

عضو ISE مادختساب (SGTs) TrustSec نيوكت (رطسلا لخاد تامالع)

تايوتحمل

قمدقمل

[قيساس الابلطت مل](#)

[تابلطت مل](#)

[قمدختس مل تانوك مل](#)

نيوكت مل

[قكبشلا ليطيطخت مل مسر مل](#)

[فده](#)

[تاننيوكت مل](#)

[ISE يلعل TrustSec نيوكت](#)

[TrustSec AAA مداخل Cisco ISE نيوكت](#)

[Cisco ISE ف رADIUS زاوكلو مل عفاضا نم ققحتلا و نيوكت مل](#)

[ققحتلا و \(WLC\) قكبشلا مل ققحتلا ف مكدختلا رصنع نيوكت عفاضا ممت](#)
[Cisco ISE ف TrustSec زاوكلو نم](#)

[\(قرايتخا\) قلوبقم اونأ نم دكأتلل قضاوت فال TrustSec تاداعا نم ققحت](#)

[نيوكشلا ليل نيومدختس مل نيومت عومجم تامالع عاشرا](#)

[ديقملا بيول مداخل SGT ليل IP نم قكبشلا ساسا ليطيطخت عاشرا](#)

[قداوشلا ققداصم فيرعت فلم عاشرا](#)

[لبق نم قداوشلا ققداصم فيرعت فلم قيوه رصم ليل سلسل عاشرا](#)

[بس انم بي قرو \(نيراشتس مل او نيوظوم مل\) نيوكشلا ليل نيومدختس مل نيويعت مق](#)

[قكبشلا ف مكدختلا رصنع و لوكلو \(قيلع فال قزوأل ليل بي قرا نيويعت مق](#)
[\(WLC\) قكبشلا ليل ققحتلا مل](#)

[چورخلا قسايس ديختل SGACLs ديخت مق](#)

[TrustSec قسايس ققفاصم يلعل قكبشلا ليل \(ACL\) لوصولا ف مكدختلا مل؛ اوق ضر ف](#)
[Cisco ISE ف](#)

Catalyst لوكلو TrustSec نيوكت

[Catalyst لوكلو TrustSec ل AAA مداخل ال لوكلو نيوكت](#)

[Cisco ISE يلعل لوكلو ققداصم رADIUS مداخل نمض PAC حاتق م نيوكت](#)

[Cisco ISE يلعل لوكلو ققداصم CTS دامتع تانايب نيوكت](#)

[Catalyst لوكلو ماع لكشب CTS نيوكت](#)

[\(قرايتخا\) قروكلو مل بيول مداخل SGT ليل IP نم تباك نيويعت](#)

[Catalyst لوكلو TrustSec نم ققحتلا](#)

WLC يلعل TrustSec نيوكت

[\(WLC\) قكبشلا ليل ققحتلا ف مكدختلا رصنع عفاضا نم ققحتلا و نيوكت مل](#)
[Cisco ISE ف رADIUS زاوكلو](#)

[ققحتلا و \(WLC\) قكبشلا ليل ققحتلا ف مكدختلا رصنع نيوكت عفاضا ممت](#)
[Cisco ISE ف TrustSec زاوكلو نم](#)

[WLC نم \(PAC\) مكدختلا لوصولا تاغوسم ريفوت نيوكت](#)

[WLC يلعل TrustSec نيوكت](#)

[قكبشلا ف مكدختلا رصنع يلعل \(PAC\) مكدختلا لوصولا تاغوسم ريفوت نم ققحتلا](#)
[\(WLC\) قكبشلا ليل ققحتلا مل](#)

[WLC ليل Cisco ISE نم CTS قيوه تانايب ليل زنت](#)

[رورمل ققفاصم يلعل اهذيفنت و SGACL تاليل زنت نيوكت](#)

[عطقنو \(WLC\) قكبشلا ليل ققحتلا ف مكدختلا رصنع صيخت مق](#)
[\(TrustSec Devices\) 2 بي قرا ل عمل لوصولا](#)

ةمدقم لىل

ةدحوو Catalyst لوجم ىلع هتحص نم ققحت لىل او TrustSec نيوكت ةيفيك دنتس ملىل اذه حضوي ةيوه لىل تامدخ كرحم مادختساب ةيكلس لىل ةيلحم لىل ةكبش لىل م كحت

ةيساس لىل تاب لىل

ةيلال لىل عيضاوم لىل اب ةفرعم كيدل نوكت نأب Cisco ي صوت

- Cisco TrustSec (CTS) تانوكمب ةيساس لىل ةفرعم
- حاتفم ةزافح ةدام نم لىل كشت CLI لىل ةيساس لىل ةفرعم
- ةكبش ي ف م كحت لىل تادحو لىل (GUI) ةيموسر لىل مدختس ملىل ةهجاو نيوكت ب ةيساس لىل ةفرعم Cisco (WLC) نم ةيكلس لىل لىل LAN
- (ISE) ةيوه لىل تامدخ كرحم نيوكت ةبجت

تاب لىل

لىل ةقداص ملىل نيئيئا ه نلىل ني مدختس ملىل ىلع بجي امك ، ككتكبش ي ف Cisco ISE رشن بجي ةيكلس و ةيكلس لىل ةكبش ب مه لىل صوت دنع (ىرخأ ةقيرط و) 802.1x مادختساب Cisco ISE اومووي نأ درجم ب (SGT) نام لىل ةومجم مقر مهب ةصاخ لىل رورم لىل ةكرح Cisco ISE ني عي ك ب ةصاخ لىل ةيكلس لىل ةكبش لىل ىلع ةقداص ملىل

كب صاخ لىل زا ه لىل ةب اوب راضح لىل ISE لىل نيئيئا ه نلىل ني مدختس ملىل هي جوت ةداع ممت ، ان لىل م ي ف ةيكلس لىل ةكبش لىل لىل نام لىل لوصول مهنكم ي ىتح ةداهش ب مه ديوزت متي و (BYOD) تاوطخ لامك لىل درجم ب (EAP-TLS) لىل قن لىل ةقبط نام - عسوت ملىل ةقداص ملىل لوكوتورب مادختساب لىل BYOD.

ةمدختس ملىل تانوكم لىل

ةيلال لىل جم ارب لىل او ةيوه لىل تامدخ لىل تانوكم لىل تارادص لىل دنتس ملىل اذه ي ف ةدراول تامولعمل دنتست

- Cisco Identity Services Engine، رادص لىل 2.4
- Cisco Catalyst 3850 Switch، رادص لىل 3.7.5E لوجم لىل
- Cisco WLC، رادص لىل 8.5.120.0
- ي لىل حم لىل عضول ي ف Cisco Aironet ةيكلس لىل لوصول ةطقن

Cisco WLC+AP Modules و/أو Cisco Catalyst Switch لوجم نأ نم ققحت ، Cisco TrustSec رشن لىل ب ق لىل ممد ه ي دل جم انرب لىل رادص لىل +

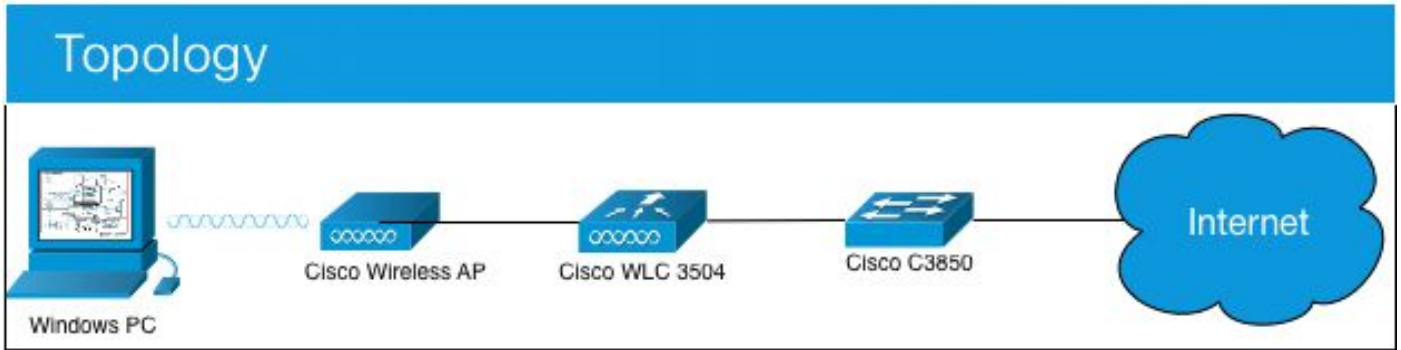
- TrustSec/نام لىل ةومجم تامالعل
- ي ف تامالعل عضو نم ال دب SXP مادختس لىل كنىم ي ، نكى مل اذ لىل رطس لىل ي ف تامالعل عضو (رطس لىل)
- (ةجالح دنع) بيقر لىل لىل (IP) تنرتن لىل لوكوتورب نم ةتبات تانوي عت

- (رمأل مزل اذإ) ببقرلل ةتباثلل ةبعرفلل تاكبشلل تانبعع
- (رمأل مزل اذإ) ببقرلل ىل ةتباثلل (VLAN) ةبرهظلل ةلحملل تاكبشلل تانبعع

ةصاخ ةبلعم ةئبب بق ةءوومل ةزهأل نم ءنئسمل اءه بق ةءراول تامولعملل ءاشنل مئ تناك اذإ. (بضارءفا) ءوسمم نبوكئب ءنئسمل اءه بق ةمدءئسمل ةزهأل بعبع ءأءب رملل لل مءءملا ربلءل لل كمهف نم ءكأءف، لبغشءل ءبق كئكئبش

نبوكئلل

ةكبشلل بطبءءلل مسرلل



زببمئب (WLC) ةبكلسللل ةلحملل ةكبشلل بق مكءءلل رصنع موقت، لءءملا اءه بق فظوم نم ناك اذإ 7 ببقرلل +، راءشئسم نم ناك اذإ 15 ببقرلل اءنل ىلء مزءلل

نبب راءشئسم لل نم كمبب الل) 8 ببقرلل ىل 15 ببقرلل نم تناك اذإ مزءلل اءه ءافملل بفربو (8 ببقرلل اءلء ةمالع ءضومئ بءلل مءاوءلل ىل لوصول

لوصول نبب فظوم لل نم كمبب الل) 8 ببقرلل ىل 7 ببقرلل نم تناك اذإ مزءلل كلئل لءءملا ءمببب (8 ببقرلل اءلء ةمالع ءضومئ بءلل مءاوءلل ىل

فءه

لوصول ببقرلل ىل لوصول ب صءش ببل ءامسلل

لوصول ببقرلل عم نكلو، EmployeeSSID ىل لوصول بنبب راءشئسم لل ءامسلل

لماكل لوصول عم EmployeeSSID ىل لوصول بنبب فظوم لل ءامسلل

ببءلل لءءملا بق	IP ناوع	VLAN
ببءلل ءامءءل ءمءم (ISE)	10.201.214.230	463
Catalyst Switch لءءملا	10.201.235.102	1115
WLC	10.201.214.229	463
لوصول ةطقن	10.201.214.138	455

مسالل	Username	ببءلل ءمءملا	ء.ء	ببقر
ءببمس نبوسببء	ءببمسببء	نبب راءشئسم الل	نبب راءشئسم الل	15
ءببمس ببلس	ءببمس	نبب فظوملل	ءوبب وفظوم	7
رفوم رببب	رفوم رببب	رفوم رببب	TrustSec_Devices	2

تاني وك تال

ISE لى TrustSec نيوك ت

TrustSec Overview

1 Prepare

Plan Security Groups
Identify resources that require different levels of protection

Classify the users or clients that will access those resources

Objective is to identify the minimum required number of Security Groups, as this will simplify management of the matrix

Preliminary Setup
Set up the [TrustSec AAA server](#).

Set up TrustSec [network devices](#).

Check default TrustSec [settings](#) to make sure they are acceptable.

If relevant, set up [TrustSec-ACI](#) policy group exchange to enable consistent policy across your network.

Consider activating the [workflow process](#) to prepare staging policy with an approval process.

2 Define

Create Components
Create [security groups](#) for resources, user groups and Network Devices as defined in the preparation phase. Also, examine if default SGTs can be used to match the roles defined.

Define the [network device authorization policy](#) by assigning SGTs to network devices.

Policy
Define [SGACLs](#) to specify egress policy.

Assign SGACLs to cells within the [matrix](#) to enforce security.

Exchange Policy
Configure [SXP](#) to allow distribution of IP to SGT mappings directly to TrustSec enforcement devices.

3 Go Live & Monitor

Push Policy
Push the [matrix](#) policy live.

Push the [SGTs](#), [SGACLs](#) and the [matrix](#) to the network devices [📌](#)

Real-time Monitoring
Check [dashboards](#) to monitor current access.

Auditing
Examine [reports](#) to check access and authorization is as intended.

TrustSec AAA مداخلك Cisco ISE نيوك ت

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID > Overview > Components > TrustSec Policy > Policy Sets > SXP > Troubleshoot > Reports > Settings. The left sidebar shows a tree view with 'Trustsec AAA Servers' selected. The main content area is titled 'AAA Servers List > corbinise' and 'AAA Servers'. It contains the following form fields:

- * Name: CISCOISE
- Description: (empty text area)
- * IP: 10.201.214.230 (Example: 10.1.1.1)
- * Port: 1812 (Valid Range 1 to 65535)

At the bottom of the form are 'Save' and 'Reset' buttons.

Cisco ISE في RADIUS زاهك لوجملا ةفاضل نم ققحتلال او نيوك تال

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu on the left includes 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', 'External MDM', and 'Location Services'. The main configuration area is titled 'Network Devices' and shows the configuration for a device named 'CatalystSwitch'. The configuration fields are as follows:

- * Name: CatalystSwitch
- Description: Catalyst 3850 Switch
- IP Address: 10.201.235.102 / 32
- * Device Profile: Cisco
- Model Name: [Empty]
- Software Version: [Empty]
- * Network Device Group:
 - Location: All Locations (Set To Default)
 - IPSEC: No (Set To Default)
 - Device Type: All Device Types (Set To Default)
- * RADIUS Authentication Settings:
 - RADIUS UDP Settings:
 - Protocol: RADIUS
 - * Shared Secret: Admin123 (Hide)
 - Use Second Shared Secret: [Unchecked]
 - CoA Port: 1700 (Set To Default)
 - RADIUS DTLS Settings:
 - DTLS Required: [Unchecked]
 - Shared Secret: radius/dtls

هنا قمنا بتهيئة الواجهة (WLC) التي تدير الواجهة في مركزنا لنصنع نيوكتة إضافية تمت
 إعدادها في Cisco ISE TrustSec

إلى IP تاني يفتح ريشن من Cisco ISE نكمي اذ هو SSH ل لوخدنا ليجست دامتعا تانايب لخدنا
 لوجملا إلى إلتباتال بيقرنا.
 Cisco ISE من بيولوا ربع (GUI) ةيموسرلا مدخستسمل ةهجاو في رصانعلا هذه عاشن إكنكمي
 انه حضوم وه امك Work Centers > TrustSec > Components > IP SGT Static Mappings تحت

Network Devices
Default Device
Device Security Settings

Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device ID:

* Password:

TrustSec Notifications and Updates

* Download environment data every:

* Download peer authorization policy every:

* Reauthentication every:

* Download SGNCL file every:

Other TrustSec devices to trust this device:

Send configuration changes to device: Using Out CLI (SSH)

Send from:

Set Key:

Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates:

Device Interface Credentials

* EXEC Mode Username:

* EXEC Mode Password:

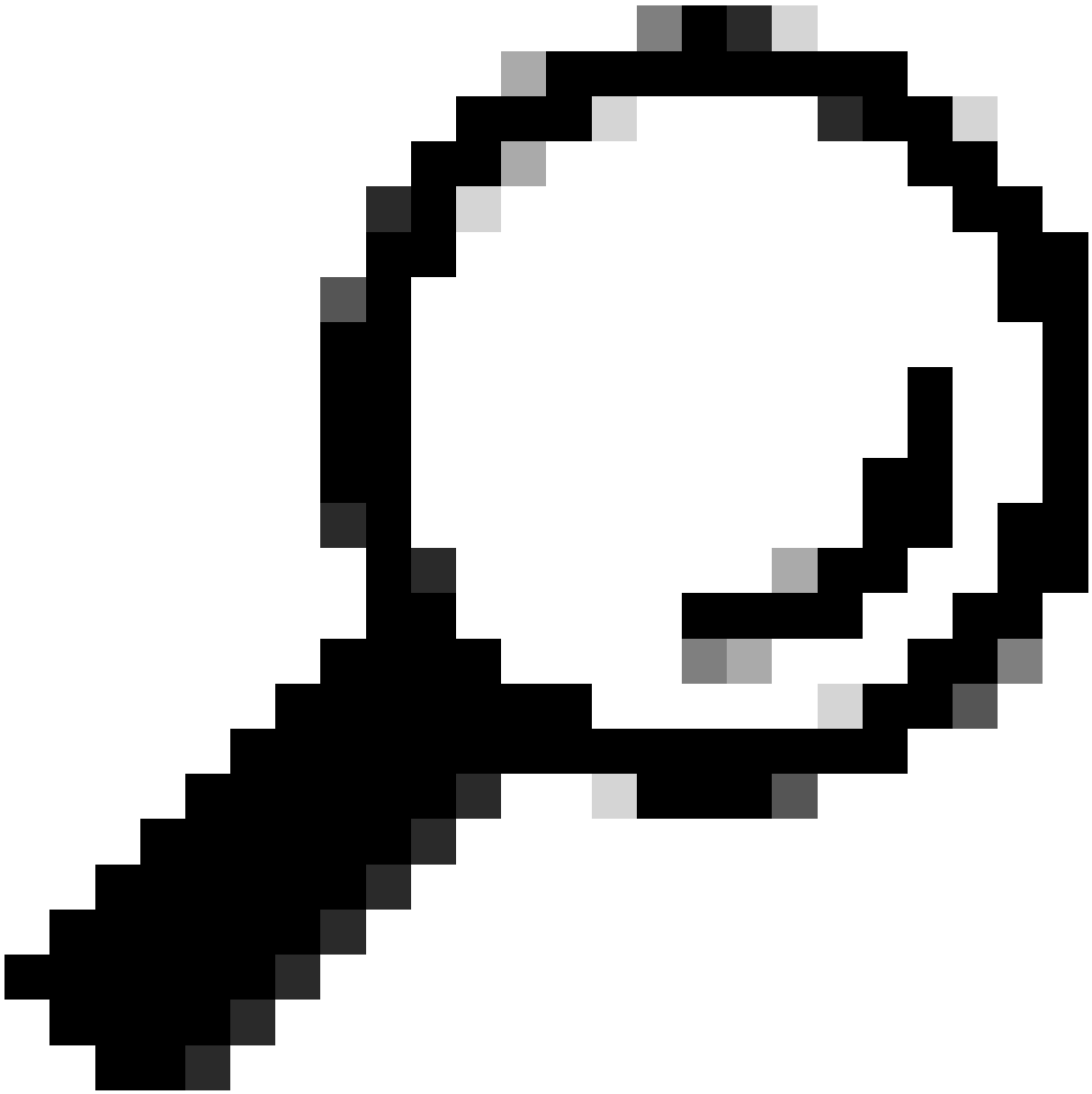
Enable Mode Password:

Out Of Band (OOB) TrustSec PAC

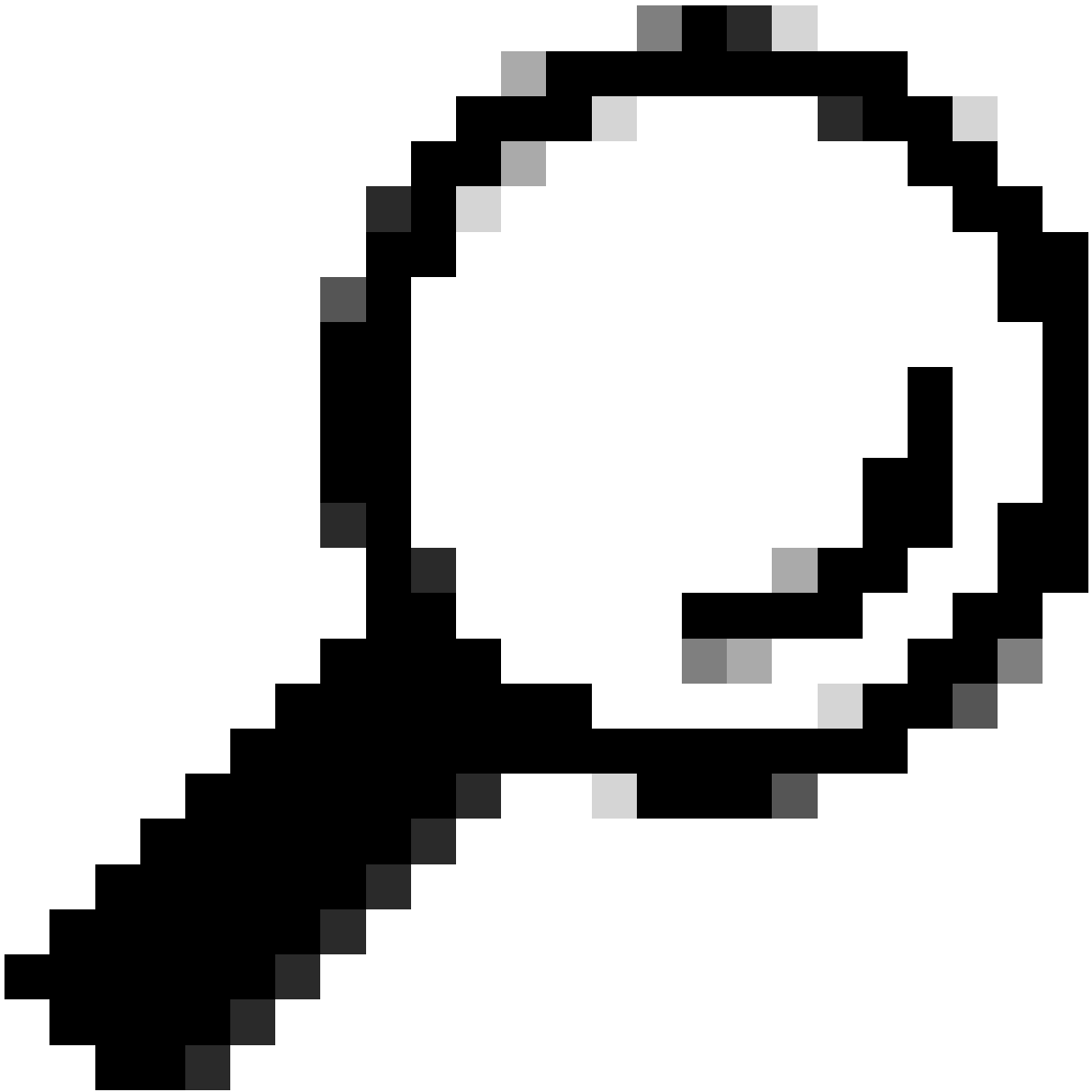
Issue Date:

Expiration Date:

Issued By:



قوبط نيوكت ؤيفي ك: ليلدلا اذه مادختس | كننكميف ، كي دل Catalyst لوجم ىلع SSH نيوكتب مق ت مل اذا :حيملت
[Catalyst لوجم ىلع \(SSH\) نامألا](#)



تانييغت عاشن | كنكمي ف SSH، ربع Catalyst لوحم | ل لوصولل Cisco ISE نكيكمت ي ف بغيرت نكت مل اذا :حيملت
ةوطخ ي ف حضورم) كلذ نم ال دب (CLI) رم اوألا رطس ةهجاو مادختساب Catalyst لوحم يلع SGT | ل لوكوتوربل ةتباث
(انه).

(ةيرايتخ) ةلوبقم اهنأ نم دكأتلل ةيضاارتفالا TrustSec تادادع | نم ققحت



General TrustSec Settings

TrustSec Matrix Settings

Work Process Settings

SXP Settings

ACI Settings

General TrustSec Settings

Verify TrustSec Deployment

Automatic verification after every deploy ⓘ

Time after deploy process minutes (10-60) ⓘ

Verify Now

Protected Access Credential (PAC)

*Tunnel PAC Time To Live

*Proactive PAC update when % PAC TTL is Left

Security Group Tag Numbering

System Will Assign SGT Numbers

Except Numbers In Range - From To

User Must Enter SGT Numbers Manually

Security Group Tag Numbering for APIC EPGs

System will assign numbers In Range - From

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Components > TrustSec Policy > Policy Sets > SXP > Troubleshoot > Reports > Settings

General TrustSec Settings

TrustSec Matrix Settings

Work Process Settings

SXP Settings

ACI Settings

Security Group Tag Numbering for APIC EPGs

System will assign numbers In Range - From

Automatic Security Group Creation

Auto Create Security Groups When Creating Authorization Rules *(i)*

SGT Number Range For Auto-Creation - From To

Automatic Naming Options

Select basis for names. (Security Group name will be shortened to 32 characters)

Name Will Include

Optional Additions

Policy Set Name *(i)*

Prefix

Suffix

Example Name - *RuleName*

IP SGT static mapping of hostnames

Create mappings for all IP addresses returned by DNS query

Create mappings only for the first IPv4 address and the first IPv6 address returned by DNS query

نېي كلساللا نېمدختسملل نېمأت ةومجم تامالع عاشنا

15 بېقرلا - BYOD ېراشتسمل نام ةومجم عاشنا

7 بېقرلا - لوقېرفال ې نېفظوملل نېمأت ةومجم عاشنا ب مق

Icon	Name	SGT (Dec / Hex)	Description	Learned from
	BYODconsultants	15/000F	SGT for consultants who use BYOD - restrict internal access	
	BYODEmployees	7/0007	SGT for employees who use BYOD - allow internal access	
	Contractors	5/0005	Contractor Security Group	
	Employees	4/0004	Employee Security Group	
	EmployeeServer	8/0008	Restricted Web Server - Only employees should be able to access	
	Guests	6/0006	Guest Security Group	
	Network_Services	3/0003	Network Services Security Group	
	Quarantined_Systems	255/00FF	Quarantine Security Group	
	RestrictedWebServer	8/0008		
	TrustSec_Devices	2/0002	TrustSec Devices Security Group	
	Unknown	0/0000	Unknown Security Group	

دي قمل بيولا مداخل SGT لى IP نم يكي تاتاس نكاس طي طخت عاشنا

MAC (MAB)، 802.1x، قداصم زواجت عم Cisco ISE لى قداصت ال كتك بش يف قداصت ال كتك بش وأ رخأ IP نيوانع يأل كلذب مق اذكو، تافيصوت.

IP SGT static mapping > 10.201.214.132

IP address(es) * 10.201.214.132

Add to a mapping group
 Map to SGT individually

SGT * EmployeeServer (8/0008) x ▼

Send to SXP Domain x default

Deploy to devices All TrustSec Devices ▼

Cancel Save

ةداهشلا قداصم فيرعت فلم عاشنا

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Certificate Authentication Profiles List > New Certificate Authentication Profile

Certificate Authentication Profile

* Name: BYODCertificateAuthProfile

Description: Allow 802.1x authentication to BYOD using username+password + EAP-TLS authentication to BYOD using certificate

Identity Store: Windows_AD_Server

Use Identity From: Certificate Attribute: Subject - Common Name
 Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store: Never
 Only to resolve identity ambiguity
 Always perform binary comparison

Submit Cancel

سبق نم ءءاهشلا ءقءاصم فيرءء فلمب ءيوه رءصم لسلسء ءاشن

Identity Source Sequences List > New Identity Source Sequence

Identity Source Sequence

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available

- Internal Endpoints
- Guest Users

Selected

- Windows_AD_Server
- Internal Users

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

پس انم بېقرو (نې راش تسم ل او نې فظوم ل) نې ځل لاس لال نې دم د خ تسم ل نې عې ت ب م ق

م س ا ل ا	Username	نې ن ا ل ع ا ل ا ة ع و م ج م ل ا	ج. س	بې ق ر
ثې م س ن و س ي ا ج	ثې م س ي ج	ن و ي ر ا ش ت س ا ل ا	ن و ي ر ا ش ت س ا	15
ثې م س ي ل ا س	ثې م س	ن و ف ظ و م ل ا	د و ي ا ب و ف ظ و م	7
ر ف و ت م ر ي غ	ر ف و ت م ر ي غ	ر ف و ت م ر ي غ	TrustSec_Devices	2

مق (WLC) ةيكلس الال ةيكلحم ال ةك بش ال ال يف مكحت ال رصنع و لوحم ال) ةلي عف ال ةزه ال ال ع بيقر ال ني عت ب مق

مق ةس ايس ديحت ل SGACLs ديحت ب مق

ي:لخاد وه ام ديقت عم نكلو، يجرخ ناكم ي ال لوصول اب نيراشت سملل حامس ال

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Components TrustSec Policy Policy Sets SXP Troubleshoot Reports Settings

Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec AAA Servers

Security Groups ACLs List > RestrictConsultant

Security Group ACLs

* Name: RestrictConsultant

Description: Deny Consultants from going to internal sites such as: https://10.201.214.132

IP Version: IPv4 IPv6 Agnostic

* Security Group ACL content:

```

permit icmp
deny tcp dst eq 80
deny tcp dst eq 443
permit ip

```

يخلق اد ناكم ي أو يجر اخ ناكم ي إلى لوصول اب ني فظوم لل حامس ل:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Components TrustSec Policy Policy Sets SXP Troubleshoot Reports Settings

Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec AAA Servers

Security Groups ACLs List > AllowEmployee

Security Group ACLs

* Name: AllowEmployee

Description: Allow Employees to ping and access sites in browser

IP Version: IPv4 IPv6 Agnostic

* Security Group ACL content:

```

permit icmp
permit tcp dst eq 80
permit tcp dst eq 443
permit ip

```

(يراي تخ) ة يساس أال تام دخل إلى لوصول اب يرخ أال ة زه أال ل حامس ل:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Components TrustSec Policy Policy Sets SXP Troubleshoot Reports Settings

Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec AAA Servers

Security Groups ACLs List > LoginServices
Security Group ACLs Generation ID: 1

* Name: LoginServices

Description: This is an ACL for Login services

IP Version: IPv4 IPv6 Agnostic

* Security Group ACL content:

```

permit udp dst eq 67
permit udp dst eq 53
permit tcp dst eq 53
permit tcp dst eq 88
permit udp dst eq 88
permit udp dst eq 123
permit tcp dst eq 135
permit udp dst eq 137
permit udp dst eq 389
permit tcp dst eq 389
permit udp dst eq 636
permit tcp dst eq 636
permit tcp dst eq 445
permit tcp dst eq 1025
permit tcp dst eq 1026

```

Save Reset

وأ DNS رورم ةكرح نيمضت ب مق ت ال (BYOD لخدم هيجوت ةداعال) Cisco ISE لى لى نينىئاها نلى نيمدخت سمل اعيمج هيجوت ةداعال
Cisco ISE لى لى لقتنت نأ نكم ي ال اهانأل WebAuth وأ ping وأ DHCP

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Components TrustSec Policy Policy Sets SXP Troubleshoot Reports Settings

Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec AAA Servers

Security Groups ACLs List > New Security Group ACLs
Security Group ACLs Generation ID: 0

* Name: ISE

Description: ACL to allow ISE services to occur

IP Version: IPv4 IPv6 Agnostic

* Security Group ACL content:

```

deny udp dst eq 67
deny udp dst eq 53
deny tcp dst eq 53
deny icmp
deny tcp dst eq 8443
permit ip

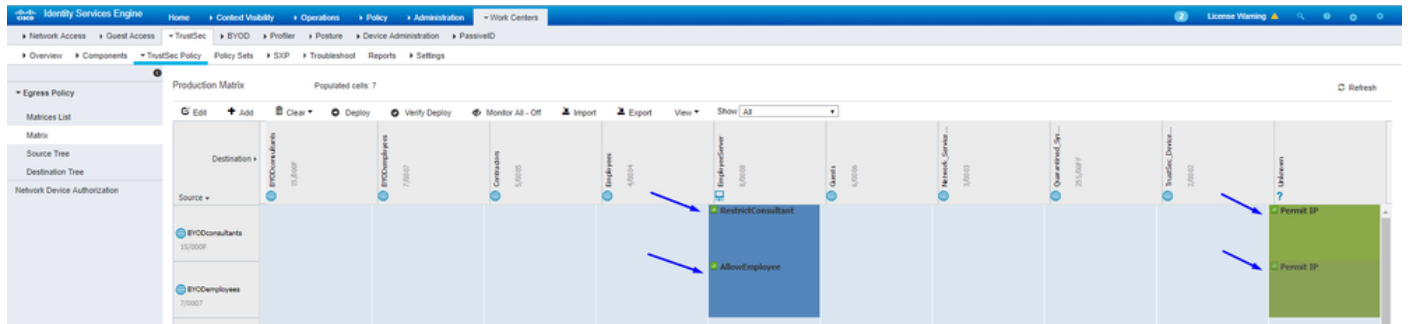
```

Submit Cancel

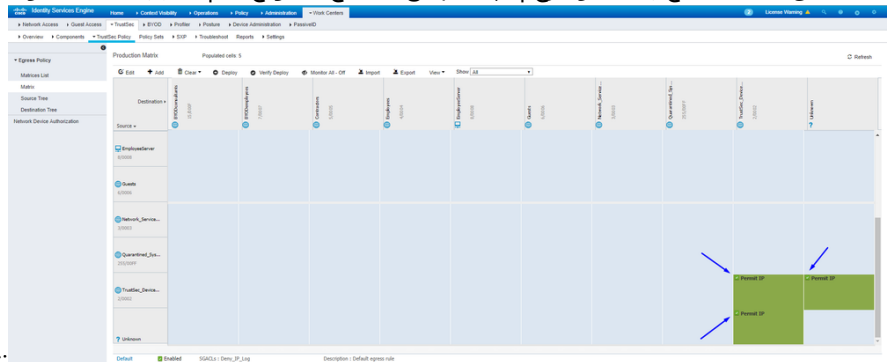
Cisco ISE يف TrustSec ةسايس ةفوفصم لىل ةصاخال (ACL) لوصولا يف مكحتال مئوقو صرف

لثم ، ةيلخادلل بيولا مداوخ ديقت نكلو ، يجرخ ناكم يأ لى لوصولاب نيراشت سملل حامسلا <https://10.201.214.132>

دقی لخدال د بی و مد او خب حامس لاولی ج راخ ناکم یی ا لوی ل و ل و ل اب نی فظ و ل ل حامس لاولی

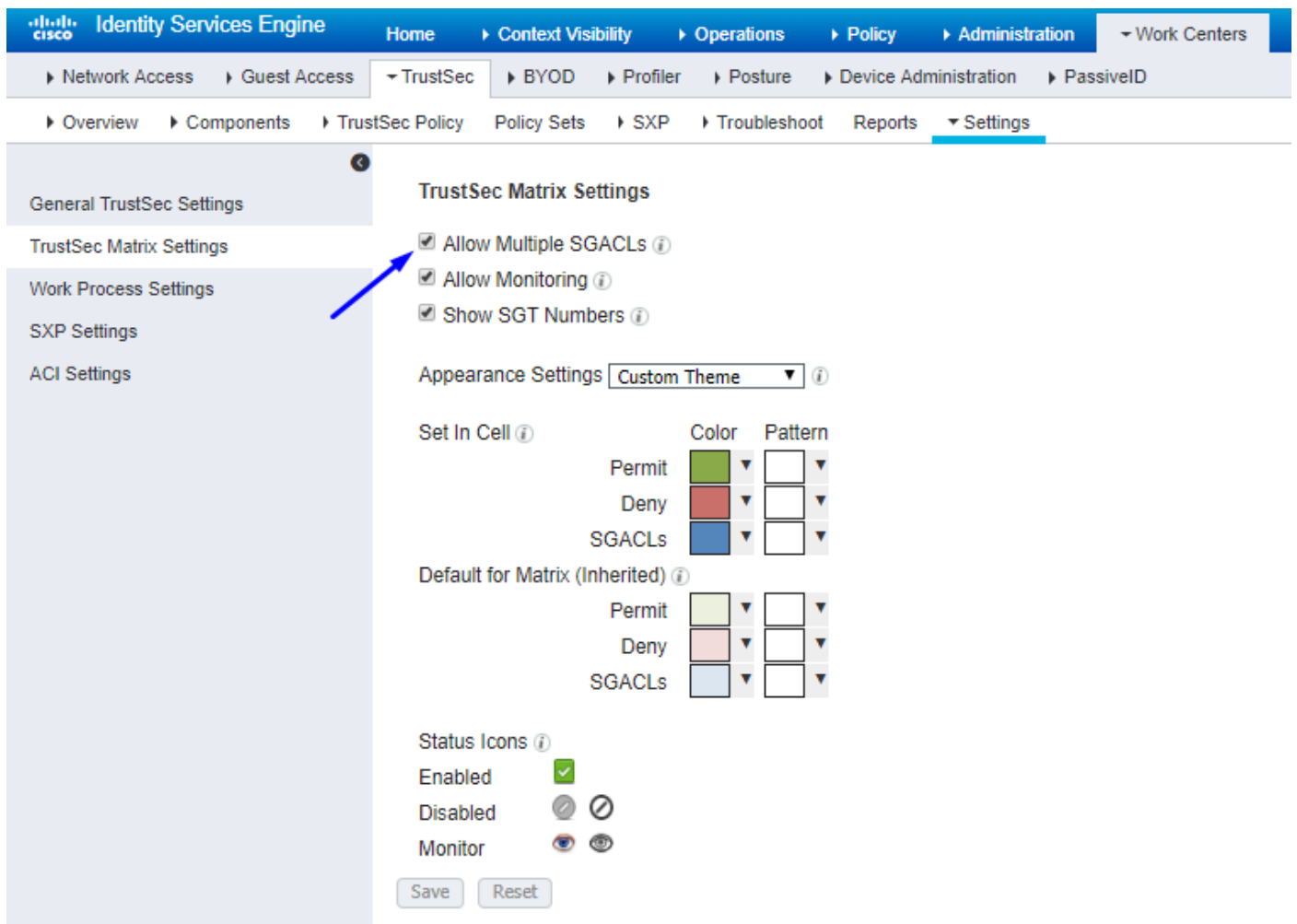


د ق ف ت ال ی ت ح (WLC و ل و ل م ل) ة ک ب ش ل ا ی ل ع ک ت ز ه ج ا م / ن ل ی (SSH و HTTPS و CAPWAP) ة ر ا د ا ل ت ا ن ا ی ب ر و ر م ة ک ر ح ب حامس لاولی



Cisco TrustSec: رشن درج م ب HTTPS و SSH ل و ل و

Allow Multiple SGACLs: م ن Cisco ISE نی کم ت



كلذب مايقول كليلع بچي .كتزهجأ لى لفسأل كب صاخلا نيوكتلا عفدل ، Cisco ISE نم ىنم يلا ايلعلا ةيوازلا ي Push رقنا
اضيا اقحال ىرخأ ةرم :

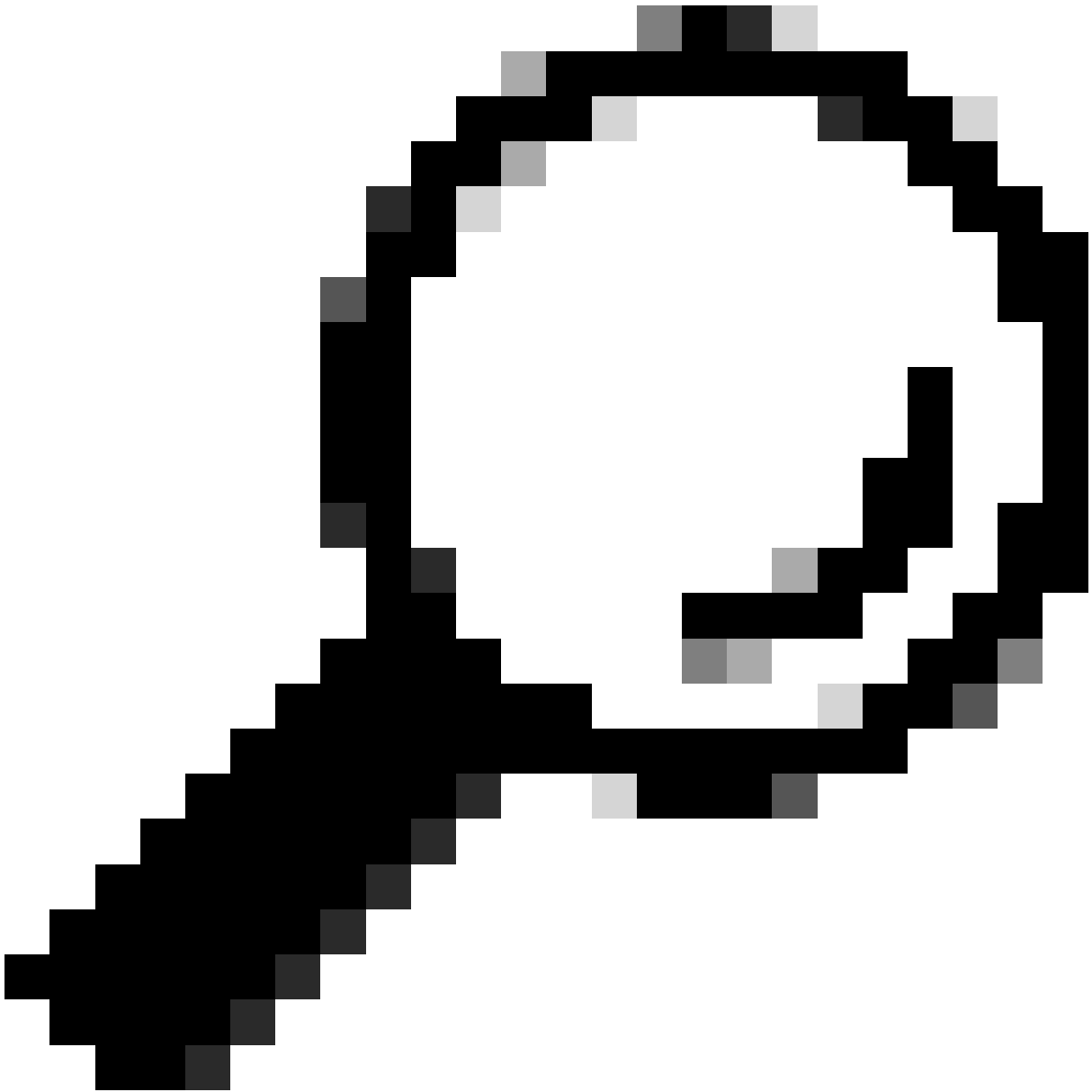
1

There are TrustSec configuration changes that has not been notified to network devices. To notify the relevant network devices about these changes click the push button.

Push

Catalyst لوحم ىلع TrustSec نيوكت

Catalyst لوحم ىلع AAA ل Cisco TrustSec مادختسال لوحملا نيوكت



Cisco ISE ةطساوب BYOD يف لعفلاب نوحجان كيدل نيكيكلساللا نيمدختسملا نأ دنسملما اذه ضررت في: حيملت
انه ره اظلال نيوكتلا لبق

(ISE مع BYOD Wireless ةدحو لمعت يكل) اذه لبق اقبسم دوسألاب ةحضمولما رماوألما نيوكت مت

<#root>

```
CatalystSwitch(config)#aaa new-model
```

```
CatalystSwitch(config)#aaa server radius policy-device
```

```
CatalystSwitch(config)#ip device tracking
```

```
CatalystSwitch(config)#radius server CISCOISE
```

```
CatalystSwitch(config-radius-server)#address ipv4 10.201.214.230 auth-port 1812 acct-port 1813
```

```
CatalystSwitch(config)#aaa group server radius AAASERVER
```

```
CatalystSwitch(config-sg-radius)#server name CISCOISE
```

```
CatalystSwitch(config)#aaa authentication dot1x default group radius
```

```
CatalystSwitch(config)#cts authorization list SGLIST
```

```
CatalystSwitch(config)#aaa authorization network SGLIST group radius
```

```
CatalystSwitch(config)#aaa authorization network default group AAASERVER
```

```
CatalystSwitch(config)#aaa authorization auth-proxy default group AAASERVER
```

```
CatalystSwitch(config)#aaa accounting dot1x default start-stop group AAASERVER
```

```
CatalystSwitch(config)#aaa server radius policy-device
```

```
CatalystSwitch(config)#aaa server radius dynamic-author
```

```
CatalystSwitch(config-locsvr-da-radius)#client 10.201.214.230 server-key Admin123
```

يف هتددح يذلا كرتشم ل RADIUS رس هسفن وه يمحمل لوصول تاغوسم حاتفم نوكي نأ بجي: **نظالم**
م.س.ق.ل **RADIUS Authentication Settings** > **Add Device** > **Network Devices** > **Administration**

<#root>

CatalystSwitch(config)#radius-server attribute 6 on-for-login-auth

CatalystSwitch(config)#radius-server attribute 6 support-multiple

```
CatalystSwitch(config)#radius-server attribute 8 include-in-access-req
```

```
CatalystSwitch(config)#radius-server attribute 25 access-request include
```

```
CatalystSwitch(config)#radius-server vsa send authentication
```

```
CatalystSwitch(config)#radius-server vsa send accounting
```

```
CatalystSwitch(config)#dot1x system-auth-control
```

Cisco ISE يلع لوجم لة قداصلم ل RADIUS م داخ نمض PAC حات فم نيوكت

```
CatalystSwitch(config)#radius server CISCOISE
```

```
CatalystSwitch(config-radius-server)#address ipv4 10.201.214.230 auth-port 1812 acct-port 1813
```

```
CatalystSwitch(config-radius-server)#pac key Admin123
```

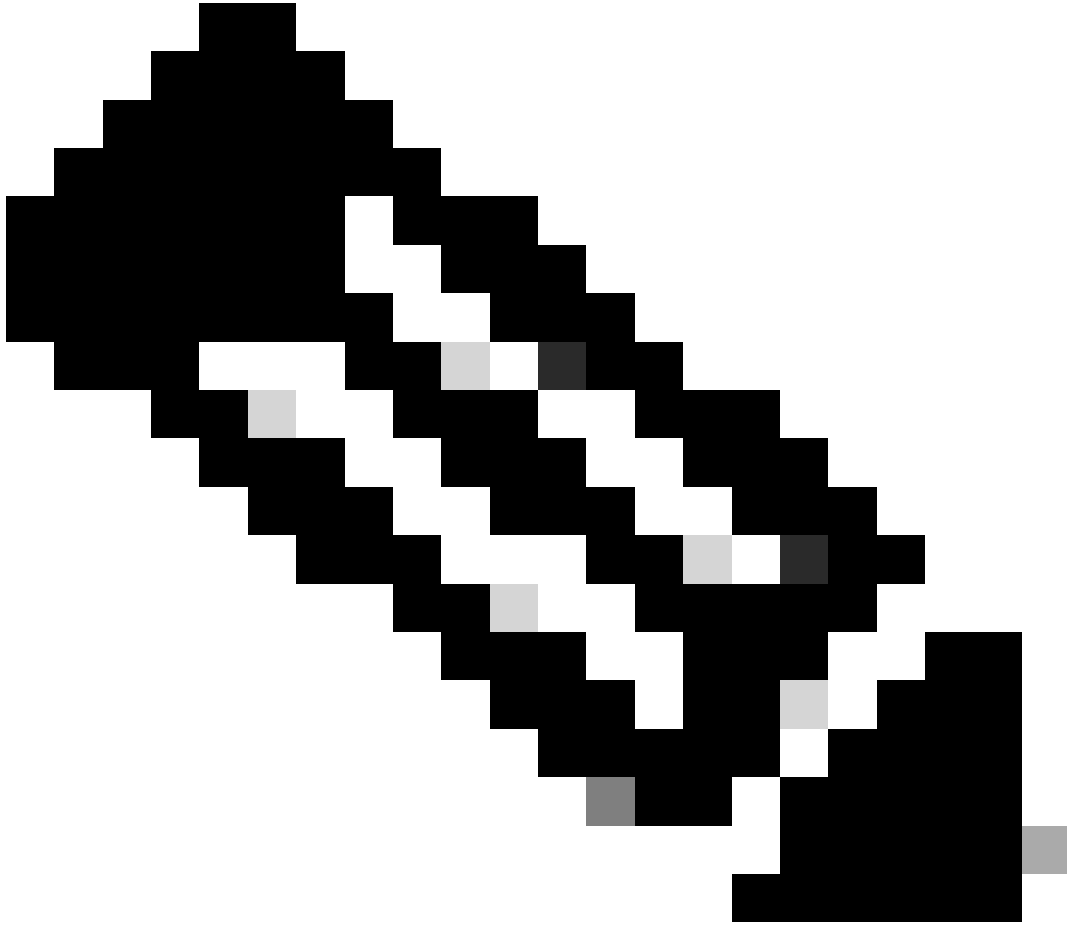
RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret

Use Second Shared Secret ⓘ



تحت هتددح يذلا كرتشم ال RADIUS رس هسفن وه يمحمل لوصول تاغوسم حاتفم نوكي نأ بجي: **نظحالم**
حضورم وه امك) Cisco ISE في مسقلا **RADIUS Authentication Settings** **Administration > Network Devices > Add Device**
(ةشاشلا طاقتلا في).

Cisco ISE لىل لوجملا ةقداصم ل CTS دامتعا تانايب نيوكت

CatalystSwitch#cts credentials id CatalystSwitch password Admin123

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Ce

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Mana

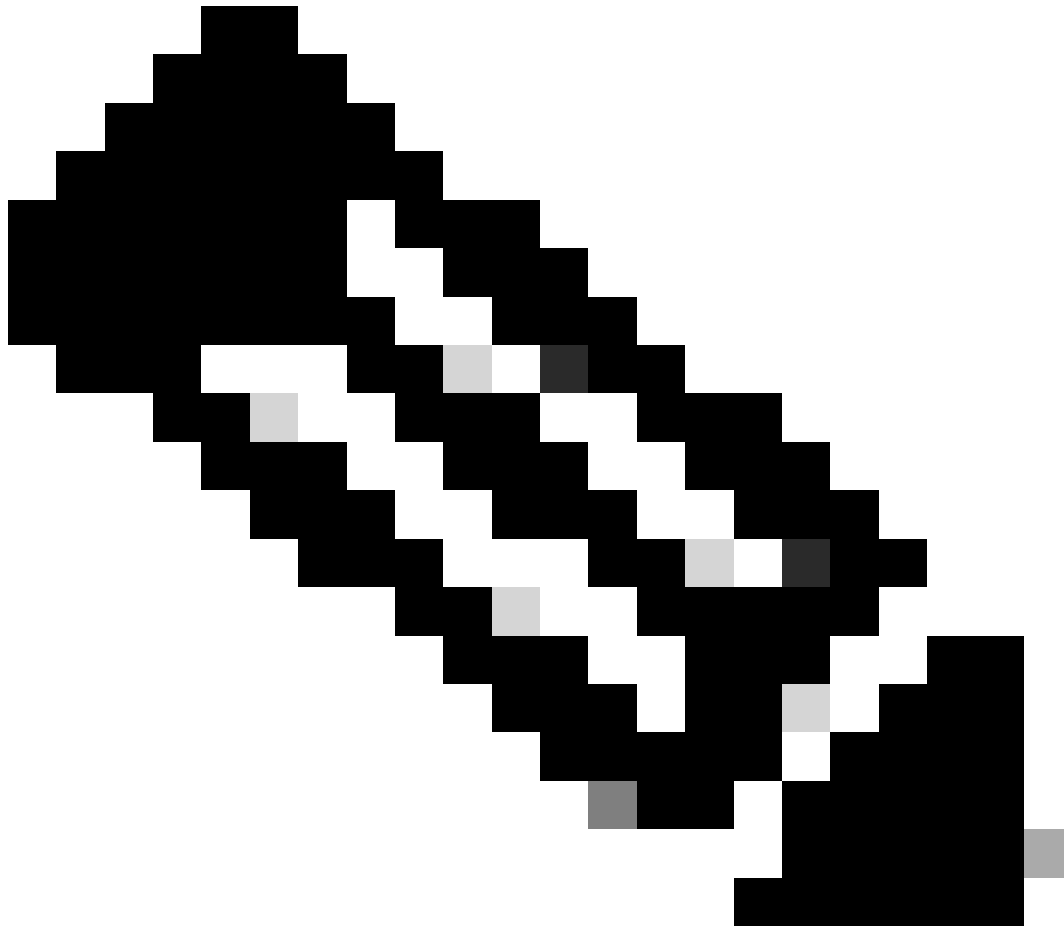
Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device Id CatalystSwitch

* Password Admin123 Hide



CTS دامتعا تانايب يف اهتدح يتال رورملا ةملك + زاهجال فرعم اهسفن يه CTS دامتعا تانايب نوكت نا بجي: ةظحالم
Administration > Network Devices > Add Device > CTS دامتعا تانايب نوكت نا بجي

Advanced TrustSec Settings في مسقلا Cisco ISE (رهظي).

ىرخأ قرم Cisco ISE لىل لصي ىتح كب صاخلا لمحملا لوصولا غوسم شيدحتب مق ،كلذ دعب

```
CatalystSwitch(config)#radius server CISCOISE
CatalystSwitch(config-radius-server)#exit
Request successfully sent to PAC Provisioning driver.
```

Catalyst لوجم لىل عماع لكشب CTS نيكمتم

```
CatalystSwitch(config)#cts role-based enforcement
CatalystSwitch(config)#cts role-based enforcement vlan-list 1115 (choose the vlan that your end user devices are on only)
```

(يرايخ) ةروطحملا بيولا مداوخل SGT لىل IP نم تباث نييتمت

ISE Web و Switch CLI مادختساب ايودي هزييمت كىل عمجى كلذل ،ادبأ ةقداصم لىل ISE لالخم نم دىقملا بيولا مداختي تايال
Cisco في بيولا مداوخم نم دىدعل نم دحاو درجم دعي يذلاو ، GUI.

```
CatalystSwitch(config)#cts role-based sgt-map 10.201.214.132 sgt 8
```

Catalyst لوجم لىل عم TrustSec نم ققحتلا

```
CatalystSwitch#show cts pac
AID: EF2E1222E67EB4630A8B22D1FF0216C1
PAC-Info:
PAC-type = Cisco Trustsec
AID: EF2E1222E67EB4630A8B22D1FF0216C1
I-ID: CatalystSwitch
A-ID-Info: Identity Services Engine
Credential Lifetime: 23:43:14 UTC Nov 24 2018
PAC-Opaque: 000200B80003000100040010EF2E1222E67EB4630A8B22D1FF0216C10006009C0003010025D40D409A0DDAF352A3F1A9884AC3F0
Refresh timer is set for 12w5d
```

CatalystSwitch#cts refresh environment-data
Environment data download in progress

CatalystSwitch#show cts environment-data
CTS Environment Data

```
=====
Current state = COMPLETE
Last status = Successful
Local Device SGT:
SGT tag = 2-02:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
*Server: 10.201.214.230, port 1812, A-ID EF2E1222E67EB4630A8B22D1FF0216C1
Status = ALIVE flag(0x11)
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
0001-31 :
0-00:Unknown
2-00:TrustSec_Devices
3-00:Network_Services
4-00:Employees
5-00:Contractors
6-00:Guests
7-00:BYODemployees
8-00:EmployeeServer
15-00:BYODconsultants
255-00:Quarantined_Systems
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 16:04:29 UTC Sat Aug 25 2018
Env-data expires in 0:23:57:01 (dd:hr:mm:sec)
Env-data refreshes in 0:23:57:01 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

CatalystSwitch#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address SGT Source

```
=====
10.201.214.132 8 CLI
10.201.235.102 2 INTERNAL
```

IP-SGT Active Bindings Summary

```
=====
Total number of CLI bindings = 1
Total number of INTERNAL bindings = 1
Total number of active bindings = 2
```

WLC TrustSec نيوكت

Cisco ISE في RADIUS زاهج (WLC) ةيكلس الال ةيكلس الال ةكبش الال في مكحت الال رصنع ةفاضل نم ققحت الال او نيوكت الال

The screenshot displays the Cisco ISE Administration console for configuring a Network Device. The breadcrumb navigation shows: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Network Devices.

The main configuration area is titled "Network Devices" and shows a list of devices with "CiscoWLC" selected. The configuration fields are as follows:

- * Name: CiscoWLC
- Description: Cisco 3504 WLC
- IP Address: 10.201.235.123 / 32
- * Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- * Network Device Group:
 - Location: All Locations (Set To Default)
 - IPSEC: No (Set To Default)
 - Device Type: All Device Types (Set To Default)
- RADIUS Authentication Settings
 - RADIUS UDP Settings:
 - Protocol: RADIUS
 - * Shared Secret: cisco (Hide)
 - Use Second Shared Secret: (i)
 - CoA Port: 1700 (Set To Default)
 - RADIUS DTLS Settings (i):
 - DTLS Required: (i)
 - Shared Secret: radius/dtls (i)
 - CoA Port: 2083 (Set To Default)
 - Issuer CA of ISE Certificates for CoA: Select if required (optional) (i)
 - DNS Name: (empty)

Cisco ISE في TrustSec زاهج هنم ققحت الال او (WLC) ةيكلس الال ةيكلس الال ةكبش الال في مكحت الال رصنع نيوكت ةفاضل مت

ةيكلس الال ةيكلس الال ةكبش الال في مكحت الال رصنع الال ةتباث الال بيقر الال الال IP تان يي رشن نم Cisco ISE ةوطخل هذه نمكمت > لمعل زكارم في Cisco ISE Web GUI ب ةصاخ الال (GUI) ةيكلس الال ةهجاو في تان يي رشن نم هذه ةاشناب تمق دقل (WLC). > TrustSec > تانوكم الال > تان يي رشن نم IP تان يي رشن نم IP بيقر الال ةتباث الال IP تان يي رشن نم >

Network Devices

- Default Device
- Device Security Settings

Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device Id

* Password

TrustSec Notifications and Updates

* Download environment data every

* Download peer authorization policy every

* Reauthentication every ⓘ

* Download SGACL lists every

Other TrustSec devices to trust this device

Send configuration changes to device Using CoA CLI (SSH)

Send from

Ssh Key

Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates

Device Interface Credentials

* EXEC Mode Username

* EXEC Mode Password

Enable Mode Password

Out Of Band (OOB) TrustSec PAC

Issue Date

Expiration Date

Issued By




بېو مدختسمه ج او Security > TrustSec > General ي ف، ة ق ح ال Password ة و ط خ ي ف و Device Id اذه مدختسنن نحن: ة ظ ح الم WLC.

WLC نم (PAC) ي م ح م ل ل و و ل ا ت ا غ و س م ر ي ف و ت ن ي ك م ت

Security

- ▼ AAA
 - General
 - ▼ RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - ▶ TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - ▼ Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- ▶ Local EAP
- Advanced EAP
- ▶ Priority Order
- ▶ Certificate
- ▶ Access Control Lists
- ▶ Wireless Protection Policies
- ▶ Web Auth
- ▶ TrustSec
 - Local Policies
- ▶ OpenDNS
- ▶ Advanced

RADIUS Authentication Servers > Edit

Server Index	2
Server Address(Ipv4/Ipv6)	10.201.214.230
Shared Secret Format	ASCII ▼
Shared Secret	***
Confirm Shared Secret	***
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Apply Cisco ISE Default settings	<input type="checkbox"/>
Port Number	1812
Server Status	Enabled ▼
Support for CoA	Enabled ▼
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
Realm List	
PAC Provisioning	<input checked="" type="checkbox"/> Enable 
IPSec	<input type="checkbox"/> Enable

WLC یل TrustSec نیكمت

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec**
- General
 - SXP Config
 - Policy
- Local Policies
- OpenDNS
- Advanced

General

Clear DeviceID Refresh Env Data Apply

CTS Enable

Device Id

Password

Inline Tagging

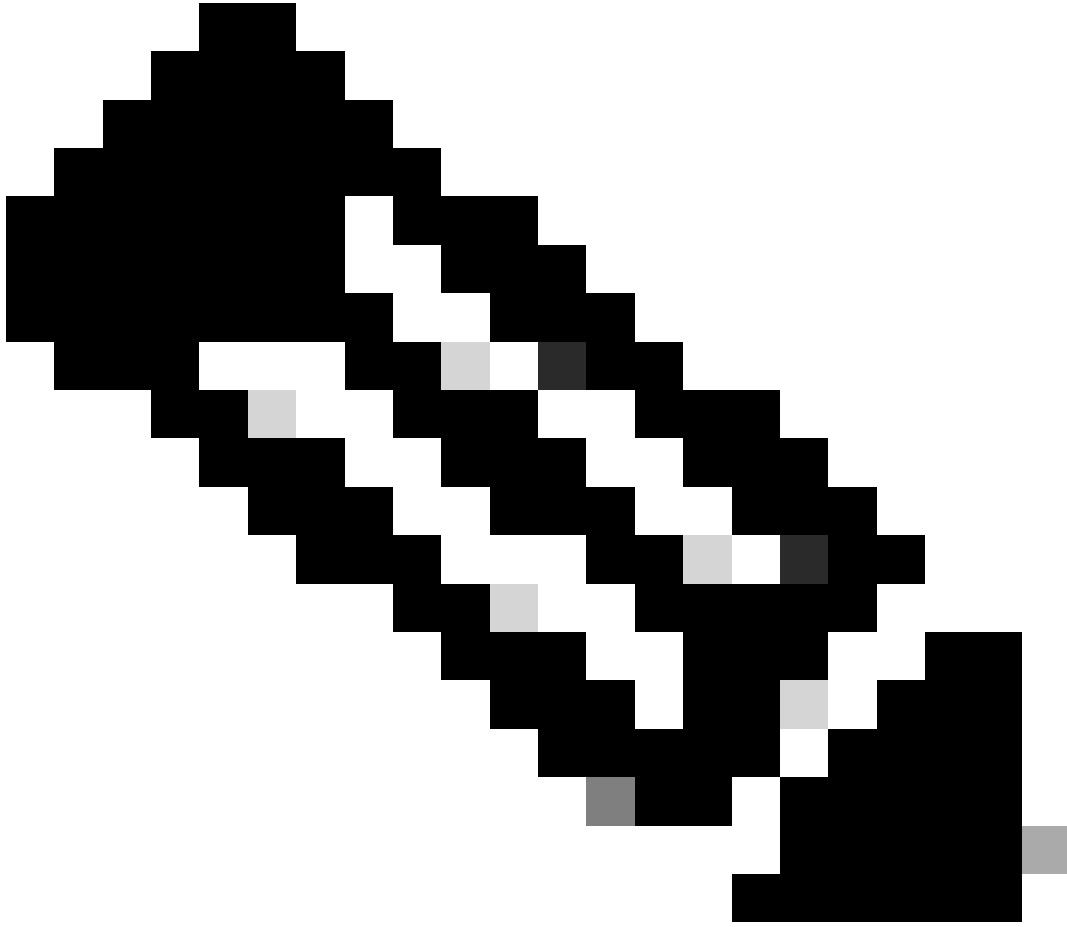
Environment Data

Current State START

Last Status WAITING_RESPONSE

1. Clear DeviceID will clear Device ID and password
2. Apply button will configure Device ID and other parameters





Administration > Network Devices > Add Device > Advanced TrustSec Settings في مسؤل Cisco ISE.
نوكت نأ Password بجي و CTS Device Id: **نظالم**

(WLC) ةكلساللة لىلحملة كبلشلا في مكحتلا رصنع ىلع (PAC) يحملة لوصول تاغوسم ريفوت نم ققحتلا

دعب حاجنب (PAC) يحملة لوصول تاغوسم ريفوت مت (WLC) ةكلساللة لىلحملة كبلشلا في مكحتلا رصنع نأ ىرت
(ةوطخلا هذه في اذهب موقت) Refresh Env Data رقرنلا

CISCO | MONITOR | WLANs | CONTROLLER | WIRELESS | **SECURITY** | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
 - Advanced EAP
 - Priority Order
 - Certificate
 - Access Control Lists
 - Wireless Protection Policies
 - Web Auth
 - TrustSec
 - General
 - SXP Config
 - Policy
 - Local Policies
 - OpenDNS
 - Advanced

RADIUS Authentication Servers > Edit

Server Index: 2
 Server Address(Ipv4/Ipv6): 10.201.214.230
 Shared Secret Format: ASCII
 Shared Secret: ***
 Confirm Shared Secret: ***

Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
 Apply Cisco ISE Default settings:
 Port Number: 1812
 Server Status: Enabled
 Support for CoA: Enabled
 Server Timeout: 5 seconds
 Network User: Enable
 Management: Enable
 Management Retransmit Timeout: 5 seconds
 Tunnel Proxy: Enable
[Realm List](#)
 PAC Provisioning: Enable

PAC Params

PAC A-ID Length	16	<input type="button" value="Clear PAC"/>
PAC A-ID	ef2e1222e67eb4630a8b22d1ff0216c1	
PAC Lifetime	Wed Nov 21 00:01:07 2018	

IPSec: Enable

WLC لى Cisco ISE ن م CTS ة ئي ب تان اي ب لي زنت

ءاب قرلا لي زنت ب (WLC) ة ك لس لال ة لى ل م ة ك ب ش ل ي ف م ك ح ت ل ة ح و م و ق ت ، Refresh Env Data ر ق ن ل د ع ب

Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | **SECURITY** | MANAGEMENT | COMMANDS | HELP | FEEDBACK | Home

Security

- ▼ AAA
 - General
 - ▼ RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - ▶ TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - ▼ Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
 - ▶ Local EAP
 - Advanced EAP
 - ▶ Priority Order
 - ▶ Certificate
 - ▶ Access Control Lists
 - Wireless Protection Policies
 - ▶ Web Auth
 - ▼ TrustSec
 - General
 - SXP Config
 - Policy
 - Local Policies
 - ▶ OpenDNS
 - ▶ Advanced

General

Clear DeviceID | Refresh Env Data | Apply

CTS Enable

Device Id

Password

Inline Tagging

Environment Data

Current State **COMPLETE**

Last Status **START**

Environment Data Lifetime (seconds) 86400

Last update time (seconds) Mon Aug 27 02:00:06 2018

Environment Data expiry 0:23:59:58 (dd:hr:mm:sec)

Environment Data refresh 0:23:59:58 (dd:hr:mm:sec)

Security Group Name Table

0: Unknown
2: TrustSec_Devices
3: Network_Services
4: Employees
5: Contractors
6: Guests
7: BYODEmployees
8: EmployeeServer
15: BYODconsultants
255: Quarantined_Systems

1. Clear DeviceID will clear Device ID and password
 2. Apply button will configure Device ID and other parameters

رورم الة كرح ىل ع اهذيفنن و SGACL تاليزنن نيكم ت

MONITOR | WLANs | CONTROLLER | WIRELESS | **SECURITY** | MANAGEMENT

Wireless

- ▼ Access Points
 - All APs
 - Direct APs
 - ▼ Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- ▶ Advanced
- Mesh
- ▶ ATF
- RF Profiles
- FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN
 - Templates

All APs > APb838.61ac.3598 > Trustsec Configuration

AP Name	APb838.61ac.3598
Base Radio MAC	b8:38:61:b8:c6:70

TrustSec Configuration

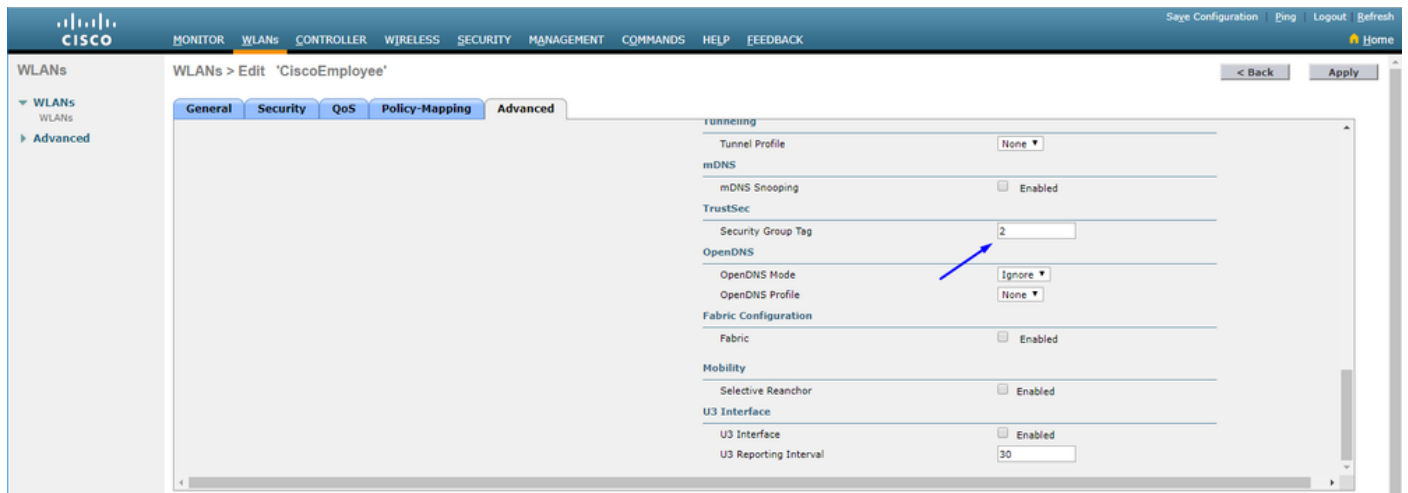
CTS Override

Sgacl Enforcement

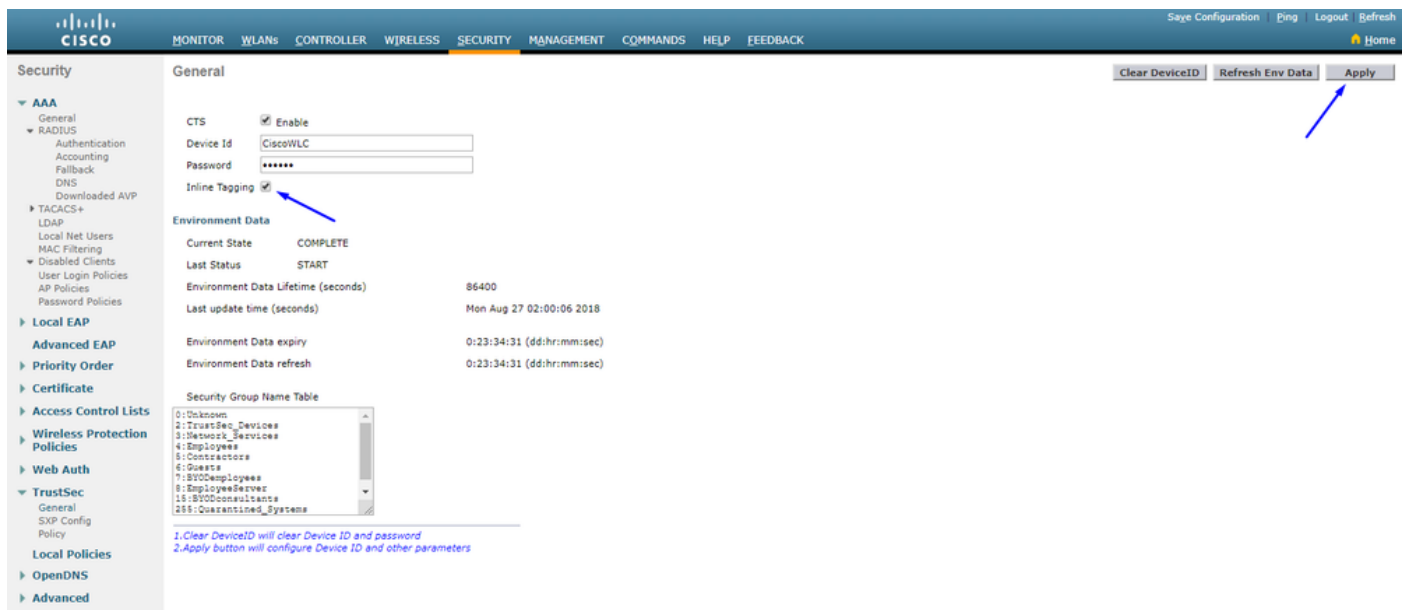
1. Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)
 2. SXPv4(Listener/Speaker/Both) is supported in Flex, Flex+bridge AP (Applicable to 11ac AP)

مق (TrustSec_Devices) 2 بيقرل عم لوصولو اطقنو (WLC) ةيكلسالل ةيكلحال ةكشلال يف مكحتال رصنع صيصختب مق

رورملا ةكرحب حامسلل (TrustSec_Devices) 2 نم ابقر (WLC+WLAN) ةيكلسالل ةيكلحال ةكشلال يف مكحتال رصنع حنملا
لوحملال لالخنم لوصولو اطقن + (WLC) ةيكلسالل ةيكلحال ةكشلال يف مكحتال رصنع نم/الى (CAPWAP و HTTPS و SSH).



WLC لىل رطسال لخالء اءم ال ءضو نىكمت



TrustSec Config ءءو لفسأل قالزنا Wireless > Access Points > Global Configuration ءءء

Wireless

- ▼ Access Points
 - All APs
 - Direct APs
 - ▼ Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- ▶ Advanced
- Mesh
- ▶ ATF
- RF Profiles
- FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN Templates
- OEAP ACLs
- Network Lists
- ▶ 802.11a/n/ac
- ▶ 802.11b/g/n
- ▶ Media Stream
- ▶ Application Visibility And Control
- Lync Server
- Country
- Timers
- ▶ Netflow
- ▶ QoS

All APs TrustSec Configuration

TrustSec

Sgac Enforcement	<input checked="" type="checkbox"/>
Inline Tagging	<input checked="" type="checkbox"/>
AP SXP State	Disabled ▼
Default Password
SXP Listener Min Hold Time (seconds)	<input type="text" value="90"/>
SXP Listener Max Hold Time (seconds)	<input type="text" value="180"/>
SXP Speaker Hold Time (seconds)	<input type="text" value="120"/>
Reconciliation Time Period (seconds)	<input type="text" value="120"/>
Retry Period (seconds)	<input type="text" value="120"/>

Peer Config

Peer IP Address	<input type="text"/>
Password	Default ▼
Local Mode	Speaker ▼
	<input type="button" value="ADD"/>

Peer IP Address Password SXP Mode

1. Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)
 2. SXPv4(Listener/Speaker/Both) is supported in Flex, Flex+bridge AP (Applicable to 11ac AP)

Catalyst لوجم ىلع رطسلا لخاد تامالعل ا عضو نيكت

<#root>

CatalystSwitch(config)#interface TenGigabitEthernet1/0/48

CatalystSwitch(config-if)#description goestoWLC

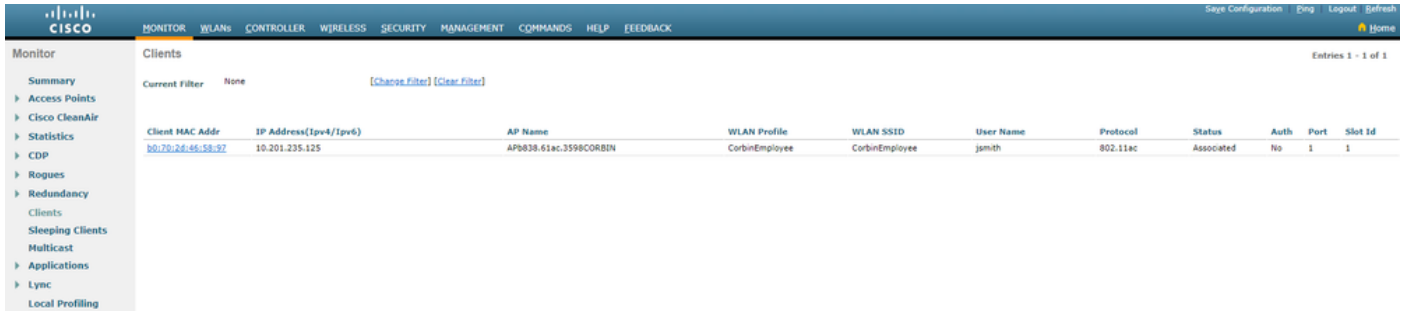
CatalystSwitch(config-if)#switchport trunk native vlan 15

CatalystSwitch(config-if)#switchport trunk allowed vlan 15,455,463,1115

CatalystSwitch(config-if)#switchport mode trunk

```
CatalystSwitch(config-if)#cts role-based enforcement
CatalystSwitch(config-if)#cts manual
CatalystSwitch(config-if-cts-manual)#policy static sgt 2 trusted
```

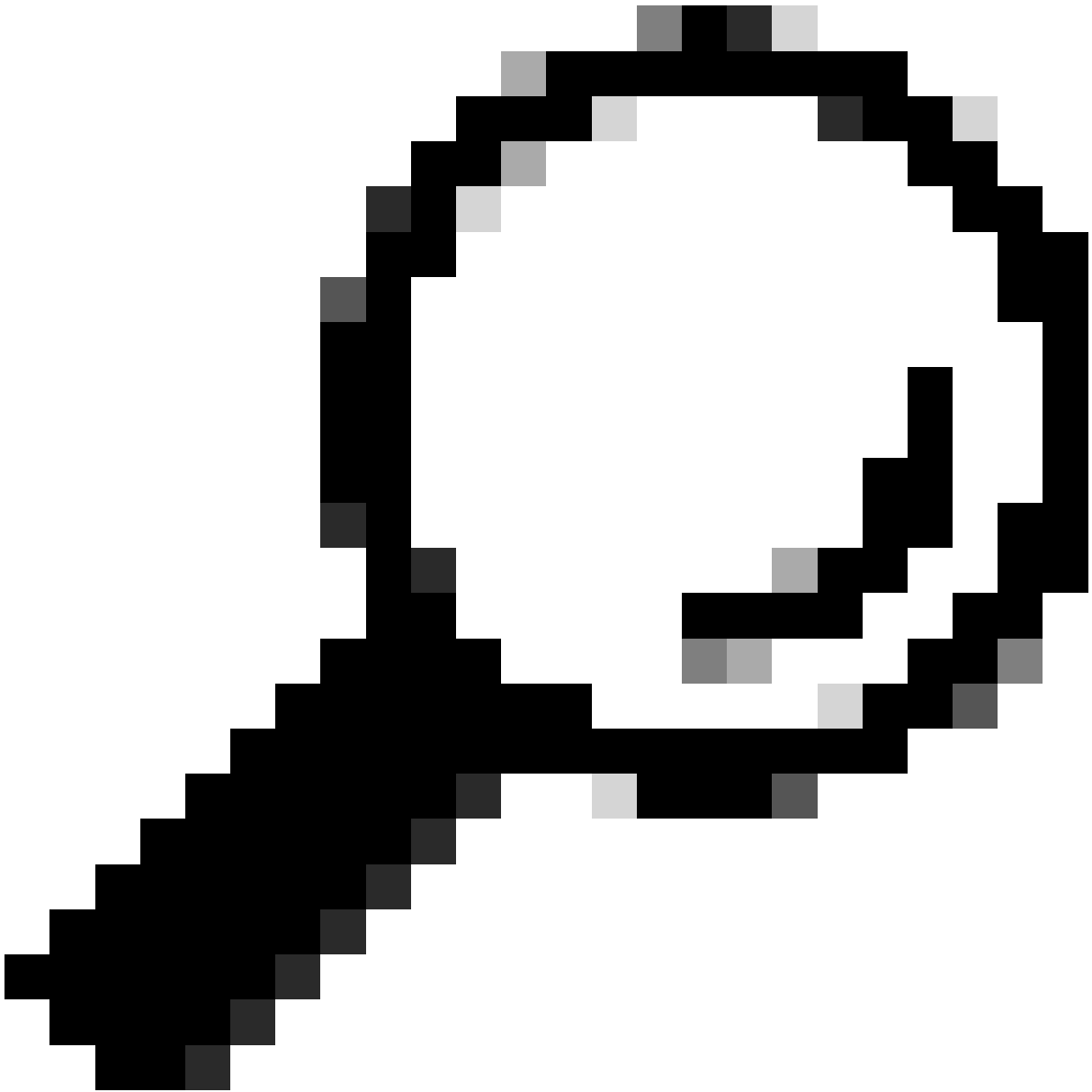
ةحصلا نم ققحتلا



The screenshot shows the Cisco Catalyst Switch Monitor interface. The 'Clients' section is active, displaying a table with the following columns: Client MAC Addr, IP Address(Ipv4/Ipv6), AP Name, WLAN Profile, WLAN SSID, User Name, Protocol, Status, Auth, Port, and Slot Id. A single client entry is visible with MAC address b0:70:26:46:58:97, IP address 10.201.235.125, AP Name AP0838.61ac.3598CORBIN, WLAN Profile CorbinEmployee, WLAN SSID CorbinEmployee, User Name jsmith, Protocol 802.11ac, Status Associated, Auth No, Port 1, and Slot Id 1.

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id
b0:70:26:46:58:97	10.201.235.125	AP0838.61ac.3598CORBIN	CorbinEmployee	CorbinEmployee	jsmith	802.11ac	Associated	No	1	1

Catalyst Switch#show | inc sgacl
تاراطا 10: (454) جورخلا دنع (SGACL) تنرتنلا لوكوتورب نم عبارلا رادصالاب ةصاخلا لوصولا يف مكحتلا ةمئاق طاقسا
تاراطا 0: جرخم (455) IPv6 لوصولا يف مكحتلا ةمئاق طاقسا
تاراطا 0: جرخم نم (456) IPv4 SGACL ةيلخ طاقسا
تاراطا 0: جرخم (457) IPv6 sgacl ةيلخ طاقسا

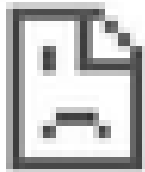


يف دعاسي نأ انه جردملا دننسم ل نكميف ،كلذ نم الادب Cisco ASA و Nexus و Cisco ASR مدختست تنك اذا :حيملت [TrustSec احوال ص او عا ط خ أ ل ف ا ش ك ت س أ ل ي ل د](#) :كب صاخال بيقرلا تامالع صرف نم ققحتلا

يف مكحتلا عمئاق هجاوت - jsmith password admin123 مدختسملا مسا مادختساب ةيكلساللا ةكبشلا ىلع ةقداصملا ب مق لوجملا يف صفرلل (ACL) لوصول



https://10.201.214.132



This site can't be reached

10.201.214.132 took too long to respond.

Try:

Checking the connection

ERR_CONNECTION_TIMED_OUT

RELOAD

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامچرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل