

Fehlerbehebung bei Smart Licensing auf Catalyst-Plattformen

Inhalt

[Einleitung](#)

[Was ist Cisco Smart Licensing?](#)

[Smart Licensing-Implementierungsmethoden](#)

[Unterstützte Cisco IOS XE-Plattformen](#)

[Migration von älteren Lizenzen zu Smart Licenses](#)

[Umwandlung durch gerätgesteuerte Konvertierung \(Device Led Conversion, kurz DLC\)](#)

[Umwandlung über Cisco Smart Software Manager \(CSSM\) oder License Registration Portal \(LRP\)](#)

[Kontakt: Cisco Global Licensing Operations \(GLO\) Department](#)

[Verhaltensänderung beim Catalyst 9500 High-Performance-Modell von 16.9 bis 16.12.3](#)

[Cisco IOS XE Version 16.11.x und früher](#)

[Cisco IOS XE Version 16.12.3 und höher](#)

[C9500 – Häufig gestellte Fragen Änderungen bei High-Performance-Modellen](#)

[Konfiguration](#)

[Basiskonfiguration](#)

[Registrierungs-Token/Geräte-ID-Token](#)

[Registrierungs- und Lizenzstatus](#)

[Überlegungen und Hinweise](#)

[Fehlerbehebung](#)

[Gerät kann nicht registriert werden](#)

[Häufige Fehlerszenarien](#)

[Szenario #1: Switch-Registrierung "Fehlerursache: Produkt bereits registriert"](#)

[Szenario #2: Switch-Registrierung "Fehlerursache: Ihre Anfrage konnte derzeit nicht bearbeitet werden. Bitte versuchen Sie es erneut"](#)

[Szenario #3: Fehlerursache "Das Gerätedatum 1526135268653 liegt außerhalb der zulässigen Toleranzgrenze.](#)

[Szenario #4: Switch-Registrierung "Fehlerursache: Kommunikationstransport nicht verfügbar."](#)

[Szenario #5: Switch-Lizenz-Autorisierung "Fehlerursache: Senden von HTTP-Nachrichten mit Call Home fehlgeschlagen."](#)

[Szenario #6: Fehlerursache "Fehlendes ID-Zertifikat-Seriennummernfeld; Fehlendes Signaturzertifikat-Seriennummernfeld; Signierte Daten und Zertifikat stimmen nicht überein" Protokoll](#)

[Szenario #7: Switch-Lizenzautorisierung "Fehlergrund: Warten auf Antwort"](#)

[Szenario #8: Lizenz im Status "NICHT KONFORM"](#)

[Szenario #9: Switch-Lizenzautorisierung "Fehlerursache: Daten und Signatur stimmen nicht überein"](#)

Einleitung

Dieses Dokument beschreibt die Arbeit mit Cisco Smart Licensing (Cloud-basiertes System) zum

Verwalten von Softwarelizenzen auf Catalyst Switches.

Was ist Cisco Smart Licensing?

Cisco Smart Licensing ist ein Cloud-basiertes Unified-Lizenzmanagementsystem, das alle Softwarelizenzen für alle Cisco Produkte verwaltet. Sie erhalten die Möglichkeit, Cisco Softwarelizenzen zu kaufen, bereitzustellen, zu verwalten, nachzuverfolgen und zu erneuern. Es bietet auch Informationen über den Besitz und die Nutzung von Lizenzen über eine zentrale Benutzeroberfläche.

Die Lösung besteht aus Online-Smart Accounts (im Cisco Smart Licensing-Portal) zum Verfolgen von Cisco Software-Ressourcen und dem Cisco Smart Software Manager (CSSM) zum Verwalten der Smart Accounts. In CSSM können alle Aufgaben im Zusammenhang mit dem Lizenzmanagement durchgeführt werden, z. B. Registrierung, Aufheben der Registrierung, Verschieben und Übertragen von Lizenzen. Benutzer können dem Smart Account und bestimmten Virtual Accounts hinzugefügt werden. Ferner können ihnen entsprechende Berechtigungen zugewiesen werden.

Weitere Informationen zu Cisco Smart Licensing finden Sie unter:

- a) [Startseite von Cisco Smart Licensing](#)
- b) [Cisco Community – On-Demand-Schulungen](#).

Weitere Informationen zum neuen Smart Licensing Using Policy in Cisco IOS® XE Version 17.3.2 und höher finden Sie unter [Smart Licensing Using Policy auf Catalyst Switches](#)

Neu bei Smart Licensing und/oder der Administration von Smart Accounts? Registrieren Sie sich für den neuen Schulungskurs und die Aufzeichnung für Administratoren:

[Cisco Community – Vertiefen Sie Ihr Wissen mit Cisco Smart Accounts / Smart Licensing und My Cisco Entitlements](#)

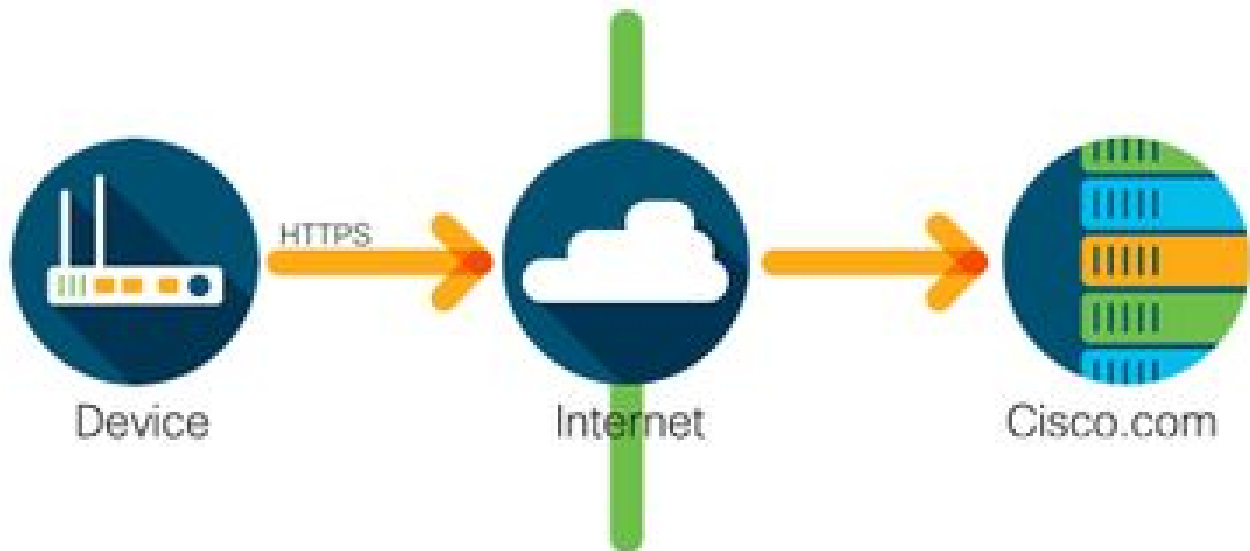
Smart Accounts können hier erstellt werden: [Smart Accounts](#)

Smart Accounts können hier verwaltet werden: [Smart Software Licensing](#)

Smart Licensing-Implementierungsmethoden

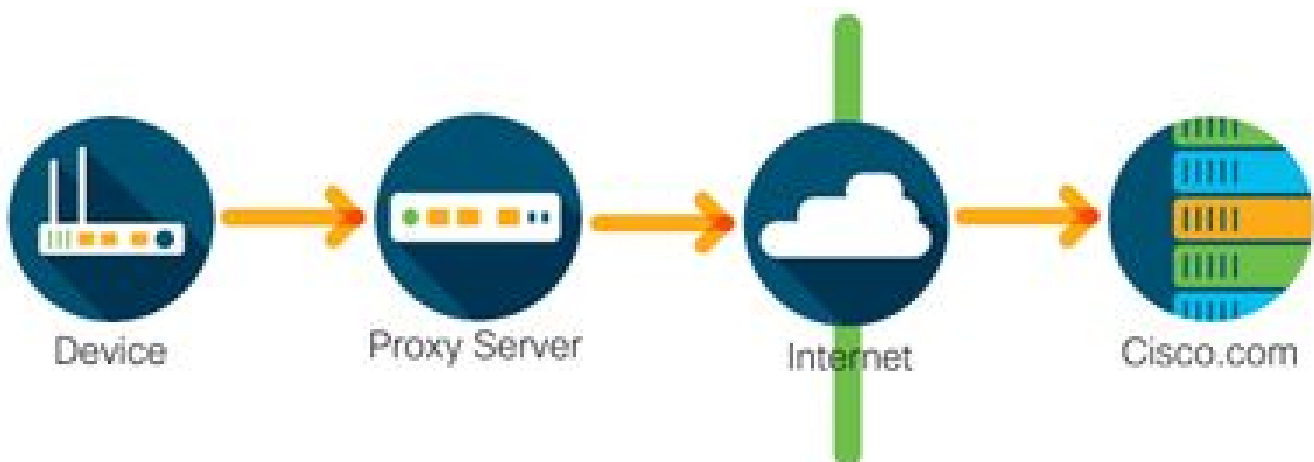
Es gibt mehrere Methoden für die Bereitstellung von Cisco Smart Licensing, die je nach Sicherheitsprofil eines Unternehmens genutzt werden können. Dazu zählen folgende:

Direkter Cloud-Zugriff



Das Cisco Produkt sendet die Nutzungsinformationen mit HTTPS sicher und direkt über das Internet. Es werden keine zusätzlichen Komponenten benötigt.

Zugriff über einen HTTPS-Proxy



Cisco Produkte senden Nutzungsinformationen mit HTTPS sicher über einen HTTP-Proxyserver. Ein vorhandener Proxyserver kann verwendet werden, oder dieser kann über das Cisco Transport Gateway bereitgestellt werden. (für weitere Informationen [hier klicken](#)).

Lokaler Lizenzserver (auch bekannt als Cisco Smart Software Manager-Satellit)



Cisco Produkte senden Nutzungsinformationen nicht direkt über das Internet, sondern an einen lokalen Server. Einmal pro Monat greift der Server über HTTPS über das Internet auf alle Geräte zu oder kann manuell übertragen werden, um seine Datenbank zu synchronisieren. CSSM vor Ort (Satellit) ist als virtuelles System verfügbar und kann [hier](#) heruntergeladen werden. Weitere Informationen finden Sie auf der Seite [Smart Software Manager Satellit](#).

Unterstützte Cisco IOS XE-Plattformen

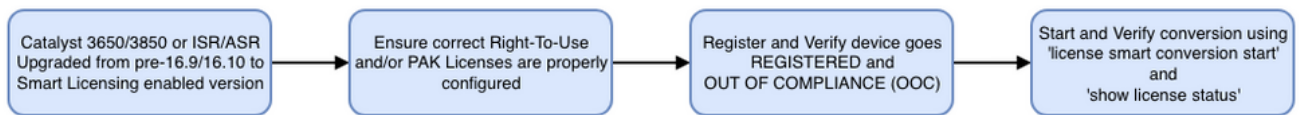
- Ab Cisco IOS XE-Version 16.9.1 unterstützen die Switch-Plattformen der Catalyst 3650/3850- und Catalyst 9000-Serie die Cisco Smart Licensing-Methode als einzige Lizenzierungsmethode.
- Ab Cisco IOS XE-Version 16.10.1 unterstützen Router-Plattformen wie ASR1K, ISR1K, ISR4K und virtuelle Router (CSRv/ISRv) die Cisco Smart Licensing-Methode als einzige Lizenzierungsmethode.

Migration von älteren Lizenzen zu Smart Licenses

Es gibt zwei Methoden, um eine ältere Lizenz, wie RTU (Right-To-Use) oder PAK (Product Activation Key), in eine Smart-Lizenz umzuwandeln. Weitere Informationen dazu, welche Methode befolgt werden muss, finden Sie in den entsprechenden Versionshinweisen und/oder im Konfigurationsleitfaden für das jeweilige Cisco Gerät.

Umwandlung durch gerätegesteuerte Konvertierung (Device Led Conversion, kurz DLC)

- Device Led Conversion (DLC) ist eine einmalige Methode, bei der das Cisco Produkt die von ihm verwendeten Lizenzen melden kann und die Lizenzen automatisch auf dem entsprechenden Smart Account im Cisco Smart Software Manager (CSSM) hinterlegt werden. Das DLC-Verfahren wird direkt über die Kommandozeile (Command Line Interface, CLI) des jeweiligen Cisco Geräts durchgeführt.
- Der DLC-Prozess wird nur auf dem Catalyst 3650/3850 und ausgewählten Router-Plattformen unterstützt. Informationen zu bestimmten Routermodellen finden Sie in der Konfigurationsanleitung für die jeweilige Plattform sowie in den Versionshinweisen. Beispiel: [DLC-Verfahren für Catalyst 3850 mit Fuji 16.9.x-Versionen](#).



Umwandlung über Cisco Smart Software Manager (CSSM) oder License Registration Portal (LRP)

Cisco Smart Software Manager(CSSM)-Methode:

1. Melden Sie sich unter <https://software.cisco.com/> bei Cisco Smart Software Manager (CSSM) an.
2. Navigieren Sie zu Smart Software Licensing > Convert to Smart Licensing
3. Wählen Sie PAK konvertieren oder Lizenzen konvertieren.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts | Inventory | **Convert to Smart Licensing** | Reports | Preferences | Satellites | Activity

License Conversion

Convert PAKs | Convert Licenses | Conversion History | Event Log

The Product Activation Keys (PAKs) below contain licenses that can be used for traditional licensing or Smart Software Licensing. To add some or all of them to a Virtual Account as Smart Software Licenses, use the 'Convert to Smart Licenses' action in the table below.

If you do not see a PAK you expect to see in the table, ensure that it has been assigned to your Smart Account in the [Product License Registration Portal](#).

4. Um eine PAK-Lizenz umzuwandeln, suchen Sie die Lizenz in dieser Tabelle. Um eine Nicht-PAK-Lizenz zu konvertieren, verwenden Sie den Lizenzkonvertierungs-Assistenten für eine schrittweise Anleitung.

Speicherort der mit dem Konto verknüpften bekannten PAK-Dateien:

License Conversion

Convert PAKs | Convert Licenses | Conversion History | Event Log

The Product Activation Keys (PAKs) below contain licenses that can be used for traditional licensing or Smart Software Licensing. To add some or all of them to a Virtual Account as Smart Software Licenses, use the 'Convert to Smart Licenses' action in the table below.

If you do not see a PAK you expect to see in the table, ensure that it has been assigned to your Smart Account in the [Product License Registration Portal](#).

The Smart Account administrator may be able to more easily convert the licenses based on the automatic conversion settings.

Last Updated : 2019-Apr-17 05:30:35

PAK	SKUs	Order Number	Order Date	Virtual Account	Status	Actions
[REDACTED]	C1-ISE-PLS-T (25)	[REDACTED]	2018-May-07	CORE TAC		Convert to Smart Licen...
[REDACTED]	C1-ISE-BASE-T (25)	[REDACTED]	2018-May-07	CORE TAC		Convert to Smart Licen...
[REDACTED]	C1-ISE-BASE-T (25)	[REDACTED]	2018-May-07	CORE TAC		Convert to Smart Licen...

Speicherort des Links „Assistent für die Lizenzumwandlung“:


Smart Software Licensing


[Feedback](#) [Support](#) [Help](#)[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [Satellites](#) | [Activity](#)Questions About Licensing? 
[Try our Virtual Assistant](#)

License Conversion

Convert PAKs | **Convert Licenses** | Conversion History | Event Log

The table below contains devices in your Smart Account that are using traditional licenses that can be converted to Smart Software Licenses. If you do not see a device you expect to see in the table, ensure that it has been assigned to your Smart Account in the [Product License Registration Portal](#). You can also try entering the device information in the [License Conversion wizard](#).

Last Updated : 2018-Nov-14 10:31:53 



Device Identifier	Product Family	Eligible SKUs	Virtual Account	Actions
No Records Found				

No Records to Display

5. Suchen Sie die gewünschte Lizenz- und Produktkombination.


6. Klicken Sie (unter Aktionen): In Smart Licensing konvertieren.


License Conversion


Convert PAKs | Convert Licenses | Conversion History | Event Log



The Product Activation Keys (PAKs) below contain licenses that can be used for traditional licensing or Smart Software Licensing. To add some or all of them to a Virtual Account as Smart Software Licenses, use the 'Convert to Smart Licenses' action in the table below.

If you do not see a PAK you expect to see in the table, ensure that it has been assigned to your Smart Account in the [Product License Registration Portal](#).

 The Smart Account administrator may be able to more easily convert the licenses based on the automatic conversion settings.

Last Updated : 2019-Apr-16 09:30:49 



PAK	SKUs	Order Number	Order Date	Virtual Account	Status	Actions
	C1-ISE-PLS-T (25)		2018-May-07	CORE TAC		Convert to Smart Licen...
	C1-ISE-BASE-T (25)		2018-May-07	CORE TAC		Convert to Smart Licen...
	C1-ISE-BASE-T (25)		2018-May-07	CORE TAC		Convert to Smart Licen...
	C1-ISE-BASE-T (25)		2018-May-07	CORE TAC		Convert to Smart Licen...

7. Wählen Sie "Virtual Account", "License" und klicken Sie auf "Weiter".

Convert to Smart Software Licenses ✕

STEP 1


Select Licenses

STEP 2

Review and Confirm

Select the licenses you want to convert to Smart Software Licenses and the Destination Virtual Account to contain them. If the PAK allows partial fulfillment, you will be able to choose the number of licenses to convert, otherwise all licenses in the PAK will be converted.

PAK Details:

PAK Number: 

Partial Fulfillment: Not Allowed

PAK Virtual Account: CORE TAC

Destination Virtual Account:

SKUs

SKU	Licenses	Type	Expiration Date	Available to Convert	Quantity to Convert
C1-ISE-PLS-T	ISE_PLUS (ISE Plus License) 1.0	Term	2023-Jul-06	25	25

8. Überprüfen Sie die Auswahl, und klicken Sie dann auf Lizenzen konvertieren.

Convert to Smart Software Licenses

STEP 1 ✓ Select Licenses | STEP 2 Review and Confirm

PAK Details:

PAK Number: [REDACTED]
Partial Fulfillment: Not Allowed
PAK Virtual Account: CORE TAC
Destination Virtual Account: CORE TAC

SKUs to Convert

SKU	Licenses	Type	Expiration Date	Available to Convert	Quantity to Convert
C1-ISE-PLS-T	ISE_PLUS (ISE Plus License) 1.0	Term	2023-Jul-06	25	25

Since all of the licenses are being converted to Smart Licensing, they will no longer appear in the Product License Registration application.

Cancel Back **Convert Licenses**

License Registration Portal(LRP)-Methode:

1. Melden Sie sich beim Lizenzregistrierungsportal (LRP) an:

<http://tools.cisco.com/SWIFT/LicensingUI/Home>

2. Navigieren Sie zu Geräte > Geräte hinzufügen.

3. Geben Sie die richtige Produktfamilie und UDI-Produkt-ID (Unique Device Identifier) sowie die Seriennummer ein, und klicken Sie dann auf OK. Die UDI-Informationen können von der Befehlszeilenschnittstelle (Command Line Interface, CLI) des Cisco Geräts abgerufen werden, z. B. aus der Version anzeigen oder aus dem Inventar anzeigen.

Add Device

Virtual Account: CSR1000v *Required with Smart Account*

Product Family: Cloud Services Router

Device Identifier: UDI PID/SN

UDI PID: CSR1000V

UDI SN: [REDACTED]

Cancel OK

4. Wählen Sie das hinzugefügte Gerät aus, und konvertieren Sie Lizenzen in Smart Licensing.

PAKs or Tokens | Licenses | **Devices** | Transactions History

Get Licenses ▾ | Move Licenses ▾ | Add Devices | Download Licenses | Email Selected Licenses

<input type="checkbox"/>	Device	Virtual Account	Family
<input type="checkbox"/>	UDI Product ID:CSR1000V UDI Serial Number: [REDACTED]		Cloud Services Router
<input type="checkbox"/>	UDI Product ID:CSR1000V UDI Serial Number: [REDACTED]		Cloud Services Router

Download license...

Email license...

Rehost license...

Rehost license from failed device (RMA)...

Assign to Smart Account...

Convert licenses to Smart Licensing...

Get device information...

5. Ordnen Sie das entsprechende Virtual Account zu, wählen Sie die zu konvertierenden Lizenzen aus, und klicken Sie auf Submit (Senden).

Convert to Smart Entitlements ✕

Device ID: UDI Product ID:CSR1000V,UDI Serial Number:

Product Family: Cloud Services Router

Smart Account: .cisco.com

Virtual Account:

<input type="checkbox"/>	SKU	Type	Term Date	Quantity Available	Quantity to Convert
<input checked="" type="checkbox"/>	L-CSR-5G-SEC=	Perpetual	--	1	<input type="text" value="1"/>

i Once these entitlements have been converted they will no longer appear in this portal.

Tipp: Sie können das LRP-Tool auch verwenden, indem Sie auf der Registerkarte "PAKs" oder "Tokens" nach der Lizenz-/Produktfamilie suchen. Klicken Sie auf das Dropdown-Menü neben dem PAK/Token, und wählen Sie In Smart Licensing konvertieren:

PAK/Token	Virtual Account	Order Number	Product	Status	Licenses Used	Available
Family: ASR1001	DEFAULT		SKU: ASR1_MFGINSTALL	CONVERTED	1	0
			Cisco ASR 1000 Advanced IP... SKU: SLASR1-AIS	CONVERTED	4	0
Family: Cisco Nexus 9000 S...	DEFAULT		NX-OS Advantage license for... SKU: NXOS-AD-XF2	UNFULFILLED	0	1
Family: Cisco Nexus 9000 S...			NX-OS Advantage license for... SKU: NXOS-AD-XF2	UNFULFILLED	0	1
Family: Cisco Nexus 9000 S...			NX-OS Advantage license for... SKU: NXOS-AD-XF2	UNFULFILLED	0	1
Family: Cisco Nexus 9000 S...			NX-OS Advantage license for... SKU: NXOS-AD-XF2	UNFULFILLED	0	1

Kontakt: Cisco Global Licensing Operations (GLO) Department

Die Abteilung Global Licensing Operations ist [hier](#) in unseren weltweiten Kontaktcentern erreichbar.

Verhaltensänderung beim Catalyst 9500 High-Performance-Modell von 16.9 bis 16.12.3

Wie andere Catalyst 9000-Modelle wurden auch die Catalyst 9500 High-Performance-Modelle mit Smart Licensing in der Cisco IOS XE-Version 16.9 und höher aktiviert. Bei den Catalyst 9500 High-Performance-Modellen hatte jedoch jedes Modell sein eigenes spezifisches Lizenzberechtigungs-Tag. Später entschieden sich die Produkt- und Marketingteams für die Vereinheitlichung der Berechtigungs-Tags der C9500-Plattformen. Durch diese Entscheidung wurde das Verhalten der C9500 High-Performance-Modelle von der Verwendung bestimmter Berechtigungs-Tags zur Verwendung generischer C9500-Lizenzen geändert.

Diese Verhaltensänderung ist an folgenden Defekten dokumentiert:

- a) [Cisco Bug-ID CSCvp30661](#)
- b) [Cisco Bug-ID CSCvt01955](#)


Nachfolgend finden Sie die Vorher-Nachher-Beispiele der oben genannten Änderungen bei Lizenzänderungen für C9500-Hochleistungsmodelle:

Cisco IOS XE Version 16.11.x und früher

Jedes C9600 High-Performance-Modell hat seine eigenen Berechtigungs-Tags.

Modell	Lizenz
C9500-32C	C9500 32C NW Essentials

	C9500 32C NW Advantage C9500 32C DNA Essentials C9500 32C DNA Advantage
C9500-32QC	C9500 32QC NW Essentials C9500 32QC NW Advantage C9500 32QC DNA Essentials C9500 32QC DNA Advantage
C9500-24Y4C	C9500 24Y4C NW Essentials C9500 24Y4C NW Advantage C9500 24Y4C DNA Essentials C9500 24Y4C DNA Advantage
C9500-48Y4C	C9500 48Y4C NW Essentials C9500 48Y4C NW Advantage C9500 48Y4C DNA Essentials C9500 48Y4C DNA Advantage


 Hinweis: Die Cisco IOS XE-Versionen 16.12.1 und 16.12.2 weisen Fehler mit der [Cisco Bug-ID CSCvp30661](#) und der [Cisco Bug-ID CSCvt01955](#) auf. Diese Mängel werden in 16.12.3a und später behoben.

Cisco IOS XE Version 16.12.3 und höher

Hochleistungsplattformen der Catalyst Serie 9500 verwenden jetzt generische Netzwerk-Lizenztags und separate DNA-Lizenztags. Diese Tabelle zeigt die Änderungen an Berechtigungen, die in Cisco IOS XE Version 16.12.3 und höher hervorgehoben wurden:

Modell	Lizenz
C9500-32C	C9500 Network Essentials

	C9500 Network Advantage C9500 32C DNA Essentials C9500 32C DNA Advantage
C9500-32QC	C9500 Network Essentials C9500 Network Advantage C9500 32QC DNA Essentials C9500 32QC DNA Advantage
C9500-24Y4C	C9500 Network Essentials C9500 Network Advantage C9500 24Y4C DNA Essentials C9500 24Y4C DNA Advantage
C9500-48Y4C	C9500 Network Essentials C9500 Network Advantage C9500 48Y4C DNA Essentials C9500 48Y4C DNA Advantage

 Hinweis: Upgrades von Cisco IOS XE-Versionen 16.12.1 und 16.12.2 zeigen dieses Lizenzverhalten. Upgrades von Cisco IOS XE-Versionen 16.9.x, 16.10.x, 16.11.x auf 16.12.3 erkennen alte Lizenzkonfigurationen.

C9500 – Häufig gestellte Fragen Änderungen bei High-Performance-Modellen

1. Warum unterstützt Cisco die Zuweisung einer generischen Netzwerklizenz, wenn mein Gerät eine gerätespezifische Netzwerklizenz nutzt?

Generische Tags werden bereitgestellt, da dies die richtigen Berechtigungs-Tags für das Netzwerkgerät sind. Dies ermöglicht die Verwendung der Berechtigungs-Tags für die gesamte Cat9500-Plattform, nicht nur für die spezifischen C9500 High-Performance-Modelle. Images vor Version 16.12.3, die nach gerätespezifischen Lizenz-Tags fragen, entsprechen den allgemeinen Lizenz-Tags, da die spezifischeren Lizenzen unter die generischen Lizenzen in der Lizenzierungshierarchie fallen.

2. Warum erscheinen manchmal zwei Netzwerk-Tags im Smart Account?

Dieses Verhalten ist auf die Lizenzierungshierarchie zurückzuführen und tritt auf, wenn das Gerät auf einem älteren Image ausgeführt wird, das gerätespezifische Lizenzierungs-Tags verwendet. Ältere Images, die nach gerätespezifischen Lizenz-Tags fragen, stimmen mit den generischen Lizenz-Tags überein, da die spezifischeren Tags unter die generischen Lizenzen in der Lizenzierungshierarchie fallen.

Konfiguration

Basiskonfiguration

Eine genaue Anleitung zur Konfiguration von Smart Licensing finden Sie im Systemmanagement-Konfigurationshandbuch, das für jede Version/Plattform zur Verfügung steht.

Beispiel: [Konfigurationsleitfaden für das Systemmanagement, Cisco IOS XE Fuji 16.9.x \(Switches der Catalyst 9300-Serie\)](#)

Registrierungs-Token/Geräte-ID-Token

Vor der Registrierung des Geräts muss ein Token generiert werden. Das Registrierungstoken, auch als Geräte-ID-Token bekannt, ist ein eindeutiges Token, das vom Smart Licensing Portal oder vom Cisco Smart Software Manager vor Ort generiert wird, wenn ein Cisco Gerät zunächst beim entsprechenden Smart Account registriert wird. Abhängig von den bei der Erstellung verwendeten Parametern kann ein einzelnes Token verwendet werden, um mehrere Cisco Geräte zu registrieren.

Das Registrierungs-Token ist auch nur bei der Erstregistrierung eines Cisco Geräts erforderlich, da es dem Gerät die Informationen zur Verfügung stellt, um am Cisco Back-End die Call-Home-Funktion durchzuführen und mit dem richtigen Smart Account verknüpft zu werden. Nach der Registrierung des Cisco Geräts ist das Token nicht mehr erforderlich.

Für weitere Informationen zu Registrierungs-Token und wie diese generiert werden, [klicken Sie hier](#) für eine allgemeine Anleitung. Weitere Informationen finden Sie im Konfigurationsleitfaden für das jeweilige Cisco Gerät.

Registrierungs- und Lizenzstatus

Bei der Bereitstellung und Konfiguration von Smart Licensing gibt es mehrere mögliche Zustände, in denen sich ein Cisco Gerät befinden kann. Diese Status können durch Prüfen von Alle Lizenzen anzeigen oder Lizenzstatus anzeigen über die Kommandozeile (Command Line Interface, kurz CLI) des Cisco Geräts angezeigt werden.

Hier ist eine Liste aller Zustände und ihrer Beschreibung:

Status „Evaluation (Unidentified)“ (Evaluierung, Nicht identifiziert)

- Die Auswertung ist der Standardstatus des Geräts beim ersten Start.
- In der Regel wird dieser Status angezeigt, wenn ein Cisco Gerät noch nicht für Smart Licensing konfiguriert oder bei einem Smart Account registriert wurde.
- In diesem Zustand sind alle Funktionen verfügbar, und das Gerät kann die Lizenzstufe frei ändern.
- Der Evaluierungszeitraum wird verwendet, wenn sich das Gerät im nicht identifizierten Zustand befindet. Das Gerät versucht in diesem Zustand nicht, mit Cisco zu kommunizieren.
- Dieser Evaluierungszeitraum beträgt 90 Tage und nicht 90 Kalendertage. Nach Ablauf des Evaluierungszeitraums wird dieser niemals zurückgesetzt.
- Es gibt einen Evaluierungszeitraum für das gesamte Gerät, nicht jedoch einen Evaluierungszeitraum pro Berechtigung.
- Wenn der Evaluierungszeitraum nach 90 Tagen abläuft, wechselt das Gerät in den Modus EVAL EXPIRY (EVAL EXPIRY). Auch nach dem Neuladen treten jedoch keine funktionalen Beeinträchtigungen oder Funktionsstörungen auf. Gegenwärtig gibt es keine Durchsetzung.
- Die Countdown-Zeit wird für alle Neustarts beibehalten.
- Der Evaluierungszeitraum wird verwendet, wenn sich das Gerät noch nicht bei Cisco registriert hat und die beiden folgenden Nachrichten vom Cisco Backend nicht erhalten hat:
 1. Erfolgreiche Antwort auf eine Registrierungsanfrage.
 2. Erfolgreiche Antwort auf eine Anfrage zur Berechtigungsautorisierung.

Status „Registered“ (Registriert)

- Registriert ist der erwartete Status nach erfolgreichem Abschluss der Registrierung.
 - Dieser Status gibt an, dass das Cisco Gerät erfolgreich mit einem Cisco Smart Account kommunizieren und sich registrieren konnte.
 - Das Gerät erhält ein ID-Zertifikat, das für ein Jahr gültig ist und für zukünftige Kommunikation verwendet wird.
 - Das Gerät sendet eine Anfrage an CSSM, um die Berechtigungen für die Lizenzen zu autorisieren, die auf dem Gerät verwendet werden.
 - Je nach CSSM-Antwort wechselt das Gerät in den Status "Authorized" (Autorisiert) oder "Out of Compliance" (Nicht konform).
 - Das ID-Zertifikat läuft am Ende eines Jahres ab. Nach sechs Monaten versucht der Software-Agent-Prozess, das Zertifikat zu erneuern. Wenn der Agent nicht mit dem CSSM kommunizieren kann, versucht er weiterhin, das ID-Zertifikat bis zum Ablaufdatum (ein Jahr) zu erneuern. Nach Ablauf eines Jahres wechselt der Agent in den Status "Nicht identifiziert" zurück und versucht, den Evaluierungszeitraum zu aktivieren. Der CSSM entfernt die Produktinstanz aus seiner Datenbank.
- Status „Authorized“ (Autorisiert)
 - Autorisiert ist der erwartete Status, wenn das Gerät eine Berechtigung verwendet und die Compliance-Anforderungen erfüllt (kein negativer Saldo).
 - Dieser Status gibt an, dass das virtuelle Konto auf dem CSSM über den richtigen Typ und die richtige Anzahl von Lizenzen verfügte, um die Nutzung der Lizenzen für dieses Gerät zu autorisieren.
 - Nach Ablauf von 30 Tagen sendet das Gerät eine neue Anforderung an den CSSM, um die Autorisierung zu erneuern.
 - Dieser Status hat eine Zeitspanne von 90 Tagen. Nach 90 Tagen (sofern nicht erfolgreich

verlängert) wird das Gerät in den Status "Autorisierung abgelaufen" versetzt.

Status „Out of Compliance“ (Keine Compliance)

- "Out of Compliance" (Nicht konform) ist der Status, in dem das Gerät eine Berechtigung verwendet und die Compliance nicht erfüllt (negativer Saldo).
- Dieser Status wird angezeigt, wenn für das Gerät keine verfügbare Lizenz im entsprechenden Virtual Account vorhanden ist, für das Cisco Gerät im Cisco Smart Account registriert ist.
- Um den Status "Compliance/Autorisiert" zu erhalten, müssen Sie dem Smart Account die richtige Anzahl und den richtigen Lizenztyp hinzufügen.
- Befindet sich ein Gerät im Status "Out of Compliance" (Nicht konform), sendet es täglich automatisch eine Anfrage zur Erneuerung der Autorisierung.
- Die Lizenzen und Funktionen bleiben weiterhin gültig, ohne dass es zu funktionalen Beeinträchtigungen kommt.

Status „Authorization Expired“ (Autorisierung abgelaufen)

- "Autorisierung abgelaufen" ist der Status, wenn das Gerät eine Berechtigung verwendet und seit mehr als 90 Tagen nicht mehr mit dem zugehörigen Cisco Smart Account kommunizieren konnte.
- Dieser Status wird in der Regel angezeigt, wenn das Cisco Gerät nach der Erstregistrierung den Internetzugang verliert oder keine Verbindung mit tools.cisco.com herstellen kann.
- Online-Methoden der intelligenten Lizenzierung erfordern, dass Cisco Geräte mindestens alle 90 Tage kommunizieren, um einen Wechsel in diesen Status zu verhindern.
- CSSM gibt alle für dieses Gerät verwendeten Lizenzen an den Pool zurück, da seit 90 Tagen keine Kommunikation mit dem Gerät stattgefunden hat.
- In diesem Zustand versucht das Gerät weiterhin, stündlich eine Verbindung mit Cisco herzustellen, um die Berechtigung zu verlängern, bis der Registrierungszeitraum (ID-Zertifikat) abläuft.
- Stellt der Softwareagent die Kommunikation mit Cisco wieder her und erhält seine Autorisierungsanfrage, verarbeitet er diese normal und wechselt in einen der festgelegten Status.

Überlegungen und Hinweise

Ab Version 16.9.1 für Switches und Version 16.10.1 für Router wird ein Call-Home-Standardprofil mit dem Namen CiscoTAC-1 erstellt, das die Migration zu Smart Licensing erleichtert. Standardmäßig ist dieses Profil für die Direct Cloud Access-Methode eingerichtet.

```
<#root>
```

```
#show call-home profile CiscoTAC-1
```

```
Profile Name: CiscoTAC-1
```

```
Profile status: ACTIVE
```

```
Profile mode: Full Reporting
```

Reporting Data: Smart Call Home, Smart Licensing
Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Transport Method: http
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Other address(es): default
<snip>

Bei Verwendung eines lokalen Cisco Smart Software Manager-Servers muss die Zieladresse in der aktiven Call-Home-Konfiguration darauf verweisen (Groß-/Kleinschreibung beachten!):

```
<#root>

(config)#call-home
(cfg-call-home)#profile "CiscoTAC-1"
(cfg-call-home-profile)#destination address http https://

<IP/FQDN>

/Transportgateway/services/DeviceRequestHandler
```

DNS ist erforderlich, um tools.cisco.com aufzulösen. Wenn sich die DNS-Server-Verbindung in einer VRF-Instanz befindet, stellen Sie sicher, dass die richtige Quellschnittstelle und VRF-Instanz definiert sind:

Global Routing Table Used:

```
(config)#ip domain-lookup [source-interface <INTERFACE>]
(config)#ip name-server <IP>
```

VRF Routing Table Used:

```
(config)#ip domain-lookup [source-interface <INTERFACE>] <<-- "ip vrf forwarding <VRF-NAME>" defined
(config)#ip name-server vrf <VRF-NAME> <SERVER-IP>
```

Wenn kein DNS verfügbar ist, können Sie alternativ die Zuordnung von lokalem DNS zu IP (basierend auf der lokalen DNS-Auflösung auf dem Endgerät) statisch konfigurieren oder den DNS-Namen in der Call-Home-Konfiguration durch eine IP-Adresse ersetzen. Beziehen Sie sich auf das Beispiel für den direkten Cloud-Zugriff (verwenden Sie beim Cisco Smart Software Manager vor Ort seinen eigenen DNS-Namen anstelle von tools.cisco.com):

```
(config)#ip host tools.cisco.com <x.x.x.x>
```

Wenn die Kommunikation mit tools.cisco.com von der Schnittstelle in einer bestimmten VRF-Instanz (z. B. Mgmt-vrf) ausgehen muss, muss diese CLI konfiguriert werden:

```
(config)#ip http client source-interface <VRF_INTERFACE>
```

Je nach Konfiguration des Cisco Geräts kann eine andere Anzahl von Lizenzen genutzt werden, z. B. für Catalyst Switches, die in StackWise oder StackWise Virtual ausgeführt werden:

Traditionelle Stack-weise unterstützte Switches (z. B. Catalyst Serie 9300):

Netzwerklicenz: 1 Lizenz pro Switch im Stack verbraucht

DNA-Lizenz: 1 Lizenz pro Switch im Stack verbraucht

Modulare Chassis (z. B. Catalyst Serie 9400):

Netzwerklicenz: 1 Lizenz wird pro Supervisor im Chassis genutzt

DNA-Lizenz: 1 Lizenz pro Chassis verbraucht

Stack-weise feste, virtuell unterstützte Switches (z. B. Catalyst Serie 9500):

Netzwerklicenz: 1 Lizenz pro Switch im Stack verbraucht

DNA-Lizenz: 1 Lizenz pro Switch im Stack verbraucht

- Für Smart Licensing kann nur ein Call-Home-Profil aktiv sein.
- Lizenzen werden nur genutzt, wenn eine entsprechende Funktion konfiguriert ist.
- Cisco Geräte, die für Smart Licensing konfiguriert sind, müssen mit der richtigen Systemzeit und dem richtigen Systemdatum konfiguriert werden, um sicherzustellen, dass sie ordnungsgemäß mit dem entsprechenden Cisco Smart Account synchronisiert werden. Wenn das Zeit-Offset des Cisco Geräts zu weit entfernt ist, kann die Registrierung des Geräts fehlschlagen. Die Uhr muss manuell über ein Zeitsteuerungsprotokoll wie Network Time Protocol (NTP) oder Precision Time Protocol (PTP) eingestellt oder konfiguriert werden. Die genauen Schritte, die zur Implementierung dieser Änderungen erforderlich sind, finden Sie im Konfigurationsleitfaden für das jeweilige Cisco Gerät.
- Der PKI-Schlüssel (Public Key Infrastructure), der bei der Cisco Geräteregistrierung generiert wird, muss gespeichert werden, wenn er nach der Registrierung nicht automatisch gespeichert wird. Wenn das Gerät den PKI-Schlüssel nicht speichern kann, wird ein Syslog generiert, in dem Sie aufgefordert werden, die Konfiguration mit dem Befehl `copy running-config startup-config` oder `write memory` zu speichern.
- Wenn der PKI-Schlüssel des Cisco Geräts nicht richtig gespeichert wird, kann der Lizenzstatus bei Failover oder Neuladen verloren gehen.
- Smart Licensing unterstützt standardmäßig kein Abfangen von HTTPS-Proxy-SSL-Zertifikaten, wenn Proxys von Drittanbietern für die HTTPS-Proxy-Methode verwendet werden. Zur Unterstützung dieser Funktion können Sie entweder das SSL-Abfangen auf dem Proxy deaktivieren oder die vom Proxy gesendete Zertifizierung manuell importieren.

<#root>

[How to Manually Import Certification as a TrustPoint:](#)

The certificate will need be in a BASE64 format to be copied and pasted onto the device as a TrustPoint

The following example shown below uses "LicRoot" as the TrustPoint name, however, this name can be changed

```
Device#conf t
Device(config)#crypto pki trustpoint LicRoot
Device(ca-trustpoint)#enrollment terminal
Device(ca-trustpoint)#revocation-check none
Device(ca-trustpoint)#exit
Device(config)#crypto pki authenticate LicRoot
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
Certificate has the following attributes:
  Fingerprint MD5: XXXXXXXX
  Fingerprint SHA1: XXXXXXXX
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Wenn Sie den Transport Gateway HTTP Proxy verwenden, muss die IP-Adresse wie in diesem Beispiel von tools.cisco.com in Proxy geändert werden:

Zieladresse: http https://tools.cisco.com/its/service/oddce/services/DDCEService

ZU

Zieladresse: http https://<TransportGW-

IP_Address>:<Portnummer>/Transportgateway/Services/DeviceRequestHandler

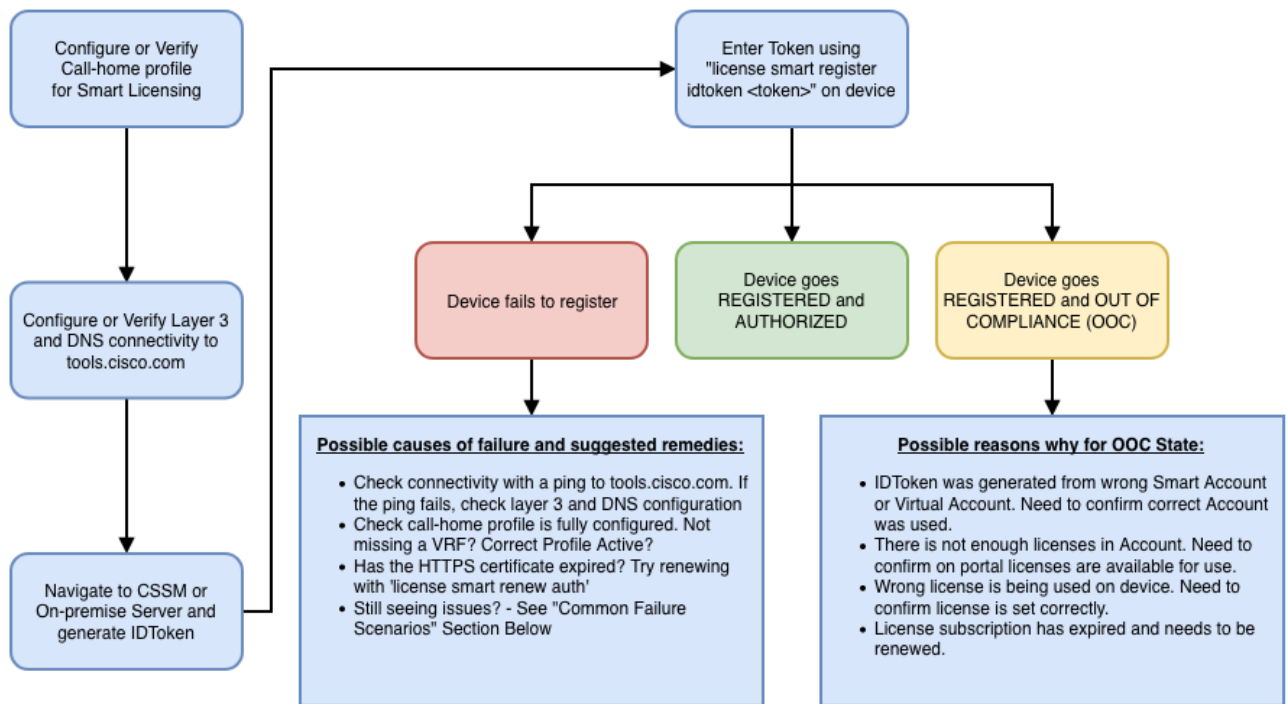
Die Transport-Gateway-IP-Adresse finden Sie, indem Sie zu den HTTP-Einstellungen navigieren und unter den HTTP-Service-URLs in der Cisco Transport Gateway-GUI suchen.

Weitere Informationen finden Sie [hier](#) im Konfigurationsleitfaden für das Cisco Transport Gateway.

Fehlerbehebung

Wenn Sie ein Cisco Gerät zu einer für Smart Licensing aktivierten Softwareversion migrieren, können Sie dieses Flussdiagramm als allgemeinen Leitfaden für alle drei Methoden (Direct Cloud Access, HTTPS Proxy und Cisco Smart Software Manager On-Prem) verwenden.

Das Gerät wurde mit einer Softwareversion aktualisiert oder geliefert, die Smart Licensing unterstützt (siehe Abschnitt 1.3 für eine Liste der unterstützten Cisco IOS-XE-Versionen).



Diese Schritte zur Fehlerbehebung konzentrieren sich hauptsächlich auf ein Szenario, in dem das Gerät sich nicht registriert.

Gerät kann nicht registriert werden

Nach der Erstkonfiguration muss zur Aktivierung von Smart Licensing ein Token, das lokal auf CSSM/Cisco Smart Software Manager vor Ort generiert wird, über die CLI auf dem Gerät erfasst werden:

```
license smart register idtoken <TOKEN>
```

Diese Aktion generiert folgende Ereignisse:

```
<#root>
```

```
! Smart licensing process starts
```

```
!
```

```
Registration process is in progress. Use the 'show license status' command to check the progress and re
```

```
!
```

```
! Crypto key is automatically generated for HTTPS communication
```

!

Generating 2048 bit RSA keys, keys will be exportable... [OK] (elapsed time was 1 seconds)
%CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or imported by crypto-engine
%PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write memory" to save new IOS PKI configur

!

! Call-home start registration process

!

%CALL_HOME-6-SCH_REGISTRATION_IN_PROGRESS: SCH device registration is in progress. Call-home will poll

!

! Smart Licensing process connects with CSSM and check entitlement.

!

%SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed
%SMART_LIC-6-AGENT_REG_SUCCESS: Smart Agent for Licensing Registration with the Cisco Smart Software Ma
%SMART_LIC-4-CONFIG_NOT_SAVED: Smart Licensing configuration has not been saved

%SMART_LIC-5-IN_COMPLIANCE: All entitlements and licenses in use on this device are authorized

%SMART_LIC-6-AUTH_RENEW_SUCCESS: Authorization renewal with the Cisco Smart Software Manager or satellit

Führen Sie folgende CLI aus, um die Call-Home-Konfiguration zu überprüfen:

<#root>

#show call-home profile all

Profile Name: CiscoTAC-1

Profile status: ACTIVE

Profile mode: Full Reporting

Reporting Data: Smart Call Home, Smart Licensing

Preferred Message Format: xml

Message Size Limit: 3145728 Bytes

Transport Method: http

HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

Other address(es): default

Periodic configuration info message is scheduled every 1 day of the month at 09:15

Periodic inventory info message is scheduled every 1 day of the month at 09:00

Alert-group	Severity
-----	-----
crash	debug
diagnostic	minor
environment	warning
inventory	normal

Syslog-Pattern	Severity
-----	-----
APF-.-WLC_.*	warning
.*	major

Führen Sie folgende CLI aus, um den Smart Licensing-Status zu überprüfen:

```
<#root>
```

```
#show license summary
```

```
Smart Licensing is ENABLED
```

```
Registration:
```

```
Status: REGISTERED
```

```
Smart Account: TAC Cisco Systems, Inc.  
Virtual Account: Krakow LAN-SW  
Export-Controlled Functionality: ALLOWED  
Last Renewal Attempt: None  
Next Renewal Attempt: Nov 22 21:24:32 2019 UTC
```

```
License Authorization:
```

```
Status: AUTHORIZED
```

```
Last Communication Attempt: SUCCEEDED
```

```
Next Communication Attempt: Jun 25 21:24:37 2019 UTC
```

```
License Usage:
```

License	Entitlement tag	Count	Status
-----	-----	-----	-----
C9500 Network Advantage	(C9500 Network Advantage)	1	AUTHORIZED
C9500-DNA-40X-A	(C9500-40X DNA Advantage)	1	AUTHORIZED

Wenn das Gerät nicht registriert werden kann (und der Status sich von REGISTRIRT unterscheidet), weist die Nichteinhaltung auf ein CSSM-Problem hin, z. B. eine fehlende Lizenz in Smart Virtual Account, eine falsche Zuordnung (z. B. ein Token von einem anderen Virtual Account, das verwendet wird, wenn keine Lizenzen verfügbar sind) usw. Überprüfen Sie diese Punkte:

1. Überprüfen Sie die Konfigurationseinstellungen und häufige Fehlerszenarien.

Siehe Abschnitt 2.1 für grundlegende Konfigurationsschritte. In Abschnitt 5 finden Sie auch häufige Fehlerszenarien, die vor Ort beobachtet wurden.

2. Grundlegende Verbindungen überprüfen

Stellen Sie sicher, dass das Gerät die Verbindung zu tools.cisco.com (und öffnen Sie den TCP-Port) (bei direktem Zugriff) oder zum Cisco Smart Software Manager-Server vor Ort herstellen kann:

```
<#root>
```

```
#show run all | in destination address http
```

```
destination address http
```

```
https://tools.cisco.com
```

```
/its/service/oddce/services/DDCEService
```

```
!
```

```
! check connectivity
```

```
!
```

```
#telnet tools.cisco.com 443 /source-interface gi0/0
```

```
Trying tools.cisco.com (x.x.x.x, 443)... Open
```

```
[Connection to tools.cisco.com closed by foreign host]
```

Wenn diese Befehle nicht funktionieren, überprüfen Sie Ihre Routing-Regeln, Quellschnittstellen und Firewall-Einstellungen.



Hinweis: HTTP (TCP/80) ist veraltet und das empfohlene Protokoll ist HTTPS (TCP/443).

Siehe Abschnitt 3. Überlegungen und Hinweise in diesem Dokument für weitere Richtlinien zur Konfiguration von DNS- und HTTP-Details.

3. Überprüfen Sie die Smart License-Einstellungen.

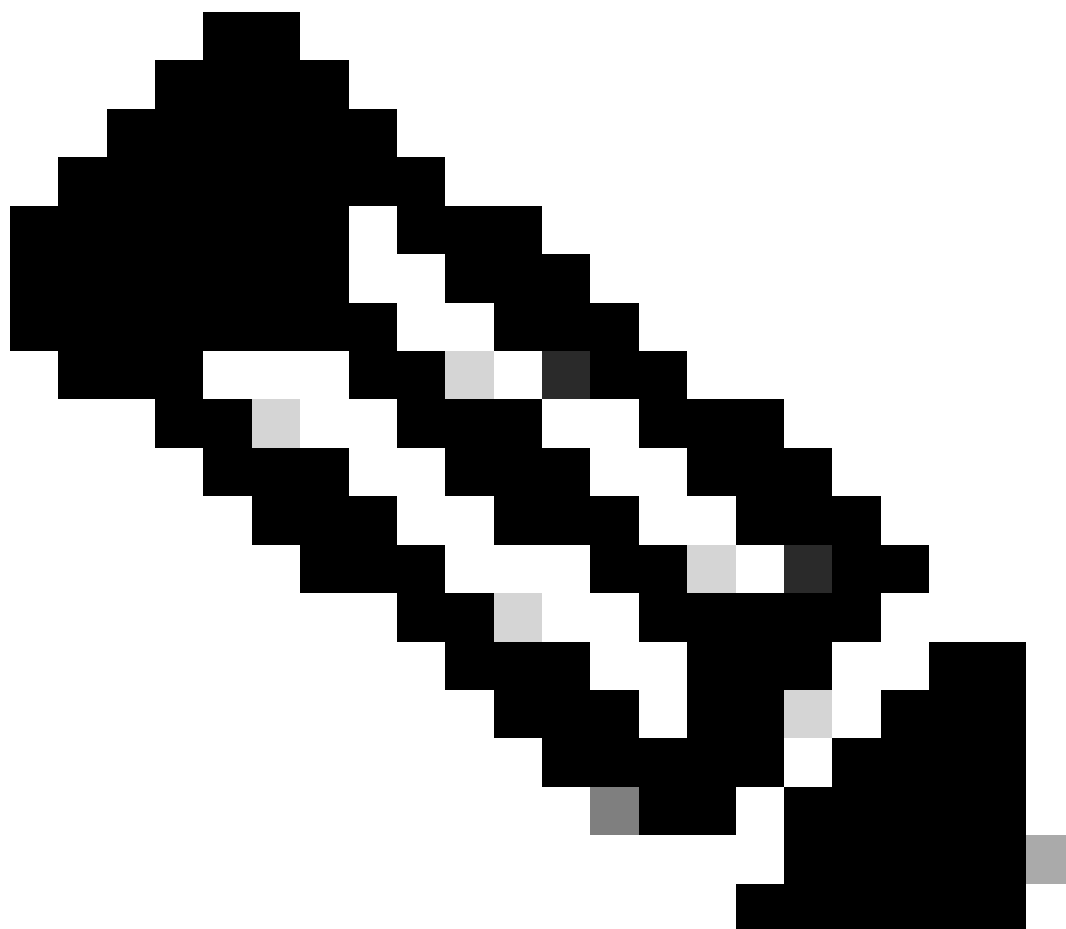
Erfassen Sie die Ausgabe von:

```
#show tech-support license
```

und validieren Sie die erfassten Konfigurationen/Protokolle (hängen Sie diese Ausgabe an, falls Sie entscheiden, den Cisco TAC-Fall für weitere Untersuchungen zu öffnen).

4. Debug-Funktionen aktivieren

Aktivieren Sie diese Debugs, um zusätzliche Informationen über den Smart Licensing-Prozess zu sammeln.



Hinweis: Nach dem Aktivieren von Debugging müssen Sie versuchen, die Lizenz erneut über CLI zu registrieren, wie in Abschnitt 4.1 erwähnt.

```
#debug call-home smart-licensing [all | trace | error]
#debug ip http client [all | api | cache | error | main | msg | socket]
```

Aktivieren und lesen Sie für die interne Fehlersuche die binäre Ablaufverfolgung:

```
! enable debug
#set platform software trace ios [switch] active R0 infra-sl debug
!
! read binary traces infra-sl process logs
#show platform software trace message ios [switch] active R0
```

Häufige Fehlerszenarien

In diesem Abschnitt werden einige häufige Fehlerszenarien beschrieben, die während oder nach der Registrierung eines Cisco Geräts auftreten können:

Szenario #1: Switch-Registrierung "Fehlerursache: Produkt bereits registriert"

Ausschnitt von „show license all“:

Registrierung:

Status: UNREGISTERED – REGISTRATION FAILED (Nicht registriert – Registrierung fehlgeschlagen)

Ausfuhrkontrollierte Funktionalität: Nicht zulässig


Erstregistrierung: FEHLGESCHLAGEN am 22. Okt. 14:25:31 2018 EST

Fehlerursache: Produkt bereits registriert

Nächster Registrierungsversuch: 22. Okt. 14:45:34 2018 EST

Weitere Schritte:

- Das Cisco Gerät muss erneut registriert werden.
- Wenn das Cisco Gerät im CSSM erkannt wird, muss der Parameter "force" verwendet werden (d. h. "license smart register idtoken <TOKEN> force").

 Hinweis: Der Fehlergrund kann auch angezeigt werden als:

- Fehlerursache: Das Produkt <X> und die Sudi, die udiSerialNumber:<SerialNumber>,udiPid:<Product> enthalten, wurden bereits registriert.
- Fehlerursache: Vorhandene Produktinstanz weist Verbrauch auf und erzwingt Markierung ist falsch

Szenario #2: Switch-Registrierung "Fehlerursache: Ihre Anfrage konnte derzeit nicht bearbeitet werden. Bitte versuchen Sie es erneut"

Ausschnitt von „show license all“:

Registrierung:

Status: REGISTRIERUNG - REGISTRIERUNG IN BEARBEITUNG

Ausfuhrkontrollierte Funktionalität: Nicht zulässig

Erstregistrierung: FEHLGESCHLAGEN am 24. Okt. 15:55:26 2018 EST

Fehlerursache: Ihre Anfrage konnte gerade nicht verarbeitet werden. Bitte versuchen Sie es erneut

Nächster Registrierungsversuch: 24. Oktober 16:12:15 2018 EST

Weitere Schritte:

- Aktivieren Sie Debug-Meldungen wie in Abschnitt 4 erwähnt, um mehr Einblicke in das Problem zu erhalten.
- Generieren Sie in Ihrem Smart Licensing ein neues Token in CSSM, und versuchen Sie es erneut.

Szenario #3: Fehlerursache "Das Gerätedatum 1526135268653 liegt außerhalb der zulässigen Toleranzgrenze.

Ausschnitt von „show license all“:

Registrierung:

Status: REGISTRIERUNG - REGISTRIERUNG IN BEARBEITUNG

Ausfuhrkontrollierte Funktionalität: Nicht zulässig

Erstregistrierung: FEHLGESCHLAGEN am 17.11.2017:55:46 EST

Fehlerursache: {"timestamp":["The device date '1526135268653' is offset beyond the allowed tolerance limit."]}

Nächster Registrierungsversuch: 11. November 18:12:17 2018 EST

Mögliche angezeigte Protokolle:

%PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Fehler bei der Validierung der Zertifikatskette. Das Zertifikat (SN: XXXXXX) ist noch nicht gültig. Der Gültigkeitszeitraum beginnt am 12.12.2018 um 12:43Z

Weitere Schritte:

- Vergewissern Sie sich, dass die Uhr des Cisco Geräts die richtige Zeit anzeigt (Uhr anzeigen).
- Konfigurieren Sie nach Möglichkeit das Network Time Protocol (NTP), um sicherzustellen, dass die Uhr richtig eingestellt ist.
- Wenn NTP nicht möglich ist, überprüfen Sie, ob die manuell eingestellte Uhr (Uhrensatz) korrekt ist (Uhr anzeigen) und als vertrauenswürdige Zeitquelle konfiguriert ist, indem Sie überprüfen, ob der Uhrenkalender gültig konfiguriert ist.



Hinweis: Standardmäßig ist die Systemuhr nicht vertrauenswürdig. Ein gültiger Uhrenkalender ist erforderlich.

Szenario #4: Switch-Registrierung "Fehlerursache: Kommunikationstransport nicht verfügbar."

Ausschnitt von „show license all“:

Registrierung: Status: NICHT REGISTRIERT - REGISTRIERUNG fehlgeschlagen

Ausfuhrkontrollierte Funktionalität: Nicht zulässig

Erstregistrierung: FEHLGESCHLAGEN am 09. März 2019 21:42:02 CST

Fehlergrund: Kommunikationstransport nicht verfügbar.

Mögliche angezeigte Protokolle:

%CALL_HOME-3-CALL_HOME_FAILED_TO_ENABLE: Fehler beim Aktivieren des Call-Home vom Smart Agent für die Lizenzierung: Der Befehl konnte Smart Call Home aufgrund eines vorhandenen aktiven Benutzerprofils nicht aktivieren. Wenn Sie ein anderes Benutzerprofil als das CiscoTAC-1-Profil verwenden, um Daten an den SCH-Server in Cisco zu senden, geben Sie unter "profile mode" (Profilmodus) den Befehl `reporting smart-license-data` ein, um dieses Profil für die intelligente Lizenzierung zu konfigurieren. Weitere Informationen zu SCH finden Sie unter

<http://www.cisco.com/go/smartcallhome>

%SMART_LIC-3-AGENT_REG_FAILED: Fehler beim Smart Agent für die Lizenzregistrierung beim Cisco Smart Software Manager oder Satelliten: Kommunikationstransport nicht verfügbar.

%SMART_LIC-3-COMM_FAILED: Kommunikationsfehler mit dem Cisco Smart Software Manager oder Satelliten: Kommunikationstransport nicht verfügbar.

Weitere Schritte:

- Überprüfen Sie, ob "call-home" mit "service call-home" in der Ausgabe "show running-config" des Cisco Geräts aktiviert ist.
- Stellen Sie sicher, dass das richtige Call-Home-Profil aktiv ist.
- Überprüfen Sie, ob die Smart Licensing-Daten für das Reporting im aktiven Call-Home-Profil konfiguriert sind.

Szenario #5: Switch-Lizenz-Autorisierung "Fehlerursache: Senden von HTTP-Nachrichten mit Call Home fehlgeschlagen."

Ausschnitt von „show license all“:

Lizenzautorisierung:

Status: OUT OF COMPLIANCE am Jul 26 09:24:09 2018 UTC

Letzter Kommunikationsversuch: FEHLGESCHLAGEN am 02.08.2018 14:26:23 UTC

Fehlergrund: Senden der Call Home-HTTP-Nachricht nicht möglich.

Nächster Kommunikationsversuch: Aug 02 14:26:53 2018 UTC

Kommunikationsfrist: 25.10.2018 09:21:38 UTC

Mögliche Protokolle werden angezeigt:

%CALL_HOME-5-SL_MESSAGE_FAILED: Smart Licensing-Nachricht konnte nicht gesendet werden an: https://<ip>/its/service/oddce/services/DDCEService (ERR 205: Anfrage abgebrochen)

%SMART_LIC-3-COMM_FAILED: Kommunikationsfehler mit dem Cisco Smart Software Manager oder Satelliten: Senden der HTTP-Nachricht für Call Home fehlgeschlagen.

%SMART_LIC-3-AUTH_RENEW_FAILED: Autorisierungsverlängerung mit Cisco Smart Software Manager oder Satellit: Fehler beim Senden der Kommunikationsnachricht für udi PID:XXX, SN: XXX

Weitere Schritte:

- Vergewissern Sie sich, dass das Cisco Gerät einen Ping an tools.cisco.com senden kann.
- Wenn DNS nicht konfiguriert ist, konfigurieren Sie einen DNS-Server oder eine IP-Host-Anweisung für die lokale nslookup-IP für tools.cisco.com.
- Versuchen Sie, über den TCP-Port 443 (von HTTPS verwendeter Port) eine Telnet-Verbindung vom Cisco Gerät zu tools.cisco.com herzustellen.
- Überprüfen Sie, ob die HTTP-Client-Quellschnittstelle definiert und korrekt ist.
- Vergewissern Sie sich, dass die URL/IP im Call Home-Profil auf dem Cisco Gerät richtig eingestellt ist, indem Sie show call-home profile all (Call-Home-Profil anzeigen) verwenden.
- Vergewissern Sie sich, dass die IP-Route auf den richtigen nächsten Hop verweist.
- Stellen Sie sicher, dass der TCP-Port 443 nicht auf dem Cisco Gerät, dem Pfad zum Smart Call Home-Server oder dem Cisco Smart Software Manager vor Ort (über Satellit) blockiert wird.
- Stellen Sie sicher, dass die richtige VRF-Instanz (Virtual Routing and Forwarding) im Call-Home konfiguriert ist, falls erforderlich.

Szenario #6: Fehlerursache "Fehlendes ID-Zertifikat-Seriennummernfeld;

Fehlendes Signaturzertifikat-Seriennummernfeld; Signierte Daten und Zertifikat stimmen nicht überein" Protokoll

Dieses Verhalten tritt auf, wenn Sie mit einem lokalen CSSM-Server arbeiten, dessen Krypto-Zertifikat wie in [Cisco Bug-ID CSCvr41393](#) dokumentiert abgelaufen ist. Dieses Verhalten wird erwartet, da der CSSM vor Ort synchronisieren und sein Zertifikat erneuern darf, um ein Synchronisierungsproblem mit registrierenden Geräten zu verhindern.

Ausschnitt von „show license all“:

Registrierung:

Status: NICHT REGISTRIERT

Smart Account: Beispielkonto

Ausfuhrkontrollierte Funktionalität: ZULÄSSIG

Lizenzautorisierung:

Status: EVAL-MODUS

Verbleibende Testperiode: 65 Tage, 18 Stunden, 43 Minuten, 0 Sekunden


Mögliche angezeigte Protokolle:

Dieser Fehler tritt unter show logging or show license eventlog auf:

SAEVT_DEREGISTER_STATUS msgStatus="LS_INVALID_DATA" error="Fehlendes Seriennummernfeld des ID-Zertifikats; fehlendes Seriennummernfeld des Signaturzertifikats; signierte Daten und Zertifikat stimmen nicht überein."

Weitere Schritte:

- Überprüfen Sie, ob das Cisco Gerät eine IP-Netzwerkverbindung zum lokalen CSSM-Server hat.
- Wenn Sie HTTPS verwenden, stellen Sie sicher, dass die Zertifizierung „C-Name“ in der Call-Home-Konfiguration des Geräts verwendet wird.
- Wenn ein DNS-Server nicht verfügbar ist, um den C-Namen der Zertifizierung aufzulösen, konfigurieren Sie eine statische IP-Host-Anweisung, um den Domännennamen und die IP-Adresse zuzuordnen.
- Überprüfen Sie, ob der Status des lokalen CSSM-Zertifikats noch gültig ist.
- Wenn das standortbasierte CSSM-Zertifikat abgelaufen ist, verwenden Sie eine der Problemumgehungen, die in [Cisco Bug-ID CSCvr41393](#) dokumentiert sind.

 Hinweis: HTTPS führt standardmäßig während des SSL-Handshakes eine Serveridentitätsprüfung durch, um zu überprüfen, ob die URL oder IP mit dem vom Server bereitgestellten Zertifikat übereinstimmt. Dies kann zu Problemen bei der Verwendung von IP-Adressen anstelle eines DNS-Eintrags führen, wenn Hostname und IP nicht übereinstimmen. Wenn DNS nicht möglich ist oder eine statische IP-Host-Anweisung verwendet wird, kann keine sichere HTTP-Serveridentitätsprüfung konfiguriert werden, um diese Zertifizierungsprüfung zu deaktivieren.

Szenario #7: Switch-Lizenzautorisierung "Fehlergrund: Warten auf Antwort"

Ausschnitt von „show license all“:

Lizenzautorisierung:

Status: OUT OF COMPLIANCE am Jul 26 09:24:09 2018 UTC

Letzter Kommunikationsversuch: AUSSTEHEND am Aug. 02 14:34:51 2018 UTC

Fehlergrund: Warten auf Antwort

Nächster Kommunikationsversuch: Aug 02 14:53:58 2018 UTC

Kommunikationsfrist: 25. Okt. 09:21:39 2018 UTC

Mögliche Protokolle werden angezeigt:

%PKI-3-CRL_FETCH_FAIL: Fehler beim Abrufen der Zertifikatsperrliste für Trustpoint SLA-TrustPoint. Grund: Fehler beim Auswählen des Sockets. Timeout: 5

(Zeitüberschreitung bei Verbindung)

%PKI-3-CRL_FETCH_FAIL: Fehler beim Abrufen der Zertifikatsperrliste für Trustpoint SLA-TrustPoint. Grund: Fehler beim Auswählen des Sockets. Timeout: 5

(Zeitüberschreitung bei Verbindung)

Weitere Schritte:

- Um dieses Problem zu beheben, muss der SLA-TrustPoint in der aktuellen Konfiguration als kein SLA konfiguriert werden.

```
show running-config
```

```
<omitted>
```

```
crypto pki trustpoint SLA-TrustPoint
```

```
revocation-check none
```

Was ist eine CRL?

Eine Certificate Revocation List (CRL) ist eine Liste widerrufenen Zertifikate. Die CRL wird von der Certificate Authority (CA) erstellt und digital signiert, die die Zertifikate ursprünglich ausgestellt hat. Die CRL enthält die Daten zur Ausstellung und zum Ablauf der einzelnen Zertifikate. Weitere Informationen zur CRL finden Sie [hier](#).

Szenario #8: Lizenz im Status "NICHT KONFORM"

Ausschnitt von „show license all“:

Lizenzautorisierung:

Status: OUT OF COMPLIANCE am Jul 26 09:24:09 2018 UTC

Letzter Kommunikationsversuch: AUSSTEHEND am Aug. 02 14:34:51 2018 UTC

Fehlergrund: Warten auf Antwort

Nächster Kommunikationsversuch: Aug 02 14:53:58 2018 UTC

Kommunikationsfrist: 25. Okt. 09:21:39 2018 UTC

Mögliche Protokolle werden angezeigt:

%SMART_LIC-3-OUT_OF_COMPLIANCE: Mindestens eine Berechtigung ist nicht konform.

Weitere Schritte:

- Überprüfen Sie, ob das Token von einem richtigen Smart Virtual Account verwendet wurde.
- Überprüfen Sie [hier](#) die Anzahl der verfügbaren Lizenzen.

Szenario #9: Switch-Lizenzautorisierung "Fehlerursache: Daten und Signatur stimmen nicht überein"

Ausschnitt von „show license all“:

Lizenzautorisierung:

Status: AUTORISIERT am 12. März 09:17:45 2020 EDT

Letzter Kommunikationsversuch: FEHLGESCHLAGEN am 12. März 09:17:45 2020 EDT

Fehlerursache: Daten und Signatur stimmen nicht überein.

Nächster Kommunikationsversuch: 12. März 09:18:15 Uhr EDT

Kommunikationsfrist: 09.05.2020 21:22:43 EDT

Mögliche Protokolle werden angezeigt:

%SMART_LIC-3-AUTH_RENEW_FAILED: Erneuerung der Autorisierung mit dem Cisco Smart Software Manager (CSSM): Fehler beim Smart Software Manager: Daten und Signatur stimmen nicht mit udi PID überein:C9000,SN:XXXXXXXXXXXX

Weitere Schritte:

- Aufheben der Registrierung des Switches mit der intelligenten Deregistrierung der Lizenz
- Dann registrieren Sie den Switch mit einem neuen Token mit Lizenz smart register idtoken <TOKEN> force.

Referenzen

- 1) [Startseite von Cisco Smart Licensing](#)
- 2) [Cisco Community - On-Demand-Schulungen](#).

3) Smart Account – Management Portal: [Smart Software Licensing](#)

4) Smart Account – Erstellen neuer Konten: [Smart Accounts](#)

5) Konfigurationsleitfaden (Beispiel) – [Konfigurationsleitfaden für das Systemmanagement, Cisco IOS XE Fuji 16.9.x \(Switches der Catalyst 9300-Serie\)](#)

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.