Risoluzione dei problemi di errore ISE 3.3 "SNS 37xx servizi non sono in grado di inizializzare"

Sommario

Introduzione

Prerequisiti

- Premesse
- Componenti richiesti

Sintomi (Messaggi di errore)

Causa principale

Registri necessari

Analisi del registro

Introduzione

Questo documento descrive l'importanza del TPM (Trusted Platform Module) per ISE 3.3 e versioni successive.

Prerequisiti

È necessario avere le conoscenze base di Cisco Identity Service Engine (ISE).

Premesse

Un TPM (Trusted Platform Module) è un chip (microcontroller) in grado di archiviare in modo sicuro gli elementi utilizzati per autenticare la piattaforma (server).

Tali elementi possono includere password, certificati o chiavi di crittografia. È inoltre possibile utilizzare un TPM per archiviare le misure della piattaforma che consentono di garantire l'attendibilità della piattaforma.

L'autenticazione (che garantisce che la piattaforma possa dimostrare di essere ciò che afferma di essere) e l'attestazione (un processo che aiuta a dimostrare che una piattaforma è affidabile e non è stata violata) sono passaggi necessari per garantire un'elaborazione più sicura in tutti gli ambienti. Uno switch anti-intrusione per lo chassis fornisce una notifica di accesso meccanico non autorizzato al server.

A partire dalla versione 3.3, il modulo TPM è necessario per inizializzare i servizi ISE.

ISE TPM Framework è costituito da due servizi, ovvero Key Manager e TPM Manager.

Gestione chiavi

Il sottosistema KeyManager è il componente principale che gestisce i segreti, le chiavi in un nodo. Ciò implica la generazione di chiavi, la sigillatura/crittografia delle chiavi, la rimozione/decrittografia delle chiavi, l'accesso alle chiavi e così via.
Il gestore delle chiavi mantiene un riferimento, per nome, di tutti i segreti che sta gestendo. I segreti e le chiavi non vengono mai archiviati sul disco da Key Manager. Durante il processo, i segreti di bootstrap vengono recuperati dal TPM tramite Gestione TPM e rimangono nella memoria del processo.

Gestione TPM

Il gestore TPM è l'unico responsabile dell'inizializzazione del TPM, della sigillatura/rimozione del sealing o della crittografia/decrittografia dei segreti e dell'archiviazione sicura dei segreti. Gestione TPM non archivia mai alcun segreto/chiave in chiaro sul disco. Nel caso sia necessario archiviare chiave/segreto nel disco, la chiave/il segreto viene crittografata con la chiave del TPM e archiviata in forma crittografata. Gestione TPM consente di mantenere le chiavi e i segreti correlati alle informazioni, ad esempio nome, data e utente, in un file locale.

Componenti richiesti

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware

- Cisco Identity Service Engine 3.3
- Appliance SNS 3715

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Sintomi (Messaggi di errore)

L'installazione di ISE 3.3 su un sistema 37xx ha esito positivo e i servizi non vengono inizializzati dopo la configurazione iniziale della rete.

Il problema può essere osservato nel nuovo SNS 37xx quando si installa 3.3 FCS o durante l'aggiornamento 3.3 da qualsiasi altra versione o durante l'installazione delle patch di 3.3 FCS

Causa principale

Il modulo TPM deve essere abilitato in SNS perché la versione 3.3 (e successive) convalida il modulo TPM. Se è disattivato, il TPM non viene inizializzato e di conseguenza non è possibile inizializzare i servizi.

Registri necessari

Dalla CLI,

Con questo tipo di problemi, si dispone dell'accesso SSH per raccogliere il bundle di supporto dalla CLI.

Il log esatto richiesto è ade/ADE.log.

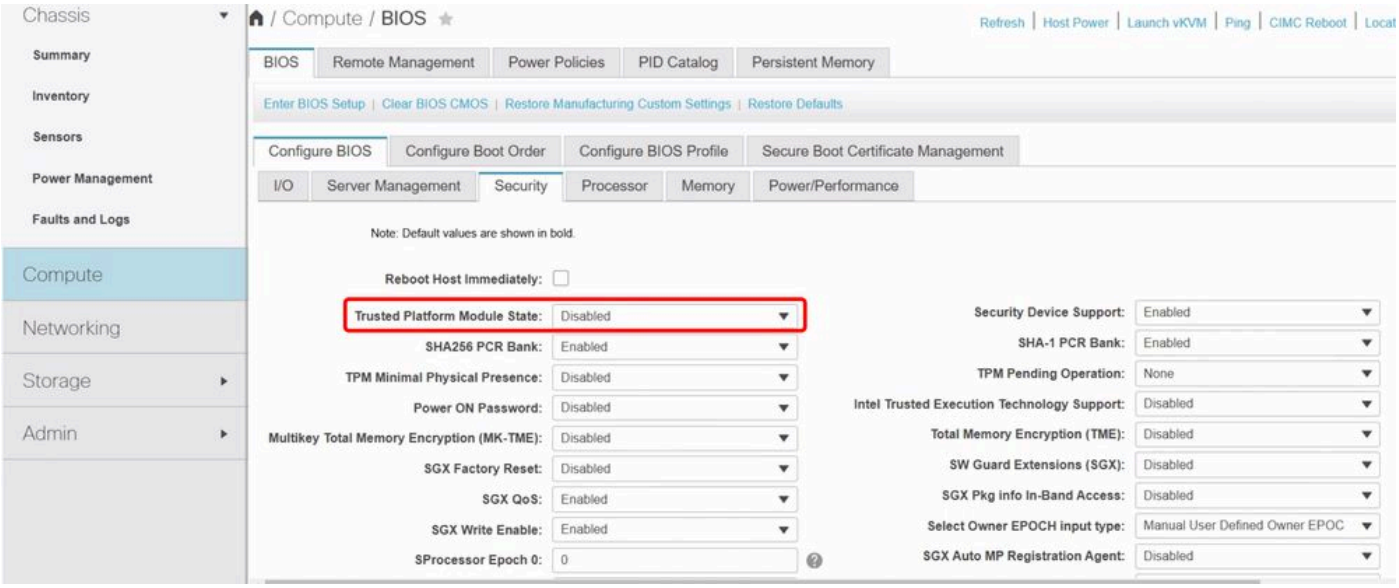
show logging system ade/ADE.log

Analisi del registro

Studio del caso 1

Causa principale: "Il modulo TPM non è abilitato."

In CIMC Compute>BIOS> Configure BIOS> Security> Trusted Platform Module State-Disabled



TPM disabilitato

La maggior parte dei servizi non è in esecuzione.

admin#show application status ise

ISE NOME PROCESSO STATO ID PROCESSO

—

Listener del database con 379643

Server di database che esegue 175 PROCESSES

Server applicazioni non in esecuzione

Database del profiler non in esecuzione

ISE Indexing Engine non in esecuzione

Connettore AD non in esecuzione

Database sessione M&T non in esecuzione

M&T Log Processor non in esecuzione

Servizio Autorità di certificazione non in esecuzione

Servizio EST non in esecuzione

Servizio motore SXP disabilitato

Servizio TC-NAC disabilitato

Servizio WMI PassiveID disabilitato

Servizio syslog ID passivo disabilitato

Servizio API PassiveID disabilitato

Servizio Agente ID passivo disabilitato

Servizio endpoint ID passivo disabilitato

Servizio SPAN ID passivo disabilitato

Server DHCP (dhcpd) disabilitato

Server DNS (denominato) disabilitato

Servizio di messaggistica ISE non in esecuzione

Il servizio di database gateway API ISE non è in esecuzione

Servizio gateway API ISE non in esecuzione

Il servizio ISE pxGrid Direct non è in esecuzione

Servizio criteri di segmentazione disabilitato

Servizio autenticazione REST disabilitato

Connettore SSE disabilitato

Hermes (agente cloud pxGrid) disabilitato

McTrust (servizio di sincronizzazione Meraki) disabilitato

ISE Node Exporter non in esecuzione

ISE Prometheus Service non in esecuzione

ISE Grafana Service non in esecuzione

ISE NT LogAnalytics Elasticsearch non in esecuzione

Il servizio ISE Logstash non è in esecuzione

Servizio ISE Kibana non in esecuzione

Servizio IPSec nativo ISE non in esecuzione

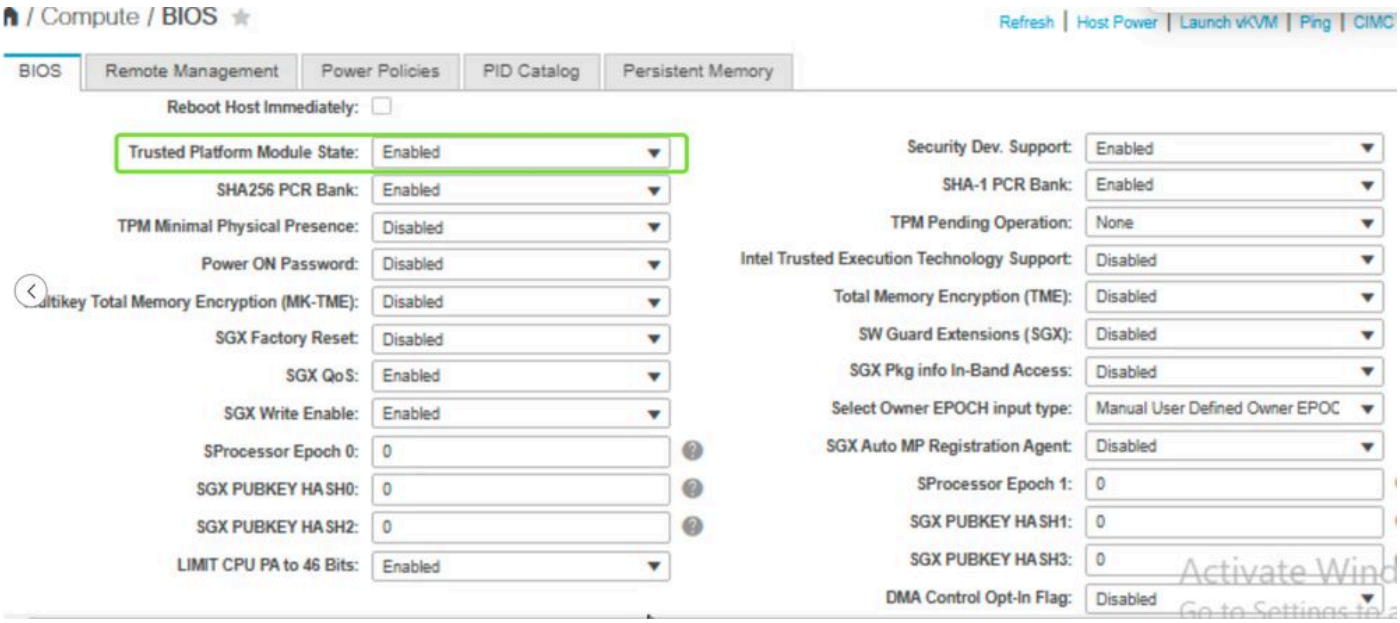
Profiler MFC non in esecuzione

Se si rileva che TPM2ManagerServer non è inizializzato e il codice di risposta è 400, abilitare il servizio TPM e creare nuovamente l'immagine del nodo.

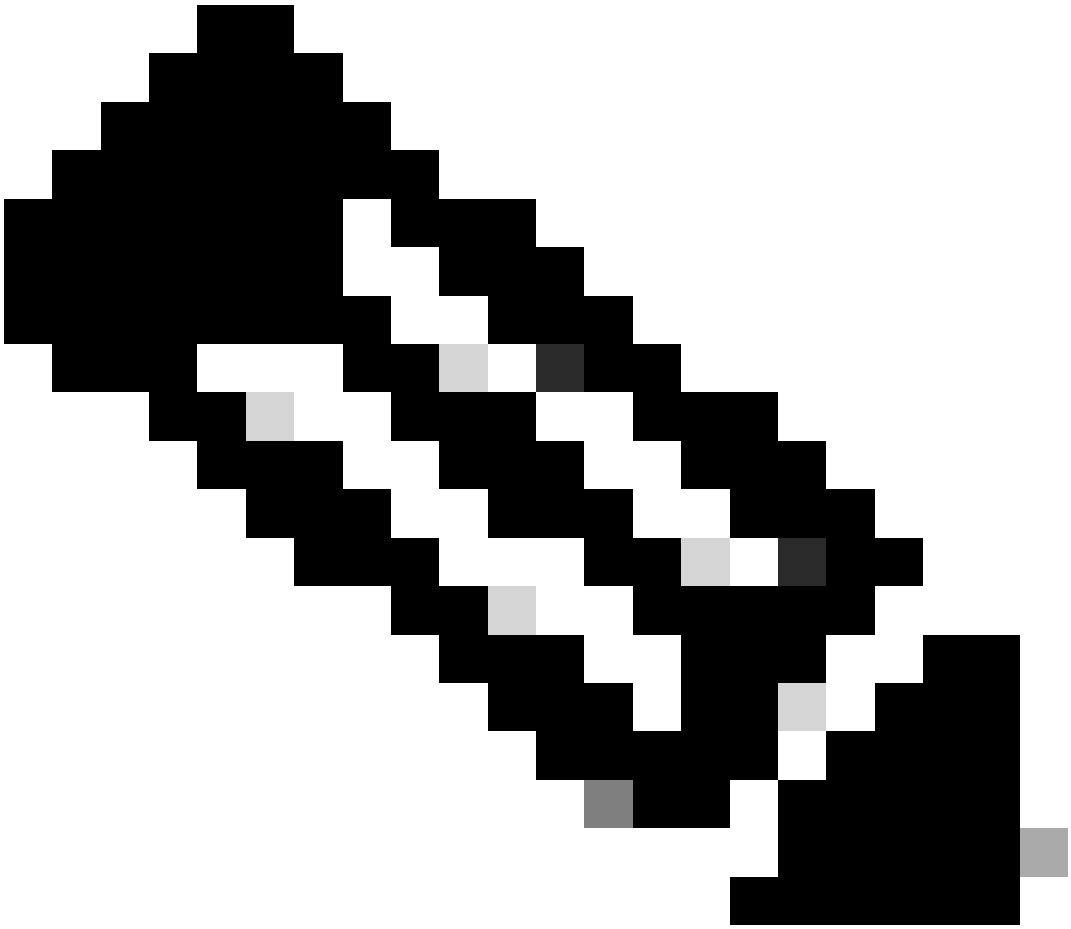
ADE.log:

2025-01-06T08:37:01.164816+00:00 giornale di registrazione della luce[141]: | 2025-01-06 08:37:01,164 | INFORMAZIONI | 1411 | ThreadPrincipale | tpm2_manager_server.py:13 | api: integrità chiamata |
2025-01-06T08:37:01.166050+00:00 giornale di registrazione della luce[141]: | 2025-01-06 08:37:01.166 ERRORE | | 1411 | ThreadPrincipale | utils.py:26 | TPM2ManagerServer non inizializzato |
2025-01-06T08:37:01.166179+00:00 giornale di registrazione della pubblicità [1411]: | 2025-01-06 08:37:01.166 | INFORMAZIONI | 1411 | ThreadPrincipale | web_log.py:206 | [06/gen/2025:08:37:01 +0000] "POST /api/system/v1/tpm2-manager/unseal HTTP/1.1" 400 215 "-" "python-Requests/2.20.0" |
2025-01-06T08:37:21.670490+00:00 cristallizzazione | 2025-01-06 08:37:21.670 | INFORMAZIONI | 372321 | ThreadPrincipale | key_manager_server.py:87 | Attendere. Inizializzazione del servizio KeyManagerServer in corso. L'operazione potrebbe richiedere alcuni minuti. |
2025-01-06T08:37:21.672808+00:00 cristallizzazione | 2025-01-06 08:37:21.672 ERRORE | | 372321 | ThreadPrincipale | key_manager_server.py:116 | Impossibile inizializzare il servizio KeyManagerServer: TPM2ManagerServer non inizializzato |

Soluzione: il modulo TPM è stato abilitato ed è possibile ricreare l'immagine del nodo.



TPM abilitato



Nota: Tenere presente che se si regolano le impostazioni del TPM dell'hardware o si apportano modifiche, ISE mostra un comportamento imprevisto. In tal caso è necessario eseguire una ricreazione immagine.

Case study 2

Causa principale: Convalida TPM non riuscita a causa della cache TPM.

Sebbene le impostazioni TPM siano abilitate nel BIOS, i problemi di blocco vengono rilevati nel file ADE.log

ADE.log:

2024-09-12T16:01:58.063806+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,063 | INFORMAZIONI | 1404 | ThreadPrincipale | tpm2_manager_server.py:13 | api: integrità chiamata |

2024-09-12T16:01:58.063933+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,063 | INFORMAZIONI | 1404 | ThreadPrincipale | web_log.py:206 | [12/set/2024:10:31:58 +0000] "GET /api/system/v1/tpm2-manager/health HTTP/1.1" 200 158 "-" "python-Requests/2.20.0" |

2024-09-12T16:01:58.064968+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,064 | INFORMAZIONI | 1404 | ThreadPrincipale | tpm2_manager_server.py:184 | api: init chiamato |

2024-09-12T16:01:58.068413+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,068 | INFORMAZIONI | 1404 | ThreadPrincipale | tpm2_proxy.py:79 | Esecuzione comando: tpm2_clear |

2024-09-12T16:01:58.075085+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,074 ERRORE | | 1404 | ThreadPrincipale | tpm2_proxy.py:85 | Impossibile eseguire tpm2_clear Causato da: tpm:warn(2.0): Le autorizzazioni per gli oggetti soggetti alla protezione DA non sono consentite in questo momento perché il TPM è in modalità di blocco DA |

2024-09-12T16:01:58.075194+05:30 GRP-ACH-ISE-PAN journal[1404]: | 2024-09-12 16:01:58,075 ERRORE | | 1404 | ThreadPrincipale | tpm2_manager_server.py:249 ERRORE |: tpm:warn(2.0): Le autorizzazioni per gli oggetti soggetti alla protezione DA non sono consentite in questo momento perché il TPM è in modalità di blocco DA |

Durante il processo di installazione, sono stati rilevati errori sulla console KVM.

Estrazione del contenuto del database ISE...

Avvio dei processi del database ISE in corso...

Eccezione nel thread "min" com.cisco.cpm.exception. Eccezione TPME: Esecuzione dello script

TPM non riuscita con codice restituito diverso da zero.)

all'indirizzo com.cisco.cpm.auth.encryptor.crypt.TPPUL11.getResult(TPMUtil.java:53

all'indirizzo com.cisco.cpm.auth.encryptor.crypt.TPMUL11.encrypt(TPER11.java:38) all'indirizzo com.cisco.cpm.auth.encryptor.crypt.KEKGenerator.returnkey (KEKGenerator.java:36)

in com.cisco.cpm.auth.encryptor.crypt.KEKGenerator.main(KEKGenerator.java:77)

java.lang.IllegalArgumentException: Chiave vuota

in javax.crypto.spec. SecretKeySpec.<init>(SecretKeySpec. Java:96) in com.cisco.cpm.auth.encryptor.crypt.Crypt.<init>(Crypt.java:73)

all'indirizzo com.cisco.cpm.auth.encryptor.crypt.DefaultCryptEncryptor encrypt(DefaultCryptEncryptar.java:81)

all'indirizzo com.cisco.cpm.auth.encryptor. PassudHelper.ma In (PasssalHelper.java:46)

Seguito da priming del database:

Registri errori:

##

ERRORE: PRIMING DEL DATABASE NON RIUSCITO.

La causa potrebbe essere una configurazione non corretta dell'interfaccia di rete o la mancanza di risorse sull'accessorio o sulla VM. Risolvere il problema ed eseguire questa CLI per reimpostare il database:

'application reset-config ise'

##############################

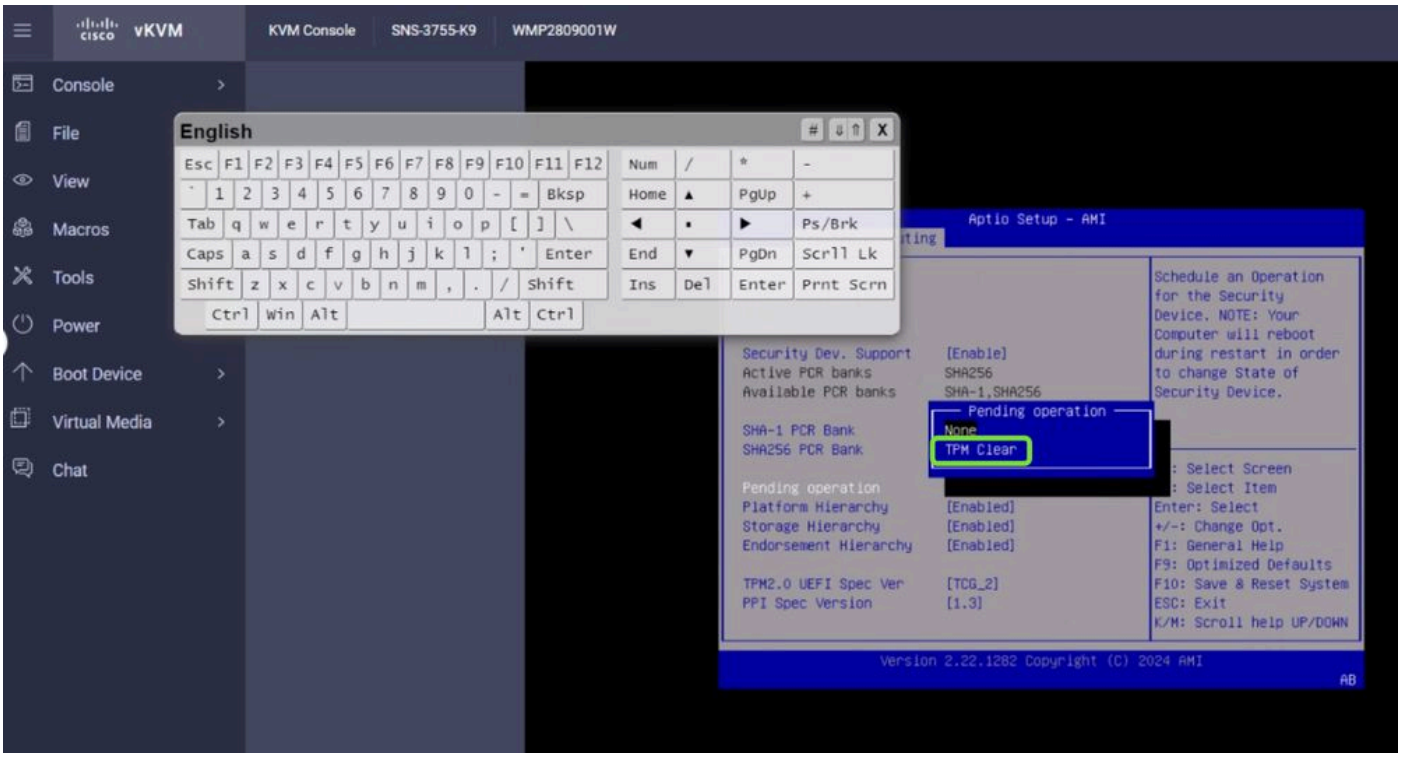
Soluzione: se si rileva che il modulo TPM è bloccato, la reimpostazione della cache TPM è di aiuto.

Operazioni da eseguire:

Avviare vKVM e riavviare il server

Quando viene visualizzato il logo Cisco

- Premere F2 (menu BIOS)
- Cancellazione TPM
- Ciclo di alimentazione


vKVM
KVM Console
SNS-3755-K9
WMP2809001W
Console
File
View
Macros
Tools
Power
Boot Device
Virtual Media
Chat
English
Aptio Setup - AMI
Security Dev. Support [Enable]
Active PCR banks SHA256
Available PCR banks SHA-1,SHA256
SHA-1 PCR Bank
SHA256 PCR Bank
Pending operation
None
TPM Clear
Pending operation
Platform Hierarchy [Enabled]
Storage Hierarchy [Enabled]
Endorsement Hierarchy [Enabled]
TPM2.0 UEFI Spec Ver [TCG_2]
PPI Spec Version [1.3]
Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
Enter: Select
+/-: Change Opt.
F1: General Help
F9: Optimized Defaults
F10: Save & Reset System
ESC: Exit
K/M: Scroll help UP/DOWN
Version 2.22.1282 Copyright (C) 2024 AMI

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).