ISE Status - Best Practices und Überlegungen zur Bereitstellung

Inhalt

Einführung

In diesem Dokument werden einige Basiskonfigurationen beschrieben, die verschiedene Anwendungsfälle mit umleitungsbasiertem Status behandeln. In diesen Konfigurationen bleibt der Client konform, aber das Netzwerkzugriffsgerät (NAD) beschränkt den Zugriff, da es sich im Umleitungsstatus befindet.

Einschränkungen

Die Konfigurationen in diesem Dokument gelten für Cisco NADs, aber nicht unbedingt für NADs von Drittanbietern.

Status-Client-Verhalten

Der Status-Client löst in folgenden Fällen Prüfungen aus:

- Erstmalige Anmeldung
- Änderung auf Layer 3 (L3)/Änderung der Netzwerkschnittstellenkarte (NIC) (neue IP-Adresse, Änderung des NIC-Status)

Anwendungsfälle

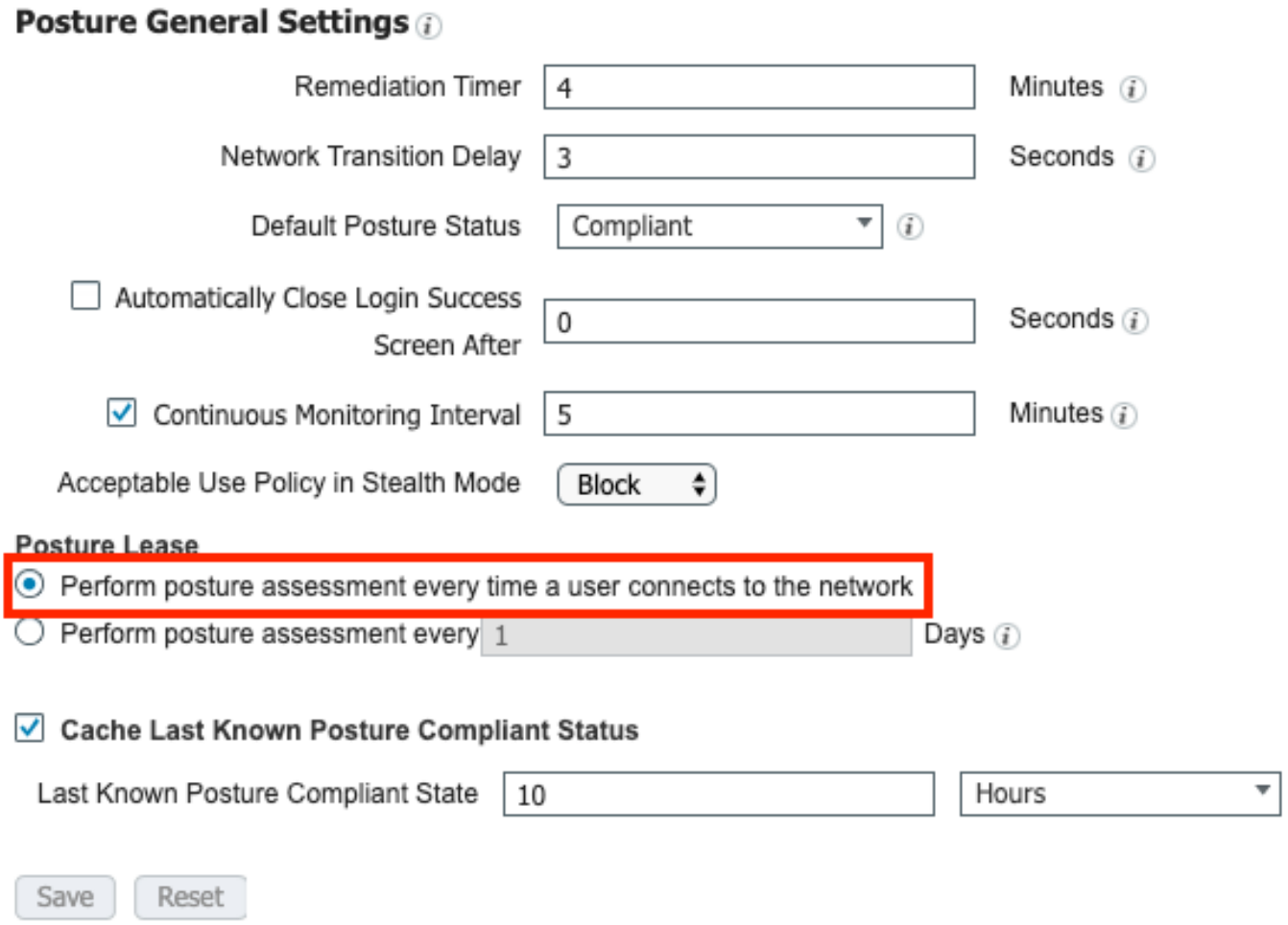
Anwendungsfall 1: Bei der Client-Neuauthentifizierung wird die NAD gezwungen,

eine neue Sitzungs-ID zu erstellen.

In diesem Anwendungsfall ist der Client immer noch konform, aber aufgrund der Neuauthentifizierung befindet sich die NAD im Umleitungszustand (Umleitung von URL und Zugriffsliste).

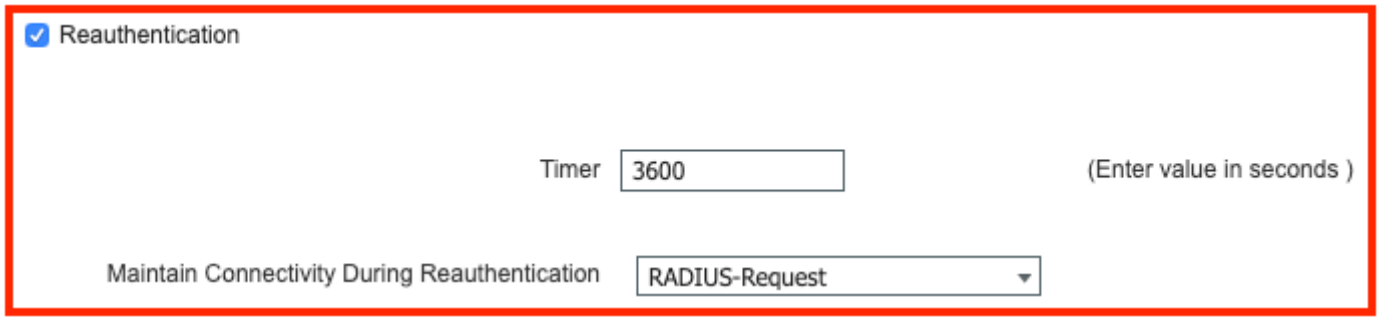
Standardmäßig wird die Identity Services Engine (ISE) so konfiguriert, dass sie bei jeder Verbindung mit dem Netzwerk eine Statusüberprüfung durchführt, insbesondere für jede neue Sitzung.

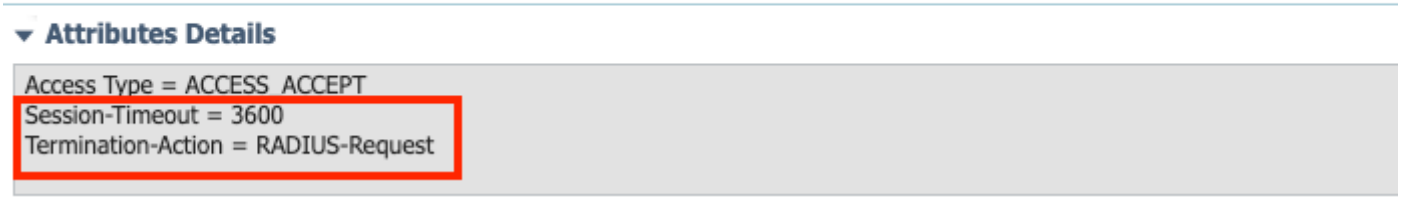
Diese Einstellung wird unter Work Center > Posture > Settings > Posture General Settings (Arbeitszentren > Status > Einstellungen > Statuseinstellungen) konfiguriert.



Um zu verhindern, dass die NAD bei der erneuten Authentifizierung eine neue Session-ID generiert, konfigurieren Sie diese Reauthentifizierungswerte im Autorisierungsprofil. Der angezeigte Authentifizierungs-Timer ist keine Standardempfehlung, Reauthentifizierungs-Timer sollten je Bereitstellung auf Basis des Verbindungstyps (kabelgebunden/drahtlos), des Designs (wie lauten die Persistenz-Regeln auf dem Load Balancer) usw. berücksichtigt werden.

Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile





Auf Switches müssen Sie jede Schnittstelle oder Vorlage konfigurieren, um den Authentifizierungs-Timer von der ISE abzurufen.

```
authentication timer reauthenticate server
```

> **Hinweis:** Wenn ein Load Balancer vorhanden ist, müssen Sie sicherstellen, dass die Persistenz so konfiguriert ist, dass Reauthentifizierungen an den ursprünglichen Policy Service (PSN) zurückgegeben werden.

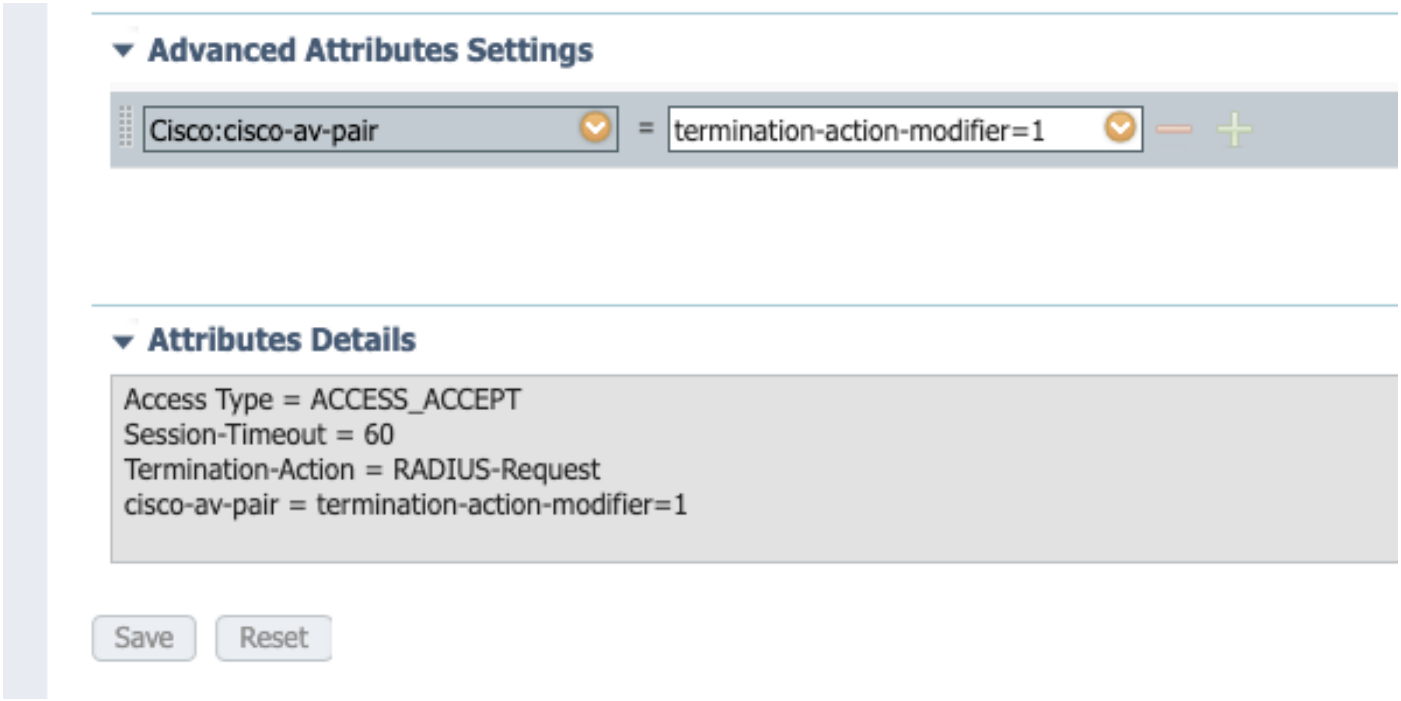
Anwendungsfall 2 - Der Switch wird mit der MAB-DOT1X-MAB-Nummer und der Priorität DOT1X-MAB (kabelgebunden) konfiguriert.

In diesem Fall werden Reauthentifizierungen beendet, da ein Abrechnungsstopp für die 802.1x-Sitzung gesendet wird, wenn während der erneuten Authentifizierung MAB (MAC Authentication Bypass) versucht wird.

- Der Abrechnungsstopp, der für den MAB-Prozess gesendet wird, wenn er die Authentifizierung nicht durchführt, ist korrekt, da der Benutzername für den Client vom 802.1X-Benutzernamen in den MAB-Benutzernamen geändert wird.
- Dot1x als method-id im Accounting-Stopp ist ebenfalls korrekt, da die Autorisierungsmethode dot1x war.
- Wenn die Dot1x-Methode erfolgreich ist, sendet sie einen Accounting-Start mit method-id als dot1x. Auch hier ist dieses Verhalten wie erwartet.

Um dieses Problem zu beheben, konfigurieren Sie cisco-av-pair:termination-action-modifier = 1 für das authZ-Profil, das verwendet wird, wenn ein Endpunkt kompatibel ist. Dieses AV-Paar (Attributwert) gibt an, dass die NAD unabhängig von der konfigurierten Reihenfolge die in der

ursprünglichen Authentifizierung gewählte Methode wiederverwenden soll.



Anwendungsfall 3: Das Roaming von Wireless-Clients und die Authentifizierung für verschiedene APs erfolgen an verschiedene Controller.

In diesem Fall muss das Wireless-Netzwerk so konzipiert sein, dass die Access Points (APs), die für Roaming-Zwecke in Reichweite anderer APs sind, denselben aktiven Controller verwenden. Ein Beispiel hierfür ist der WLC-Failover (Wireless LAN Controller). Weitere Informationen zu HA-SSO (High Availability) für WLC finden Sie im Bereitstellungsleitfaden für Hochverfügbarkeit (High Availability, SSO).

Anwendungsfall 4 - Bereitstellung mit Load Balancern (Patch 6, 2.7 Patch P2 und 3.0 vor 2.6).

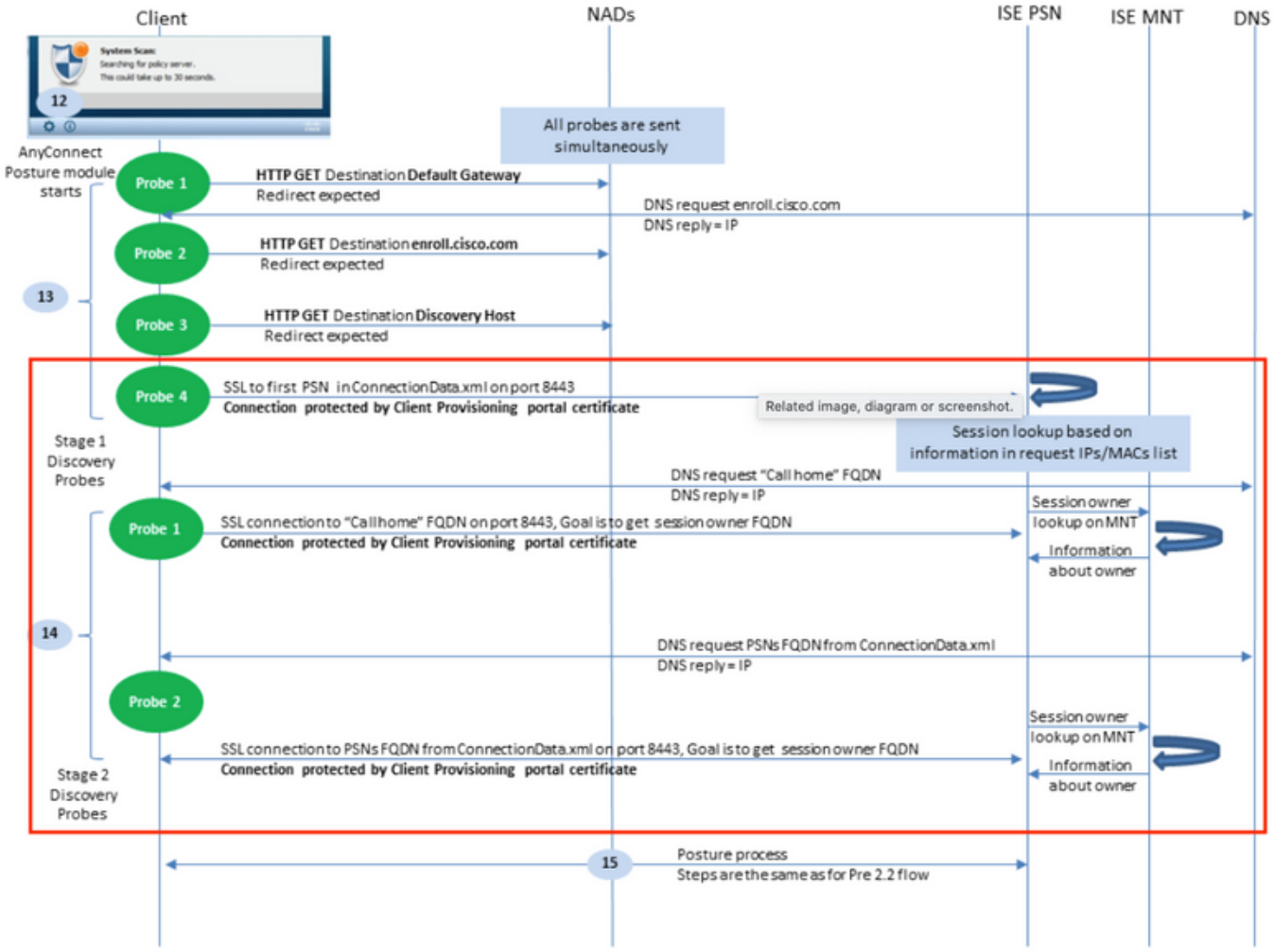
Bei Bereitstellungen mit beteiligten Load Balancern ist es wichtig, sicherzustellen, dass nach den Änderungen in den vorherigen Anwendungsfällen die Sitzungen demselben PSN zugeordnet werden. Vor den für diesen Schritt aufgelisteten Versionen/Patches wird der Status zwischen den Knoten nicht über Light Data Distribution (ehemals Light Session Directory) repliziert. Daher können verschiedene PSNs unterschiedliche Statusstatusergebnisse zurückgeben.

Wenn die Persistenz nicht korrekt konfiguriert ist, können Sitzungen, die sich erneut authentifizieren, zu einem anderen PSN als dem, der ursprünglich verwendet wurde, geleitet werden. In diesem Fall kann das neue PSN den Status der Sitzungen-Compliance als unbekannt markieren, das Ergebnis authZ mit der ACL/URL (Redirect Access Control List) übergeben und den Zugriff auf die Endpunkte einschränken. Auch diese Änderung am NAD wird vom Statusmodul nicht erkannt, und Tests werden nicht ausgelöst.

Weitere Informationen zum Konfigurieren von Load Balancern finden Sie im Cisco & F5 Deployment Guide: ISE-Lastenausgleich über BIG-IP. Sie bietet einen allgemeinen Überblick und eine F5-spezifische Konfiguration eines Best Practice-Designs für ISE-Bereitstellungen in einer Umgebung mit Lastenausgleich.

Anwendungsfall 5 - Die Tests zur Erkennung in Phase 2 werden von einem anderen Server als dem authentifizierten Client durchgeführt (Patch 6, 2.7 Patch 2 und 3.0, älter als 2.6).

Sehen Sie sich die Probes in der roten Box in diesem Diagramm an.



PSNs speichern Sitzungsdaten fünf Tage lang, sodass Sitzungsdaten für eine "konforme" Sitzung manchmal noch auf dem ursprünglichen PSN gespeichert sind, selbst wenn sich der Client nicht mehr mit diesem Knoten authentifiziert. Wenn die in der roten Box enthaltenen Tests von einem anderen PSN als demjenigen beantwortet werden, der die Sitzung derzeit authentifiziert UND zuvor von PSN als solcher gekennzeichnet wurde, besteht die Möglichkeit, dass der Status des Statusmoduls auf dem Endpunkt nicht übereinstimmt und das aktuelle authentifizierende PSN nicht übereinstimmt.

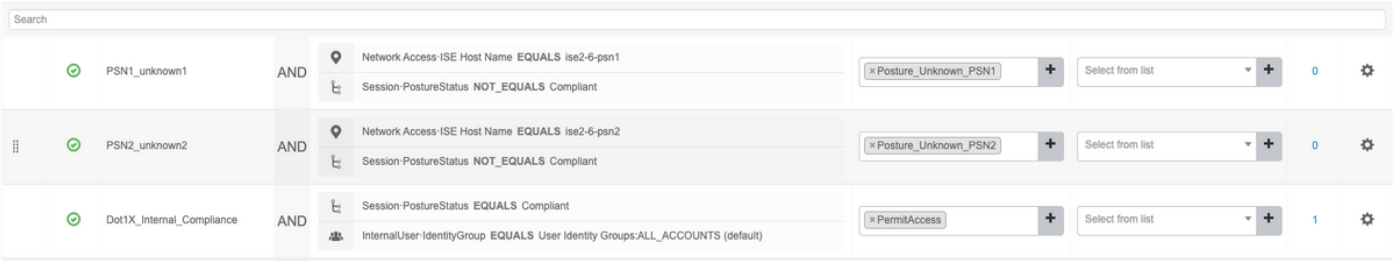
In den folgenden Szenarien kann diese Abweichung auftreten:

- Ein Abrechnungsstopp wird für einen Endpunkt nicht empfangen, wenn er vom Netzwerk getrennt wird.
- Die NAD wurde von einem PSN auf ein anderes übertragen.
- Ein Load Balancer leitet Authentifizierungen an verschiedene PSNs für denselben Endpunkt weiter.

Zum Schutz vor diesem Verhalten kann die ISE so konfiguriert werden, dass nur Erkennungssonden von einem bestimmten Endpunkt auf das PSN zugreifen können, an dem sie

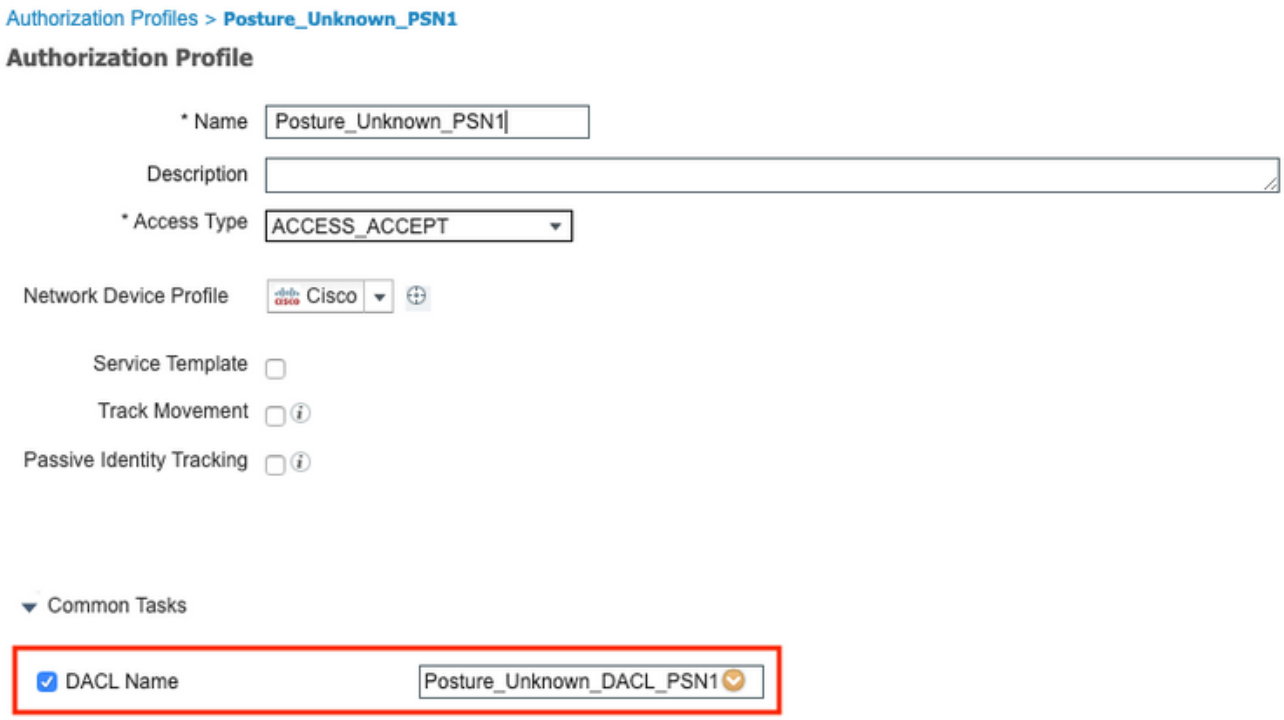
sich derzeit authentifiziert. Um dies zu erreichen, müssen Sie für jedes PSN in Ihrer Bereitstellung eine andere Autorisierungsrichtlinie konfigurieren. Verweisen Sie in diesen Richtlinien auf ein anderes authZ-Profil, das eine herunterladbare Zugriffssteuerungsliste (DACL) enthält, die nur das in der authZ-Bedingung angegebene PSN zulässt. Siehe folgendes Beispiel:

Jedes PSN verfügt über eine Regel für den Status eines unbekannten Status:

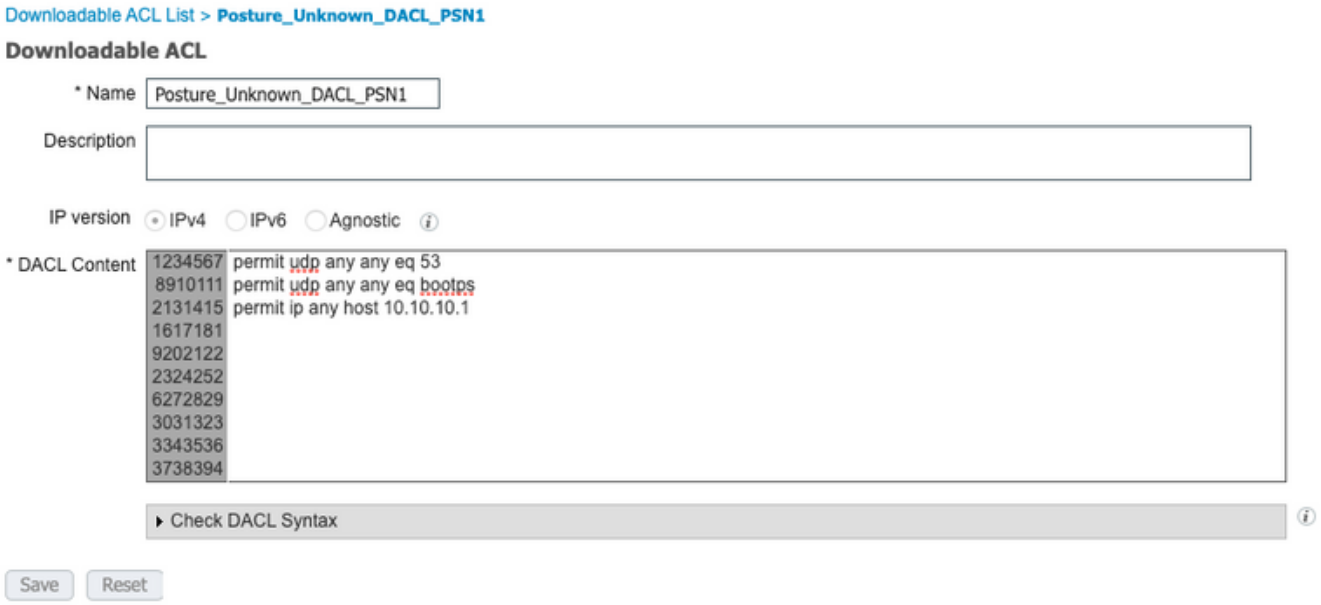


Jedes einzelne Profil verweist auf eine andere DACL.

Hinweis: Verwenden Sie für Wireless-Netzwerke Airespace ACLs.



Jede DACL ermöglicht nur den Zugriff auf das PSN, das die Authentifizierung übernimmt.



Im vorherigen Beispiel ist 10.10.10.1 die IP-Adresse von PSN 1. Die referenzierte DACL kann bei Bedarf für zusätzliche Services/IPs geändert werden, sollte jedoch den Zugriff auf das PSN beschränken, das die Authentifizierung übernimmt.

Änderung des Verhaltens nach 2.6 Patch 6, 2.7 Patch 2 und 3.0

Der Status wurde dem RADIUS Session Directory über das Light Data Distribution Framework hinzugefügt. Jedes Mal, wenn ein Statusupdate auf einem PSN eingeht, wird es auf ALLE PSNs in der Bereitstellung repliziert. Sobald diese Änderung in Kraft ist, werden die Auswirkungen von Authentifizierungen und/oder Tests, die verschiedene PSNs auf verschiedene Authentifizierungen erreichen, entfernt, und alle PSNs sollten auf alle Endpunkte antworten können, unabhängig davon, wo sie derzeit authentifiziert sind.

In den fünf Anwendungsfällen dieses Dokuments werden folgende Verhaltensweisen berücksichtigt:

Anwendungsfall 1: Bei der Client-Neuauthentifizierung wird die NAD gezwungen, eine neue Sitzungs-ID zu erstellen. Der Client ist immer noch kompatibel, aber aufgrund der Neuauthentifizierung befindet sich die NAD im Umleitungsstatus (Umleitung von URL und Zugriffsliste).

- Dieses Verhalten ändert sich nicht, und diese Konfiguration sollte weiterhin auf der ISE und den NADs implementiert werden.

Anwendungsfall 2 - Der Switch wird mit der MAB-DOT1X-MAB-Nummer und der Priorität DOT1X-MAB (kabelgebunden) konfiguriert.

- Dieses Verhalten ändert sich nicht, und diese Konfiguration sollte weiterhin auf der ISE und den NADs implementiert werden.

Anwendungsfall 3: Das Roaming von Wireless-Clients und die Authentifizierung für verschiedene APs erfolgen an verschiedene Controller.

- Dieses Verhalten ändert sich nicht, und diese Konfiguration sollte weiterhin auf der ISE und den

NADs implementiert werden.

Anwendungsfall 4: Bereitstellung mit Load Balancern

- Die im Lastenausgleichs-Leitfaden definierten Best Practices sollten weiterhin befolgt werden. Falls jedoch Authentifizierungen vom Load Balancer an verschiedene PSNs weitergeleitet werden, sollte der korrekte Status an den Client zurückgegeben werden.

Anwendungsfall 5 - Discovery-Tests in Stufe 2 werden von einem anderen Server als dem authentifizierten Client mit folgenden Daten beantwortet:

- Dies sollte kein Problem mit dem neuen Verhalten sein, und das Per-PSN-Autorisierungsprofil sollte nicht erforderlich sein.

Überlegungen zum Beibehalten derselben SessionID

Wenn Sie die in diesem Dokument aufgeführten Methoden verwenden, kann ein Benutzer, der weiterhin mit dem Netzwerk verbunden ist, über längere Zeit möglicherweise die Richtlinien einhalten. Obwohl sie sich erneut authentifizieren, ändert sich die sessionID nicht, und die ISE übergibt daher weiterhin das AuthZ-Ergebnis für ihre Regel, die mit dem konformen Status übereinstimmt.

In diesem Fall muss eine regelmäßige Neubewertung konfiguriert werden, damit die Statusüberprüfung durchgeführt werden kann, um sicherzustellen, dass der Endpunkt in festgelegten Abständen die Unternehmensrichtlinien erfüllt.

Sie können diese Einstellungen unter Work Center > Status > Settings > Ressment Configuration (Work Center > Status > Einstellungen > Sitzungen) konfigurieren.