# Konfigurieren von SNMPv3 auf Cisco ONS15454-/NCS2000-Geräten

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfiguration Auf einem Standalone/Multishelf-Knoten Konfigurieren des authPriv-Modus auf ONS15454-/NCS2000-Geräten NMS-Server konfigurieren (blr-ong-lnx10) Authentifizierungsmodus überprüfen Konfigurieren des authNoPriv-Modus auf ONS15454/NCS2000-Geräten Überprüfen des Authentifizierungsmodus "NoPriv" Konfigurieren des AutoNoPriv-Modus auf ONS15454/NCS2000-Geräten Überprüfen des AutoNoPriv-Modus SNMP V3-Trap für GNE/ENE-Einrichtung Auf GNE-Knoten Auf ENE-Knoten **GNE/ENE-Einrichtung überprüfen** Fehlerbehebung

## Einführung

Dieses Dokument beschreibt Schritt-für-Schritt-Anweisungen zur Konfiguration des Simple Network Management Protocol Version 3 (SNMPv3) auf ONS15454/NCS2000-Geräten. Alle Themen enthalten Beispiele.

**Hinweis:** Die Liste der in diesem Dokument enthaltenen Attribute ist weder vollständig noch autoritär und kann jederzeit ohne Aktualisierung dieses Dokuments geändert werden.

## Voraussetzungen

### Anforderungen

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

- Benutzeroberfläche des Cisco Transport Controller (CTC)
- Grundlegendes Serverwissen
- Grundlegende Linux-/Unix-Befehle

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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 potenziellen Auswirkungen eines Befehls verstehen.

## Konfiguration

### Auf einem Standalone/Multishelf-Knoten

#### Konfigurieren des authPriv-Modus auf ONS15454-/NCS2000-Geräten

Schritt 1: Melden Sie sich mit den Super User-Anmeldeinformationen über CTC beim Knoten an.

Schritt 2: Navigieren Sie zu Node View > Provisioning > SNMP > SNMP V3.

Schritt 3: Navigieren Sie zur Registerkarte Benutzer. Erstellen Sie Benutzer.

User Name: <anything based on specifications>

Group name:default\_group

Authentication

Protocol:MD5

Password: <anything based on specifications>

Privacy

Protocol:DES

Password:<anythingbased on specifications> Schritt 4: Klicken Sie auf OK, wie im Bild gezeigt.

	X User Name:	Create User			
	Group Name: Authentication Protocol: Password: Privacy Protocol: Password:	default_group MD5 ******* DES			
Tab View       Alarms     Conditions       History     Circuits       Pro       General       Network   SNMP V1/V2 SNMP V3	Common	OK Cancel			
OSI General Protection Users Security MIB views SNMP Group Access Comm Channels Trap Destinations(V3) Alarm Profiles Notification Filters Defaults WDM-ANS SVLAN	User Name	Authentication Protocol	Privacy Protocol	Group Name	
Certificate	Create Edit	Delete			

Spezifikationen:

Benutzername: Geben Sie den Namen des Benutzers auf dem Host an, der mit dem Agenten verbunden ist. Der Benutzername muss mindestens 6 und höchstens 40 Zeichen enthalten (maximal 39 Zeichen für die TACACS- und RADIUS-Authentifizierung). Es enthält alphanumerische Zeichen (a-z, A-Z, 0-9), und die zulässigen Sonderzeichen sind @, "-" (Bindestrich) und "". (Punkt). Der Benutzername muss aus Gründen der TL1-Kompatibilität 6 bis 10 Zeichen lang sein.

Gruppenname: Geben Sie die Gruppe an, der der Benutzer angehört.

Authentifizierung:

Protokoll - Wählen Sie den Authentifizierungsalgorithmus aus, den Sie verwenden möchten. Die Optionen sind KEINE, MD5 und SHA.

Passwort: Geben Sie ein Passwort ein, wenn Sie MD5 oder SHA auswählen. Standardmäßig ist die Kennwortlänge auf mindestens acht Zeichen festgelegt.

Datenschutz - Initiiert eine Sitzung zum Festlegen der Datenschutzstufe, die es dem Host ermöglicht, den Inhalt der Nachricht zu verschlüsseln, die an den Agenten gesendet wird.

Protokoll - Wählen Sie den Algorithmus zur Datenschutzauthentifizierung aus. Die verfügbaren Optionen sind None (Keine), DES und AES-256-CFB.

Kennwort: Geben Sie ein Kennwort ein, wenn Sie ein anderes Protokoll als "Keine" auswählen.

Schritt 5: Stellen Sie sicher, dass MIB-Ansichten gemäß diesem Image konfiguriert sind.

Tab View						
Alarms Conditions History Circu	Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN					
General Network OSI Protection Security SNMP Comm.Channels Alarm.Profiles Defaults WDM-ANS SVLAN Certificate	SNMP V3 Common tal View Name fullview fullview Create Edit	Sub Tree OID	Mask 1	Type included		

Spezifikationen:

Name - Name der Ansicht.

Subtree OID - Die MIB-Unterstruktur, die in Kombination mit der Maske die Familie der Unterbäume definiert.

Bitmaske - Eine Familie von View-Unterbäumen. Jedes Bit in der Bitmaske entspricht einer Unterkennung der Substruktur-OID.

Typ - Wählen Sie den Ansichtstyp aus. Optionen sind inklusive und ausgeschlossen.

Der Typ legt fest, ob die durch die Unterstruktur-OID und die Bit-Maske-Kombination definierte Unterbaufamilie in den Benachrichtigungsfilter eingeschlossen oder ausgeschlossen wird.

Schritt 6: Konfigurieren Sie den Gruppenzugriff, wie im Bild gezeigt. Standardmäßig ist der Gruppenname default\_group und die Sicherheitsstufe authPriv.

**Hinweis:** Der Gruppenname muss mit dem beim Erstellen des Benutzers in Schritt 3 übereinstimmen.

Tab View					
Alarms Conditions History Circuits Provis	ioning Inventory Maintenance OTN				
General					
Network SNMP V1/V2 SNMP V3	Common				
OSI					
Protection	Group Name Security Level	Read View Access	Allow SNMP Sets	Notify View Access	
Conversion Users	default_group authPriv	fullview		fullview	
Security MIB views					
SNMP Group Access					
Comm Channels Trap Destinations(V3)					
Alarm Profiles Notification Filters					
Defaults					
WDM-ANS					
SVLAN					
Certificate	Create Edit Delete				
Second Second	Colum Colum Deletern				
L					

Spezifikationen:

Gruppenname: Der Name der SNMP-Gruppe oder eine Auflistung von Benutzern, die eine gemeinsame Zugriffsrichtlinie verwenden.

Sicherheitsstufe - Die Sicherheitsstufe, für die die Zugriffsparameter definiert sind. Wählen Sie

eine der folgenden Optionen aus:

noAuthNoPriv: Verwendet eine Übereinstimmung mit dem Benutzernamen für die Authentifizierung.

AuthNoPriv - Stellt Authentifizierung auf Basis der HMAC-MD5- oder HMAC-SHA-Algorithmen bereit.

AuthPriv - Bietet Authentifizierung auf Basis der HMAC-MD5- oder HMAC-SHA-Algorithmen. DES 56-Bit-Verschlüsselung, die neben der Authentifizierung auf dem CBC-DES-Standard (DES-56) basiert.

Wenn Sie authNoPriv oder authPriv für eine Gruppe auswählen, muss der entsprechende Benutzer mit einem Authentifizierungsprotokoll und einem Kennwort, mit Datenschutzprotokoll und Kennwort oder beidem konfiguriert werden.

Ansichten

Read View Name (Name anzeigen) - Name der Leseansicht für die Gruppe.

Benachrichtigungsansichtname - Benachrichtigungsansichtsname für die Gruppe.

SNMP-Sets zulassen - Aktivieren Sie dieses Kontrollkästchen, wenn der SNMP-Agent SNMP-SET-Anforderungen akzeptieren soll. Wenn dieses Kontrollkästchen nicht aktiviert ist, werden SET-Anforderungen abgelehnt.

Hinweis: Der SNMP SET-Anforderungszugriff wird für sehr wenige Objekte implementiert.

Schritt 7: Navigieren Sie zu Knotenansicht > Provisioning > SNMP > SNMP V3 > Trap Destination (V3). Klicken Sie auf Erstellen und Konfigurieren.

Target address:<any build server> (eg: blr-ong-lnx10)

UDP port: <anything between 1024 to 65535>

User name:<same as we created in step 3>

Security Level:AuthPriv Schritt 8: Klicken Sie auf OK, wie im Bild gezeigt.

	000	-   <mark></mark>	
	Configure SnmpV3 Trap		×
	Target Address:	blr-ong-lnx10	
	UDP Port:	4545	5
	User Name:	ank	▼ 4
	Security Level:	authPriv	▼ 3
<b>T</b> 1 12	Filter Profile:		
Alarms Conditions History Circuits	Proxy Traps Only:		
	Proxy Tags:		
General Network	OK	Cancel	
OSI General			/ Level Filter Profile
Protection Users			y Level The Prome
SNMP Group Access			
Comm Channels Trap Destinations	((/3)		
Timing Notification Filt	ers		
Alarm Profiles			
Defaults WDM-ANS	•		
SVLAN	Create Edit Delete		
Alarm Extenders	L		

Hinweis: blr-ong-lnx10 ist der NMS-Server.

Spezifikationen:

Zieladresse: Ziel, an das die Traps gesendet werden sollen. Verwenden Sie eine IPv4- oder eine IPv6-Adresse.

UDP-Port - UDP-Portnummer, die der Host verwendet. Der Standardwert ist 162.

Benutzername: Geben Sie den Namen des Benutzers auf dem Host an, der mit dem Agenten verbunden ist.

Sicherheitsstufe - Wählen Sie eine der folgenden Optionen aus:

noAuthNoPriv: Verwendet eine Übereinstimmung mit dem Benutzernamen für die Authentifizierung.

AuthNoPriv - Stellt Authentifizierung auf Basis der HMAC-MD5- oder HMAC-SHA-Algorithmen bereit.

AuthPriv - Bietet Authentifizierung auf Basis der HMAC-MD5- oder HMAC-SHA-Algorithmen. DES 56-Bit-Verschlüsselung, die neben der Authentifizierung auf dem CBC-DES-Standard (DES-56) basiert.

Filterprofil: Aktivieren Sie dieses Kontrollkästchen, und geben Sie den Namen des Filterprofils ein. Traps werden nur gesendet, wenn Sie einen Filterprofilnamen angeben und einen Benachrichtigungsfilter erstellen.

Nur Proxy-Traps: Bei Auswahl dieser Option werden nur Proxy-Traps aus der ENE weitergeleitet. Traps von diesem Knoten werden nicht an das Trap-Ziel gesendet, das durch diesen Eintrag identifiziert wird. Proxytags: Geben Sie eine Liste von Tags an. Die Tag-Liste ist nur dann auf einem GNE erforderlich, wenn ein ENE Traps an das Trap-Ziel senden muss, das durch diesen Eintrag identifiziert wird, und das GNE als Proxy verwenden möchte.

#### NMS-Server konfigurieren (blr-ong-lnx10)

Schritt 1: Erstellen Sie im Stammverzeichnis des Servers ein Verzeichnis mit dem Namen snmp.

Schritt 2: Erstellen Sie unter diesem Verzeichnis eine Datei snmptrapd.conf.

Schritt 3: Ändern Sie die Datei snmptrapd.conf in:

vi snmptrapd.conf createUser -e 0xEngine ID <user\_name>< MD5> <password > DES <password> Beispiele: createUser -e 0x0000059B1B00F0005523A71C ank MD5 ciscol23 DES ciscol23 In diesem Beispiel: user\_name=ank MD5 password = ciscol23 DES password = ciscol23 DES password = ciscol23 Engine ID = can be available from CTC. Node view > Provisioning > SNMP > SNMP V3 > General

#### Authentifizierungsmodus überprüfen

Schritt 1: Navigieren Sie im CTC zu Node View > Provisioning > Security > Access > Change snmp access state to Secure (Knotenansicht > Bereitstellung > Sicherheit > Zugriff > SNMP-Zugriffsstatus ändern wie im Bild gezeigt.

Tab View	
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN	
General	
Network Users Active Logins Policy Data Comm Access RADIUS Server TACACS Server Leg	al Disclaimer
OSI LAN Access	Pseudo IOS Access
Protection LAN Access: Front Craft & E *	Access State: Non-sec *
Security Restore Timeout: 5 - minute(s)	
Comm Channels	Port: 65000
Alarm Profiles	
Defaults Shell Access	EMS Access
WDM-ANS	TCC CORBA (IIOP) Listener Port
Certificate Telnet Port: 23 Use Standard Port	Default - TCC Fixed
	Standard Constant (683)
Enable Shell Password	O Other Constant:
TL1 Access	SNMP Access
Access State:	Access state:
Other	Serial Craft Access
PM Clearing Privilege: Provisioni *	☑ Enable Craft Port

Schritt 2: Navigieren Sie zum NMS-Server, und führen Sie einen Snapshot aus.

Syntax:

```
snmpwalk -v 3 -l authpriv -u <user name> -a MD5 -A <password> -x DES -X <password> <node IP>
<MIB>
Beispiel:
blr-ong-lnx10:151> snmpwalk -v 3 -l authpriv -u ank -a MD5 -A ciscol23 -x DES -X ciscol23
10.64.106.40 system
RFC1213-MIB::sysDescr.0 = STRING: "Cisco ONS 15454 M6 10.50-015E-05.18-SPA Factory Defaults
PLATFORM=15454-M6"
RFC1213-MIB::sysObjectID.0 = OID: CERENT-GLOBAL-REGISTRY::cerent454M6Node
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (214312) 0:35:43.12
RFC1213-MIB::sysContact.0 = ""
RFC1213-MIB::sysName.0 = STRING: "Ankit_40"
RFC1213-MIB::sysLocation.0 = ""
RFC1213-MIB::sysServices.0 = INTEGER: 79
SNMP-Trap:
```

 $\label{eq:snmptrapd-f-lo-OQ-Ob-Ot-F"$V\n&B\n&W\n&q\n&P\n&v\n\n" < port number>\\ Trap cmd ist für alle Versionen identisch.$ 

#### Konfigurieren des authNoPriv-Modus auf ONS15454/NCS2000-Geräten

Schritt 1: Navigieren Sie im CTC zu Node View > Provisioning > Security > Access > Change snmp access state to Non secure mode as in the image.

Tab View		7 _ 2
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN		
General Users Active Logins Policy Data Comm Access RADIUS Server TACACS Server	Legal Disclaimer	
Protection Security Telnet Port: 23 Use Standard Port	TCC CORA (IIOP) Isterer Port • Default – TCC Fixed	Apply Reset
Comm Channels Enable Shell Password	Standard Constant (683)     Other Constant:	Help
WDM-ANS         Access	SNMP Access Access State: Non-sec *	
SVLAN Other Certificate PM Clearing Privilege: Provisioni *	Serial Craft Access ✓ Enable Craft Port	<b>•</b>

Schritt 2: Navigieren Sie zu Knotenansicht > Provisioning > SNMP > SNMP V3 > Users > Create User und konfigurieren Sie wie im Bild gezeigt.

		· •	
	Create User	×	
	User Name:	ank1	6
	Group Name:	default_group	5
	Authentication		
	Protocol:	MD5 👻	
	Password:	skalanderske kalender som	3
Tab View	Privacy		
Alarms Conditions History Circuit	Protocol:	NONE	
	Password:		
General SNMP V1/V2			
	OK	Cancel	
Protection Users			Group Name
Security MIB views	s ank MD5	DES	default_group
SNMP Group Acce	255		
Comm Channels Trap Destinatio	ns(V3)		
Timing Notification F	ilters		
Defaults			
WDM-ANS			
SVLAN	Create Edit Delet	2	
Alarm Extenders	·		

Schritt 3: Stellen Sie sicher, dass die MIB-Ansichten wie im Bild gezeigt konfiguriert sind.

Tab Vie	w									
Alarms	Conditions	٦٢	History Circuits Provis	sioning Inventory	Mainter	nance OTN				
	General Network		SNMP V1/V2 SNMP V3	Common						
	Protection	1	Users	View Name		Sub Tree OID		Mask	Туре	
	Security	1	MIB views	fullview		1	1	l	included	]
	SNMP		Group Access							
Con	nm Channels		Trap Destinations(V3)							
قاه_	arm Profiles		Notification Filters							
	Defaults									
	NDM-ANS									
	SVLAN									
	Certificate			Create E	dit	Delete				
		Ľ								

Schritt 4: Konfigurieren Sie den Gruppenzugriff, wie im Bild für den Authentifizierungsmodus dargestellt.

			0	
	Create Group Access		×	
	Group Name:	default_group	<b></b>	
	Security Level:	authNoPriv	<b></b>	
Tab View           Alarms         Conditions         History         Circuits         Provisi	Read View Name: Notify View Name:	fullview		
General SNMP V1/V2 SNMP V3	Allow SNMP Sets:			
OSI General Protection Users		OK Cancel	fy Viev v	v Access
Security MIB views SNMP Group Access				
Timing Notification Filters				
Alarm Profiles				
Defaults				
WDM-ANS	Create Edit Delete	)		
Alarm Extenders				

Schritt 5: Navigieren Sie zu Knotenansicht > Provisioning > SNMP > SNMP V3 > Trap Destination (V3). Klicken Sie auf Erstellen und Konfigurieren, wie im Bild gezeigt.

	Configure SnmpV3 Trap	×	®	
	a second		7	
	Target Address:	bir-ong-inx10	0	L
	UDP Port:	4565	5	
	User Name:	ank1 💌	4	
	Security Level:	authNoPriv 👻	3	
	Filter Profile:			
Tab View	Prove Trans Only			r _×
Alarms Conditions History Circuits	s and the second			
	Proxy Tags:			
SNMP V1/V2 S		Const		
Capacity Contract Contract	OK	Cancel		
Protection			Level Filter Profile Name	Proxy Traps Only
Security MIB view:	64.103.217.88 4545 a	nk authPriv		
SNMP Group Acce	855			
Comm Channels Trap Destinatio	ins(V3)			
Timing Notification F	ilters			
Alarm Profiles				
Defaults	•			
WDM-ANS	Create Edit Delete			Help
SVLAN				
Alarm Extenders				

#### Überprüfen des Authentifizierungsmodus "NoPriv"

Schritt 1: Navigieren Sie zum NMS-Server, und führen Sie einen Snapshot aus.

Syntax:

snmpwalk -v 3 -l authnopriv -u <user name> -a MD5 -A <password> <node IP> <MIB>
Beispiel:

blr-ong-lnx10:154> snmpwalk -v 3 -l authnopriv -u ankl -a MD5 -A ciscol23 10.64.106.40 system RFCl213-MIB::sysDescr.0 = STRING: "Cisco ONS 15454 M6 10.50-015E-05.18-SPA Factory Defaults

```
RFC1213-MIB::sysObjectID.0 = OID: CERENT-GLOBAL-REGISTRY::cerent454M6Node
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (430323) 1:11:43.23
RFC1213-MIB::sysContact.0 = ""
RFC1213-MIB::sysName.0 = STRING: "Ankit_40"
RFC1213-MIB::sysLocation.0 = ""
RFC1213-MIB::sysServices.0 = INTEGER: 79
SNMP-Trap:
```

PLATFORM=15454-M6"

 $\label{eq:snmptrapd-f-lo-OQ-Ob-Ot-F"$V\n&B\n&W\n&q\n&P\n&v\n\n" < port number>\\ Trap cmd ist für alle Versionen identisch.$ 

#### Konfigurieren des AutoNoPriv-Modus auf ONS15454/NCS2000-Geräten

Schritt 1: Navigieren Sie im CTC zu Node View > Provisioning > Security > Access > Change snmp access state to Non secure mode as in the image.

Tab View		<ul> <li></li> <li></li></ul>
Alarms Conditions History Circuits Provisioning Inventory Main	ntenance OTN	
General     Users     Active Logins     Policy     Data Comm     Active Logins       OSL     Vxccess state.     Ivon-sec     Ivon-sec       Protection     Staturity     Telnet Port:     23     Use Stand       SNMP     Enable Shell Password	ADUUS Server TACACS Server Legal Disclaimer  ACCESS State: TCC CORBA (IIOP) Listener Port Default - TCC Fixed Standard Constant (683) Other Constant:	Apply Reset Help
Defaults TL1 Access WDM-ANS Access State: Non-sec *	SNMP Access Access State: Non-sec *	
SVLAN         Other           Certificate         PM Clearing Privilege: Provisioni *	Serial Craft Access	

Schritt 2: Navigieren Sie zu Node View > Provisioning > SNMP > SNMP V3 > Users > Create User and Configure (Knotenansicht > Bereitstellung > SNMP > SNMP V3 > Benutzer > Benutzer erstellen und Konfigurieren, wie im Bild gezeigt.

Create User     User Name:   ank2   Group Name:   default_group     Authentication   Protocol:   NONE     Password:     Privacy   Protocol:     NONE			1 ( ) : .		
User Name: ank2 Group Name: default_group Authentication Protocol: Protocol: Password: Privacy Protocol: NONE		Create User		×	
Group Name:     default_group       Authentication       Protocol:       Password:       Tab View       Privacy       Protocol:       NONE		User Name:	ank2		
Authentication       Protocol:       Password:		Group Name:	default_group		5
Protocol:     NONE       Password:     3       Tab View     Privacy       Protocol:     NONE		Authentication			4
Tab View Privacy Protocol: NONE		Protocol:	NONE	<b>.</b>	
Tab View Privacy Protocol: NONE		Password:			3
Alexan Constitional Utimes Constit	Tah View	Privacy			
	Alarma Conditions History Circuit	Protocol:	NONE	•	
Password:	Manns Conditions History Circuit	Password:			
General	General				
Network OK Cancel	Network		OK Cancel		
OSI General Group Name	OSI General				Group Name
Protection Users ank MD5 DES default_group	Protection Users	ank	MD5	DES	default_group
Security MIB views ank1 MD5 NONE default_group	Security MIB view	s ank1	MD5	NONE	default_group
SNMP Group Access	SNMP Group Acce	ess			
Timina NetGenia Silver	Timing	(ns(V3)			
Alarm Profiles	Alarm Profiles	liters			
Defaults	Defaults				
WDM-ANS	WDM-ANS				
SVLAN Edit Delete	SVLAN	Create Edit	Delete		
Alarm Extenders	Alarm Extenders				

Schritt 3: Stellen Sie sicher, dass MIB-Ansichten wie im Bild gezeigt konfiguriert sind.

Tab Viev	w										
Alarms	Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN										
	General										
	Network	SNMP V	1/V2 SN	MP V3	Common						
	OSI		General		View Nam	ie	Sub Tree OID		Mask	Туре	
	Security		Users MIB views		fullview		1	1		included	
	SNMP	G	roup Acces	s							
Com	m Channels	Trap	Destination	s(V3)							
Ala	rm Profiles	Not	ification Eilt	ers							
	Detaults										
	DM-ANS										
	ertificate				Create	Edit	Delete				
				l							
	l										

Schritt 4: Konfigurieren Sie den Gruppenzugriff, wie im Bild für den noauthnopriv-Modus gezeigt.

	(	Create G	roup Access				×	7	
Group Name:				default_group 💌			•		
		Security	Level:		noAuthNoPriv - 6			•	
		Views:	/5:				4		
		Read V	iew Name:		fullview	1	*	3	
		Notify	View Name:		fullview	r			
Tab View					_				
Alarms Conditions	History Circ	Allows	SNMP Sets:						
General	SNIN4D VILAZ			ОК	Cancel				
Network	SIMIAIN ATLAS								
IZO	General	_	Group Name	Security Le	vel A	Read View Access	Allow SNMP Set	s Notify View Access	_
Protection	Users		default group	authPriv	PCI /	fullview		fullview	
Security	MIB views	5	default group	authNoPriv		fullview		fullview	
SNMP	Group Acce	:55							
Comm Channels	Trap Destinatio	ns(V3)							
Timing	Notification F	ilters							
Alarm Profiles									
Defaults									
WDM-ANS			Create Edit	Delete					
SVLAN			Creatern	Deleter					
Alarm Extenders									

Schritt 5: Navigieren Sie zu Knotenansicht > Provisioning > SNMP > SNMP V3 > Trap Destination (V3). Klicken Sie auf Erstellen und Konfigurieren, wie im Bild gezeigt.

c			Configure SnmpV3 Trap					8
		Targ	et Address:		blr-ong-lnx10			6
		UDP	Port:		4576			6
		User Name:			ank2 💌			4
		Secu	arity Level:		noAuthNoPriv 🔻			3
			Filter Profile:					1
Tab View		Prox	y Traps Only:					
Alarms Conditions	History    Circuits	Prox	y Tags:				<u> </u>	
General	SNMP V1/V2							
Network				ОК	Cancel			
02	General						/ Level	
Protection	Users	_	64.103.217.88	4545	ank	authPriv		
Security	MIB views		64.103.217.88	4565	ank1	authNoPri	v	
SNMP	Group Access							
Comm Channels	Trap Destinations	(V3)						
Timing	Notification Filte	ers						
Alarm Profiles								
Defaults			4					
WDM-ANS								
SVLAN			Create	Ealt Delete				
Alarm Extenders								
L								

### Überprüfen des AutoNoPriv-Modus

Schritt 1: Navigieren Sie zum NMS-Server, und führen Sie einen Snapshot aus.

```
Beispiel:
blr-ong-lnxl0:155> snmpwalk -v 3 -l noauthnopriv -u ank2 10.64.106.40 system
RFC1213-MIB::sysDescr.0 = STRING: "Cisco ONS 15454 M6 10.50-015E-05.18-SPA Factory Defaults
PLATFORM=15454-M6"
RFC1213-MIB::sysObjectID.0 = OID: CERENT-GLOBAL-REGISTRY::cerent454M6Node
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (486910) 1:21:09.10
RFC1213-MIB::sysContact.0 = ""
RFC1213-MIB::sysName.0 = STRING: "Ankit_40"
RFC1213-MIB::sysLocation.0 = ""
RFC1213-MIB::sysServices.0 = INTEGER: 79
blr-ong-lnx10:156>
SNMP-Trap:
```

 $\label{eq:snmptrapd-f-lo-OQ-Ob-Ot-F"$V\n&B\n&W\n&q\n&P\n&v\n\n" < port number>\\ Trap cmd ist für alle Versionen identisch.$ 

### SNMP V3-Trap für GNE/ENE-Einrichtung

snmpwalk -v 3 -l noauthnopriv -u <user name> <node IP> <MIB>

#### Auf GNE-Knoten

Schritt 1: Navigieren zu Bereitstellung > SNMP > SNMP V3 und CGruppenzugriff erstellen (Registerkarte "Gruppenzugriff"): Geben Sie einen Gruppennamen mit Sicherheitsstufe (noAuthnoPriv|AuthnoPriv|authPriv) und eine vollständige Ansicht mit Lesen und Benachrichtigen an, wie im Bild gezeigt.

-  :  36 - PTS	A_GE 🚽	<b>1</b> 0	Create Group Access	×	6
Summary 🔡 Ne	twork	Group Name:	gnegrp1	<b>_</b>	
15454 M6 ANSI	107.114	Security Level:	authPriv	-	
Alarms Condition	ns History	Views:			
General	SNMP V1/V2	Read View Name:	fullview	<b>_</b>	
OSI	Gener	Notify View Name:	fullview		Sets Notify Vi fullview
Protection	MIR vie	Allow SNMP Sets			fullview
Security	Group Ac	Allow Shirin Secs.		[	
SNMP	Tran Destina		<u> </u>		
Comm Channels	Notification		OK Cancel		
Timing	Notification				
Alarm Profiles	L				
Defaults					
WDM-ANS					
SVLAN					
Alarm Extenders					
		Create Ed	lit Delete		

Schritt 2: Benutzerzugriff erstellen (Registerkarte "Benutzer"): Erstellen Sie einen Benutzer mit dem Gruppennamen, der mit dem zuvor in der Registerkarte Gruppenzugriff erstellten Namen identisch ist. Stellen Sie außerdem die Authentifizierung basierend auf der Zugriffsebene bereit, wie im Bild gezeigt.

— 🔝 8 – TSC			Act 🕒				
- : 36 - PTS	A_GE 🚽	80	Creat	e User	×		
<ul> <li>III</li> <li>Summary <sup>1</sup>/<sub>2</sub> Ne</li> </ul>	twork	User Name: Group Name:		gneuser1		<mark>, </mark>	
Alarms Condition	107.114 ns History Circ	Authentication		3			
Canaral		Protocol:		MD5	-		
Network	SNMP V1/V2 S	Password:		•••••			
OSI	General	Privacy				tocol	
Protection	Users MIR views	Protocol:		DES	-		def
Security	Group Access						
SNMP	Trap Destination	Password:		•••••			
Timing	Notification Filt						
Alarm Profiles			ОК	Cancel R			
Defaults	L					1	
WDM-ANS							
SVLAN Alarm Extenders							
Alarm Extenders							
		Create	Edit De	ete			
l							

Schritt 3: Registerkarte Trap Destination (V3):

Zieladresse: Adresse des NMS-Servers, von dem aus das Trap ausgeführt wird (z. B. Blr-ong-Inx10). UDP-Port: Alle Portnummern, unter denen das Trap überwacht wird (z. B. 9977).

Benutzername: Name des Benutzers auf der Registerkarte Benutzer.

Sicherheitsstufe: Wie zuvor auf der Registerkarte "Benutzer" konfiguriert.

Proxy-Tags: Geben Sie ein Proxy-Tag (z. B. Tag75).

	<u>ی</u>	Configure SnmpV3 Trap	×	for the second sec
	Target Address:	blr-ong-lnx10		r s
Summary Retwork	UDP Port:	9999		<b></b>
Alarms Conditions History Circ	User Name:	gneuser1	-	
General SNMP V1/V2 St	Security Level:	aut <mark>i</mark> , Priv	•	
Network General	Filter Profile:			Security Level
Protection Users	Proxy Traps Only:			thPriv thPriv
Security Group Access	Proxy Tags:	TagV3		
Comm Channels				
Timing Notification File		OK Cancel		
Alarm Profiles Defaults				
WDM-ANS				
SVLAN				
Alarm Extenders				
	4			
	Create	Edit Delete		

#### Auf ENE-Knoten

Schritt 1: Navigieren Sie zu **Provisioning > SNMP > SNMP V3 und Create Group Access** (Gruppenzugriff erstellen): Geben Sie einen Gruppennamen mit Zugriffsebene (noAuthnoPriv|AuthnoPriv|authPriv) und eine vollständige Ansicht mit Lesen und Benachrichtigen an, wie im Bild gezeigt.

				,		the second se
ENE]Node2	10 -	8	Create Gr	oup Access	X	
Summary 📲 Ne	twork	Group Name:		enegrp1	-	
Alarms Condition	l Node-75	Security Level:		authPriv	•	
Alams Condicio	ins miscory	Views:				
General	SNMP V1/V2	Read View Name:		fullview	-	
OSI	Gener	Notify View Name:		fullview	-	Sets
Protection	MIR via	Allow SNMP Sets				f
Security	Croup Ac	Allow SIMIL Sets.	7			
SNMP	Tran Destina					
Comm Channels	Notification		ОК	Cancel		
Timing	Notification					
Alarm Profiles	L					
Defaults						
WDM-ANS						
SVLAN						
		Create	Edit Del	ete		

Schritt 2: Benutzerzugriff erstellen (Registerkarte "Benutzer"): Erstellen Sie einen Benutzer mit dem Gruppennamen, der mit dem zuvor in der Registerkarte Gruppenzugriff erstellten Namen identisch ist. Stellen Sie darüber hinaus die Authentifizierung basierend auf der Zugriffsebene bereit.

- 1:1 36 - PTS	A_GE	<b>•••</b>	• TTF-4 : • • • • • • • • • • • • • • • • • •	×
I: 36 - PTS File (ENE)Node2 (ENE)NO (ENE)N	A_GE 10 V etwork I Node-75 ns History Circ SNMP V1/V2 Sh General Users MIB views Group Access Trap Destination: Notification Filt	User Name: Group Name: Authentication Protocol: Password: Privacy Protocol: Password:	Create User  Create User  eneuser1 enegrp1  MD5  DEX OK Cancel	
SVLAN		Create E	dit Delete	

Stellen Sie sicher, dass auf der Registerkarte "Gruppenzugriff" eine default\_group erstellt wird, falls diese in der Registerkarte "Gruppenzugriff" fehlt.

Schritt 3: Registerkarte Trap Destination (V3):

Zieladresse: GNE-Knoten-IP.

UDP-Port: 162.

Benutzername: Name des Benutzers auf der Registerkarte Benutzer.

Sicherheitsstufe: Wie zuvor auf der Registerkarte "Benutzer" konfiguriert.

Proxy-Tags: Geben Sie ein beliebiges Proxy-Tag wie GNE (z. B. Tag75).

- : 36 - PTS	A_GE			
► 🔐 [ENE]Node2	10 -	8J	Configure SnmpV3 Trap	×
		Target Address:	10.64.107.114	
Summary Revealed the second se	Node-75	UDP Port:	162	
Alarms Condition	ns History Circ	User Name:	eneuser 🚶	<b></b>
General	SNMP V1/V2 St	Security Level:	authPriv	
Network OSI	General	Filter Profile:		Securit
Protection	Users MIB views	Proxy Traps Only:		thPriv
Security	Group Access	Proxy Tags:	TagENE	
Comm Channels Timing	Notification Filt			
Alarm Profiles			OK Cancel	
Defaults WDM-ANS	L			
SVLAN				
		•	Ш	
		Create E	dit Delete	

Navigieren Sie im CTC zur Netzwerkansicht:

Schritt 1: Navigieren Sie zur Registerkarte SNMPv3.

Schritt 2: SNMPv3-Proxy-Trap-Weiterleitungstabelle: Sie können entweder **manuell** oder **automatisch erstellen**.

Wählen Sie Auto Create (Automatisch erstellen). Im Rahmen dieser Verordnung

- Ziel-Tag: Proxy-Tag in GNE festgelegt.
- Remote-Trap-Quellliste: Wählen Sie die ENE-Knoten-IP aus, wie im Bild gezeigt.

Network Explorer 🗆 ×	Automatic Configuration of SNMPv3 Proxy Trap Forwar X	
	Target Tag: TagV3	
Summary 🔡 Network	Remote Trap Source List	9.4×
Alarms Conditions History	Circui 10.64.107.114	
Security	10.64.107.187	
Alarm Profiles	10.64.107.210	
BLSR	10.04.101.15	
Overhead Circuits		
Provisionable Patchcords (PPC)	Man	
Server Trails		
SNMPV3	OK Cancel Help	Late User
		authPriv
	0000059B2DFAA0003E8A8362 Tag114 ons_trap_user	authPriv
	Manual Create Delete SNMPv3 Remote Users Context Engine JD User Name Authenti	ication Protocol Prince/ Protocol
		Help

#### GNE/ENE-Einrichtung überprüfen

NMS-Server konfigurieren (blr-ong-lnx10):

Schritt 1: Erstellen Sie im Stammverzeichnis des Servers ein Verzeichnis, und nennen Sie es snmp.

Schritt 2: Erstellen Sie unter diesem Verzeichnis eine Datei snmptrapd.conf.

Schritt 3: Erstellen Sie in snmptrapd.conf die folgende Konfiguration:

Engine\_NO = can be available from CTC. Open GNE node-->Node view->Provisioning->SNMP->SNMP V3-->General. SNMP-Trap:

snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n"
snmpwalk auf ENE:

Für den Authentifizierungs-Modus:

createUser -e 0x

snmpwalk -v 3 -l authpriv -u <user\_name> -a MD5 -A <auth\_password>123 -x DES -X <des\_password> E <ene\_engine\_id> <gne\_ip\_address> <OID>

Für den Authentifizierungsmodus:

<gne\_ip\_address> <OID> Für den noauthnopriv-Modus:

snmpwalk -v 3 -l authpriv -u

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.