Table of Contents

Cisco Secure VPN Client: Troubleshooting with View Log

Document ID: 14127

Introduction

This document describes Cisco Secure VPN Client View Log messages and explains how to use the View Log messages to troubleshoot problems with establishing IPSec communications. The user must enable the View Log before logging occurs. Log files can be saved to a disk for future analysis.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco Secure VPN Client 1.1.

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

View Log Message Format

Two types of messages can appear in the View Log: error messages and Internet Key Exchange (IKE) messages. Error messages are defined in the Cisco Secure VPN Client View Log error message table. The format of the IKE message is as follows:

TIME	Connection Name	Transmit direction	IKE Message

The following example is a typical message from the View Log:

```
01:38:02.570 Balt Corporate Access − SENDING>>>> ISAKMP OAK MM (SA)
```

View Log Field	Field Definition	Example
Time	Time the message is written to the log.	`01:38:02.570`
Connection Name	Policy Editor Connection name associated with the IKE activity.	`Balt Corporate Access`
Transmit Direction	Direction of the IKE message (Sending or Receiving).	`SENDING>>>>`
IKE Message	IKE message indicating type of Internet Security Association and Key Management Protocol (ISAKMP) message being processed. IKE messages are defined in the Cisco Secure VPN Client View Log IKE message table.	`ISAKMP OAK MM (SA)`

Troubleshooting with the View Log

The following table lists different scenarios and the accompanying debug messages. You can refer to this information when interpreting the View Log file. Use this table in conjunction with the Cisco Secure VPN Client View Log IKE Message table.

Successful IKE Establishment

If the IKE establishment is successful, a key is displayed in the Cisco Secure VPN Client icon (located on the Taskbar at the bottom of your screen).

Description	Problem Symptoms	Debug Messages
Successful main mode negotiation (pre−share)	Successful Security Association (SA) established. Key is displayed in Cisco Secure VPN Client icon.	Pre−share − Initiating IKE Phase 1 (IP ADDR=IPSec peer) Pre−share − SENDING>>>> ISAKMP OAK MM (SA) Pre−share − RECEIVED<<< ISAKMP OAK MM (SA) Pre−share − SENDING>>>> ISAKMP OAK MM (KE, NON, VID, VID) Pre−share − RECEIVED<<< ISAKMP OAK MM (KE, NON) Pre−share − SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT) Pre−share − RECEIVED<<< ISAKMP OAK MM *(ID, HASH) Pre−share − Established IKE SA MY COOKIE 1f f5 e4 d 84 30 f9 5c HIS COOKIE 4c af 1f 2c 20 16 d0 ec Pre−share − Initiating IKE Phase 2 with Client IDs (message id: 61965C8D) Initiator = IP ADDR= your_address, prot = 0 port = 0 Responder = IP ADDR= IPSec peer, prot = 0 port = 0 Pre−share − SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) Pre−share − RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NOTIFY:STATUS_RESP_LIFETIME, NON, ID, ID) Pre−share − SENDING>>>> ISAKMP OAK QM *(HASH) Pre−share − RECEIVED<<< ISAKMP OAK QM *(HASH, NOTIFY:NOTIFY_CONNECTED) Pre−share − Loading IPSec SA (Message ID = 61965C8D OUTBOUND SPI = 405 INBOUND SPI = 493B30CC)
Successful aggressive mode negotiation (pre−share)	Successful SA established. Key is displayed in Cisco Secure VPN Client icon.	Pre−share − Initiating IKE Phase 1 (IP ADDR= IPSec peer) Pre−share − SENDING>>>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID) Pre−share − RECEIVED<<< ISAKMP OAK AG (SA, KE, NON, ID, HASH) Pre−share − SENDING>>>> ISAKMP OAK AG *(HASH) Pre−share − Established IKE SA MY COOKIE 73 9c 76 19 4f 5e 35 c8 HIS COOKIE e9 94 9c 82 64 b2 fa 44 Pre−share − Initiating IKE Phase 2 with Client IDs (message id: 99F08C75) Initiator = IP ADDR= your_address, prot = 0 port = 0 Responder = IP ADDR= IPSec peer, prot = 0 port = 0 Pre−share − SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) Pre−share − RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NOTIFY:STATUS_RESP_LIFETIME, NON, ID, ID) Pre−share − SENDING>>>> ISAKMP OAK QM *(HASH) Pre−share − RECEIVED<<< ISAKMP OAK QM *(HASH, NOTIFY:NOTIFY_CONNECTED) Pre−share − Loading IPSec SA (Message ID = 99F08C75 OUTBOUND SPI = 189 INBOUND SPI = BA78A2CD)

Failed IKE Establishment

If IKE establishment fails, the key is not displayed in the Cisco Secure VPN Client icon (located on the Taskbar at the bottom of your screen).

Description	Possible Cause	Debug Messages
IPSec peer not responding.	Remote peer unreachable or not responding to SA request. Verify that IP connectivity	Demo − Initiating IKE Phase 1 (IP ADDR=IPSec peer) Demo − SENDING>>>> ISAKMP OAK MM (SA) Demo − message not received! Retransmitting! Demo − SENDING>>>> ISAKMP OAK MM (Retransmission) Demo − message not received! Retransmitting! Demo − SENDING>>>> ISAKMP OAK MM (Retransmission) Demo − message not received! Retransmitting!

	exists to the local router and then to the IPSec peer.	Demo − SENDING>>>> ISAKMP OAK MM (Retransmission) Demo − Exceeded 3 IKE SA negotiation attempts
Failed Quick Mode (QM) negotiation.	Improper IPSec peer configuration. The VPN Client was configured for three re−transmissions to establish SA.	Demo − Initiating IKE Phase 1 (IP ADDR=IPSec peer) Demo − SENDING>>>> ISAKMP OAK MM (SA) Demo − RECEIVED<<< ISAKMP OAK MM (SA) Demo − SENDING>>>> ISAKMP OAK MM (KE, NON, VID, VID) Demo − RECEIVED<<< ISAKMP OAK MM (KE, NON) Demo − SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT) Demo − RECEIVED<<< ISAKMP OAK MM *(ID, HASH) Demo − Established IKE SA MY COOKIE 1f f5 e4 d 84 30 f9 5c HIS COOKIE 4c AF 1f 2c 20 16 d0 EC Demo − Initiating IKE Phase 2 with Client IDs (message id: 61965C8D) Initiator = IP ADDR= your_address, prot = 0 port = 0 Responder = IP ADDR= IPSec peer, prot = 0 port = 0 Demo − SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) Demo − RECEIVED<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN) Received NO_PROPOSAL_CHOSEN message Demo − SENDING>>>> ISAKMP OAK QM *(Retransmission) Demo − RECEIVED<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN) Received NO_PROPOSAL_CHOSEN message Demo − SENDING>>>> ISAKMP OAK QM *(Retransmission) Demo − RECEIVED<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN) Received NO_PROPOSAL_CHOSEN message Demo − SENDING>>>> ISAKMP OAK QM *(Retransmission) Demo − RECEIVED<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN) Received NO_PROPOSAL_CHOSEN message Exceeded retry attempts − deleting IPSec Security Association

IKE Message Table

IKE Message	Description	Explanation
ISAKMP OAK MM (SA)	Proposed parameters for securing sensitive exchange messages.	ISAKMP proposal list exchange. Each proposal has a setting for encryption algorithm, hash algorithm and Diffie−Hellman Group. The agreed−upon settings are used to protect the final messages

		of Main Mode (MM) and all of Quick Mode (QM). If the settings are not compatible, a "NO PROPOSAL" message is displayed.
ISAKMP OAK MM (KE, NON)	Diffie−Hellman exchanged and nonce used as key material for securing sensitive exchange messages.	ISAKMP Diffie−Hellman key exchange with nonce. The key (KE) is created by each party using an agreed−upon formula, plugging values in the formula, and raising the result of the formula to the power of a secret value. As each party knows their secret exponent, they can take the KE received from the other party and raise that by their exponent. When each party performs this procedure, they get a shared secret key. The nonce (NON) is a "nonsense" random value used in the calculation to add randomness to the KE.
ISAKMP OAK MM *(ID, HASH)	Party's identity used as authentication and a	ISAKMP message containing the identity one

	calculated hash as assurance of identification.	party is using as identification (ID) to the other. This could be the IP address, domain name, e−mail address, or distinguished name. That identity would have to be accepted by the receiving party for a positive identification. The hash (HASH) is created by selecting bits of the message as samples and sending those selected bits through an algorithm. The pattern for selection and the algorithm are agreed upon in the MM proposal exchange as the hash algorithm setting. This message, one of the final MM messages, is protected, encrypted and hashed, as denoted by the asterisk (*).
ISAKMP OAK QM *(HASH, SA, NON, ID, ID)	Proposed parameters for securing the IP data, the two parties' identification, and nonces for a non−PFS	IPSec exchange message containing a hash of the message contents (HASH) a list of the proposed

	exchange.	parameters to be used on the user's data, SA, each party's nonce (NON) and each party's ID. The parameters agreed−upon are IPSec protocol (Encapsulation Security Protocol [ESP] or Authentication Header [AH]), encryption algorithm (if ESP is to be used), hash algorithm, and if tunneling is to be performed. Hash algorithms and tunneling settings are for either ESP or AH. This message was sent by the responder in an IKE that did not use Perfect Forward Secrecy (PFS) as their were no KE's. This means the parties will reuse some of the agreed−upon key in the calculation of the IPSec key. This message is secured using the agreed−upon ISAKMP parameters and key as denoted by the asterisk (*).

ISAKMP OAK QM *(HASH)	Conclusion of the QM exchange containing a hash of the agreed−upon key, protocol, the responder's SPI, and the two nonces.	IPSec message used to finalize the entire exchange. This also provides a form of verification as the hash is calculated using the IPSec key, IPSec protocol agreed−upon, the other party's Security Parameter Index (SPI) number, and the two nonces each party used. Each party uses the SPI to keep track of the parameters and keys to be used for the traffic they send and receive. I would tell you my SPI so when you transmit a protected message to me I know how to handle the message properly, and vice versa. This message is secured using the agreed−upon ISAKMP parameters and key as denoted by the asterisk (*).
ISAKMP OAK MM (KE, NON, VID)	Diffie−Hellman exchanged and nonce used as key material for securing sensitive	ISAKMP message containing a Diffie−Hellman key (KE), nonce used to add

	exchange messages and the product vendor ID.	randomness to the key, and a Vendor ID (VID) used to notify the receiver of the transmitting party's vendor. This can be used to determine what the transmitter's capabilities are and allow parameter preferences to be made, as well as determining if the connection should be established.
ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN)	Exchange has failed because the QM exchange parameters were incompatible.	IPSec message sent when the list of proposed parameters did not have any common settings for the transmitter. This means the IPSec parameters for each party need to be verified. This message is secured using the agreed−upon ISAKMP parameters and key as denoted by the asterisk (*).
ISAKMP OAK QM *(Retransmission)	A previously sent message is sent once more because no response was received in the allotted time.	IPSec message sent when a previous message was not responded to within the configured amount of time. This indicates that one of the

		parties may be unavailable to complete the exchange. This message is secured using the agreed−upon ISAKMP parameters and key as denoted by the asterisk (*).

How IKE Works

The following steps explain how IKE functions:

1. In Phase 1, ID and parameters are established for protecting Phase 2.

   Device A sends a list of proposed parameters to protect the Phase 2 key exchange and the level of key strength it would like to use for Phase 1's key exchange.
2. Device B selects the proposed parameters it prefers and send its selection to Device A.

   If none of the proposals fit Device A's requirements, then a "NO PROPOSAL" message is sent and the exchange ceases. The two parties need to be reconfigured to work.
3. If the exchange continues, Device A calculates a number ax where a is known by each device and x is a random number known only by Device A.

   The NON is a random number thrown into the calculation to add randomness.
4. Device B receives that message and performs a similar calculation.
5. Both sides exchange identification. Alternate Subject Fields can be used as ID, for example, IP address, e−mail address and domain name.

   The ID field contains the information the party is using to identify itself. This could be any of the ID types, such as IP address, domain name, and so forth.
6. If either side fails to accept the other's ID, then the exchange ceases and the two parties need to be reconfigured to work.

   If both sides have accepted the other's ID, Phase 1 is completed and Phase 2 begins.
7. Phase 2 combines some Phase 1 steps.

   A list of proposed parameters is sent from Device A using the new key material established in Phase 1.
8. Phase 2 concludes with a HASH which is the IDs and NONs of each device and the Responder's (Device B in this case) SPI to use when sending packets.

IKE Example

```
Device A                                                      Device B

Phase 1 − Authentication
```

```
1. MM −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−ðÝ
      SA(Security Association) DES/SHA−1/DHG1; TDES/SHA−1/DHG2

2.    <−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− MM
      SA: TDES/SHA−1/DHG

3. MM −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−ðÝ
      KE (Diffie−Hellman a^x), NON (nonsense, random number)

4.    <−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− MM
      KE (Diffie−Hellman a^y), NON (nonsense, random number)

5. MM −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−ðÝ
      ID (the identification of one party), HASH


6.    <−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− MM
      ID, HASH

****************************** Phase 1 Completed ****************************

Phase 2 − Key Exchange (with Perfect Forward Secrecy (PFS))

1. QM −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−ðÝ
      SA: ESP/DES/SHA−1; ESP/TDES/SHA−1; AH/MD5, KE, NON

2.    <−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−− QM
      SA: ESP/TDES/SHA−1, KE, NON

3. QM −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−ðÝ
HASH
```

Related Information

- **IPSec Support Page**
- **Cisco VPN Client Support Page**
- **Cisco Secure VPN Client documentation**
- **Technical Support − Cisco Systems**

Updated: Sep 13, 2005 Document ID: 14127