# Überwachen des Cisco AireOS WLC über SNMP mit OIDs

## Inhalt



## Einleitung

In diesem Artikel wird erläutert, wie die SNMP-Überwachung auf dem Cisco 3504 Wireless LAN Controller (WLC) konfiguriert, Objektnamen in Objektkennungen und umgekehrt übersetzt werden. Außerdem wird eine Liste der von Cisco Kunden am häufigsten verwendeten OIDs bereitgestellt.

## Voraussetzungen

### Anforderungen

Ein Standard-SNMP-Tool auf Ihrem Betriebssystem zu haben oder eines zu installieren.

### Verwendete Komponenten

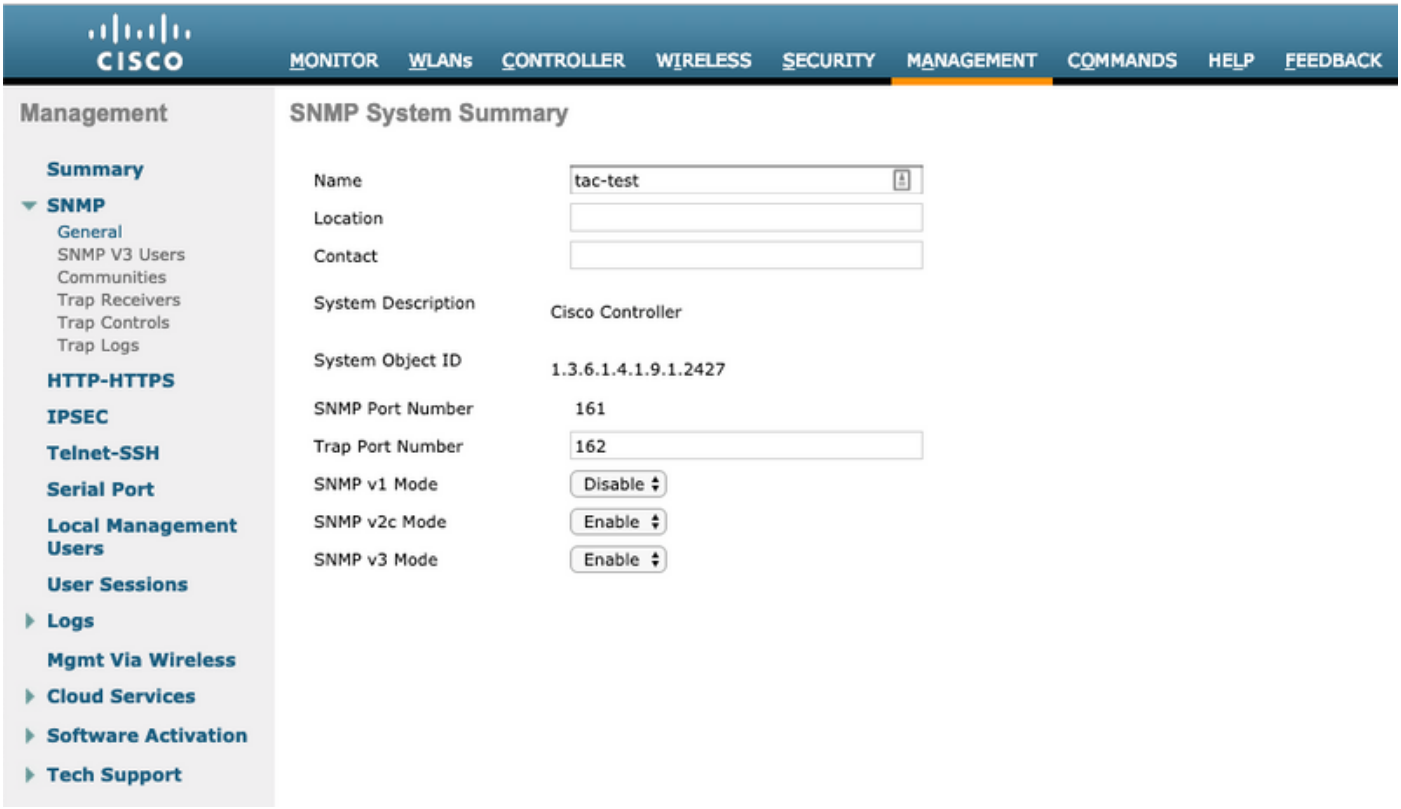
Alle Tests wurden auf einem 3504 WLC mit Image Version 8.9 und MacOS 10.14 durchgeführt. Die OIDs in diesem Artikel gelten auch für ältere AireOS-Versionen und andere Wireless Controller mit AireOS-Unterstützung (8540/5508/5520/2504).

## Konfigurieren der SNMP-Einstellungen auf dem WLC

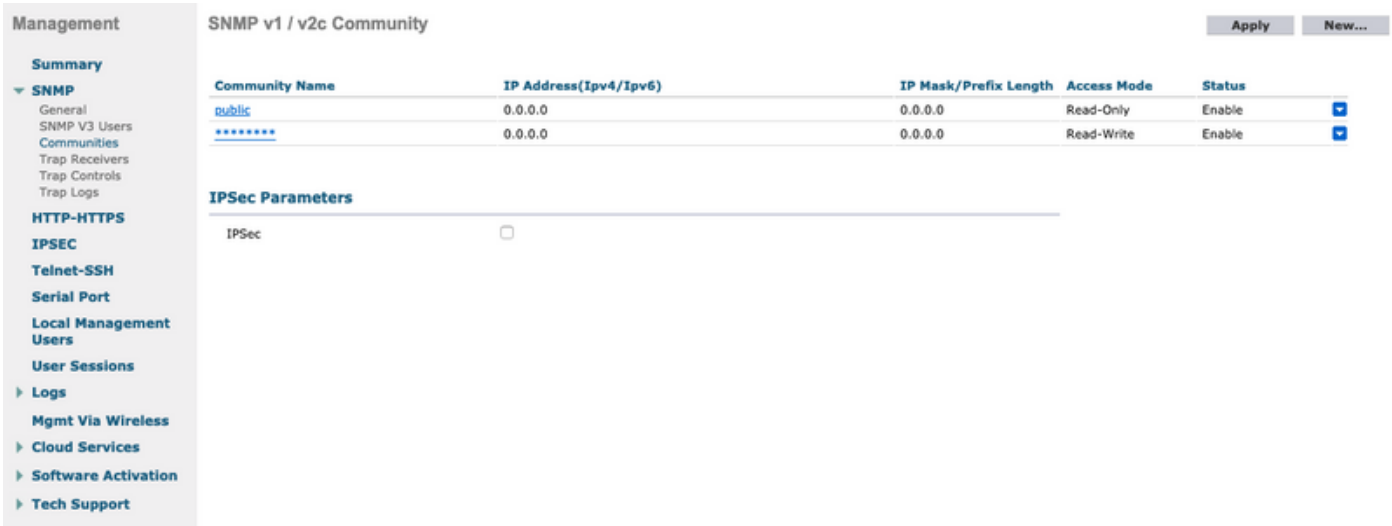
SNMPv2c ist eine auf der Community basierende Version von SNMP, und die gesamte Kommunikation zwischen den Geräten erfolgt in Klartext. SNMPv3 ist die sicherste Version, die Integritätsprüfungen, Authentifizierung und Verschlüsselung von Paketen ermöglicht. SNMPv1 ist extrem veraltet, existiert aber weiterhin, um die Kompatibilität älterer Software zu gewährleisten.

**Wichtig: SNMPv2c ist standardmäßig aktiviert, wobei die Community "private" über Lese- und Schreibrechte und die Community "public" über schreibgeschützte Berechtigungen verfügt. Es wird empfohlen, sie zu entfernen und eine neue Community mit einem anderen Namen zu erstellen.**

In diesem Artikel werden nur SNMPv2c und SNMPv3 verwendet. Melden Sie sich bei der Webschnittstelle des Controllers an. Stellen Sie sicher, dass Sie unter Management->SNMP->Allgemein die gewünschte Protokollversion aktivieren.

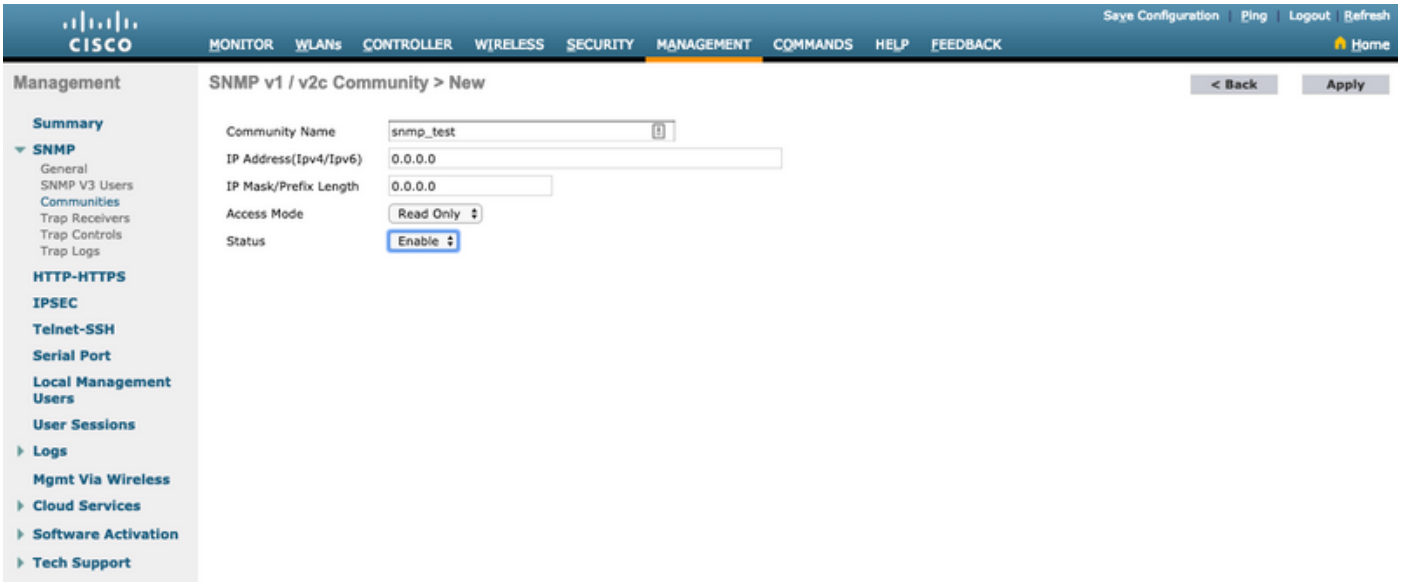



Im Menü Communitys werden alle aktuell erstellten Communitys angezeigt.

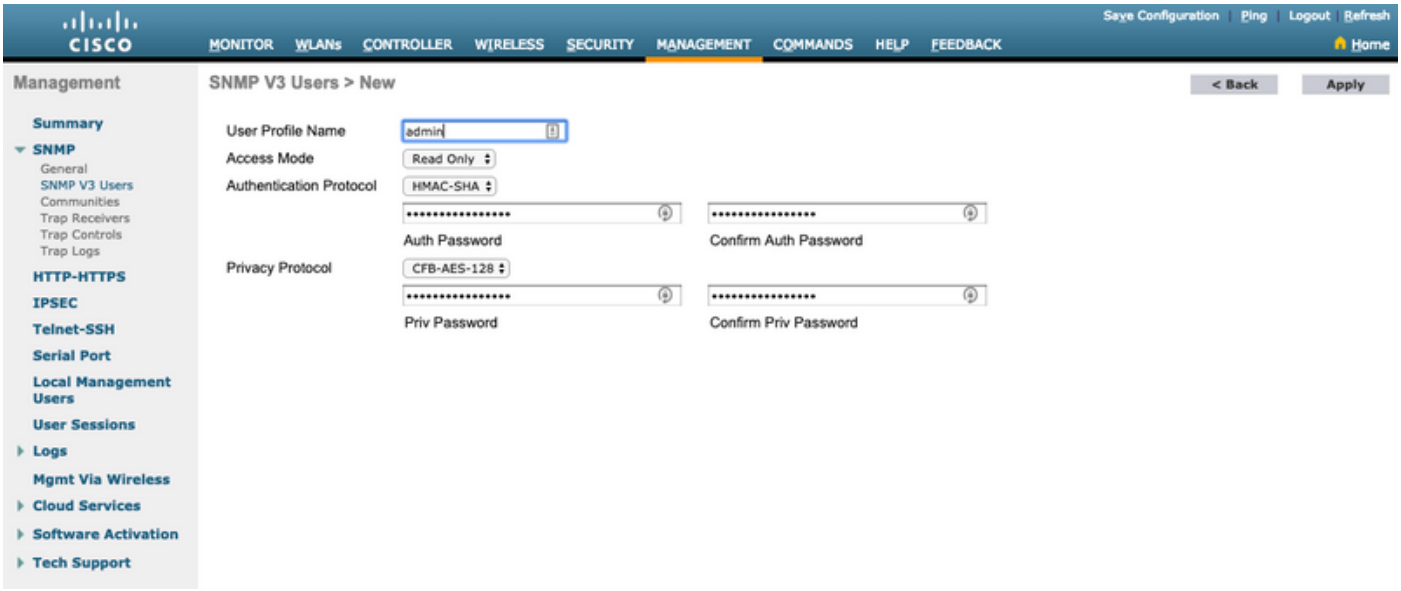



Es hat sich bewährt, vorkonfigurierte Communitys zu entfernen und eine neue zu erstellen. IP-Adresse und Netzmaske verhalten sich wie eine Zugriffsliste. Standardmäßig wird "0.0.0.0" für beide festgelegt, d. h. alle IP-Adressen dürfen SNMP-Abfragen für diese Community ausführen. Das Feld für den Zugriffsmodus wird auf "Read Only" gesetzt, da diese Community nur für die Überwachung und nicht für die Konfiguration des WLC verwendet werden soll.

**Wichtig: Alle Versionen unter 8.7.1.135 werden mit einem Fehler CSCvg61933 betroffen, bei dem die Netzmaske nicht auf 255.255.255.255 gesetzt werden darf. Aktualisieren Sie den Controller entweder auf die neueste empfohlene Version höher als 8.7.1.135, oder verwenden Sie den folgenden CLI-Befehl, um eine neue Community zu erstellen: config snmp community ipaddr <ip_address> <netmask> <community_name>**




Im Menü "SNMP V3 Users" (SNMP V3-Benutzer) werden alle konfigurierten Benutzer, ihre Berechtigungen und die für die Authentifizierung und Verschlüsselung verwendeten Protokolle angezeigt. Schaltfläche **Neu** ermöglicht die Erstellung eines neuen Benutzers. Es wird empfohlen, HMAC-SHA als Authentifizierungsprotokoll und CFB-AES-128 als Datenschutzprotokoll auszuwählen. Wir erstellen einen Benutzer mit dem Namen "admin", dessen Authentifizierungs- und Datenschutzkennwort auf "Cisco123Cisco123" gesetzt ist:

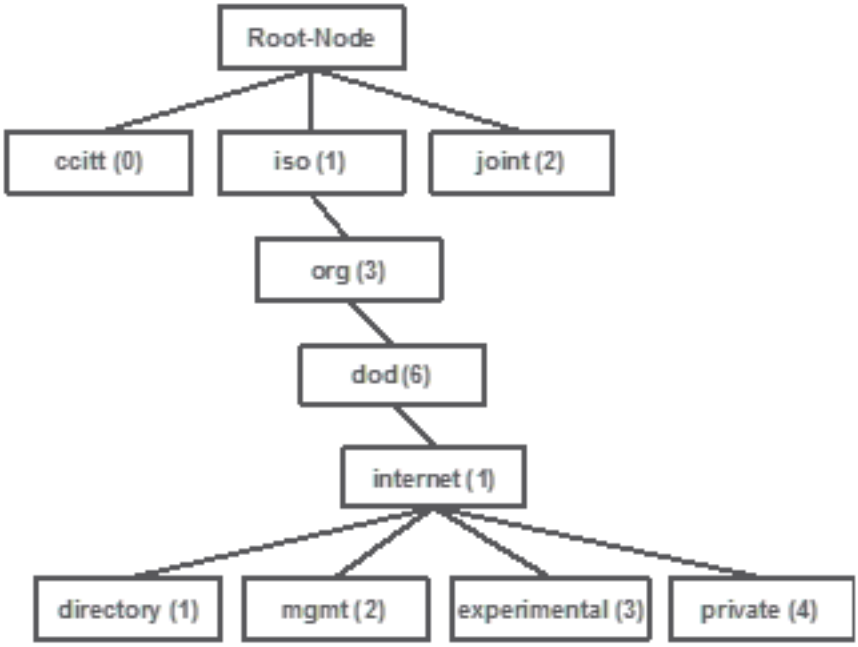



# Objektnamen und Objekt-IDs (OIDs)

## Was sind Objektnamen und OIDs?

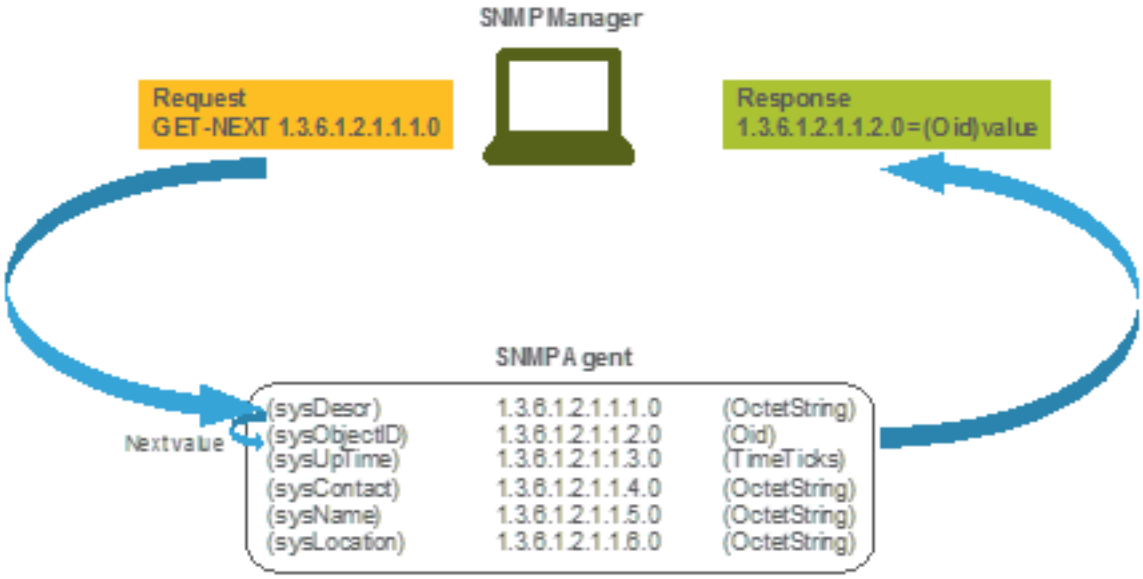
Objekt-IDs, kurz OIDs, sind eindeutige Bezeichner, die eine bestimmte Variable oder ein bestimmtes Objekt darstellen. Beispielsweise wird die aktuelle CPU-Nutzung als variabel betrachtet, welche Werte durch Aufrufen ihrer Objekt-ID abgerufen werden können. Jede OID ist eindeutig, und keine zwei OIDs sollten weltweit gleich sein, ähnlich wie MAC-Adressen. Diese Bezeichner folgen einer Baumhierarchie, und jede OID kann bis zu ihrem Ursprung zurückverfolgt werden. Jeder Anbieter hat nach einer gemeinsamen Wurzel eine eigene Zweigstelle.
Eine Analogie könnte eine Privatadresse sein, deren Ursprung das Land oder der Staat wäre, gefolgt von einer Postleitzahl, der Straße und schließlich der Hausnummer.

Die Zahlen, gefolgt von einem Punkt, stellen jeden Schritt dar, der erforderlich ist, um zu einem bestimmten Punkt in diesem Baum oder Zweig zu gelangen.




Alle diese Werte werden in einer Management Information Base, kurz MIB, in jedem Netzwerkgerät gespeichert. Jeder Bezeichner hat einen Namen und eine Definition (Wertebereich, Typ usw.).

Das Laden von MIBs auf Ihr SNMP-Tool ist nicht erforderlich, um SNMP zu verwenden und ein Gerät abzufragen. Wenn eine gültige OID bekannt ist, antwortet das Gerät mit dem Wert, der in der Variablen gespeichert ist, die die OID darstellt. In der Abbildung unten fragt der SNMP-Manager beispielsweise den SNMP-Agenten eines Geräts unter Verwendung der OID 1.3.6.1.2.1.1.1.0 nach seiner Systembeschreibung ab.




Das Laden der MIB in das Abfrage-Tool bietet jedoch den Vorteil, dass die OID-Nummern in Namen übersetzt werden und ihre Definition kennen.

## MIBs und Liste aller Objektnamen und -IDs auf Cisco WLCs

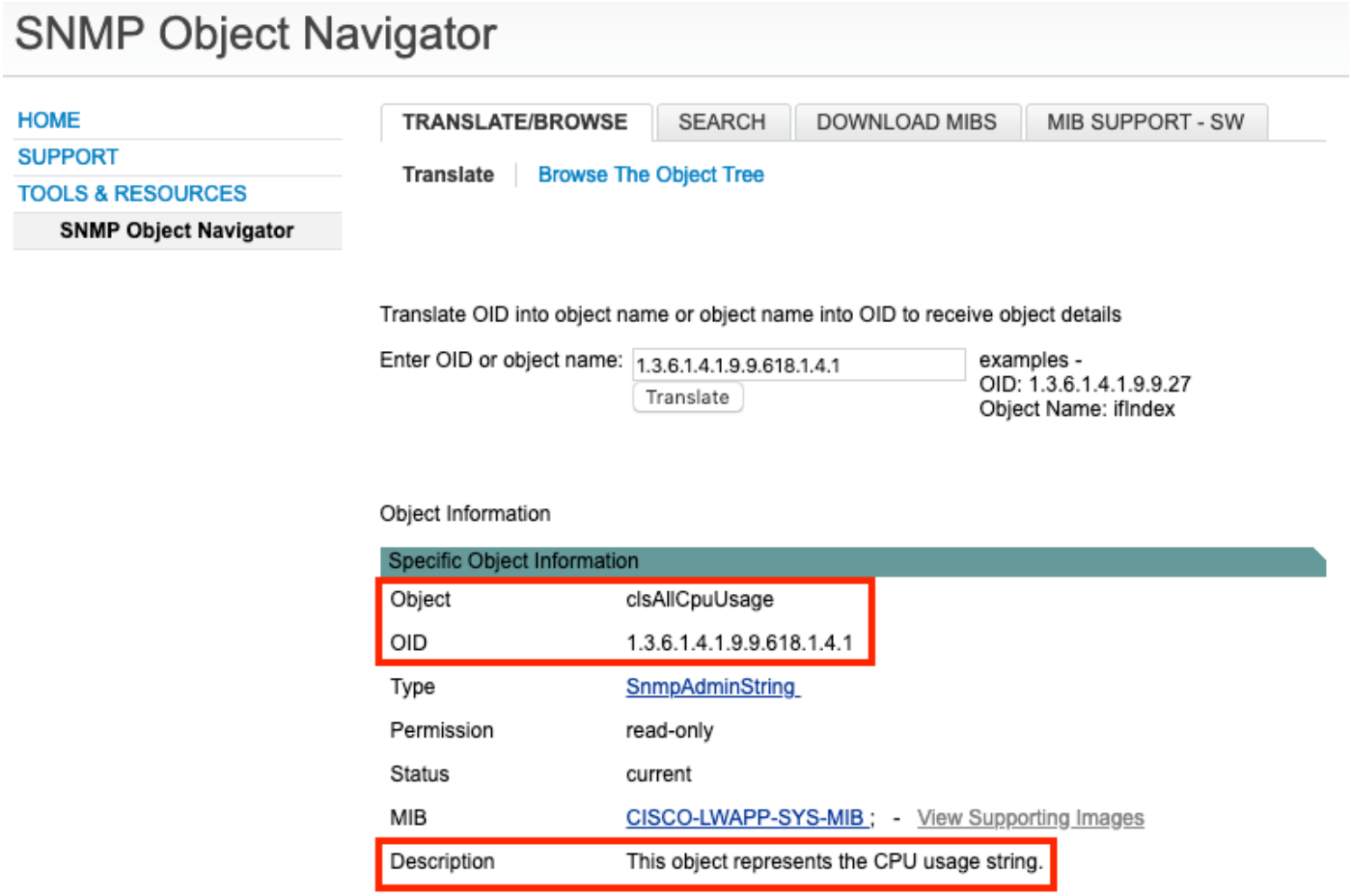
Ab Mai 2019 existiert keine einfache, benutzerfreundliche Tabelle mehr, die alle verfügbaren Objektnamen und deren jeweilige OIDs für Wireless LAN Controller enthält. Alternativ bietet Cisco eine Management Information Base (MIBs) an, die zwar nicht leicht lesbar ist, aber alle verfügbaren Objektnamen und deren Beschreibung enthält. Cisco 3504 WLC MIB kann HIER heruntergeladen werden.

Die heruntergeladene Archivdatei enthält mehrere .my-Textdateien, die entweder in einen SNMP-Überwachungsserver eines Drittanbieters importiert oder einfach mit einem regulären Texteditor geöffnet werden können. Um die OID eines bestimmten Objektnamens zu finden, müssen Sie zunächst die genaue Datei suchen, die ihn enthält.

So befinden sich beispielsweise alle Objekte zur Überwachung des physischen Gerätezustands (wie Temperatur und Lüftergeschwindigkeit) innerhalb einer MIB namens CISCO-ENVMON-MIB.my. Hier ist "ciscoEnvMonFanState" der Objektname, der verwendet wird, um den Status des WLC-Lüfters anzugeben. MIB-Dateien folgen der unten angegebenen Syntax. Die Informationen zum Lüfterstatus-Objekt sehen wie folgt aus:

```
ciscoEnvMonFanState OBJECT-TYPE
    SYNTAX CiscoEnvMonState
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
            "The current state of the fan being instrumented."
    ::= { ciscoEnvMonFanStatusEntry 3 }
```

Der Großteil der Überwachungssoftware eines Drittanbieters basiert auf OIDs und nicht auf Objektnamen. Die Übersetzung zwischen Objektname und Objekt-ID kann mit dem SNMP-Objektnavigationstool von Cisco durchgeführt werden. Geben Sie den Objektnamen in die Suchleiste ein. Die Ausgabe enthält die OID und eine kurze Beschreibung. Darüber hinaus kann mit dem gleichen Tool der entsprechende Objektname der OID gesucht werden.




# Verwenden von OIDs zum Überwachen des Zustands von WLC

Nach dem Erfassen der OID des zu überwachenden Objekts kann die erste SNMP-Abfrage ausgeführt werden. Die folgenden Beispiele zeigen, wie eine WLC-CPU-Auslastung pro Kern (OID = 1.3.6.1.4.1.9.9.618.1.4.1) für SNMPv2-Community, **snmp_test** und SNMPv3-**Benutzeradministrator** mit SHA-Auth-Kennwort **Cisco123Cisco123** und das AES-Datenschutzkennwort auf "Cisco123Cisco123" gesetzt. Die Schnittstelle für das Controller-Management befindet sich unter 10.48.39.164.

## Überwachung über snmpwalk

SNMPwalk ist eine SNMP-Anwendung, die SNMP GETNEXT-Anforderungen verwendet, um eine Netzwerkentität nach einem Informationsbaum abzufragen. Es ist standardmäßig auf MacOS und den meisten Linux-Distributionen vorhanden. Für SNMPv2c, tDer Befehl folgt der folgenden Syntax:

```
snmpwalk -v2c -c <community_name> <WLC_management_interface_ip> <OID>
```

Beispiel:

```
VAPEROVI-M-H1YM:~ vaperovi$ snmpwalk -v2c -c snmp_test 10.48.39.164 1.3.6.1.4.1.9.9.618.1.4.1
SNMPv2-SMI::enterprises.9.9.618.1.4.1.0 = STRING: "0%/1%, 0%/1%, 0%/1%, 0%/1%"
```

Wenn SNMPv3 verwendet wird, folgt der Befehl der folgenden Syntax:

```
snmpwalk -v3  -l authPriv -u <username> -a [MD5|SHA] -A <auth_password> -x [AES|DES] -X
<priv_password> <WLC_management_interface_ip> <OID>
```

Wählen Sie je nach Erstellung des SNMPv3-Benutzers auf dem Controller MD5/SHA und AES/DES aus.

Beispiel:

```
VAPEROVI-M-H1YM:~ vaperovi$ snmpwalk -v3  -l authPriv -u admin -a SHA -A Cisco123Cisco123 -x AES
-X Cisco123Cisco123 10.48.39.164 1.3.6.1.4.1.9.9.618.1.4.1

SNMPv2-SMI::enterprises.9.9.618.1.4.1.0 = STRING: "0%/1%, 0%/1%, 0%/0%, 0%/1%"
```

## Überwachung über Python 3 und die Pysnmp-Bibliothek

Die folgenden Codeausschnitte sind in Python 3.7 geschrieben und verwenden das pysnmp-Modul (pip install pysnmp), um SNMP-Abfragen für die CPU-Nutzung des Cisco 3504 WLC durchzuführen. In diesen Beispielen wird die gleiche SNMPv2-Community und der gleiche SNMPv3-Benutzer verwendet, die in einem der vorherigen Kapitel erstellt wurden. Ersetzen Sie einfach die Variablenwerte und integrieren Sie den Code mit Ihren eigenen Skripten.

### SNMPv2c-Beispiel:

```
from pysnmp.hlapi import *

communityName = 'snmp_test'
ipAddress = '10.48.39.164'
OID = '1.3.6.1.4.1.14179.2.3.1.13.0'
errorIndication, errorStatus, errorIndex, varBinds = next( getCmd(SnmpEngine(),
CommunityData(communityName), UdpTransportTarget((ipAddress, 161)), ContextData(),
ObjectType(ObjectIdentity(OID))) ) if errorIndication: print(errorIndication) elif errorStatus:
print('%s at %s' % (errorStatus.prettyPrint(), errorIndex and varBinds[int(errorIndex) - 1][0]
or '?')) else: for varBind in varBinds: print(' = '.join([x.prettyPrint() for x in varBind]))
```

Ausgabe wird ausgegeben:

```
SNMPv2-SMI::enterprises.14179.2.3.1.13.0 = 73
```

### SNMPv3-Beispiel:

```
from pysnmp.hlapi import *

username = 'admin'
ipAddress = '10.48.39.164'
OID = '1.3.6.1.4.1.14179.2.3.1.13.0'
authKey = 'Cisco123Cisco123'
privKey = 'Cisco123Cisco123'

errorIndication, errorStatus, errorIndex, varBinds = next(
    getCmd(SnmpEngine(),
           UsmUserData(username, authKey, privKey,
                       authProtocol=usmHMACSHAAuthProtocol,
                       privProtocol=usmAesCfb128Protocol),
           UdpTransportTarget((ipAddress, 161)),
           ContextData(),
```

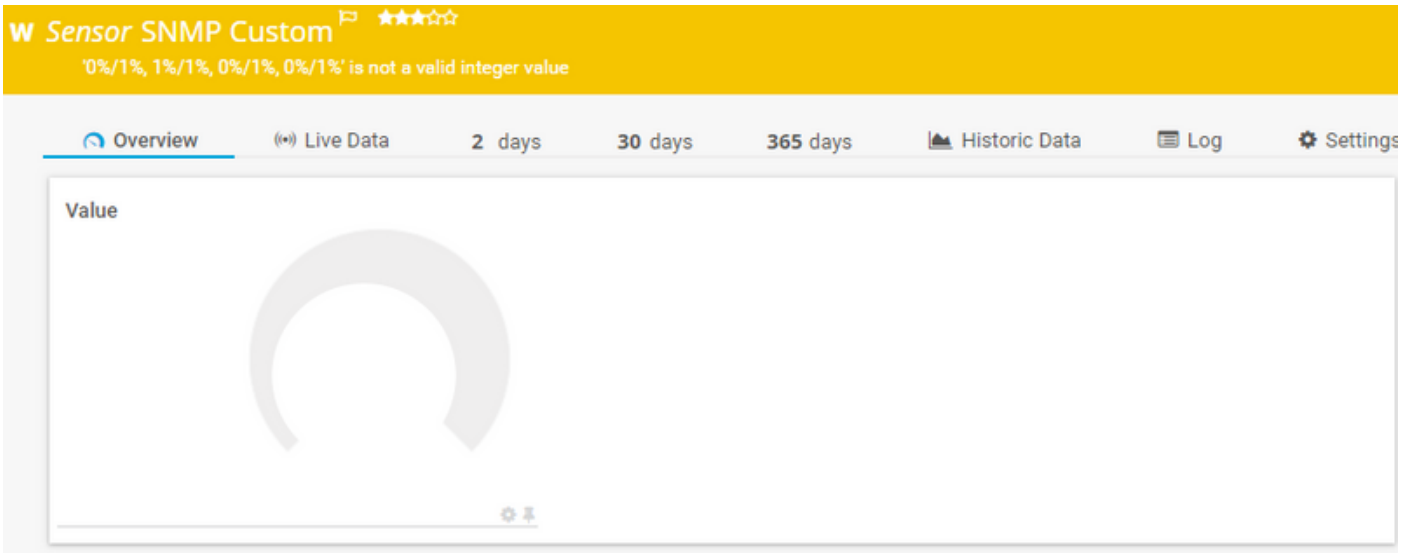
```
            ObjectType(ObjectIdentity(OID)))
)

if errorIndication:
    print(errorIndication)
elif errorStatus:
    print('%s at %s' % (errorStatus.prettyPrint(),
                        errorIndex and varBinds[int(errorIndex) - 1][0] or '?'))
else:
    for varBind in varBinds:
        print(' = '.join([x.prettyPrint() for x in varBind]))
```

### Integration mit Drittanbietersoftware (Grafana/PRTG Network Monitor/SolarWinds)

Die Cisco Prime-Infrastruktur ermöglicht die einfache Überwachung und Konfiguration mehrerer Netzwerkgeräte, einschließlich Wireless-Controllern. Die Prime-Infrastruktur ist mit allen OIDs vorinstalliert, und die Integration mit WLC erfolgt durch Hinzufügen der WLC-Anmeldeinformationen zu Prime. Nach der Synchronisierung ist es möglich, Alarme festzulegen und Konfigurationsvorlagen für mehrere Wireless-Controller gleichzeitig per Push bereitzustellen.

Andererseits kann der Cisco WLC auch in mehrere Überwachungslösungen von Drittanbietern integriert werden, sofern die OIDs bekannt sind. Programme wie Grafana, PRTG Network Monitor und SolarWinds Server ermöglichen den Import der MIBs oder OIDs und die Darstellung der Werte in einem benutzerfreundlichen Diagramm.

Diese Integration erfordert möglicherweise einige Anpassungen auf der Seite des Überwachungsservers. Im folgenden Beispiel wird der PRTG-Überwachungsserver mit der Pro-Core-CPU-Nutzungs-OID versehen, die den String "0%/1%, 1%/1%, 0%/1%, 0%/1%" zurückgibt. PRTG erwartet einen Integerwert und löst einen Fehler aus.




## Tabelle der am häufigsten überwachten OIDs

Da MIBs die Daten in einer nicht benutzerfreundlichen Syntax darstellen, enthält die folgende Tabelle einige der gebräuchlichsten Objektnamen und deren OIDs, die Cisco Kunden verwenden.

| Beschreibung | Objektname | OID | Erwartete Antwort |
|---|---|---|---|
| Gesamte CPU-Auslastung in % | AgentAktuellerVerbrauch | 1.3.6.1.4.1.14179.1.1.5.1.0 | GANZZAHL: 0 |
| CPU-Auslastung pro | clsGesamteCPUutzung | 1.3.6.1.4.1.9.9.618.1.4. | ZEICHENFOLGE: "0 %/1 |

| | | | |
|---|---|---|---|
| Kern | | 1.0 | %/1 %, 0 %/1 %, 0 %/1 |
| RAM-Nutzung in % | clsSysCurrentMemoryUsage | 1.3.6.1.4.1.9.9.618.1.8.6.0 | Anzeige 32: 33 |
| CPU-Temperatur in °C | bsnSensorTemperatur | 1.3.6.1.4.1.14179.2.3.1.13.0 | GANZZAHL: 76 |
| Anzahl der verbundenen APs | clsSysAppConnectCount | 1.3.6.1.4.1.9.9.618.1.8.4.0 | Anzeige 32: 2 |
| Anzahl der Clients | clsMaxClientsCount | 1.3.6.1.4.1.9.9.618.1.8.12.0 | Anzeige32: 0 |
| Anzahl der Clients pro WLAN | bsnDot11EssAnzahlvonMobilstationen | 1.3.6.1.4.1.14179.2.1.1.1.38.0 | Leistungsindikator32: 3<br>Leistungsindikator32: 2 |

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.