

ضيوفت مادختس اب رماوا AAA

تاي وتحملا

OEM ملما

[ئي ساس ألا تاب لطتملا](#)

[تاب لطتملا](#)

[OEM دختس ملما تانوكملما](#)

[ئي ساس ألا تامولعم](#)

[دادع ا لاثم TACACs](#)

[نيو كتل لاثم HTTPS](#)

[OEM CM ىلع ئي ساس اب رماوا لىغشت متى ربع WAAS Express/APPNAV-XE HTTP](#)

[نيو كتل ا عضو للا \(CLI\) لوصولا يف مكح تلا مئا وق](#)

[عضو للا \(CLIs\) لوصولا يف مكح تلا مئا وق EXEC](#)

[ئلا جلا - Waasx](#)

[نيو كتل - WAASX](#)

[تاي ا صحالا - WAASX](#)

[لىج س تلا](#)

[AppNav-XE](#)

[احالص او عاطخ ألا فاش كتسا](#)

[OEM ل يزك رملاريدملاب ئاصاخلا \(CLI\) رماوا لارطس ئه جا ىلع WAAS](#)

[ضرعتس ملما نم HTTPS لوصولا رابتخا](#)

[هجوم ىلع عاطخ ألا حيحصت WAAS Express](#)

OEM ملما

عس اولا قي ب طتلا نيو كت لي صافت دنت سملما اذه OEM Express/APPNAV-XE ئيف رطلاب ئاطحملما ىلا لوصولا مكح ت ئدحو للا لوصولا يف مكح تلا OEM ماظن ا مادختس اب (TACACS). OEM داص ملما او ضيوفت ل او (AAA).

ئي ساس ألا تاب لطتملا

تاب لطتملا

ئيلاتلا عي ض او ملاب ئفرعم كيدل نوكت نأب Cisco يصوت:

- Cisco WAAS
- AAA ضيوفت
- Tacacs

OEM دختس ملما تانوكملما

ئيلاتلا OEM تانوكمل او جماربلا تارادصا ىلا دنت سملما اذه يف ئيرادصا ىلا دنت سملما تامولعملا دنت سملما

- WAAS 6.1.1x
- تاهجوملا 2900
- IOS نم 15.2(4)M3 رادصإا

ةصالخ ةيملعم ةئيب يف ةدوچوملا ةزهجلأا نم دنتسملا اذه يف ةدراولأا تامولعملاءاشنإ مت تناك اذا . (يضاارتفا) حوسن مم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجلأا عيمج تأدب رمأ يأ لموتحملاري ثأتلل كمهف نم دكأتف ،ةرشابم كتكبش.

ةيساسأ تامولعم

تاهجوم ىلإ لوصولل نمآلا HTTPS و Secure Shell (SSH) و WAAS دوجو ل ةيذكرملا ةرادالا بـ لـ طـ تـ تـ WAAS Express APPNAV - XE.

يـ لـ وـ لـ اـ لـ يـ جـ سـ تـ لـ /ـ نـ يـ وـ كـ تـ لـ لـ (Secure Shell (SSH) مـ اـ دـ خـ تـ سـ اـ مـ تـ يـ .

نـ يـ رـ مـ تـ سـ مـ لـ اـ ةـ بـ قـ اـ رـ مـ لـ اوـ نـ يـ وـ كـ تـ لـ لـ HTTPS مـ اـ دـ خـ تـ سـ اـ مـ تـ يـ .

ةـ زـ هـ جـ جـ لـ اـ هـ ذـ هـ بـ لـ اـ صـ تـ الـ اـ نـ مـ يـ زـ كـ رـ مـ لـ اـ رـ يـ دـ مـ لـ اـ زـ اـ هـ جـ لـ اـ ئـ لـ عـ AAA وـ HTTPS نـ يـ وـ كـ تـ جـ مـ دـ عـ نـ مـ يـ اـ مـ اـ بـ لـ اـ حـ يـ حـ صـ لـ كـ شـ بـ .

دادعإ لاثم TACACs

```
aaa new-model
!
!
aa group server tacacs+ tacacsgroup
  server name server1
  server name server2

aaa authentication login AUTH group AAA-Servers
aaa authorization commands 1 PRIV1 group AAA-Servers
aaa authorization commands 15 PRIV15 group AAA-Servers
aaa authorization exec AUTHLIST group AAA-Servers
```

نيوكتل لاثم HTTPS

```
ip http server
ip http authentication aaa exec-authorization AUTHLIST
ip http authentication aaa command-authorization 1 PRIV1 ip http authentication aaa command-authorization 15 PRIV15 ip http authentication aaa login-authentication AUTH ip http secure-server
ip http secure-trustpoint TP-self-signed-2945720990
ip http client source-interface GigabitEthernet0/0
ip http client secure-trustpoint TP-self-signed-2945720990
```

CM ىلع ةطساوب رمأ لىغشت متى Express/APPNAV-XE رباع HTTP

زاهجلالىلعلىغشتلا نم نكمتيىتح يزكرملاريدملاءاهيلإ جاتحي يـ تـ لـ اـ رـ مـ اـ لـ اـ بـ ةـ مـ ئـ اـ قـ هـ ذـ هـ دـ يـ عـ بـ لـ اـ .

نيوكتلـا عـضـوـلـا يـفـ مـكـحـتـلـا مـئـاـوـقـ

```
do show running-config | section crypto pki trustpoint  
crypto pki export
```

EXEC مىڭەتلىك (CLI) لۇصۇلما يەقۇم

Waasx - اچلىخ

```
show waas token | format  
show waas status | format  
show waas alarms | format  
show running-config | section hostname  
show ip interface brief | format  
show interfaces | include line protocol | Internet address | address is | *uplex  
show running-config brief | include clock timezone  
show clock  
show crypto pki trustpoints | include Trustpoint  
show inventory
```

WAASX - كەنەتكەتلىك

```
show parameter-map type waas waas_global | format  
show class-map type waas | format  
show policy-map type waas | format  
write memory
```

WAASX - اچلىخ

```
show waas statistics peer | format  
show waas statistics application | format  
show waas connection brief  
show waas statistics accelerator http-express | format  
show waas statistics accelerator http-express https | format  
show waas statistics accelerator ssl-express | format  
show waas statistics class | format  
show waas statistics accelerator cifs-express detail | format
```

لىجىستلىك

```
registration  
show waas status extended | format
```

```
show service-insertion token | format
show service-insertion status | format
show class-map type appnav | format
show ip int br | format
show service-insertion service-context | format
show service-insertion service-node-group | format
show service-insertion statistics service-node-group | format
show policy-map type appnav | format
show policy-map target service-context | format
show service-insertion config service-context | format
show service-insertion config service-node-group | format
show service-insertion config appnav-controller-group | format
show service-insertion alarms | format
show ip access-list
show vrf
show running-config | section interface
show running-config | include service-insertion swap src-ip
```

اچالص اور عاطخآلہ فاشکتسا

يـف لـشـف تـالـاح ثـودـح إـلـا يـفـرـطـلـا زـاهـجـلـا إـلـعـ حـيـحـصـلـا رـيـغـ HTTP وـأـ AAA نـيـوـكـتـ يـدـؤـيـ دقـقـةـلـاحـلـا ثـيـدـحـتـ لـشـفـ تـالـاحـوـ لـيـجـسـتـلـا.

مذکوس م دادع ایه ضیوفت ۃلکشم کانه تن اک اذا ام رابتخال ۃقیرط طس بأ: ةظحالم
اذه رابتخالا نیوکت حجن اذا. ۃیلحM IP ۃقداصم و ۃیلحM AAA ۃقداصم و ۃیلحM
WAAS دیعبلأا مذکوس ملأا رم اوأ ضیوفت یف ۃلکشم هجاوت دق کنأ ینعی اذهب.

WAAS ل يزك رمل ا ريد ملاب ۋە صاخلا (CLI) رم اولى رطس ۋە جاۋىلۇ

زاهجلا ىلإ CM ب ٰصاخلا (CLI) رمأوألا رطس ٰههجاونم SSH لوكوتورب كنكمي هنأ نم دكأت ديعبلأا.

عانثأ CMS و gwaasx-audit.log تافلم عجارو CM ىلع حيحةست نيكمتب مق تايماصح إلأ عيمجتو نيكوتلا جارخا ىلإ يدؤي امم ،ليجستلا #ssh <device-name>

```
# debug cms waasx-regis
# debug cms router-config
# debug cms stats
(config)# logging disk priority 7
# cd errorlog
# type-tail cms.log follow
# type-tail waasx-audit.log follow
```

```
05/27/2016 00:14:03.760 [I] cdm(RtrSync-40) Configuration commands failed on the device  
CeConfig_2875943/USNY25W39-R02. Not Taking backup of complete device configuration.  
05/27/2016 00:14:03.774 [W] cdm(RtrSync-64) 700001 Failed configuration commands are ...  
05/27/2016 00:14:03.774 [W] cdm(RtrSync-64) 700001  
class-map type appnav match-any HTTPS  
CLI:class-map type appnav match-any HTTPS  
Status:8  
Output:Command authorization failed.
```

ضرع سملانم HTTPS لوصو رابت خا

ةهـج اوـلـا لـوـخـدـلـا لـيـجـسـتـ كـنـكـمـيـ HTTP.

https://<ip_address>/level/15/exec/-

[Home](#) [Exec](#) [Configure](#)

Command

Output

Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-

Exec commands:

NUMBER 1-1

Slot Number

[access-enable](#)

Create a temporary Access-List entry

[access-profile](#)

Apply user-profile to interface

[access-template](#)

Create a temporary Access-List entry

[archive](#)

manage archive files

مسـقـلـاـ يـفـ كـبـ ةـصـاخـلـاـ رـمـ اوـلـاـ بـتـكـاـ مـثـ

Command

يـضـارـتـعـاـ رـمـ اـلـمـعـ ضـرـعـ نـمـ لـاثـمـ

Command **show inventory**

Output

Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-/show/inventory/CR
Command was: show inventory

NAME: "CISCO2911/K9", DESCRIPTOR: "CISCO2911/K9 chassis, Hw Serial#: FTX1425A1AA, Hw :
PID: CISCO2911/K9 , VID: V01 , SN: FTX1425A1AA

NAME: "High Speed Wan Interface Card with 4 serial ports(HWIC-4T) on Slot 0 SubS
PID: HWIC-4T , VID: V01 , SN: FOC09023M5F

NAME: "Services Module with Services Ready Engine on Slot 1", DESCRIPTOR: "Services M
PID: SM-SRE-900-K9 , VID: V03 , SN: FOC15324NOL

NAME: "C2911 AC Power Supply", DESCRIPTOR: "C2911 AC Power Supply"
PID: PWR-2911-AC , VID: V01 , SN: AZS142220G4

command completed.

لشاف show inventory رمأى لع لاثم

Command

Output

Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-/show/inv/CR
Command was: show inv

Command authorization failed.

حصـنـ حـيـ حـاصـنـ ءـاطـخـاـلـاـ حـيـ حـاصـنـ وـاـسـ اـسـ اـسـ

#debug ضيوفت AAA

جاجنب رمألا ليغشت مت

```
Jul  5 07:09:19.161: AAA/AUTHOR/TAC+: (2935402750): user=waasx
Jul  5 07:09:19.161: AAA/AUTHOR/TAC+: (2935402750): send AV service=shell
Jul  5 07:09:19.161: AAA/AUTHOR/TAC+: (2935402750): send AV cmd=show
Jul  5 07:09:19.161: AAA/AUTHOR/TAC+: (2935402750): send AV cmd-arg=vrf
Jul  5 07:09:19.161: AAA/AUTHOR/TAC+: (2935402750): send AV cmd-arg=
Jul  5 07:09:19.365: AAA/AUTHOR (2935402750): Post authorization status = PASS_ADD
```

ليوختلا لشف

```
Jul  5 07:08:32.485: AAA/AUTHOR/TAC+: (819547031): user=waasx
Jul  5 07:08:32.485: AAA/AUTHOR/TAC+: (819547031): send AV service=shell
Jul  5 07:08:32.485: AAA/AUTHOR/TAC+: (819547031): send AV cmd=show
Jul  5 07:08:32.485: AAA/AUTHOR/TAC+: (819547031): send AV cmd-arg=inventory
Jul  5 07:08:32.485: AAA/AUTHOR/TAC+: (819547031): send AV cmd-arg=
Jul  5 07:08:32.685: AAA/AUTHOR (819547031): Post authorization status = FAIL
```

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).