

Statusstatussynchronisierung konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Überprüfung](#)

[Aus DART-Paket](#)

[Von der Paketerfassung auf dem Client](#)

[Von der ISE](#)

[Statusüberprüfung bei Statusstatusänderung neu starten](#)

[Fehlerbehebung](#)

[Statusstatussynchronisierung startet nicht](#)

[Statusstatussynchronisierung schlägt mit Alarm im ISE-Dashboard fehl](#)

[Überprüfen Sie, ob dACL für das Berechtigungsprofil "Compliance" konfiguriert wurde.](#)

[Bekannte Probleme](#)

[Statusstatussynchronisierung schlägt mit Alarm auf der ISE fehl](#)

Einleitung

In diesem Dokument werden die Konfiguration und Verwendung der in Version 3.1 der Cisco Identity Service Engine (ISE) eingeführten Statussynchronisierung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Statusablauf auf der Cisco ISE
- Konfiguration von Statuskomponenten auf der Cisco ISE

Es wird davon ausgegangen, dass Sie eine Statuskonfiguration anstelle eines beliebigen Typs haben.

Um die später beschriebenen Konzepte besser zu verstehen, sollten Sie die folgenden Schritte durchführen:

- [Administratorleitfaden für die Cisco Identity Services Engine, Version 3.1](#)
- [Vergleich früherer ISE-Versionen mit dem ISE-Statusverlauf in ISE 2.2](#)
- [ISE-Sitzungsmanagement und Status](#)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE Version 3.1
- Cisco Secure Client 5.0.00556

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Der ISE-Statusflow lässt in der Regel keine Statusaktualisierung auf dem Client von der ISE zu. Das Cisco Secure Client Posture Module wird verwendet, um den Status des Endgeräts zu bewerten und so lange aufrechtzuerhalten, bis eine Netzwerkänderung, eine regelmäßige Neubewertung oder andere clientseitige Auslöser eintreten. Wenn sich der Endpunkt-Status auf der ISE aufgrund eines Sitzungsabbruchs oder aus anderen Gründen ändert, kann dies dazu führen, dass das Secure Client Posture-Modul von dieser Änderung nichts bemerkt. Der Endpunkt bleibt also im Status Posture Unknown mit eingeschränktem Netzwerkzugriff, bis einer der clientseitigen Auslöser eintritt.

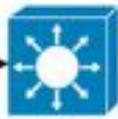
Dieses Dokument befasst sich mit einer neuen Funktion - der Statussynchronisierung. Diese Funktion wurde entwickelt, um dieses Problem zu beheben und es der ISE zu ermöglichen, dem Secure Client Posture Module Feedback zum aktuellen Status des Endpunkts zu geben.

Konfigurieren

Der Port für die Statusprüfung wurde auf jedem ISE-PSN-Knoten eingerichtet, wenn die Statusprüfung aktiviert ist - standardmäßig TCP 8449. Es soll vom Endpunkt aus erreichbar sein, wenn der Endpunkt-Status "Unbekannt" oder "Ausstehend" lautet, und nicht erreichbar, wenn der Endpunkt-Status "Konformität" lautet.

Netzwerkdiagramm

https probe to
PSNs new
port i.e:8449



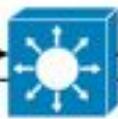
ACL: **deny** tcp any
host PSNIP eq 8449



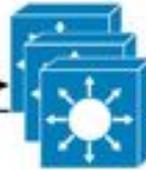
Compliant



https probe to
PSNs new
port i.e:8449



ACL: **permit** tcp any
host PSNIP eq 8449



Pending



357798

Konfigurationen

Die Konfiguration der Statusüberprüfung besteht aus zwei Teilen:

1. Konfiguration des AnyConnect-Statusprofils

1.1 Navigieren Sie in der Cisco ISE-GUI zu Richtlinie > Richtlinienelemente > Ergebnisse > Client-Bereitstellung > Ressourcen.

1.2 Wählen Sie das AnyConnect Posture Profile, das Sie bereits verwenden, oder erstellen Sie ein neues Profil.

1.3 Konfigurieren Sie im Bereich "Agent Behavior" das Statusstatus-Synchronisierungsintervall auf einen beliebigen Wert zwischen 1 und 300 Sekunden, 0 - deaktiviert die Statusstatus-Synchronisierung

1.4 Sie können die Liste mit den Statusprüfungen konfigurieren - Secure Client verwendet diese Liste, um den Status ausgewählter PSNs zu überprüfen. Wenn Sie kein PSN auswählen, werden das verbundene PSN und zwei Backup-Server als Backups für die Statusstatus-Synchronisierung verwendet.

Dictionary	Conditions	Results
Authentication		Posture probing 🔍 AnyConnect will send periodic probes with the given interval continuously till valid ISE is found.
Authorization		Posture State Synchronisation Interval <input type="text" value="60"/> Supported range is between 0 - 300 seconds. '0' disables periodic probing.
Profiling		Posture probing Backup List 🔍 <input type="text" value="1 PSN(s)"/> AnyConnect sends probes to backup list during discovery phase to find ISE server. By default, if it is empty. It uses all PSNs as a backup servers.
Posture		Automated DART Count <input type="text" value="3"/> Set the number of automated dart bundles to be collected during failure scenarios.
Client Provisioning		Warning, prior to grace period expiration 🔍 <input type="text" value="0"/> mins Set how many minutes prior to the end of the grace period to show the warning. 0 means do not show warning.
Resources		

2. Konfiguration einer herunterladbaren ACL (dACL) zum Blockieren des Zugriffs auf den Port zur Statussynchronisierung der Cisco ISE, wenn der Status des Clients "Compliant" oder "Non Compliant" lautet. Sie müssen dem Posture State Synchronization-Port für jedes PSN am oberen Rand der ACLs, die für konforme Endpunkte verwendet werden, einen Deny-Eintrag für die Zugriffskontrolle hinzufügen, um den Zugriff auf den Posture State Synchronization-Port zu beschränken, wenn der Endpunktstatus bekannt ist. Beispiel:

```
deny tcp any host PSN1-IP-ADDRESS eq 8449
deny tcp any host PSN2-IP-ADDRESS eq 8449
permit ip any any
```

permit ip any any ist nicht obligatorisch, Sie können es mit einem beliebigen Satz von Regeln entsprechend Ihren Bedürfnissen ersetzen.



Hinweis: Wenn der Eintrag "deny" in der dACL nicht konfiguriert ist, wird im Cisco ISE-Dashboard der Alarm "Posture Configuration Detection" ausgelöst, und die Synchronisierung des Status auf dem Endpunkt wird deaktiviert, bis der Cisco Secure Client neu gestartet wird.

Port zur Statussynchronisierung (bidirektionaler Port) kann auf der Konfigurationsseite des Client-Bereitstellungsportals geändert werden. Navigieren Sie zu Administration > Device Portal Management > Client Provisioning > Wählen Sie das gewünschte Portal > Portal Behavior and Flow Settings aus, und öffnen Sie Portal Settings. Der Port für die Statusstatussynchronisierung für das Standard-Client-Bereitstellungsportal kann nicht geändert werden.

Cisco ISE Administration - Device Portal Management

Blocked List BYOD Certificate Provisioning **Client Provisioning** Mobile Device Management My Devices Custom Portal Files Settings

Portals Settings and Customization

Portal Name: Client Provisioning Portal (default) Description: Default portal and user experience user

Language File

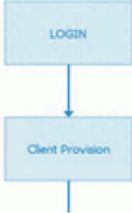
Portal test URL

Portal Behavior and Flow Settings Portal Page Customization

Portal & Page Settings Client Provisioning Portals Flow (base)

Portal Settings

HTTPS port:*	8443	(8000 - 8999)
Bidirectional port:*	8449	(8000 - 8999)



```

graph TD
    LOGIN[LOGIN] --> ClientProvision[Client Provision]
  
```

Überprüfung

Aus DART-Paket

Die Synchronisierung des Statusstatus kann auf Client-Seite überprüft werden, indem Sie die Cisco Secure Client Posture Module-Protokolle (AnyConnect_ISEPosture.txt) aus dem DART-Paket einsehen:

1. Statusüberprüfung abgeschlossen, Status der Statusüberprüfung ist konform.

```
2022/11/09 12:22:47 [Information] aciseagent Function: Authenticator::sendUIStatus Thread Id: 0xC60 Fi
```

2. Statusstatussynchronisierungsüberprüfung wurde gestartet.

```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
```

```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

3. Die HTTPS-Verbindung mit ISE PSN auf dem Port zur Statussynchronisierung (8449) wird initiiert.

2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt

2) Der Cisco Secure Client bestätigt die Änderung des Status und startet die Statuserkennung neu:

2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296C
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296C
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC60

3) Der Cisco Secure Client beendet die Synchronisierung des Status, bis die Statusüberprüfung durchgeführt wird:

2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::processMessage Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: hs_transport_free Thread Id: 0xC60 File: hs_tran
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296C

Fehlerbehebung

Statusstatussynchronisierung startet nicht

Wenn in der Protokolldatei AnyConnect_ISEPosture.txt kein Hinweis auf den Start der Statussynchronisierung vorhanden ist und der Client nicht versucht, eine Verbindung mit dem ISE-PSN-Knoten am Port für die Statussynchronisierung herzustellen (8449), überprüfen Sie die Statuskonfigurationsdatei ISEPostureCFG.xml aus dem DART-Paket oder direkt auf dem Client-Computer: "%ProgramData%\Cisco\Cisco\Cisco Secure Client\ISE-Status\" für einen Windows-PC.

Der für die Statussynchronisierung verantwortliche Parameter ist "StateSyncProbeInterval". Er muss mit einem Wert größer als 0 festgelegt werden:

```
<ServerNameRules>*</ServerNameRules>
<OperateOnNonDot1XWireless>0</OperateOnNonDot1XWireless>
<NonCompliantButtonText/>
<GracePeriodStartDescriptionDetails/>
<RemediationTimer>12</RemediationTimer>
<DhcpRenewDelay>1</DhcpRenewDelay>
<CallHomeList/>
<LogFileSize>5</LogFileSize>
<WarningTimer>0</WarningTimer>
<PRARetransmissionTime>120</PRARetransmissionTime>
<EnableAgentIpRefresh>0</EnableAgentIpRefresh>
<NetworkTransitionDelay>10</NetworkTransitionDelay>
<DartCount>3</DartCount>
<CwaByodProbingInterval>10</CwaByodProbingInterval>
<NonCompliantTitle/>
<NonCompliantDescriptionDetails/>
<PingArp>0</PingArp>
<DhcpReleaseDelay>4</DhcpReleaseDelay>
<StealthWithNotification>0</StealthWithNotification>
<NonCompliantButtonLink/>
<SignatureCheck>0</SignatureCheck>
<DiscoveryHost/>
<StateSyncProbeInterval>10</StateSyncProbeInterval>
<GracePeriodStartDescription/>
<EnableRescanButton>1</EnableRescanButton>
<VlanDetectInterval>0</VlanDetectInterval>
<DisableUAC>0</DisableUAC>
```

Das Fehlen von "StateSyncProbeInterval" oder eines Werts von "0" bedeutet, dass die Statussynchronisierung deaktiviert ist.

Wenn "Posture State Synchronization Interval" (Statusstatussynchronisierungsintervall) im Statusprofil auf der ISE festgelegt ist, dies jedoch nicht in einer Konfigurationsdatei auf dem Client angezeigt wird, muss die Statusbereitstellung untersucht werden.

Statusstatussynchronisierung schlägt mit Alarm im ISE-Dashboard fehl

Wenn die Statusüberprüfung mit einem Alarm auf der ISE fehlschlägt, bedeutet dies, dass der Cisco Secure Client die ISE auf dem Port für die Statusüberprüfung (8449) erreichen konnte und einen Status für die Sitzung mit dem Status "Konformität" angefordert hat.

- Alarm in der ISE-GUI:


```

2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt

```

3) Die Statusstatussynchronisierung wird aufgrund einer falschen Konfiguration beendet:

```

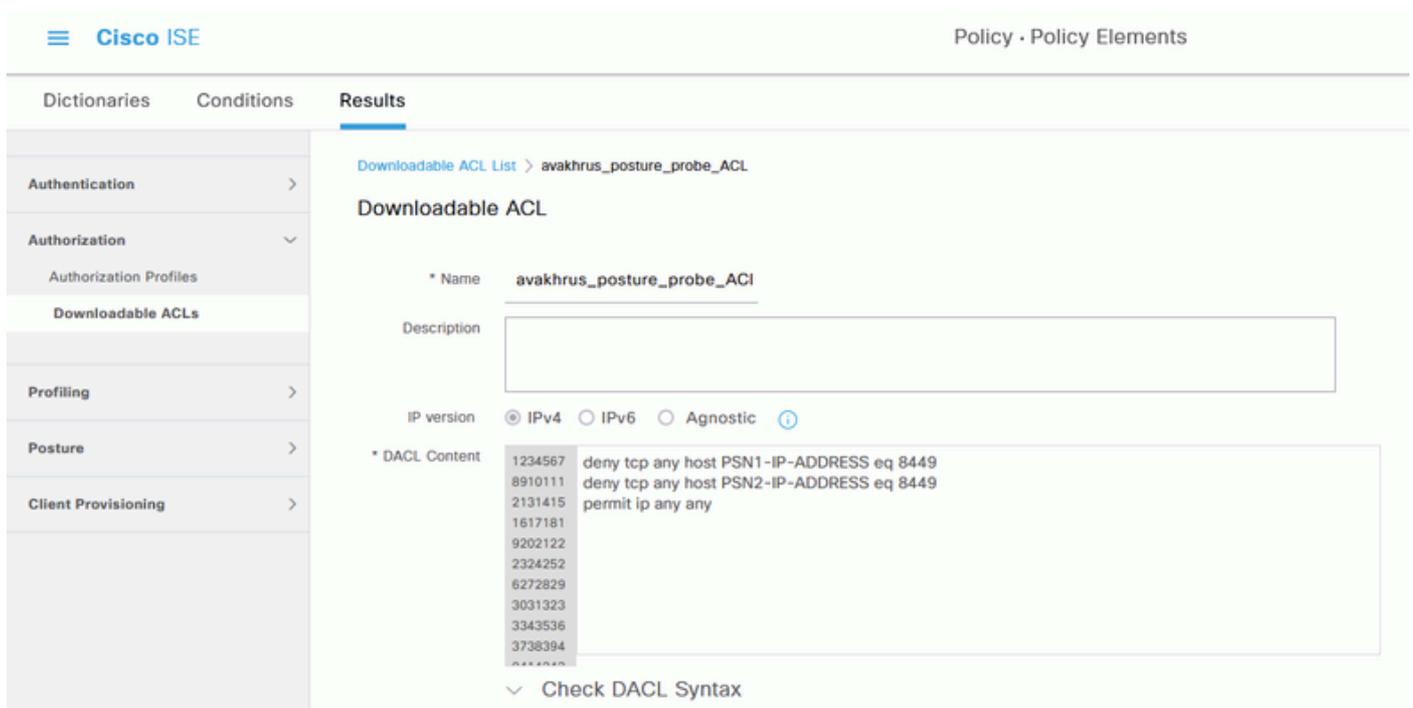
2022/11/09 12:26:34 [Error] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x2750 File
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x2750
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F

```

Die Statusüberprüfung kann über die Benutzeroberfläche des Cisco Secure Client nicht neu gestartet werden, indem die Statusüberprüfung oder eine Netzwerkänderung neu gestartet werden. Stattdessen muss der Cisco Secure Client neu gestartet werden, damit die Statusstatussynchronisierung wieder funktioniert.

Überprüfen Sie, ob dACL für das Berechtigungsprofil "Compliance" konfiguriert wurde.

1. Validieren Sie, ob die richtige dACL für das Berechtigungsprofil "Compliance" (konform) konfiguriert ist:



2. Validierung des detaillierten Authentifizierungsberichts dACL wurde als Ergebnis der Authentifizierung des "konformen" Endpunkts korrekt gesendet.

```
CPMSessionID          c0a830e71FjmLTxwC_6BfWNqU3RwKrGfaDTw5krqr1QOzEm/ej0
CiscoAVPair            aaa:service=ip_admission,aaa:event=acl-download
```

Result

```
Class                  CACS:c0a830e71FjmLTxwC_6BfWNqU3RwKrGfaDTw5krqr1QOzEm/
                       ej0:ISE-PSN-FQDN/482174459/480
cisco-av-pair          ip:inacl#1=deny tcp any host PSN1-IP-ADDRESS eq 8449
cisco-av-pair          ip:inacl#2=deny tcp any host PSN2-IP-ADDRESS eq 8449
cisco-av-pair          ip:inacl#3=permit ip any any
```

3. Überprüfen Sie, ob dACL auf einem Netzwerkzugriffsgesetz ordnungsgemäß angewendet wurde:

```
avakhrus_3560C#sh auth sess int fa0/12 det
  Interface: FastEthernet0/12
  MAC Address: 0050.56a8.be02
  IPv6 Address: Unknown
  IPv4 Address: 192.168.255.193
  User-Name: TRAINING\bob
  Status: Authorized
  Domain: DATA
  Oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Restart timeout: N/A
  Periodic Acct timeout: 172800s (local), Remaining: 92111s
  Session Uptime: 1515s
  Common Session ID: C0A8FF0C00000012679EAF14
  Acct Session ID: 0x00000012
  Handle: 0x5D000005
  Current Policy: POLICY_Fa0/12

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
  ACS ACL: xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac

Method status list:
  Method          State
  mab              Stopped
  dot1x            Authc Success
```

```
avakhrus_3560C#sh access-lists | s xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac
Extended IP access list xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac (per-user)
```

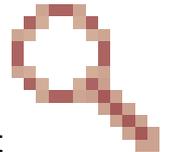
```
1 deny tcp any host PSN1-IP-ADDRESS eq 8449
2 deny tcp any host PSN2-IP-ADDRESS eq 8449
3 permit ip any any
```

Bekannte Probleme

Statusstatussynchronisierung schlägt mit Alarm auf der ISE fehl

Die Statusstatussynchronisierung kann mit einem Alarm auf der ISE fehlschlagen, selbst wenn auf einem Netzwerkzugriffsgeschäft eine geeignete dACL auf den Client-Endpunkt angewendet wird.

Dies geschieht, wenn der Status-Synchronisationstest schneller ausgeführt wird, als dACL angewendet wird, oder wenn der Status-Synchronisationstest bereits ausgeführt wird, wenn dACL



angewendet wird. Das Problem wurde unter der Cisco Bug-ID [CSCwd58316](https://tools.cisco.com/bugcenter/bug/?bugID=CSCwd58316) untersucht

. Als Workaround müssen Sie die "Network Transition Delay" im AnyConnect Posture-Profil (ISE Posture Agent Profile Settings) auf 10 Sekunden einstellen.

The screenshot shows the Cisco ISE interface for Client Provisioning. The left sidebar contains navigation options: Overview, Network Devices, Client Provisioning (selected), Policy Elements, Posture Policy, Policy Sets, Troubleshoot, and Reports. The main content area is titled "IP Address Change" and displays a table of parameters and their values. The "Network transition delay" parameter is highlighted in blue and set to 10 seconds.

Parameter	Value
Enable agent IP refresh ⓘ	No ▾
VLAN detection interval ⓘ	0 secs
Ping or ARP ⓘ	Ping ▾
Maximum timeout for ping	1 secs
DHCP renew delay	1 secs
DHCP release delay	4 secs
Network transition delay ⓘ	10 secs

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.