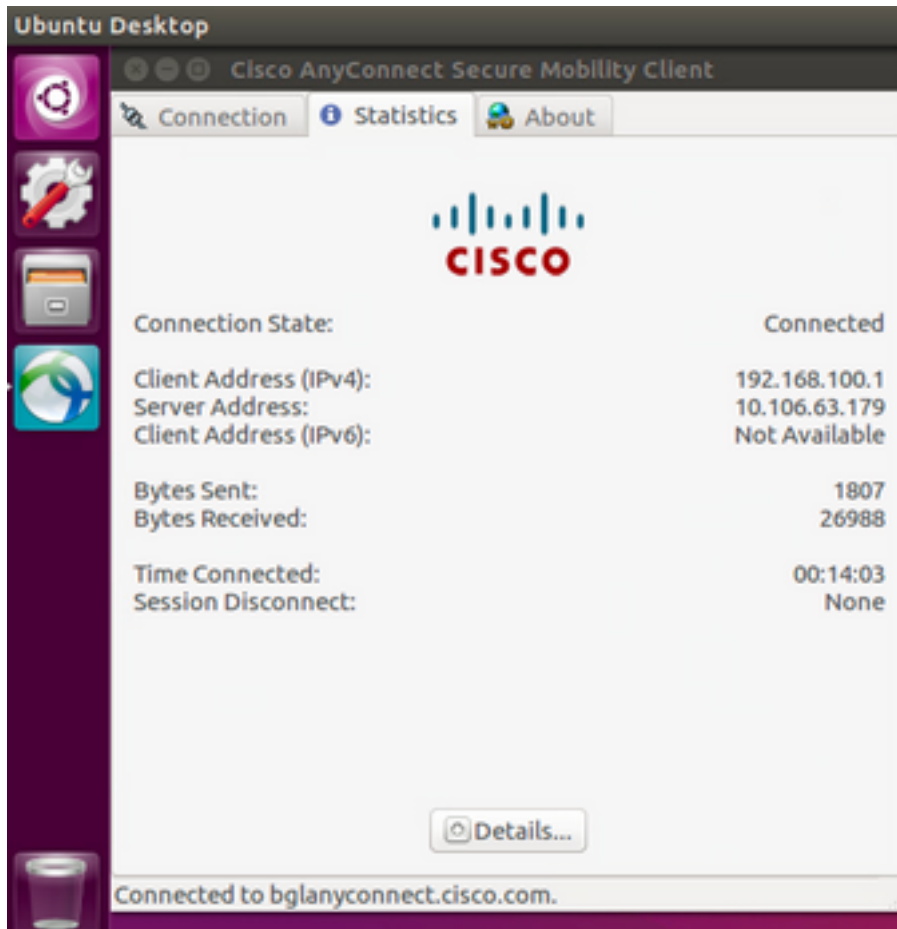
Note: If AnyConnect GUI client is already opened and you try to connect AnyConnect by the CLI, you get this error.


```

VPN> connect bglanyconnect.cisco.com
connect bglanyconnect.cisco.com
>> contacting host (bglanyconnect.cisco.com) for login information...
>> state: Disconnected
>> error: Connect not available. Another AnyConnect application is running
or this functionality was not requested by this application.
VPN>

```

4. Once successfully connected, AnyConnect client details can be verified by the selection of the **Statistics** tab in the AnyConnect GUI client



5. This command is used to confirm the CA and Identity certificates present on the Adaptive Security Appliance (ASA).

```

bglanyconnect# show crypto ca certificate
Certificate
  Status: Available
  Certificate Serial Number: 640000004944fa39c42d24c199000000000049
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=SHERLOCK-CA
    dc=calo
    dc=lab
  Subject Name:
    cn=bglanyconnect.cisco.com
  CRL Distribution Points:

```

```
[1] ldap:///CN=SHERLOCK-
CA,CN=sherlock,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=calo,DC=lab?certificateRevocationList?base?objectClass=cRLDistributionPoint
Validity Date:
  start date: 03:00:53 UTC Jun 28 2019
  end   date: 03:00:53 UTC Jun 27 2021
Storage: config
Associated Trustpoints: IDENTITY
```

```
CA Certificate
Status: Available
Certificate Serial Number: 4a39345869f0e2aa4e8d60143b6d90f7
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
  cn=SHERLOCK-CA
  dc=calo
  dc=lab
Subject Name:
  cn=SHERLOCK-CA
  dc=calo
  dc=lab
Validity Date:
  start date: 10:23:28 UTC Sep 22 2017
  end   date: 10:33:28 UTC Sep 22 2037
Storage: config
Associated Trustpoints: IDENTITY
```

6. These *show* commands can be executed to confirm the status of AnyConnect client and its statistics.

7. In order to confirm if the Linux client has the certificate in the correct format (**Base64 encoding with .pem extension**), browse to the given path and use this command:

```
tactest:client$ cd /home/tactest/.cisco/certificates/client
tactest-client$
tactest:client$ ls
myclient.pem
tactest-client$
tactest:client$ openssl x509 -in myclient.pem -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      64:00:00:00:47:14:e8:bc:85:e5:1d:bf:c4:00:00:00:00:00:47
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC=lab, DC=calo, CN=SHERLOCK-CA
    Validity
      Not Before: Jun 27 15:02:04 2019 GMT
      Not After : Jun 26 15:02:04 2021 GMT
    Subject: C=US, ST=CA, L=SJ, O=Cisco, OU=HTTS, CN=dimenet
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:c3:42:18:d8:fc:09:72:92:81:2f:5d:aa:d4:c6:
        bf:4c:10:b0:f6:ad:21:ae:f9:9c:50:0b:f0:aa:b7:
        02:a0:11:52:e0:23:68:e0:71:f7:67:b9:9f:bd:0b:
        9d:88:70:66:d2:26:3d:ac:a9:1a:ad:1f:47:0c:9f:
        5e:51:09:68:4a:31:f1:ed:86:48:bb:82:24:06:ad:
```

```
d4:e4:0a:9e:56:f2:7d:f9:bc:11:97:d1:b6:52:3e:
4b:a6:fe:99:ff:6b:c3:ab:32:d9:24:ae:15:70:82:
d5:1e:62:ef:68:f0:e3:b7:84:29:58:b0:d2:8f:40:
60:96:cf:ca:fd:04:72:a4:0a:37:ab:88:2e:59:3b:
eb:86:41:6f:da:be:a6:64:b1:6c:be:e5:00:42:af:
a8:82:1f:2c:14:78:26:4f:c4:61:19:94:96:df:cc:
05:21:e5:12:36:ff:4d:f5:ac:f5:f6:45:1f:4c:16:
47:73:9b:84:ad:48:66:04:a9:15:49:ba:cc:d6:58:
f9:30:71:c5:46:f9:05:e1:b5:09:3b:ee:3c:ce:f5:
fa:89:54:d3:7f:14:8a:b3:32:1c:3f:19:07:6c:1a:
cb:95:23:16:8b:ca:44:c7:d6:0a:3c:35:a3:ec:5d:
f9:2b:58:41:11:32:00:53:43:31:70:36:cc:86:04:
6d:4b
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

45:64:99:B1:5F:A1:7C:5F:4F:77:0D:12:CE:B8:F8:CA:40:4D:FA:A8

X509v3 Authority Key Identifier:

keyid:1B:51:FF:8A:71:E7:9C:2B:66:29:28:FD:44:16:BF:44:A4:A1:7D:E1

X509v3 CRL Distribution Points:

Full Name:

URI:ldap:///CN=SHERLOCK-

CA,CN=sherlock,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=calo,DC=lab?certificateRevocationList?base?objectClass=cRLDistributionPoint

Authority Information Access:

CA Issuers - URI:ldap:///CN=SHERLOCK-

CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=calo,DC=lab?cACertificate?base?objectClass=certificationAuthority

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

1.3.6.1.4.1.311.21.7:

0..&+.....7.....E.....U..r.T...V.....d...

X509v3 Extended Key Usage:

TLS Web Client Authentication

1.3.6.1.4.1.311.21.10:

0.0

..+.....

Signature Algorithm: sha256WithRSAEncryption

```
0b:4d:46:fe:dd:0b:78:1a:35:ea:2b:d6:d6:33:ef:5a:86:5a:
07:63:db:ef:ae:b3:87:e3:4d:c7:e8:d2:39:fe:5a:f2:8b:40:
1e:f0:92:3f:48:ed:4d:67:e3:a6:44:05:6f:db:d8:96:bb:a6:
a4:c7:98:fa:40:a5:aa:2d:1f:4b:49:32:1a:86:71:3d:72:69:
f3:3f:e6:9f:f7:94:56:2e:10:0c:4c:c1:74:f1:ee:0e:28:00:
bb:84:84:99:4d:07:ba:1b:68:1d:b5:98:f6:b7:96:55:c1:b8:
5e:14:53:88:82:07:4e:3c:d8:7e:b0:f4:8d:1c:05:fd:8b:20:
12:a4:94:05:7c:ad:81:63:50:05:8d:44:40:31:7c:e0:a8:33:
1e:a3:19:c2:cb:bf:c8:03:b3:05:08:52:23:7e:11:ad:45:04:
bd:0e:5a:8b:26:60:8f:3e:1c:98:41:f9:4d:3e:1a:1f:c8:d5:
97:e3:0a:40:cb:0b:23:ba:9a:f7:27:d6:a1:c5:fd:91:dc:6d:
04:ab:b7:d5:1d:54:d7:b3:ab:99:45:df:c1:01:b8:16:6e:40:
c9:76:9e:36:36:b8:fc:e3:a1:03:86:61:2b:ac:ec:6d:c9:f4:
91:ff:81:58:30:24:d3:81:8b:f0:20:23:49:7a:84:0f:91:80:
2b:54:96:4d
```

If you received the error shown here, it means that you attempted to view a DER-encoded certificate and it was not a PEM-encoded certificate

unable to load certificate

```
12626:error:0906D06C:PEM routines:PEM_read_bio:no start line:pem_lib.c:647:Expecting:
TRUSTED CERTIFICATE
```

Troubleshoot

This section provides the information you can use in order to troubleshoot your configuration.

Note: Refer to [Important Information on Debug Commands](#) before you use **debug** commands.

Caution: On the ASA, you can set various debug levels; by default, level 1 is used. If you change the debug level, the verbosity of the debugs can increase. Do this with caution, especially in production environments.

To troubleshoot an inbound AnyConnect client connection from Linux OS client, use:

- **For AnyConnect process on an ASA**

debug webvpn anyconnect 255

Here is a sample debug taken on an ASA from a work scenario:

```
%ASA-7-609001: Built local-host outside:10.106.44.166
%ASA-6-302013: Built inbound TCP connection 13540 for outside:10.106.44.166/58944
(10.106.44.166/58944) to identity:10.106.63.179/443 (10.106.63.179/443)
%ASA-6-725001: Starting SSL handshake with client outside:10.106.44.166/58944 to
10.106.63.179/443 for TLS session
%ASA-7-725010: Device supports the following 20 cipher(s)
%ASA-7-725011: Cipher[1] : ECDHE-ECDSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[2] : ECDHE-RSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[3] : DHE-RSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[4] : AES256-GCM-SHA384
%ASA-7-725011: Cipher[5] : ECDHE-ECDSA-AES256-SHA384
%ASA-7-725011: Cipher[6] : ECDHE-RSA-AES256-SHA384
%ASA-7-725011: Cipher[7] : DHE-RSA-AES256-SHA256
%ASA-7-725011: Cipher[8] : AES256-SHA256
%ASA-7-725011: Cipher[9] : ECDHE-ECDSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[10] : ECDHE-RSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[11] : DHE-RSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[12] : AES128-GCM-SHA256
%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES128-SHA256
%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[15] : DHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[16] : AES128-SHA256
%ASA-7-725011: Cipher[17] : DHE-RSA-AES256-SHA
%ASA-7-725011: Cipher[18] : AES256-SHA
%ASA-7-725011: Cipher[19] : DHE-RSA-AES128-SHA
```

```
%ASA-7-725011: Cipher[20] : AES128-SHA
%ASA-7-725008: SSL client outside:10.106.44.166/58944 to 10.106.63.179/443 proposes the
following 21 cipher(s)
%ASA-7-725011: Cipher[1] : ECDHE-ECDSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[2] : ECDHE-RSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[3] : DHE-RSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[4] : AES256-GCM-SHA384
%ASA-7-725011: Cipher[5] : ECDHE-ECDSA-AES256-SHA384
%ASA-7-725011: Cipher[6] : ECDHE-RSA-AES256-SHA384
%ASA-7-725011: Cipher[7] : DHE-RSA-AES256-SHA256
%ASA-7-725011: Cipher[8] : AES256-SHA256
%ASA-7-725011: Cipher[9] : ECDHE-ECDSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[10] : ECDHE-RSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[11] : DHE-RSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[12] : AES128-GCM-SHA256
%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES128-SHA256
%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[15] : DHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[16] : AES128-SHA256
%ASA-7-725011: Cipher[17] : DHE-RSA-AES256-SHA
%ASA-7-725011: Cipher[18] : AES256-SHA
%ASA-7-725011: Cipher[19] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[20] : AES128-SHA
%ASA-7-725011: Cipher[21] : DES-CBC3-SHA
%ASA-7-725012: Device chooses cipher ECDHE-RSA-AES256-GCM-SHA384 for the SSL session with client
outside:10.106.44.166/58944 to 10.106.63.179/443
%ASA-6-725016: Device selects trust-point IDENTITY for client outside:10.106.44.166/58944 to
10.106.63.179/443
%ASA-6-725002: Device completed SSL handshake with client outside:10.106.44.166/58944 to
10.106.63.179/443 for TLSv1.2 session
%ASA-6-725007: SSL session with client outside:10.106.44.166/58944 to 10.106.63.179/443
terminated
%ASA-6-302014: Teardown TCP connection 13540 for outside:10.106.44.166/58944 to
identity:10.106.63.179/443 duration 0:00:00 bytes 2948 TCP Reset-I from identity
%ASA-7-609002: Teardown local-host outside:10.106.44.166 duration 0:00:00
%ASA-7-609001: Built local-host outside:10.106.44.166
%ASA-6-302013: Built inbound TCP connection 13541 for outside:10.106.44.166/58946
(10.106.44.166/58946) to identity:10.106.63.179/443 (10.106.63.179/443)
%ASA-6-725001: Starting SSL handshake with client outside:10.106.44.166/58946 to
10.106.63.179/443 for TLS session
%ASA-7-725010: Device supports the following 20 cipher(s)
%ASA-7-725011: Cipher[1] : ECDHE-ECDSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[2] : ECDHE-RSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[3] : DHE-RSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[4] : AES256-GCM-SHA384
%ASA-7-725011: Cipher[5] : ECDHE-ECDSA-AES256-SHA384
%ASA-7-725011: Cipher[6] : ECDHE-RSA-AES256-SHA384
%ASA-7-725011: Cipher[7] : DHE-RSA-AES256-SHA256
%ASA-7-725011: Cipher[8] : AES256-SHA256
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: bglanyconnect.cisco.com'
Processing CSTP header line: 'Host: bglanyconnect.cisco.com'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Linux 4.6.03049'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Linux 4.6.03049'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Linux 4.6.03049'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=05B9EB@192512@A755@0A99DF461C27977CA12A0EAB41F5D7CD46AD8162'
Processing CSTP header line: 'Cookie:
webvpn=05B9EB@192512@A755@0A99DF461C27977CA12A0EAB41F5D7CD46AD8162'
Found WebVPN cookie: 'webvpn=05B9EB@192512@A755@0A99DF461C27977CA12A0EAB41F5D7CD46AD8162'
WebVPN Cookie: 'webvpn=05B9EB@192512@A755@0A99DF461C27977CA12A0EAB41F5D7CD46AD8162'
```

```
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tactest-virtual-machine'
Processing CSTP header line: 'X-CSTP-Hostname: tactest-virtual-machine'
Setting hostname to: 'tactest-virtual-machine'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1399'
Processing CSTP header line: 'X-CSTP-MTU: 1399'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Local-Address-IP4: 10.106.44.166'
Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 10.106.44.166'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1500'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1500'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Remote-Address-IP4: 10.106.63.179'
Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 10.106.63.179'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret:
F731F1B9371EC4E34DF4FF3FE230D5150B621C30F45D44D9579918C0CFF03BC7EEA7AEA1A59D247F6B70FC8B24237639
'
Processing CSTP header line: 'X-DTLS-Master-Secret:
F731F1B9371EC4E34DF4FF3FE230D5150B621C30F45D44D9579918C0CFF03BC7EEA7AEA1A59D247F6B70FC8B24237639
'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:AES256-SHA:AES128-
SHA:DES-CBC3-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-
SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
SHA:AES256-SHA:AES128-SHA:DES-CBC3-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
cstp_util_address_ipv4_accept: address assigned: 192.168.100.1
cstp_util_address_ipv6_accept: No IPv6 Address
np_svc_create_session(0x2F000, 0x00007f884ad8fb00, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.100.1!
No SVC ACL
Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406
tcp-mss = 1460
path-mtu = 1460(mss)
TLS Block size = 16, version = 0x303
mtu = 1460(path-mtu) - 12(opts) - 5(ssl) - 16(iv) = 1427
mod-mtu = 1427(mtu) & 0xfff0(complement) = 1424
```

```
tls-mtu = 1424(mod-mtu) - 8(cstp) - 48(mac) - 1(pad) = 1367
DTLS Block size = 16
mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1443
mod-mtu = 1443(mtu) & 0xffff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1418
computed tls-mtu=1367 dtls-mtu=1418 conf-mtu=1406
DTLS enabled for intf=3 (outside)
override computed dtls-mtu=1418 with conf-mtu=1406
tls-mtu=1367 dtls-mtu=1406
SVC: adding to sessmgmt
Sending X-CSTP-DNS: 10.10.10.99
Sending X-CSTP-Split-Include msgs: for ACL - SPLIT-TUNNEL: Start
    Sending X-CSTP-Split-Include: 10.0.0.0/255.255.255.0
Sending X-CSTP-MTU: 1367
Sending X-DTLS-MTU: 1406
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Sending X-CSTP-Client-Bypass-Protocol: false
%ASA-7-725011: Cipher[9] : ECDHE-ECDSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[10] : ECDHE-RSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[11] : DHE-RSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[12] : AES128-GCM-SHA256
%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES128-SHA256
%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[15] : DHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[16] : AES128-SHA256
%ASA-7-725011: Cipher[17] : DHE-RSA-AES256-SHA
%ASA-7-725011: Cipher[18] : AES256-SHA
%ASA-7-725011: Cipher[19] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[20] : AES128-SHA
%ASA-7-725008: SSL client outside:10.106.44.166/58946 to 10.106.63.179/443 proposes the
following 21 cipher(s)
%ASA-7-725011: Cipher[1] : ECDHE-ECDSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[2] : ECDHE-RSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[3] : DHE-RSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[4] : AES256-GCM-SHA384
%ASA-7-725011: Cipher[5] : ECDHE-ECDSA-AES256-SHA384
%ASA-7-725011: Cipher[6] : ECDHE-RSA-AES256-SHA384
%ASA-7-725011: Cipher[7] : DHE-RSA-AES256-SHA256
%ASA-7-725011: Cipher[8] : AES256-SHA256
%ASA-7-725011: Cipher[9] : ECDHE-ECDSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[10] : ECDHE-RSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[11] : DHE-RSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[12] : AES128-GCM-SHA256
%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES128-SHA256
%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[15] : DHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[16] : AES128-SHA256
%ASA-7-725011: Cipher[17] : DHE-RSA-AES256-SHA
%ASA-7-725011: Cipher[18] : AES256-SHA
%ASA-7-725011: Cipher[19] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[20] : AES128-SHA
%ASA-7-725011: Cipher[21] : DES-CBC3-SHA
%ASA-7-725012: Device chooses cipher ECDHE-RSA-AES256-GCM-SHA384 for the SSL session with client
outside:10.106.44.166/58946 to 10.106.63.179/443
%ASA-6-725016: Device selects trust-point IDENTITY for client outside:10.106.44.166/58946 to
10.106.63.179/443
%ASA-7-717025: Validating certificate chain containing 1 certificate(s).
%ASA-7-717029: Identified client certificate within certificate chain. serial number:
640000004714E8BC85E51DBFC400000000047, subject name:
cn=dimenet,ou=HTTPS,o=Cisco,l=SJ,st=CA,c=US.
%ASA-7-717030: Found a suitable trustpoint IDCERT to validate certificate.
```

%ASA-6-717022: Certificate was successfully validated. serial number: 640000004714E8BC85E51DBFC400000000047, subject name: cn=dimenet,ou=HTTPS,o=Cisco,l=SJ,st=CA,c=US.

%ASA-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.

%ASA-6-725002: Device completed SSL handshake with client outside:10.106.44.166/58946 to 10.106.63.179/443 for TLSv1.2 session

%ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with serial number: 640000004714E8BC85E51DBFC400000000047, subject name: cn=dimenet,ou=HTTPS,o=Cisco,l=SJ,st=CA,c=US, issuer_name: cn=SHERLOCK-CA,dc=calo,dc=lab.

%ASA-4-717037: Tunnel group search using certificate maps failed for peer certificate: serial number: 640000004714E8BC85E51DBFC400000000047, subject name: cn=dimenet,ou=HTTPS,o=Cisco,l=SJ,st=CA,c=US, issuer_name: cn=SHERLOCK-CA,dc=calo,dc=lab.

%ASA-7-113028: Extraction of username from VPN client certificate has been requested. [Request 36]

%ASA-7-113028: Extraction of username from VPN client certificate has started. [Request 36]

%ASA-7-113028: Extraction of username from VPN client certificate has finished successfully. [Request 36]

%ASA-7-113028: Extraction of username from VPN client certificate has completed. [Request 36]

%ASA-6-113009: AAA retrieved default group policy (GroupPolicy_ANYCONNECT-PROFILE) for user = dimenet

%ASA-7-734003: DAP: User dimenet, Addr 10.106.44.166: Session Attribute aaa.cisco.grouppolicy = GroupPolicy_ANYCONNECT-PROFILE

%ASA-7-734003: DAP: User dimenet, Addr 10.106.44.166: Session Attribute aaa.cisco.username = dimenet

%ASA-7-734003: DAP: User dimenet, Addr 10.106.44.166: Session Attribute aaa.cisco.username1 = dimenet

%ASA-7-734003: DAP: User dimenet, Addr 10.106.44.166: Session Attribute aaa.cisco.username2 =

%ASA-7-734003: DAP: User dimenet, Addr 10.106.44.166: Session Attribute aaa.cisco.tunnelgroup = ANYCONNECT_PROFILE

%ASA-6-734001: DAP: User dimenet, Addr 10.106.44.166, Connection AnyConnect: The following DAP records were selected for this connection: DfltAccessPolicy

%ASA-6-113039: Group <GroupPolicy_ANYCONNECT-PROFILE> User <dimenet> IP <10.106.44.166> AnyConnect parent session started.

%ASA-6-725016: Device selects trust-point IDENTITY for client outside:10.106.44.166/58946 to 10.106.63.179/443

%ASA-6-302013: Built inbound TCP connection 13542 for outside:10.106.44.166/58952 (10.106.44.166/58952) to identity:10.106.63.179/443 (10.106.63.179/443)

%ASA-6-725001: Starting SSL handshake with client outside:10.106.44.166/58952 to 10.106.63.179/443 for TLS session

%ASA-7-725010: Device supports the following 20 cipher(s)

%ASA-7-725011: Cipher[1] : ECDHE-ECDSA-AES256-GCM-SHA384

%ASA-7-725011: Cipher[2] : ECDHE-RSA-AES256-GCM-SHA384

%ASA-7-725011: Cipher[3] : DHE-RSA-AES256-GCM-SHA384

%ASA-7-725011: Cipher[4] : AES256-GCM-SHA384

%ASA-7-725011: Cipher[5] : ECDHE-ECDSA-AES256-SHA384

%ASA-7-725011: Cipher[6] : ECDHE-RSA-AES256-SHA384

%ASA-7-725011: Cipher[7] : DHE-RSA-AES256-SHA256

%ASA-7-725011: Cipher[8] : AES256-SHA256

%ASA-7-725011: Cipher[9] : ECDHE-ECDSA-AES128-GCM-SHA256

%ASA-7-725011: Cipher[10] : ECDHE-RSA-AES128-GCM-SHA256

%ASA-7-725011: Cipher[11] : DHE-RSA-AES128-GCM-SHA256

%ASA-7-725011: Cipher[12] : AES128-GCM-SHA256

%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES128-SHA256

%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES128-SHA256

%ASA-7-725011: Cipher[15] : DHE-RSA-AES128-SHA256

%ASA-7-725011: Cipher[16] : AES128-SHA256

%ASA-7-725011: Cipher[17] : DHE-RSA-AES256-SHA

%ASA-7-725011: Cipher[18] : AES256-SHA

%ASA-7-725011: Cipher[19] : DHE-RSA-AES128-SHA

%ASA-7-725011: Cipher[20] : AES128-SHA

%ASA-7-725008: SSL client outside:10.106.44.166/58952 to 10.106.63.179/443 proposes the following 21 cipher(s)

%ASA-7-725011: Cipher[1] : ECDHE-RSA-AES256-GCM-SHA384

%ASA-7-725011: Cipher[2] : ECDHE-ECDSA-AES256-GCM-SHA384

%ASA-7-725011: Cipher[3] : ECDHE-RSA-AES256-SHA384
%ASA-7-725011: Cipher[4] : ECDHE-ECDSA-AES256-SHA384
%ASA-7-725011: Cipher[5] : DHE-RSA-AES256-GCM-SHA384
%ASA-7-725011: Cipher[6] : DHE-RSA-AES256-SHA256
%ASA-7-725011: Cipher[7] : DHE-RSA-AES256-SHA
%ASA-7-725011: Cipher[8] : AES256-GCM-SHA384
%ASA-7-725011: Cipher[9] : AES256-SHA256
%ASA-7-725011: Cipher[10] : AES256-SHA
%ASA-7-725011: Cipher[11] : ECDHE-RSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[12] : ECDHE-ECDSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[13] : ECDHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[14] : ECDHE-ECDSA-AES128-SHA256
%ASA-7-725011: Cipher[15] : DHE-RSA-AES128-GCM-SHA256
%ASA-7-725011: Cipher[16] : DHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[17] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[18] : AES128-GCM-SHA256
%ASA-7-725011: Cipher[19] : AES128-SHA256
%ASA-7-725011: Cipher[20] : AES128-SHA
%ASA-7-725011: Cipher[21] : DES-CBC3-SHA
%ASA-7-725012: Device chooses cipher ECDHE-RSA-AES256-GCM-SHA384 for the SSL session with client
outside:10.106.44.166/58952 to 10.106.63.179/443
%ASA-6-725016: Device selects trust-point IDENTITY for client outside:10.106.44.166/58952 to
10.106.63.179/443
%ASA-7-725017: No certificates received during the handshake with client
outside:10.106.44.166/58952 to 10.106.63.179/443 for DTLSv1 session
%ASA-6-725002: Device completed SSL handshake with client outside:10.106.44.166/58952 to
10.106.63.179/443 for TLSv1.2 session
%ASA-7-737035: IPAA: Session=0x0002f000, 'IPv4 address request' message queued
%ASA-7-737035: IPAA: Session=0x0002f000, 'IPv6 address request' message queued
%ASA-7-737001: IPAA: Session=0x0002f000, Received message 'IPv4 address request'
%ASA-5-737003: IPAA: Session=0x0002f000, DHCP configured, no viable servers found for tunnel-
group 'ANYCONNECT_PROFILE'
%ASA-6-737026: IPAA: Session=0x0002f000, Client assigned 192.168.100.1 from local pool
%ASA-6-737006: IPAA: Session=0x0002f000, Local pool request succeeded for tunnel-group
'ANYCONNECT_PROFILE'
%ASA-7-737001: IPAA: Session=0x0002f000, Received message 'IPv6 address request'
%ASA-5-737034: IPAA: Session=0x0002f000, IPv6 address: no IPv6 address available from local
pools
%ASA-5-737034: IPAA: Session=0x0002f000, IPv6 address: callback failed during IPv6 request
%ASA-4-722041: TunnelGroup <ANYCONNECT_PROFILE> GroupPolicy <GroupPolicy_ANYCONNECT-PROFILE>
User <dimenet> IP <10.106.44.166> No IPv6 address available for SVC connection
%ASA-7-609001: Built local-host outside:192.168.100.1
%ASA-5-722033: Group <GroupPolicy_ANYCONNECT-PROFILE> User <dimenet> IP <10.106.44.166> First
TCP SVC connection established for SVC session.
**%ASA-6-722022: Group <GroupPolicy_ANYCONNECT-PROFILE> User <dimenet> IP <10.106.44.166> TCP SVC
connection established without compression**
%ASA-7-746012: user-identity: Add IP-User mapping 192.168.100.1 - LOCAL\dimenet Succeeded - VPN
user
%ASA-6-722055: Group <GroupPolicy_ANYCONNECT-PROFILE> User <dimenet> IP <10.106.44.166> Client
Type: Cisco AnyConnect VPN Agent for Linux 4.6.03049
%ASA-4-722051: Group <GroupPolicy_ANYCONNECT-PROFILE> User <dimenet> IP <10.106.44.166> IPv4
Address <192.168.100.1> IPv6 address <::> assigned to session
%ASA-6-302015: Built inbound UDP connection 13543 for outside:10.106.44.166/42354
(10.106.44.166/42354) to identity:10.106.63.179/443 (10.106.63.179/443)
%ASA-6-725001: Starting SSL handshake with client outside:10.106.44.166/42354 to
10.106.63.179/443 for DTLS session
%ASA-7-609001: Built local-host outside:10.10.10.99
%ASA-6-302016: Teardown UDP connection 13544 for outside:192.168.100.1/60514(LOCAL\dimenet) to
outside:10.10.10.99/53 duration 0:00:00 bytes 0 (dimenet)
%ASA-7-609002: Teardown local-host outside:10.10.10.99 duration 0:00:00
%ASA-6-302016: Teardown UDP connection 13543 for outside:10.106.44.166/42354 to
identity:10.106.63.179/443 duration 0:00:00 bytes 147
%ASA-6-302015: Built inbound UDP connection 13545 for outside:10.106.44.166/42354
(10.106.44.166/42354) to identity:10.106.63.179/443 (10.106.63.179/443)

```
%ASA-6-725001: Starting SSL handshake with client outside:10.106.44.166/42354 to
10.106.63.179/443 for DTLS session
%ASA-6-725003: SSL client outside:10.106.44.166/42354 to 10.106.63.179/443 request to resume
previous session
%ASA-6-725002: Device completed SSL handshake with client outside:10.106.44.166/42354 to
10.106.63.179/443 for DTLSv0.9 session
%ASA-5-722033: Group <GroupPolicy_ANYCONNECT-PROFILE> User <dimenet> IP <10.106.44.166> First
UDP SVC connection established for SVC session.
%ASA-6-722022: Group <GroupPolicy_ANYCONNECT-PROFILE> User <dimenet> IP <10.106.44.166> UDP SVC
connection established without compression
%ASA-6-725007: SSL session with client outside:10.106.44.166/58946 to 10.106.63.179/443
terminated
```

- **For client certificate authentication on an ASA**

```
debug crypto ca 255
debug crypto ca messages 255
debug crypto ca transactions 255
```

Here is a sample debug taken for a successful client certificate authentication on an ASA:

```
CERT_API: PKI session 0x05ba525b open Successful with type SSL
CERT_API: Authenticate session 0x05ba525b, non-blocking cb=0x00007f88839daf00
CERT_API thread wakes up!
CERT_API: process msg cmd=0, session=0x05ba525b
CERT_API: Async locked for session 0x05ba525b

CRYPTO_PKI: Begin sorted cert chain
-----Certificate-----:
Serial: 640000004714E8BC85E51DBFC4000000000047
Subject: cn=dimenet,ou=HTTS,o=Cisco,l=SJ,st=CA,c=US
Issuer: cn=SHERLOCK-CA,dc=calo,dc=lab

CRYPTO_PKI: End sorted cert chain
CRYPTO_PKI: Cert chain pre-processing: List size is 1, trustpool is not in use
CRYPTO_PKI: List pruning is not necessary.
CRYPTO_PKI: Sorted chain size is: 1
CRYPTO_PKI: Found ID cert. serial number: 640000004714E8BC85E51DBFC4000000000047, subject name:
cn=dimenet,ou=HTTS,o=Cisco,l=SJ,st=CA,c=US
CRYPTO_PKI: Verifying certificate with serial number: 640000004714E8BC85E51DBFC4000000000047,
subject name: cn=dimenet,ou=HTTS,o=Cisco,l=SJ,st=CA,c=US, issuer_name: cn=SHERLOCK-
CA,dc=calo,dc=lab, signature alg: SHA256/RSA.

CRYPTO_PKI: Checking to see if an identical cert is
already in the database...

CRYPTO_PKI(Cert Lookup) issuer="cn=SHERLOCK-CA,dc=calo,dc=lab" serial number=64 00 00 00 47 14
e8 bc 85 e5 1d bf c4 00 00 00 | d...G.....
00 00 47 | ..G

CRYPTO_PKI: looking for cert in handle=0x00007f8825ce6c90, digest=
9c 05 9b 71 14 9a 6b 35 35 9f f3 4f c5 eb d8 2a | ...q..k55..O...*

CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.

CRYPTO_PKI: Looking for suitable trustpoints for connection type SSL

CRYPTO_PKI: Found suitable tp: IDCERT
CRYPTO_PKI: Storage context locked by thread CERT_API
```

```
CRYPTO_PKI: Found a suitable authenticated trustpoint IDCERT.
CRYPTO_PKI: ExtendedKeyUsage OID = 1.3.6.1.5.5.7.3.2 acceptable for usage type: SSL VPN Peer
CRYPTO_PKI:check_key_usage:Key Usage check OK

CRYPTO_PKI: Certificate validation: Successful, status: 0
CRYPTO_PKI: bypassing revocation checking based on policy configuration
CRYPTO_PKI:Certificate validated. serial number: 640000004714E8BC85E51DBFC400000000047, subject name: cn=dimenet,ou=HTTS,o=Cisco,l=SJ,st=CA,c=US.

CRYPTO_PKI: Storage context released by thread CERT API

CRYPTO_PKI: Certificate validated without revocation check

CRYPTO_PKI: valid cert with warning.

CRYPTO_PKI: valid cert status.
CERT_API: calling user callback=0x00007f88839daf00 with status=0(Success)
CERT_API: Close session 0x05ba525b asynchronously
CERT_API: Async unlocked for session 0x05ba525b
CERT_API: process msg cmd=1, session=0x05ba525b
CERT_API: Async locked for session 0x05ba525b
CERT_API: Async unlocked for session 0x05ba525b
CERT API thread sleeps!
```

- **For the AnyConnect process on a Linux client**

On a Linux device, AnyConnect logs can be found in the file named `syslog` at path: `/var/log/`
Here is a sample of work logs taken from a Linux client. This command can be run to gather live logs for an AnyConnect client connection:

```
tactest:client$ tail -f /var/log/syslog
```

```
Jul 1 08:42:48 machine acvpnuui[11774]: An SSL VPN connection to bglanyconnect.cisco.com has been requested by the user.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getProfileNameFromHost File:
../vpn/Api/ProfileMgr.cpp Line: 1250 No profile available for host bglanyconnect.cisco.com.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getHostInitSettings File:
../vpn/Api/ProfileMgr.cpp Line: 1334 Profile () not found. Using default settings.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: loadProfiles File:
../vpn/Api/ProfileMgr.cpp Line: 189 No profile is available.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getProfileNameFromHost File:
../vpn/Api/ProfileMgr.cpp Line: 1250 No profile available for host bglanyconnect.cisco.com.
Jul 1 08:42:48 machine acvpnuui[11774]: Using default preferences. Some settings (e.g. certificate matching) may not function as expected if a local profile is expected to be used. Verify that the selected host is in the server list section of the profile and that the profile is configured on the secure gateway.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: setConnectionData File:
../vpn/Api/ConnectMgr.cpp Line: 2015 Resetting certificate list.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getProfileNameFromHost File:
../vpn/Api/ProfileMgr.cpp Line: 1250 No profile available for host bglanyconnect.cisco.com.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getHostInitSettings File:
../vpn/Api/ProfileMgr.cpp Line: 1334 Profile () not found. Using default settings.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getCertList File: ../vpn/Api/ApiCert.cpp Line: 497 Number of certificates found: 1
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getProfileNameFromHost File:
../vpn/Api/ProfileMgr.cpp Line: 1250 No profile available for host bglanyconnect.cisco.com.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getHostInitSettings File:
../vpn/Api/ProfileMgr.cpp Line: 1334 Profile () not found. Using default settings.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: setConnectionData File:
```

```
../../../../vpn/Api/ConnectMgr.cpp Line: 2148 Using certificate which matched stored preferences
Jul 1 08:42:48 machine acvpnuui[11774]: Function: setConnectionData File:
../../../../vpn/Api/ConnectMgr.cpp Line: 2287 Certificate retrieved from preferences: Subject Name:
C=US, ST=CA, L=SJ, O=Cisco, OU=HTTS, CN=dimenet Issuer Name : DC=lab, DC=calo, CN=SHERLOCK-CA
Store : PEM File User
Jul 1 08:42:48 machine acvpnuui[11774]: Message type information sent to the user: Contacting
bglanyconnect.cisco.com.
Jul 1 08:42:48 machine acvpnuui[11774]: Initiating VPN connection to the secure gateway
https://bglanyconnect.cisco.com
Jul 1 08:42:48 machine acvpnagent[1785]: Using default preferences. Some settings (e.g.
certificate matching) may not function as expected if a local profile is expected to be used.
Verify that the selected host is in the server list section of the profile and that the profile
is configured on the secure gateway.
Jul 1 08:42:48 machine acvpnagent[1785]: Function: processConnectNotification File:
../../../../vpn/Agent/MainThread.cpp Line: 13590 Received connect notification (host
bglanyconnect.cisco.com, profile N/A)
Jul 1 08:42:48 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface ens32.
Jul 1 08:42:48 machine acvpnagent[1785]: message repeated 2 times: [ Function:
getDnsConfiguration File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to
get domain list for interface ens32.]
Jul 1 08:42:48 machine acvpnagent[1785]: Function: resolveHostName File:
../../../../vpn/Common/Utility/HostLocator.cpp Line: 721 Invoked Function:
CHostLocator::resolveHostNameAlt Return Code: -29229035 (0xFE420015) Description:
DNSREQUEST_ERROR_EMPTY_RESPONSE
Jul 1 08:42:48 machine acvpnagent[1785]: Function: getHostIPAddrByName File:
../../../../vpn/Common/IPC/SocketSupport.cpp Line: 344 Invoked Function: ::getaddrinfo Return Code: 11
(0x0000000B) Description: unknown
Jul 1 08:42:48 machine acvpnagent[1785]: Function: resolveHostName File:
../../../../vpn/Common/Utility/HostLocator.cpp Line: 733 Invoked Function:
CSocketSupport::getHostIPAddrByName Return Code: -31129588 (0xFE25000C) Description:
SOCKETSSUPPORT_ERROR_GETADDRINFO
Jul 1 08:42:48 machine acvpnagent[1785]: Function: ResolveHostname File:
../../../../vpn/Common/Utility/HostLocator.cpp Line: 843 Invoked Function:
CHostLocator::resolveHostName Return Code: -31129588 (0xFE25000C) Description:
SOCKETSSUPPORT_ERROR_GETADDRINFO failed to resolve host name bglanyconnect.cisco.com to IPv6
address
Jul 1 08:42:48 machine acvpnagent[1785]: Function: logResolutionResult File:
../../../../vpn/Common/Utility/HostLocator.cpp Line: 927 Host bglanyconnect.cisco.com has been
resolved to IP address 10.106.63.179
Jul 1 08:42:48 machine acvpnagent[1785]: Writing to hosts file:
10.106.63.179#011bglanyconnect.cisco.com ###Cisco AnyConnect VPN client modified this file.
Please do not modify contents until this comment is removed.
Jul 1 08:42:48 machine acvpnagent[1785]: Function: respondToConnectNotification File:
../../../../vpn/Agent/MainThread.cpp Line: 5831 The requested VPN connection to
bglanyconnect.cisco.com will target the following IP protocols and addresses: primary - IPv4
(address 10.106.63.179), secondary - N/A.
Jul 1 08:42:48 machine acvpnagent[1785]: Function: determineAcidexMacAddrMapForTlv File:
../../../../vpn/Agent/MainThread.cpp Line: 6143 [ACIDEX] Determined public interface MAC address 00-
50-56-bd-87-1f (interface IPv4 address: 10.106.44.166)
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getUserName File:
../../../../vpn/Api/CTransportCurlStatic.cpp Line: 2249 PasswordEntry username is tactest
Jul 1 08:42:48 machine acvpnuui[11774]: Function: findProfile File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 666 NSS Profile directory:
/home/tactest/.mozilla/firefox/6ai2dwqd.default
Jul 1 08:42:48 machine acvpnuui[11774]: Function: InitNSS File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 408 Invoked Function: NSS_Initialize
Return Code: -8015 (0xFFFFE0B1) Description: unknown Unknown
Jul 1 08:42:48 machine acvpnuui[11774]: Function: CNSSCertStore File:
../../../../vpn/CommonCrypt/Certificates/NSSCertStore.cpp Line: 76 Invoked Function:
CNSSCertUtils::InitNSS Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:48 machine acvpnuui[11774]: Function: addNSSStore File:
```

```
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 1874 Invoked Function:
CNSSCertStore::CNSSCertStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:48 machine acvpnuui[11774]: Function: OpenStores File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 449 Invoked Function:
CCollectiveCertStore::addNSSStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:48 machine acvpnuui[11774]: Function: verify_callback File:
../../../../vpn/CommonCrypt/Certificates/FileCertificate.cpp Line: 417 Invoked Function:
X509_verify_cert Return Code: 0 (0x00000000) Description: ok
Jul 1 08:42:48 machine acvpnuui[11774]: Function: verify_callback File:
../../../../vpn/CommonCrypt/Certificates/FileCertificate.cpp Line: 417 Invoked Function:
X509_verify_cert Return Code: 0 (0x00000000) Description: ok
Jul 1 08:42:48 machine acvpnuui[11774]: Function: PeerCertVerifyCB File:
../../../../vpn/Api/CTransportCurlStatic.cpp Line: 959 Return success from VerifyServerCertificate
Jul 1 08:42:48 machine acvpnuui[11774]: Function: processResponseStringFromSG File:
../../../../vpn/Api/ConnectMgr.cpp Line: 11991 Client certificate requested by peer (via AggAuth)
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getUserName File:
../../../../vpn/Api/CTransportCurlStatic.cpp Line: 2249 PasswordEntry username is tactest
Jul 1 08:42:48 machine acvpnuui[11774]: Function: findProfile File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 666 NSS Profile directory:
/home/tactest/.mozilla/firefox/6ai2dwqd.default
Jul 1 08:42:48 machine acvpnuui[11774]: Function: InitNSS File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 408 Invoked Function: NSS_Initialize
Return Code: -8015 (0xFFFFE0B1) Description: unknown Unknown
Jul 1 08:42:48 machine acvpnuui[11774]: Function: CNSSCertStore File:
../../../../vpn/CommonCrypt/Certificates/NSSCertStore.cpp Line: 76 Invoked Function:
CNSSCertUtils::InitNSS Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:48 machine acvpnuui[11774]: Function: addNSSStore File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 1874 Invoked Function:
CNSSCertStore::CNSSCertStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:48 machine acvpnuui[11774]: Function: OpenStores File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 449 Invoked Function:
CCollectiveCertStore::addNSSStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:48 machine acvpnuui[11774]: Function: verify_callback File:
../../../../vpn/CommonCrypt/Certificates/FileCertificate.cpp Line: 417 Invoked Function:
X509_verify_cert Return Code: 0 (0x00000000) Description: ok
Jul 1 08:42:48 machine acvpnuui[11774]: Function: verify_callback File:
../../../../vpn/CommonCrypt/Certificates/FileCertificate.cpp Line: 417 Invoked Function:
X509_verify_cert Return Code: 0 (0x00000000) Description: ok
Jul 1 08:42:48 machine acvpnuui[11774]: Function: PeerCertVerifyCB File:
../../../../vpn/Api/CTransportCurlStatic.cpp Line: 959 Return success from VerifyServerCertificate
Jul 1 08:42:48 machine acvpnuui[11774]: Function: ClientCertSetCB File:
../../../../vpn/Api/CTransportCurlStatic.cpp Line: 1063 Client certificate requested by peer
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getUserName File:
../../../../vpn/Api/CTransportCurlStatic.cpp Line: 2249 PasswordEntry username is tactest
Jul 1 08:42:48 machine acvpnuui[11774]: Function: findProfile File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 666 NSS Profile directory:
/home/tactest/.mozilla/firefox/6ai2dwqd.default
Jul 1 08:42:48 machine acvpnuui[11774]: Function: InitNSS File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 408 Invoked Function: NSS_Initialize
Return Code: -8015 (0xFFFFE0B1) Description: unknown Unknown
Jul 1 08:42:48 machine acvpnuui[11774]: Function: CNSSCertStore File:
../../../../vpn/CommonCrypt/Certificates/NSSCertStore.cpp Line: 76 Invoked Function:
CNSSCertUtils::InitNSS Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:48 machine acvpnuui[11774]: Function: addNSSStore File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 1874 Invoked Function:
CNSSCertStore::CNSSCertStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:48 machine acvpnuui[11774]: Function: OpenStores File:
```

```
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 449 Invoked Function:
CCollectiveCertStore::addNSSStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:48 machine acvpnuui[11774]: Function: GetCertChain File:
../../../../vpn/CommonCrypt/Certificates/FileCertStore.cpp Line: 618 Invoked Function: enumerateCert
Return Code: -31457266 (0xFE20000E) Description: CERTSTORE_ERROR_CERT_NOT_FOUND
Jul 1 08:42:48 machine acvpnuui[11774]: Function: ProcessPromptData File:
../../../../vpn/Api/SDIMgr.cpp Line: 336 Authentication is not token based (OTP).
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getProfileNameFromHost File:
../../../../vpn/Api/ProfileMgr.cpp Line: 1250 No profile available for host bglanyconnect.cisco.com.
Jul 1 08:42:48 machine acvpnuui[11774]: Function: getHostInitSettings File:
../../../../vpn/Api/ProfileMgr.cpp Line: 1334 Profile () not found. Using default settings.
Jul 1 08:42:48 machine acvpnuui[11774]: Message type prompt sent to the user: Your client
certificate will be used for authentication
Jul 1 08:42:50 machine acvpnuui[11774]: Function: userResponse File:
../../../../vpn/Api/ConnectMgr.cpp Line: 1606 Processing user response.
Jul 1 08:42:50 machine acvpnuui[11774]: Function: processIfcData File:
../../../../vpn/Api/ConnectMgr.cpp Line: 3650 Authentication succeeded
Jul 1 08:42:50 machine acvpnuui[11774]: VPN state: Connecting Network state: Network Accessible
Network control state: Network Access: Available Network type: Undefined
Jul 1 08:42:50 machine acvpnuui[11774]: Message type information sent to the user: Establishing
VPN session...
Jul 1 08:42:50 machine acvpnuui[11774]: Function: getProfileConfiguredOnSG File:
../../../../vpn/Api/ConnectMgr.cpp Line: 10896 VPN Profile Manifest entry not present
Jul 1 08:42:50 machine acvpnuui[11774]: Function: initiateTunnel File:
../../../../vpn/Api/ConnectMgr.cpp Line: 11279 Invoked Function: ConnectMgr::getProfileConfiguredOnSG
Return Code: -29556727 (0xFE3D0009) Description: CONNECTMGR_ERROR_UNEXPECTED
Jul 1 08:42:50 machine acvpnuui[11774]: Function: launchCachedDownloader File:
../../../../vpn/Api/ConnectMgr.cpp Line: 8228 Launching Cached Downloader: path:
'/opt/cisco/anyconnect/bin/vpndownloader' cmd: '"-ipc#011gc#011-cd"'
Jul 1 08:42:50 machine acvpnuui[11774]: Function: IsValid File:
../../../../vpn/CommonCrypt/VerifyFileSignatureOpenSSL.cpp Line: 280 Not validating original name for
file (/opt/cisco/anyconnect/bin/vpndownloader)
Jul 1 08:42:50 machine acvpnuui[11774]: Function: findProfile File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 666 NSS Profile directory:
/home/tactest/.mozilla/firefox/6ai2dwqd.default
Jul 1 08:42:50 machine acvpnuui[11774]: Function: InitNSS File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 408 Invoked Function: NSS_Initialize
Return Code: -8015 (0xFFFFE0B1) Description: unknown Unknown
Jul 1 08:42:50 machine acvpnuui[11774]: Function: CNSSCertStore File:
../../../../vpn/CommonCrypt/Certificates/NSSCertStore.cpp Line: 76 Invoked Function:
CNSSCertUtils::InitNSS Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnuui[11774]: Function: addNSSStore File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 1874 Invoked Function:
CNSSCertStore::CNSSCertStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnuui[11774]: Function: OpenStores File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 449 Invoked Function:
CCollectiveCertStore::addNSSStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnuui[11774]: Function: verify_callback File:
../../../../vpn/CommonCrypt/Certificates/FileCertificate.cpp Line: 417 Invoked Function:
X509_verify_cert Return Code: 0 (0x00000000) Description: ok
Jul 1 08:42:50 machine acvpnuui[11774]: message repeated 2 times: [ Function: verify_callback
File: ../../vpn/CommonCrypt/Certificates/FileCertificate.cpp Line: 417 Invoked Function:
X509_verify_cert Return Code: 0 (0x00000000) Description: ok]
Jul 1 08:42:50 machine acvpnuui[11774]: Server certificate validation was successful
Jul 1 08:42:50 machine acvpnuui[11774]: Function: launchCachedDownloader File:
../../../../vpn/Api/ConnectMgr.cpp Line: 8247 Invoked Function: ConnectMgr::launchCachedDownloader
Return Code: 0 (0x00000000) Description: Successfully launched the cached downloader
Jul 1 08:42:50 machine acvpndownloader[13609]: Cisco AnyConnect Secure Mobility Client
Downloader (VPN) started, version 4.6.03049
Jul 1 08:42:50 machine acvpndownloader[13609]: Function: handleInvalidPid File:
```

```
../../../../vpn/Common/FirstInstance.cpp Line: 524 PID file does not exist.
Jul  1 08:42:50 machine acvpndownloader[13609]: Function: init File:
../../../../vpn/Common/il8n/MsgCatalog.cpp Line: 373 initialized catalog: AnyConnect with locale:
Jul  1 08:42:50 machine acvpndownloader[13609]: Function: loadProfiles File:
../../../../vpn/Api/ProfileMgr.cpp Line: 189 No profile is available.
Jul  1 08:42:50 machine acvpndownloader[13609]: Function: invokePreferenceUpdateCBs File:
../../../../vpn/Api/PreferenceMgr.cpp Line: 1512 Callback interface address is NULL.
Jul  1 08:42:50 machine acvpndownloader[13609]: Current Preference Settings: ServiceDisable:
false ShowPreConnectMessage: false AutoConnectOnStart: false MinimizeOnConnect: true
LocalLanAccess: false DisableCaptivePortalDetection: false AutoReconnect: true AutoUpdate: true
ProxySettings: Native AllowLocalProxyConnections: true PPPEExclusion: Disable
PPPEExclusionServerIP: AutomaticVPNPolicy: false TrustedNetworkPolicy: Disconnect
UntrustedNetworkPolicy: Connect TrustedDNSDomains: TrustedDNSServers: TrustedHttpsServerList:
EnableScripting: false TerminateScriptOnNextEvent: false EnableAutomaticServerSelection: false
AuthenticationTimeout: 12 IPProtocolSupport: IPv4,IPv6 AllowManualHostInput: true
BlockUntrustedServers: false PublicProxyServerAddress: CertificatePinning: false
Jul  1 08:42:50 machine acvpndownloader[13609]: The AnyConnect Downloader is performing update
checks...
Jul  1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: The
AnyConnect Downloader is performing update checks...
Jul  1 08:42:50 machine acvpnui[11774]: Function: processDnlldrArgsRequest File:
../../../../vpn/Api/ConnectMgr.cpp Line: 15162 Determine proxy: false
Jul  1 08:42:50 machine acvpnui[11774]: Function: findProfile File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 666 NSS Profile directory:
/home/tactest/.mozilla/firefox/6ai2dwqd.default
Jul  1 08:42:50 machine acvpnui[11774]: Function: InitNSS File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 408 Invoked Function: NSS_Initialize
Return Code: -8015 (0xFFFFFE0B1) Description: unknown Unknown
Jul  1 08:42:50 machine acvpnui[11774]: Function: CNSSCertStore File:
../../../../vpn/CommonCrypt/Certificates/NSSCertStore.cpp Line: 76 Invoked Function:
CNSSCertUtils::InitNSS Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul  1 08:42:50 machine acvpnui[11774]: Function: addNSSStore File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 1874 Invoked Function:
CNSSCertStore::CNSSCertStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul  1 08:42:50 machine acvpnui[11774]: Function: OpenStores File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 449 Invoked Function:
CCollectiveCertStore::addNSSStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul  1 08:42:50 machine acvpnui[11774]: Function: GetCertChain File:
../../../../vpn/CommonCrypt/Certificates/FileCertStore.cpp Line: 618 Invoked Function: enumerateCert
Return Code: -31457266 (0xFE20000E) Description: CERTSTORE_ERROR_CERT_NOT_FOUND
Jul  1 08:42:50 machine acvpndownloader[13609]: Function: getManifestFromConfigXml File:
../../../../vpn/Downloader/DownloaderArgs.cpp Line: 657 Language manifest not present
Jul  1 08:42:50 machine acvpndownloader[13609]: Function: getManifestFromConfigXml File:
../../../../vpn/Downloader/DownloaderArgs.cpp Line: 666 Customization manifest not present
Jul  1 08:42:50 machine acvpndownloader[13609]: Function: getManifestFromConfigXml File:
../../../../vpn/Downloader/DownloaderArgs.cpp Line: 675 Profile manifest not present
Jul  1 08:42:50 machine acvpndownloader[13609]: Function: parseBaseConfig File:
../../../../vpn/Downloader/DownloaderArgs.cpp Line: 872 No optional modules in aggregate config
xml.
Jul  1 08:42:50 machine acvpndownloader[13609]: Function: parseMiscInfo File:
../../../../vpn/Downloader/DownloaderArgs.cpp Line: 898 VPN Profile Manifest entry not present
Jul  1 08:42:50 machine acvpndownloader[13609]: Function: parseCustomAttributes File:
../../../../vpn/Downloader/DownloaderArgs.cpp Line: 937 Custom attribute entry not present
Jul  1 08:42:50 machine acvpndownloader[13609]: Function: setHostnameAndPort File:
../../../../vpn/Downloader/DownloaderArgs.cpp Line: 545 Defaulting to port 443
Jul  1 08:42:50 machine acvpndownloader[13609]: Connecting to bglanyconnect.cisco.com.
Jul  1 08:42:50 machine acvpndownloader[13609]: Authorized Server List is not defined in local
policy. Treating bglanyconnect.cisco.com as authorized. Any configured local policy software and
profile locks do not apply.
Jul  1 08:42:50 machine acvpndownloader[13609]: Checking for profile updates...
Jul  1 08:42:50 machine acvpndownloader[13609]: Checking for product updates...
```

Jul 1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: Checking for profile updates...

Jul 1 08:42:50 machine acvpndownloader[13609]: Skipping update of AnyConnect Secure Mobility Client 4.6.03049 because an up-to-date version is already installed.

Jul 1 08:42:50 machine acvpndownloader[13609]: Skipping update of AnyConnect DART 4.6.03049 because an up-to-date version is already installed.

Jul 1 08:42:50 machine acvpndownloader[13609]: Checking for customization updates...

Jul 1 08:42:50 machine acvpndownloader[13609]: Performing any required updates...

Jul 1 08:42:50 machine acvpndownloader[13609]: The AnyConnect Downloader updates have been completed.

Jul 1 08:42:50 machine acvpnagent[1785]: Function: OnIpcMessageReceived File:/vpn/Common/IPC/IPCDepot.cpp Line: 1115 Invoked Function: CipcTransport::OnSocketReadComplete Return Code: -33292279 (0xFE040009) Description: IPCTRANSPORT_ERROR_UNEXPECTED

Jul 1 08:42:50 machine acvpndownloader[13609]: Function: Serialize File:/vpn/Common/TLV/CertificateInfoTlv.cpp Line: 799 Data to serialize is empty

Jul 1 08:42:50 machine acvpndownloader[13609]: Function: Assign File:/vpn/Common/TLV/CertificateInfoTlv.cpp Line: 87 Invoked Function: CCertificateInfoTlv::Serialize Return Code: -21954549 (0xFEB1000B) Description: CERTIFICATEINFO_ERROR_NO_DATA:No certificate data was found

Jul 1 08:42:50 machine acvpndownloader[13609]: Function: GetAggAuthCertificateInfo File:/vpn/Downloader/DownloaderArgs.cpp Line: 1828 Invoked Function: CCertificateInfoTlv::Assign Return Code: -21954549 (0xFEB1000B) Description: CERTIFICATEINFO_ERROR_NO_DATA:No certificate data was found

Jul 1 08:42:50 machine acvpnagent[1785]: Function: GetAggAuthCertificateInfo File:/vpn/Common/TLV/startparameters.cpp Line: 1365 Invoked Function: CStartParameters::GetInfoByType Return Code: -32440304 (0xFE110010) Description: TLV_ERROR_NO_ATTRIBUTE

Jul 1 08:42:50 machine acvpnagent[1785]: Tunnel initiated by GUI Client.

Jul 1 08:42:50 machine acvpnagent[1785]: Using default preferences. Some settings (e.g. certificate matching) may not function as expected if a local profile is expected to be used. Verify that the selected host is in the server list section of the profile and that the profile is configured on the secure gateway.

Jul 1 08:42:50 machine acvpnagent[1785]: Function: GetAggAuthCertificateInfo File:/vpn/Common/TLV/startparameters.cpp Line: 1365 Invoked Function: CStartParameters::GetInfoByType Return Code: -32440304 (0xFE110010) Description: TLV_ERROR_NO_ATTRIBUTE

Jul 1 08:42:50 machine acvpnagent[1785]: Function: Serialize File:/vpn/Common/TLV/CertificateInfoTlv.cpp Line: 799 Data to serialize is empty

Jul 1 08:42:50 machine acvpnagent[1785]: Function: Assign File:/vpn/Common/TLV/CertificateInfoTlv.cpp Line: 87 Invoked Function: CCertificateInfoTlv::Serialize Return Code: -21954549 (0xFEB1000B) Description: CERTIFICATEINFO_ERROR_NO_DATA:No certificate data was found

Jul 1 08:42:50 machine acvpnagent[1785]: Function: SetAggAuthCertificateInfo File:/vpn/AgentUtilities/vpnparam.cpp Line: 1165 Invoked Function: CCertificateInfoTlv::Assign Return Code: -21954549 (0xFEB1000B) Description: CERTIFICATEINFO_ERROR_NO_DATA:No certificate data was found

Jul 1 08:42:50 machine acvpnagent[1785]: Secure Gateway Parameters: Primary IP Address: 10.106.63.179 Secondary IP Address: N/A Domain name: bglanyconnect.cisco.com Port: 443 URL: "https://bglanyconnect.cisco.com:443/CACHE/stc/2/" Auth method: SSL Proxy Server: "

Jul 1 08:42:50 machine acvpnagent[1785]: Initiating Cisco AnyConnect Secure Mobility Client connection, version 4.6.03049

Jul 1 08:42:50 machine acvpnagent[1785]: Function: OnTunnelStateChange File:/vpn/Agent/TND.cpp Line: 2030 tunnel state change notification (new 0, old 4)

Jul 1 08:42:50 machine acvpnagent[1785]: Function: STLoadLibrary File:/vpn/Common/Utility/Win/HModuleMgr.cpp Line: 148 Invoked Function: dlopen Return Code: 0 (0x00000000) Description: libz.so: cannot open shared object file: No such file or directory

Jul 1 08:42:50 machine acvpnagent[1785]: Function: LoadLibrary File:/vpn/Agent/CZLib.cpp Line: 246 Invoked Function: CHModuleMgr::STLoadLibrary Return Code: -33554425 (0xFE000007) Description: GLOBAL_ERROR_NOT_INITIALIZED

Jul 1 08:42:50 machine acvpnagent[1785]: Function: CCstpProtocol File:/vpn/Agent/CstpProtocol.cpp Line: 327 Invoked Function: CZLib Return Code: -31981557 (0xFE18000B) Description: CZLIB_ERROR_LOAD_LIBRARY

Jul 1 08:42:50 machine acvpnagent[1785]: Function: findProfile File:


```
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 666 NSS Profile directory:
/home/tactest/.mozilla/firefox/6ai2dwqd.default
Jul 1 08:42:50 machine acvpnagent[1785]: Function: InitNSS File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 408 Invoked Function: NSS_Initialize
Return Code: -8015 (0xFFFFFE0B1) Description: unknown Unknown
Jul 1 08:42:50 machine acvpnagent[1785]: Function: CNSSCertStore File:
../../../../vpn/CommonCrypt/Certificates/NSSCertStore.cpp Line: 76 Invoked Function:
CNSSCertUtils::InitNSS Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnagent[1785]: Function: addNSSStore File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 1874 Invoked Function:
CNSSCertStore::CNSSCertStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnagent[1785]: Function: OpenStores File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 449 Invoked Function:
CCollectiveCertStore::addNSSStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnagent[1785]: The Primary SSL connection to the secure gateway is
being established.
Jul 1 08:42:50 machine acvpnagent[1785]: Function: OnTunnelStateChange File:
../../../../vpn/Agent/TND.cpp Line: 2030 tunnel state change notification (new 0, old 0)
Jul 1 08:42:50 machine acvpnagent[1785]: Function: postSocketConnectProcessing File:
../../../../vpn/Agent/SslTunnelTransport.cpp Line: 1421 Opened SSL socket from [10.106.44.166]:58980
to [10.106.63.179]:443
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.2702] manager: (cscotun0): new
Tun device (/org/freedesktop/NetworkManager/Devices/16)
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.2730] devices added (path:
/sys/devices/virtual/net/cscotun0, iface: cscotun0)
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.2730] device added (path:
/sys/devices/virtual/net/cscotun0, iface: cscotun0): no ifupdown configuration found.
Jul 1 08:42:50 machine acvpnagent[13620]: Function: findProfile File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 666 NSS Profile directory:
/home/tactest/.mozilla/firefox/6ai2dwqd.default
Jul 1 08:42:50 machine acvpnagent[13620]: Function: InitNSS File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 408 Invoked Function: NSS_Initialize
Return Code: -8015 (0xFFFFFE0B1) Description: unknown Unknown
Jul 1 08:42:50 machine acvpnagent[13620]: Function: CNSSCertStore File:
../../../../vpn/CommonCrypt/Certificates/NSSCertStore.cpp Line: 76 Invoked Function:
CNSSCertUtils::InitNSS Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnagent[13620]: Function: addNSSStore File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 1874 Invoked Function:
CNSSCertStore::CNSSCertStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnagent[13620]: Function: OpenStores File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 449 Invoked Function:
CCollectiveCertStore::addNSSStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnagent[13620]: Function: findProfile File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 666 NSS Profile directory:
/home/tactest/.mozilla/firefox/6ai2dwqd.default
Jul 1 08:42:50 machine acvpnagent[13620]: Function: InitNSS File:
../../../../vpn/CommonCrypt/Certificates/NSSCertUtils.cpp Line: 408 Invoked Function: NSS_Initialize
Return Code: -8015 (0xFFFFFE0B1) Description: unknown Unknown
Jul 1 08:42:50 machine acvpnagent[13620]: Function: CNSSCertStore File:
../../../../vpn/CommonCrypt/Certificates/NSSCertStore.cpp Line: 76 Invoked Function:
CNSSCertUtils::InitNSS Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnagent[13620]: Function: addNSSStore File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 1874 Invoked Function:
CNSSCertStore::CNSSCertStore Return Code: -31457269 (0xFE20000B) Description:
CERTSTORE_ERROR_PROVIDER_ERROR
Jul 1 08:42:50 machine acvpnagent[13620]: Function: OpenStores File:
../../../../vpn/CommonCrypt/Certificates/CollectiveCertStore.cpp Line: 449 Invoked Function:
```

CCollectiveCertStore::addNSSStore Return Code: -31457269 (0xFE20000B) Description: CERTSTORE_ERROR_PROVIDER_ERROR

Jul 1 08:42:50 machine acvpnagent[13620]: Function: init File: ../../vpn/Common/il8n/MsgCatalog.cpp Line: 373 initialized catalog: AnyConnect with locale:

Jul 1 08:42:50 machine acvpnagent[13620]: Function: loadProfiles File: ../../vpn/Api/ProfileMgr.cpp Line: 189 No profile is available.

Jul 1 08:42:50 machine acvpnagent[13620]: Function: invokePreferenceUpdateCBs File: ../../vpn/Api/PreferenceMgr.cpp Line: 1512 Callback interface address is NULL.

Jul 1 08:42:50 machine acvpnagent[13620]: Current Preference Settings: ServiceDisable: false ShowPreConnectMessage: false AutoConnectOnStart: false MinimizeOnConnect: true LocalLanAccess: false DisableCaptivePortalDetection: false AutoReconnect: true AutoUpdate: true ProxySettings: Native AllowLocalProxyConnections: true PPPEExclusion: Disable PPPEExclusionServerIP: AutomaticVPNPolicy: false TrustedNetworkPolicy: Disconnect UntrustedNetworkPolicy: Connect TrustedDNSDomains: TrustedDNSServers: TrustedHttpsServerList: EnableScripting: false TerminateScriptOnNextEvent: false EnableAutomaticServerSelection: false AuthenticationTimeout: 12 IPProtocolSupport: IPv4,IPv6 AllowManualHostInput: true BlockUntrustedServers: false PublicProxyServerAddress: CertificatePinning: false

Jul 1 08:42:50 machine acvpnagent[13620]: Using default preferences. Some settings (e.g. certificate matching) may not function as expected if a local profile is expected to be used. Verify that the selected host is in the server list section of the profile and that the profile is configured on the secure gateway.

Jul 1 08:42:50 machine acvpnagent[13620]: Function: GetCertificatePins File: ../../vpn/Api/PreferenceMgr.cpp Line: 1795 Invoked Function: ProfileMgr::GetProfileNameFromAddress Return Code: -26083317 (0xFE72000B) Description: PROFILEMGR_ERROR_HOST_ADDRESS_NOT_FOUND_IN_ANY_PROFILE Server address bglanyconnect.cisco.com not found in any profile.

Jul 1 08:42:50 machine acvpnagent[13620]: Function: verify_callback File: ../../vpn/CommonCrypt/Certificates/FileCertificate.cpp Line: 417 Invoked Function: X509_verify_cert Return Code: 0 (0x00000000) Description: ok

Jul 1 08:42:50 machine acvpnagent[13620]: Function: verify_callback File: ../../vpn/CommonCrypt/Certificates/FileCertificate.cpp Line: 417 Invoked Function: X509_verify_cert Return Code: 0 (0x00000000) Description: ok

Jul 1 08:42:50 machine acvpnagent[1785]: Function: verifyServerCertificate File: ../../vpn/Agent/CertOpenSSLAdapter.cpp Line: 834 certificate confirmation reason=0x0

Jul 1 08:42:50 machine acvpnagent[1785]: A SSL connection has been established using cipher ECDHE-RSA-AES256-GCM-SHA384

Jul 1 08:42:50 machine acvpnagent[1785]: Function: calculateTunnelMTU File: ../../vpn/Agent/CstpProtocol.cpp Line: 2846 The candidate MTU (1399) is derived from the physical interface MTU.

Jul 1 08:42:50 machine acvpnagent[1785]: Function: startHTTPNegotiation File: ../../vpn/Agent/CstpProtocol.cpp Line: 1018 Proposed base MTU is 1500.

Jul 1 08:42:50 machine acvpnagent[1785]: Current Profile: none Received VPN Session Configuration Settings: Keep Installed: enabled Rekey Method: disabled Proxy Setting: do not modify Proxy Server: none Proxy PAC URL: none Proxy Exceptions: none Proxy Lockdown: enabled IPv4 Split Exclude: disabled IPv6 Split Exclude: disabled IPv4 Dynamic Split Exclude: disabled IPv6 Dynamic Split Exclude: disabled IPv4 Split Include: 1 IPv4 private networks IPv6 Split Include: disabled IPv4 Dynamic Split Include: disabled IPv6 Dynamic Split Include: disabled IPv4 Split DNS: disabled IPv6 Split DNS: disabled Tunnel all DNS: disabled IPv4 Local LAN Wildcard: local LAN access preference is disabled IPv6 Local LAN Wildcard: local LAN access preference is disabled Firewall Rules: none Client Address: 192.168.100.1 Client Mask: 255.255.255.0 Client IPv6 Address: FE80:0:0:0:72F5:2CAF:BCCC:5145 (auto-generated) Client IPv6 Mask: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFC TLS MTU: 1367 TLS Compression: disabled TLS Keep Alive: 20 seconds TLS Rekey Interval: none TLS DPD: 30 seconds DTLS: enabled DTLS MTU: 1406 DTLS Compression: disabled DTLS Keep Alive: 20 seconds DTLS Rekey Interval: none DTLS DPD: 30 seconds Session Timeout: none Session Timeout Alert Interval: 60 seconds Session Timeout Remaining: none Disconnect Timeout: 1800 seconds Idle Timeout: 1800 seconds Server: ASA (9.9(2)36) MUS Host: unknown DAP User Message: none Quarantine State: disabled Always On VPN: not disabled Lease Duration: 1209600 seconds Default Domain: cisco.com Home page: unknown Smart Card Removal Disconnect: enabled License Response: unknown SG TCP Keep Alive: enabled Peer's Local IPv4 Address: N/A Peer's Local IPv6 Address: N/A Peer's Remote IPv4 Address: N/A Peer's Remote IPv6 Address: N/A Peer's host name: bglanyconnect.cisco.com Client Protocol Bypass: false

Jul 1 08:42:50 machine acvpnagent[1785]: The Primary SSL connection to the secure gateway has been established.

```
Jul 1 08:42:50 machine acvpnagent[1785]: Function: OnTunnelStateChange File:
../../vpn/Agent/TND.cpp Line: 2030 tunnel state change notification (new 0, old 0)
Jul 1 08:42:50 machine acvpnagent[1785]: Function: addSplitIncludeNetworksForTunnelDnsServers
File: ../../vpn/Agent/VpnMgr.cpp Line: 1108 Added split-include network for tunnel DNS server
10.10.10.99
Jul 1 08:42:50 machine acvpnagent[1785]: VPN Adapter Configuration: IPv4 address:
192.168.100.1/24 IPv6 address: FE80:0:0:0:72F5:2CAF:BCCC:5145/126 (auto-generated) Default
domain: cisco.com DNS suffixes: N/A DNS servers: 10.10.10.99 WINS servers: N/A MTU: 1406
Jul 1 08:42:50 machine acvpnagent[1785]: Host Configuration: Public address: 10.106.44.166/24
Potential public addresses: 10.106.44.166 Private Address: 192.168.100.1/24 Private IPv6
Address: FE80:0:0:0:72F5:2CAF:BCCC:5145/126 (auto-generated) Remote Peers: 10.106.63.179 (TCP
port 443, UDP port 443, source address 10.106.44.166) Private Networks: 2 (10.0.0.0/24,
10.10.10.99/32) Private IPv6 Networks: none Public Networks: none Public IPv6 Networks: none
Tunnel Mode: yes Tunnel all DNS: no
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3025] device (cscotun0): state
change: unmanaged -> unavailable (reason 'connection-assumed') [10 20 41]
Jul 1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: Checking for
product updates...
Jul 1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: Checking for
customization updates...
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3046] keyfile: add connection
in-memory (c9f1c86e-5e5c-4966-8260-be7e751b642d,"cscotun0")
Jul 1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: Performing
any required updates...
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3051] device (cscotun0): state
change: unavailable -> disconnected (reason 'connection-assumed') [20 30 41]
Jul 1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: The
AnyConnect Downloader updates have been completed.
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3058] device (cscotun0):
Activation: starting connection 'cscotun0' (c9f1c86e-5e5c-4966-8260-be7e751b642d)
Jul 1 08:42:50 machine acvpnui[11774]: VPN state: Connecting Network state: Network Accessible
Network control state: Network Access: Available Network type: Undefined
Jul 1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: Establishing
VPN session...
Jul 1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: Establishing
VPN - Initiating connection...
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3064] device (cscotun0): state
change: disconnected -> prepare (reason 'none') [30 40 0]
Jul 1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: Establishing
VPN - Examining system...
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3067] device (cscotun0): state
change: prepare -> config (reason 'none') [40 50 0]
Jul 1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: Establishing
VPN - Activating VPN adapter...
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3068] device (cscotun0): state
change: config -> ip-config (reason 'none') [50 70 0]
Jul 1 08:42:50 machine acvpnui[11774]: Message type information sent to the user: Establishing
VPN - Configuring system...
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3070] device (cscotun0): state
change: ip-config -> ip-check (reason 'none') [70 80 0]
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3073] device (cscotun0): state
change: ip-check -> secondaries (reason 'none') [80 90 0]
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3075] device (cscotun0): state
change: secondaries -> activated (reason 'none') [90 100 0]
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.3111] device (cscotun0):
Activation: successful, device activated.
Jul 1 08:42:50 machine dbus[935]: [system] Activating via systemd: service
name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm_dispatcher.service'
Jul 1 08:42:50 machine systemd[1]: Starting Network Manager Script Dispatcher Service...
Jul 1 08:42:50 machine dbus[935]: [system] Successfully activated service
'org.freedesktop.nm_dispatcher'
Jul 1 08:42:50 machine systemd[1]: Started Network Manager Script Dispatcher Service.
Jul 1 08:42:50 machine nm-dispatcher: req:1 'up' [cscotun0]: new request (1 scripts)
Jul 1 08:42:50 machine nm-dispatcher: req:1 'up' [cscotun0]: start running ordered scripts...
```

```
Jul 1 08:42:50 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface ens32.
Jul 1 08:42:50 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface cscotun0.
Jul 1 08:42:50 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface ens32.
Jul 1 08:42:50 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface ens32.
Jul 1 08:42:50 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface cscotun0.
Jul 1 08:42:50 machine NetworkManager[940]: <info> [1561984970.6920] policy: set 'cscotun0'
(cscotun0) as default for IPv6 routing and DNS
Jul 1 08:42:51 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface ens32.
Jul 1 08:42:51 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface cscotun0.
Jul 1 08:42:51 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface ens32.
Jul 1 08:42:51 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface ens32.
Jul 1 08:42:51 machine systemd[1]: Reloading OpenBSD Secure Shell server.
Jul 1 08:42:51 machine systemd[1]: Reloaded OpenBSD Secure Shell server.
Jul 1 08:42:51 machine acvpnagent[1785]: Function: getDnsConfiguration File:
../../../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1247 Unable to get domain list for
interface cscotun0.
Jul 1 08:42:52 machine acvpnagent[1785]: Function: applyFirewallConfiguration File:
../../../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 1187 No Firewall Rules to configure
Jul 1 08:42:52 machine acvpnagent[1785]: The network control state changed to restricted.
Jul 1 08:42:52 machine acvpnui[11774]: Message type information sent to the user: Establishing
VPN...
Jul 1 08:42:52 machine acvpnui[11774]: Function: setSessionInfo File:
../../../../vpn/Api/VPNStatsBase.cpp Line: 1097 Invoked Function:
CSessionInfoTlv::GetAppliedSecureRouteCount Return Code: -32440304 (0xFE110010) Description:
TLV_ERROR_NO_ATTRIBUTE
Jul 1 08:42:52 machine acvpnui[11774]: Function: setSessionInfo File:
../../../../vpn/Api/VPNStatsBase.cpp Line: 1204 Invoked Function:
CSessionInfoTlv::GetAppliedNonsecureRouteCount Return Code: -32440304 (0xFE110010) Description:
TLV_ERROR_NO_ATTRIBUTE
Jul 1 08:42:52 machine acvpnui[11774]: VPN state: Connected Network state: Network Accessible
Network control state: Network Access: Restricted Network type: Undefined
Jul 1 08:42:52 machine acvpnui[11774]: Using default preferences. Some settings (e.g.
certificate matching) may not function as expected if a local profile is expected to be used.
Verify that the selected host is in the server list section of the profile and that the profile
is configured on the secure gateway.
Jul 1 08:42:52 machine acvpnui[11774]: Function: getProfileNameFromHost File:
../../../../vpn/Api/ProfileMgr.cpp Line: 1250 No profile available for host bglanyconnect.cisco.com.
Jul 1 08:42:52 machine acvpnui[11774]: Function: getHostInitSettings File:
../../../../vpn/Api/ProfileMgr.cpp Line: 1334 Profile () not found. Using default settings.
Jul 1 08:42:52 machine acvpnui[11774]: Message type information sent to the user: Connected to
bglanyconnect.cisco.com.
Jul 1 08:42:52 machine acvpnagent[1785]: Function: OnTunnelStateChange File:
../../../../vpn/Agent/TND.cpp Line: 2030 tunnel state change notification (new 1, old 0)
Jul 1 08:42:52 machine acvpnagent[1785]: The VPN connection has been established and can now
pass data.
Jul 1 08:42:52 machine acvpnagent[1785]: The Primary DTLS connection to the secure gateway is
```

```

being established.
Jul  1 08:42:52 machine acvpnagent[1785]: Function: OnTunnelStateChange File:
../../../../vpn/Agent/TND.cpp Line: 2030 tunnel state change notification (new 1, old 1)
Jul  1 08:42:52 machine acvpnagent[1785]: Function: initiateTransport File:
../../../../vpn/Agent/DtlsTunnelTransport.cpp Line: 238 Opened DTLS socket from [10.106.44.166]:35312
to [10.106.63.179]:443
Jul  1 08:42:52 machine acvpndownloader[13609]: Function: WaitForCompletion File:
../../../../vpn/Common/Utility/Thread.cpp Line: 311 The thread has successfully completed execution.
Jul  1 08:42:52 machine acvpndownloader[13609]: Cisco AnyConnect Secure Mobility Client
Downloader (VPN) exiting, version 4.6.03049 , return code 0 [0x00000000]
Jul  1 08:42:52 machine acvpnagent[1785]: A routing table change notification has been received.
Starting automatic correction of the routing table.
Jul  1 08:42:52 machine acvpnagent[1785]: Automatic correction of the routing table has been
successful.
Jul  1 08:42:52 machine acvpnagent[1785]: Function: OnIpcMessageReceived File:
../../../../vpn/Common/IPC/IPCDepot.cpp Line: 1115 Invoked Function:
CIpcTransport::OnSocketReadComplete Return Code: -33292279 (0xFE040009) Description:
IPCTransport_ERROR_UNEXPECTED
Jul  1 08:42:52 machine acvpnagent[1785]: Function: writeSocketBlocking File:
../../../../vpn/Common/IPC/UdpTcpTransports_unix.cpp Line: 429 Invoked Function: ::write Return Code:
32 (0x00000020) Description: unknown
Jul  1 08:42:52 machine acvpnagent[1785]: Function: terminateIpcConnection File:
../../../../vpn/Common/IPC/IPCTransport.cpp Line: 459 Invoked Function:
CSocketTransport::writeSocketBlocking Return Code: -31588341 (0xFE1E000B) Description:
SOCKETTRANSPORT_ERROR_WRITE
Jul  1 08:42:52 machine acvpnagent[1785]: A DTLS connection has been established using cipher
DHE-RSA-AES256-SHA
Jul  1 08:42:52 machine acvpnagent[1785]: The Primary DTLS connection to the secure gateway has
been established.
Jul  1 08:42:52 machine acvpnui[11774]: Function: launchCachedDownloader File:
../../../../vpn/Api/ConnectMgr.cpp Line: 8274 Invoked Function: ConnectMgr::launchCachedDownloader
Return Code: 0 (0x00000000) Description: Cached Downloader terminated normally
Jul  1 08:42:52 machine acvpnui[11774]: Using default preferences. Some settings (e.g.
certificate matching) may not function as expected if a local profile is expected to be used.
Verify that the selected host is in the server list section of the profile and that the profile
is configured on the secure gateway.
Jul  1 08:42:52 machine acvpnui[11774]: Function: getProfileNameFromHost File:
../../../../vpn/Api/ProfileMgr.cpp Line: 1250 No profile available for host bglanyconnect.cisco.com.
Jul  1 08:42:52 machine acvpnui[11774]: message repeated 2 times: [ Function:
getProfileNameFromHost File: ../../vpn/Api/ProfileMgr.cpp Line: 1250 No profile available for
host bglanyconnect.cisco.com.]
Jul  1 08:42:52 machine acvpnui[11774]: Function: reloadPreferencesAfterUpdates File:
../../../../vpn/Api/ConnectMgr.cpp Line: 10859 Secure gateway (bglanyconnect.cisco.com) was not found
in profile .
Jul  1 08:42:52 machine acvpnui[11774]: Function: getProfileNameFromHost File:
../../../../vpn/Api/ProfileMgr.cpp Line: 1250 No profile available for host bglanyconnect.cisco.com.
Jul  1 08:42:52 machine acvpnui[11774]: Function: getHostInitSettings File:
../../../../vpn/Api/ProfileMgr.cpp Line: 1334 Profile () not found. Using default settings.
Jul  1 08:42:52 machine acvpnui[11774]: Function: getProfileNameFromHost File:
../../../../vpn/Api/ProfileMgr.cpp Line: 1250 No profile available for host bglanyconnect.cisco.com.
Jul  1 08:42:52 machine acvpnui[11774]: Function: getHostInitSettings File:
../../../../vpn/Api/ProfileMgr.cpp Line: 1334 Profile () not found. Using default settings.
Jul  1 08:42:52 machine acvpnui[11774]: VPN state: Connected Network state: Network Accessible
Network control state: Network Access: Restricted Network type: Undefined
Jul  1 08:42:52 machine acvpnagent[1785]: Function: OnTunnelStateChange File:
../../../../vpn/Agent/TND.cpp Line: 2030 tunnel state change notification (new 1, old 1)
Jul  1 08:42:53 machine systemd[1]: Reloading OpenBSD Secure Shell server.
Jul  1 08:42:53 machine systemd[1]: Reloaded OpenBSD Secure Shell server.
Jul  1 08:42:53 machine acvpnui[11774]: Message type information sent to the user: Connected to
bglanyconnect.cisco.com.

```

- **DART (Diagnostic and Reporting Tool) on Linux Client**

Similar to Windows and MAC, the Linux client also has DART functionality. This can be used either by the GUI or CLI.

DART needs to be run as an admin user in order to collect complete logs on a Linux client.

1. DART can be executed from the command line by navigation to this path:

```
tactest:bin$ cd /opt/cisco/anyconnect/dart
tactest:dart$ ls
anyconnect-linux64-4.6.03049-dart-webdeploy-k9-20190627095410.log  dartui      xml
dartcli                                                            resources
tactest:dart$ ./dartcli

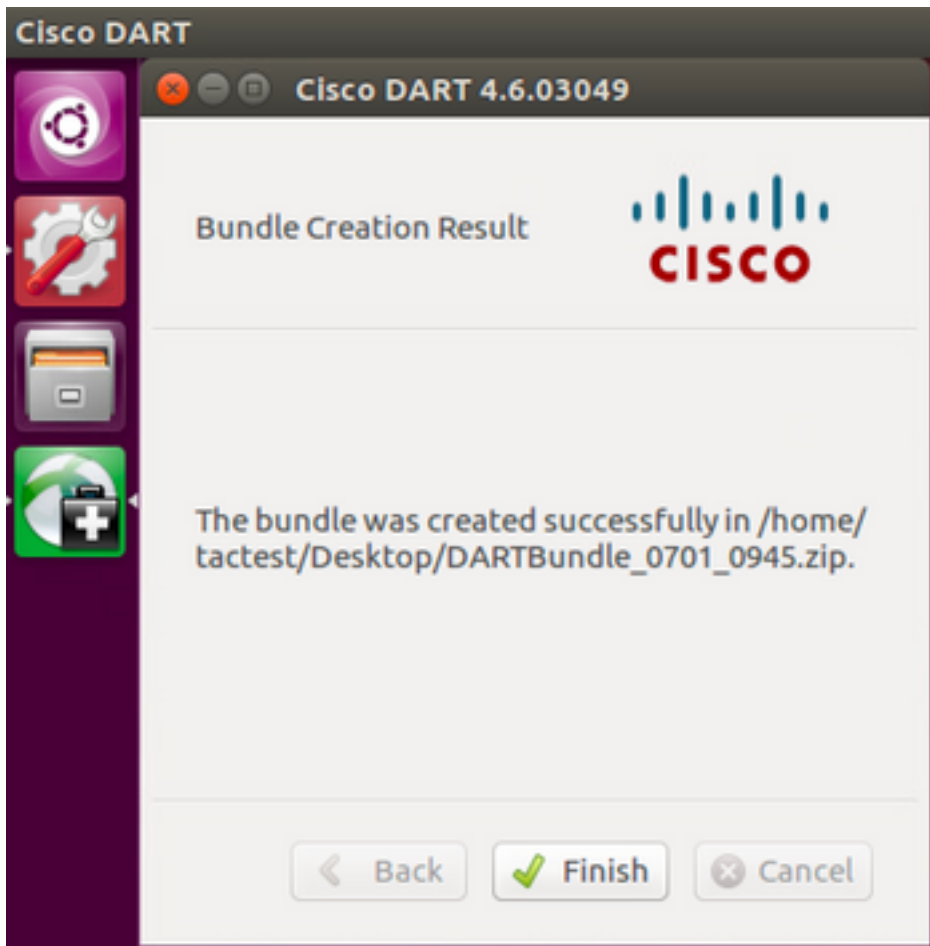
Cisco AnyConnect Diagnostic and Reporting Tool 4.6.03049 .

Copyright (c) 2008 - 2018 Cisco Systems, Inc.
All Rights Reserved.

Bundle option selected: default
Bundle location: /home/tactest/Desktop/DARTBundle_0701_0933.zip

Parsing request and configuration XMLs...          1%iptables v1.6.0: can't initialize
iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
ip6tables v1.6.0: can't initialize ip6tables table `filter': Permission denied (you must be
root)
Perhaps ip6tables or your kernel needs to be upgraded.
Processing Posture application logs...              76%sh: 1:
/home/tactest/.cisco/hostscan/lib/wadiagnose: not found
sh: 1: /opt/cisco/hostscan/lib/wadiagnose: not found
DART has finished...                            100%
```

2. To execute DART from GUI, search for **anyconnect** on the Linux GUI and click **Cisco DART** and perform the instructions. The collected DART bundle is stored on the desktop.



3. To copy the DART bundle from the Linux client to your workstation, use the command:

```
scp username@10.106.44.166:/home/<username>/Desktop/DARTBundle_0701_0945.zip /Users/dmoudgil/Desktop/Ubuntu/
```

Here is a document for reference to DART on different OS: [How to collect the DART bundle for Anyconnect](#)

- In case of any unknown issues, VPN client can be restarted by this command line:

```
tactest:bin$ sudo /etc/init.d/vpnagentd restart  
[sudo] password for tactest:  
[ ok ] Restarting vpnagentd (via systemctl): vpnagentd.service.  
tactest:bin$
```