

ةكرح مداخ ةداهش نم ققحتل اءاطخأ فاشكتسأ MRA تامدخل Expressway Traffic Server رورم اهحالصإو

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[هب قوئوملا قءصملا عجرملا ءلسلس](#)

[CN و SAN صءف](#)

[كولسل ريغت](#)

[X14.2.0 نم لقالا تارادصل](#)

[ءءال تارادصل او X14.2.0 نم تارادصل](#)

[اهحالص او تاهويرانيسلا فاشكتسأ](#)

[هب قوئوم ريغت ءءىءلا ءداهشلا عىقوتب ماقىءلا قءصملا عجرملا 1.](#)

[ءداهشلا ءف ءووم ريغت \(IP و FQDN\) لاصلال ناوع 2.](#)

[ءلوهسب اهءءص نم ققحتل اءىءفءك](#)

[لءلا](#)

[ءلص تاء تامولعم](#)

ةمدقملا

ىلءال تارادصل او X14.2.0 نم Expressway تارادصل ىلء كولسل ريغت ءنتسملا اءه فصءى
Cisco نم اءاطءال اءىءصء فرعم و [CSCwc69661](#) Cisco نم اءاطءال اءىءصء فرعمب ءطءترملا
[CSCwa25108](#).

ةيساسألا تابلطتملا

تابلطتملا

ءىلءال عىضاوملاب ءفرعم كءىءل نوكء نأب Cisco ىصوء:

- Expressway ل ىساسألا نىوكءل
- MRA ىساسألا نىوكءل

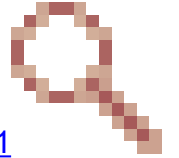
ةمدختسملا تانوكملا

X14.2 رادصلال ىلء Cisco Expressway ىلء ءنتسملا اءه ءف ءءراول تامولعملا ءنتسء

ثدخال تارادصال او

ةصاخ ةي لمعم ةئيبي ف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجال عيمج تادب رمأ يال لمحتحمل ريثأتلل كمهف نم دكأتف ، ليغشتلا ديق كتكبش

ةيساسأ تامولعم



نم عا طخال حيحصت فرع م ب زي م م لا كولس لا يف ريغيغتل اذه عم [Cisco CSCwc69661](#)

نم عا طخال حيحصت فرع م وأ [Cisco CSCwa25108](#)

تالاصتالا ري دم ةداهش نم ققحتلا عارجب Expressway ةصنم ىلع رورملا ةكرح م داخ موقبي ، م داخ دقعو Cisco نم (IM&P) دجاوتلاو ةدحوملا ةيروفلا ةلسارملاو Cisco نم (CUCM) ةدحوملا تالاح ثودح ىلإ ريغيغتل اذه ي دؤي دق. (MRA) دع ب نع لوصولو لومحمل لوصولو تامدخل Unity ةيساسألا Expressway ماظن ىلع ةيقرت عارجب دع ب MRA ىلإ لوخدلا ليحست يف لشف

نامأ مدختسي نم لاصتالا لوكوتورب وه (HTTPS) نم آلا يبعشتلا صنلا لقن لوكوتورب مادختساب ةنم آلا ةانقلا هذه عاشنإ موقبي وه. لاصتالا ريغشتلا (TLS) لقنلا ةقبط ةقداصملا: نيضرغ ةمدخل هذه مدخت. TLS ةحفاصم يف اهلدا بت متي يتلا TLS ةداهش تامجه ةقداصملا يمح. (ريغشتلا) ةيصوصخالو (ه ب لصتت يذلا ديعبل فرطلا ةفرعمل) تالاصتالا ب ثبعلاو تصنتلا نم ني مجاهملا ةيصوصخالو ع نم تو ليخدلا

كل لاصتالا نم دكأتلاب كل حمسيو ةقداصملا ني ع يف (ةداهشلا) TLS نم ققحتلا عارجب متي ني يدر ف ني رصنع نم ققحتلا فلأتيو. نم يال ديعبل فرطلاب

1. (CA) ه ب قو ثوملا قي دصتلا عجرم ةلسلس
2. (CN) عئاشلا مسالا وأ (SAN) عوضوملل لي دبل مسالا

ه ب قو ثوملا قداصملا عجرملا ةلسلس

نوكت نأ مزلي، CUCM / IM&P / Unity اهلسري يتلا ةداهشلا يف Expressway-C قثت يكل قثت يذلا (CA) ىلعألا (رذجال) قدصملا عجرملا ىلا ةداهشلا كلت نم طابترأ عاشنإ ىلع ةرداق ةداهشب تانايف ةداهش طبرت يتلا تاداهشلا نم يمره لسلسلت وهو، طبارلا اذه ىمسي. هيف لك يوتحت، هذه ةقثلا ةلسلس نم ققحتلا نم نكمتلل. ةقث ةلسلس، رذج قدصم عجرم ("لجأ نم رداصلا" وأ) عوضوملاو ("ةطساوب رداصلا" وأ) رداصملا: نيلقح ىلع ةداهش

لقح يف Expressway-C ىلا لسري يذلا CUCM نم دحاو لثم، مداخل تاداهش نمضتت CN يف (FQDN) لمكالب لهؤملا لاجملا مسا صاخ لكشب "عوضوملا"

Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=cucm.vngtp.lab

لقح CN ةمس يف FQDN ىلع يوتحي CUCM.vngtp.lab CUCM ل مداخل ةداهش ىلع لاثم نأ ىرن نأ اننكمي امك ... (L) عقوملا، (ST) ةلاجال، (C) ةلودلا لثم ىرخأ تامس عم عوضوملا vngtp-active-DIR-CA ىمسي قدصم عجرم لبق نم (اهرادصا) اهمي لسست متي مداخل ةداهش

رادصاب (رذجال قدصملا عجرملا) ىوتسملا ةيلاع ةقدصملا عجارملا موقت نأ اضيأ نكمي اهمل عوضوملاو رداصملا نأ ىرن، هذه رذجال قدصملا عجرملا ةداهش يف. اهسفن فيرعتل ةداهش : ةمقلا سفن

Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA

اهسفن فيرعتل يرذج قدصم عجرم لبق نم اهمي لسست متي ةداهش اهنا

كذلذ نم ال دب. ةرشابم مداخل تاداهش رذجال CA صيخارت رصت ال، ةيجذومنل تالاجل يف مسا كذلذ دعب ةداحل ىونلا نم ىرخألا عاونألا هذه ىلع قلطيو. ىرخأ CAS ل تاداهش رصت اهناف تاداهش وأ تاداهش رادصاب اهروذب ةطيسولا CAS موقت نأ نكمي. ةطسوتملا ةيججرملا ىونلا مداخل ةداهش رادصا متي شيح ةلاح انيدل نوكي نأ نكمي. ىرخألا ةطيسولا CAS ل ةرشابم مداخل عجرملا لصحي ىتح. اذكهو طسوتم CA 2 نم ةداهش ىلع لصحي هرودب يذلا، طسوتم CA 1 نم رذجال قدصملا عجرملا نم ةرشابم هتداهش ىلع اريخأ طيسولا قدصملا

Server certificate :

Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1
Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=cucm.vngtp.lab

Intermediate CA 1 certificate :

Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1

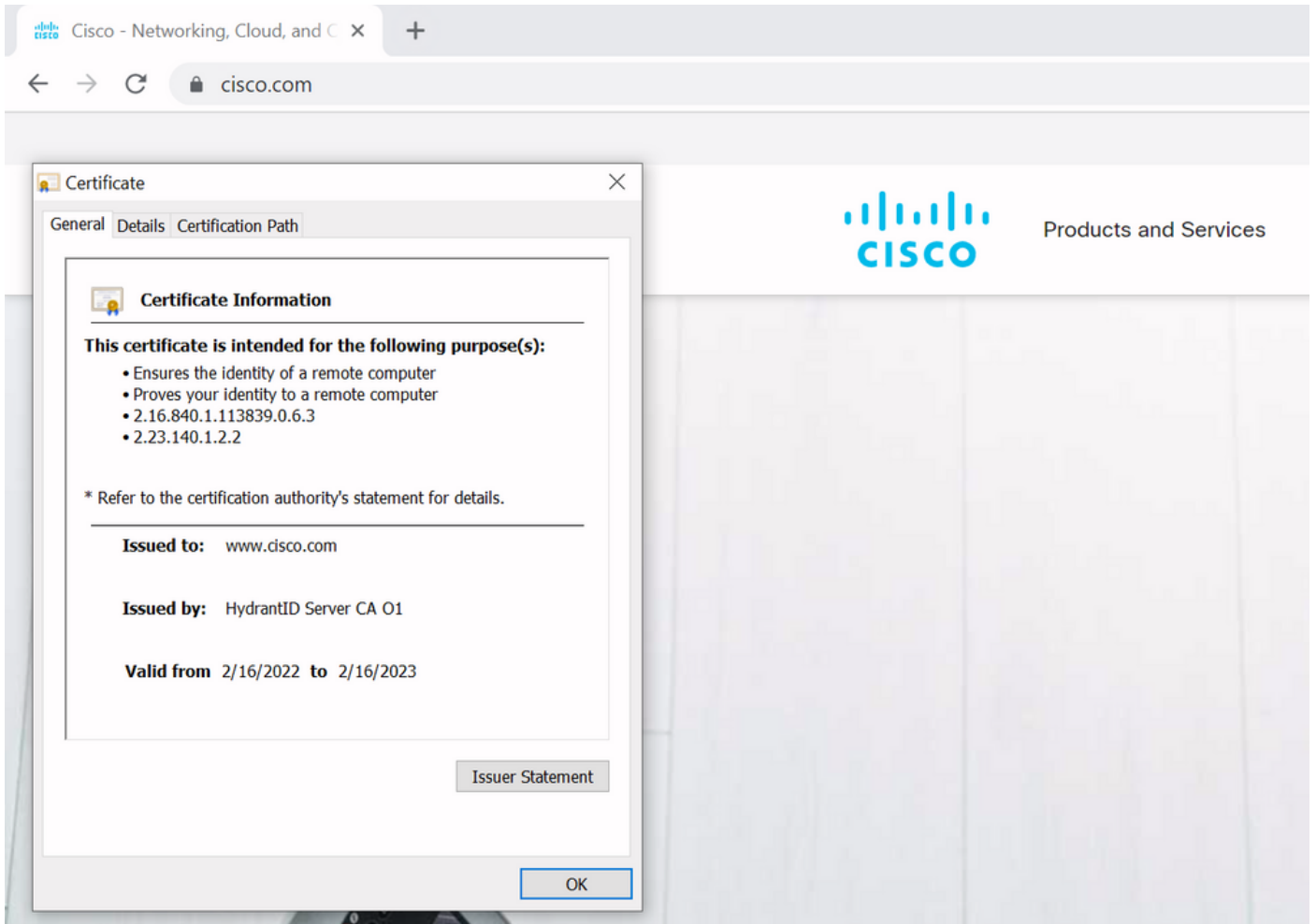
Intermediate CA 2 certificate :

Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-3
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2

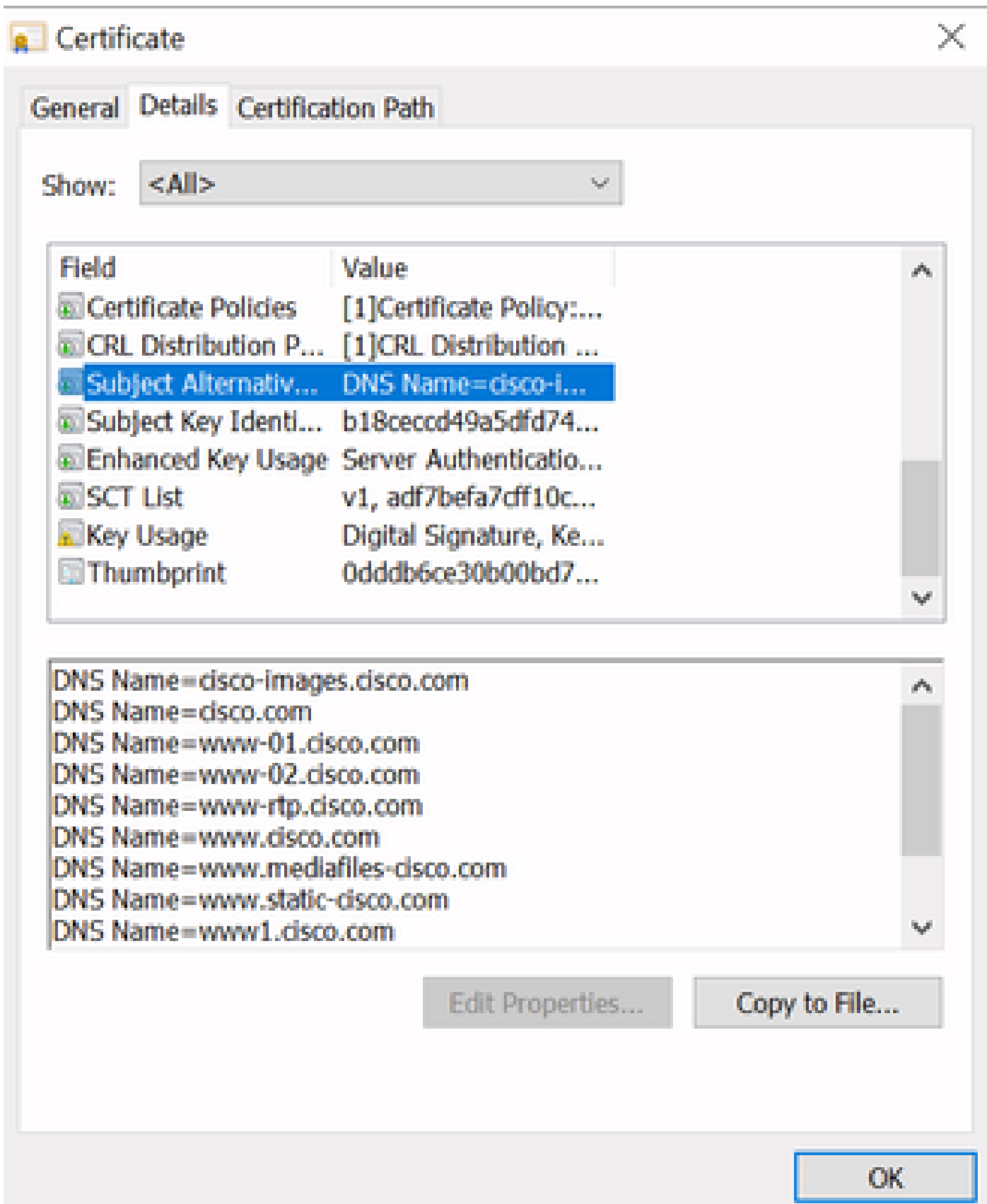
...

Intermediate CA n certificate :

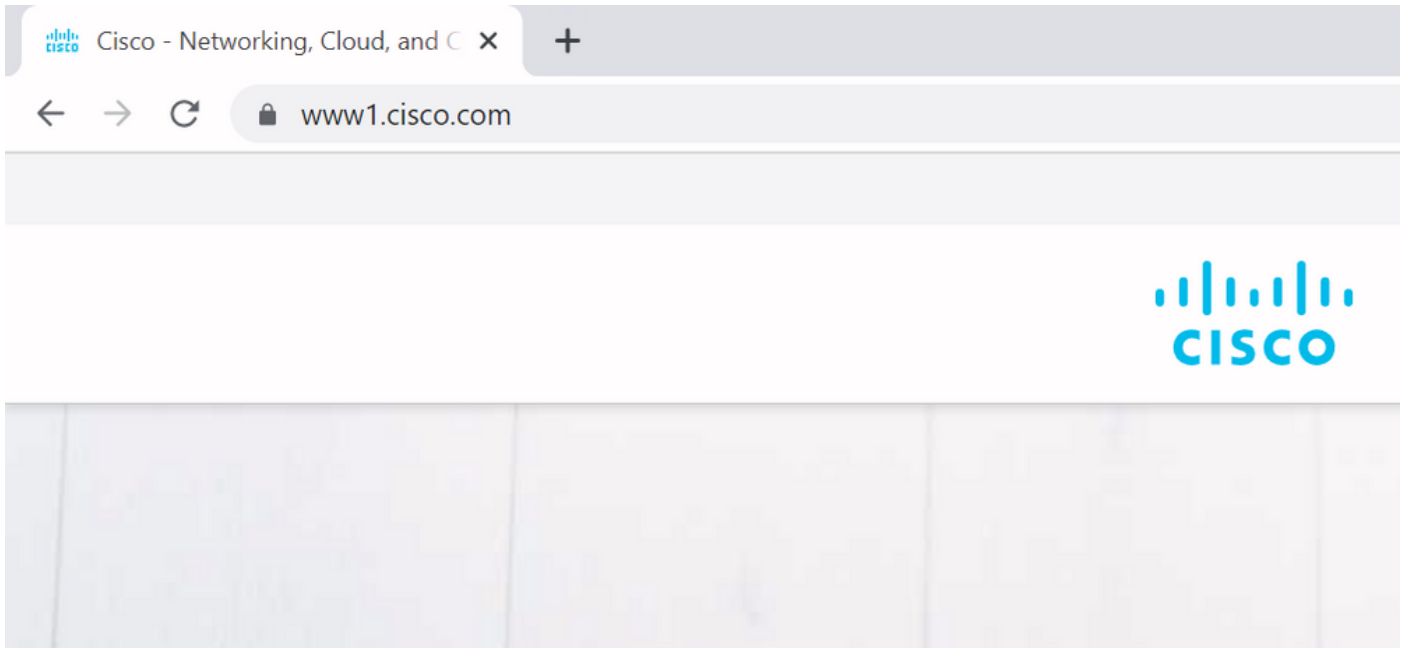
Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-n



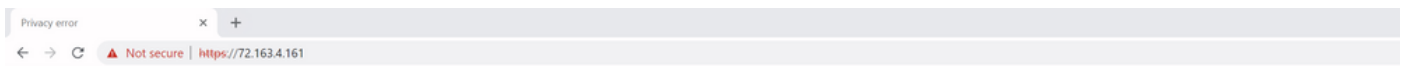
لكش ب (SAN) نيزختلا قطنم ةكبش تالخدإ ىلعو ةداهشلا ليصافت ىلع عالطالا دن ع نيزختلا قطنم ةكبش تالخدإ ضعب ىلإ ةفاضل اب ررك تي عيشلا سفن نا ظجالن، صاخ ىرخألا (FQDN):



رهظيس ،لاثملا لىبس ىلع <https://www1.cisco.com> ب لاصتالا بلطن ام دنع هنا ينعى اذهو (SAN) نىزختلا ةكبش تالخدإ يف دوجوم هنا لاضيا نم لاصتاك



IP ناونع ىلإ قرشابم نكلو <https://www.cisco.com> ىلإ ضارعتس الاب موقن ال امدنع ،كلذ عموه عي قوتب ماق يذلا CA يف قثي ال هنأل انمآ ال اصتا رهظي ال هنإف ، (<https://72.163.4.161>) هانمدختسأ يذلا (72.163.4.161) ناونع ال ىلع يوتحي الو ، انل ةمدقملا ةداهشلا نكلو مداخلاب لاصتال.



```
Command Prompt - nslookup
C:\Users\stejans>
C:\Users\stejans>nslookup
Default Server: dns-aer1.cisco.com
Address: 173.38.200.100

> cisco.com
Server: dns-aer1.cisco.com
Address: 173.38.200.100

Name: cisco.com
Addresses: 2001:420:1101:1::a
          72.163.4.161
>
```



Your connection is not private

Attackers might be trying to steal your information from 72.163.4.161 (for example, passwords, messages, or credit cards). [Learn more](#)

NET:ERR_CERT_COMMON_NAME_INVALID

🔒 To get Chrome's highest level of security, [turn on enhanced protection](#)

Hide advanced

Back to safety

This server could not prove that it is 72.163.4.161; its security certificate is from www.cisco.com. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 72.163.4.161 (unsafe)

TLS تالاصتال ىلع هنيكمت كنكمي ، لاج يأل ىلع ، دادعإل اذه زواجت كنكمي ، ضرعتسملا يف ىلع كب ةصاخلا تاداهشلا يوتحت نأ مهمل نم ، كلذل . فافتلالاب حامسلا متي ال ثيحب اهب لاصتال اهمادختسال ديعلال فرطال ططخي يتلا ةحیحصلا SAN وأ CN ءامسأ

كولسلا ريغت

هاجت ةعيرسلا قرطال ربع HTTPS تالاصتال نم ديدعلا ىلع ريبك لكشب MRA تامدخ دمعت

داهش نأ ضارت فاب . cucm.steven.lab نم FQDN مادختساب Expressway-C ىل ع CUCM ةفاضل
كلذ دعب ، IP ناو نك سي ل و SAN ىل لاخداك cucm.steven.lab ىل ع يوتحت CUCM نم tomcat
MRA ءالمع نم ةي ل ع ف ال ا ص ت ال ا ن ك ل و 'On' ىل ع 'TLS Verify Mode' عم فاشتكال ا ح ج ن ي
TLS نم ق ق ح ت ال ا ل ش ف ت ي ل ا ت ال ا ب و ف ل ت ح م IP و FQDN ف د ه ت س ت ن ا ن ك م ي

ث د ح أ ل ا ت ا ر ا د ص إ ل ا و X14.2.0 نم ت ا ر ا د ص إ ل ا

ب ل ط ل ك ل TLS ة د ا ه ش نم ق ق ح ت ال ا ىل ع Expressway م د ا خ ل م ع ي ، ا د ع ا ص ف X14.2.0 ر ا د ص إ ل ا نم
م ت ي ا م د ن ع ا ض ي ا ا ذ ه ذ ف ن ت ا ه ن ا ي ن ع ي ا ذ ه و . ت ا ن ا ي ب ل ا ر و ر م ة ك ر ح م د ا خ ل ل ا ل خ نم ه و ا ر ج ا م ت ي HTTPS
ا م د ن ع CUCM / IM&P / Unity د ق ع ف ا ش ت ك ا ء ا ن ا ث ا " ف ا ق ي ا " ىل ع " TLS نم ق ق ح ت ال ا ع ض و " ن ي ي ع ت
ن ا ن ك م ي ي ذ ل ا ب ل ط ل ا ل ش ف ي و TLS ل ا ص ت ا د ي ك ا ت م ت ي ا ل ، ة ح ص ل ا نم ق ق ح ت ال ا ة ي ل م ع ح ج ن ت ال
ل و خ د ل ا ل ي ج س ت ل ش ف و ا ل ش ف ل ا ز و ا ج ت و ا ر ا ك ت ال ا ل ك ا ش م ل ث م ف ا ئ ا ط و ل ا د ق ف ىل ا ي د و ي
ال ، " ل ي غ ش ت " ىل ع " TLS نم ق ق ح ت ال ا ع ض و " ن ي ي ع ت عم ا ض ي ا . ل ا ث م ل ا ل ي ب س ىل ع ل م ا ك ل ا
ا ق ح ا ل ل ا ث م ل ا ي ف ه ي ل ع ص و ص نم وه ا م ك ح ي ح ص ل ك ش ب ت ا ل ا ص ت ال ا ع ي م ج ل م ع ت ن ا ن م ض ي

وه ا م ك CUCM / IM&P / Unity د ق ع نم ع ي ر س ل ا ق ي ر ط ل ا ه ص ح ف ي ي ت ل ا ة ق ي ق د ل ا ت ا د ا ه ش ل ا د ر ت
MRA ل ي ل د م س ق ي ف ح ض و م

ي ف ه م ي د ق ت م ت ر ي ي غ ت ا ض ي ا ك ا ن ه ، TLS نم ق ق ح ت ال ا ىل ع ي ض ا ر ت ف ا ل ا د ا د ع ا ل ا ىل ا ة ف ا ض ا ل ا ب
د م ت ع ي ي ذ ل ا و ، ر ي ف ش ت ل ا ة م ئ ا ق ل ف ل ت ح م ل ي ض ف ت ب ي ت ر ت ن ع ن ل ع ي ن ا ن ك م ي ي ذ ل ا و X14.2
د ع ب ة ع ق و ت م ر ي غ TLS ت ا ل ا ص ت ا ث و د ح ي ف ك ل ذ ب ب س ت ي د ق . ك ب ص ا خ ل ا ة ي ق ر ت ل ا ر ا س م ىل ع
Cisco Tomcat و Cisco ة د ا ه ش ل ة ب و ل ط م ل ا ة ي ق ر ت ل ل ل ب ق ه ن ا ث د ح ي د ق ه ن ا ل ج م ا ن ر ب ل ا ة ي ق ر ت
ن ك ل و (ECDSA ة ي م ز ر ا و خ ل ة ل ص ف نم ة د ا ه ش ىل ع ي و ت ح ي ر خ ا ج ن ت م ي ا و) CUCM نم Cisco CallManager
RSA نم ا ي ل ع ف ا ن ا م ا ر ث ك ا ل ا ر ي ف ش ت ل ا ر ي غ ت م وه) ECDSA ر ي غ ت م ب ل ط ي ه ن ا ف ة ي ق ر ت ل ا د ع ب
ف ل ت ح م CA ل ب ق نم Cisco CallManager-ECDSA و Cisco Tomcat-ECDSA ت ا د ا ه ش ع ي ق و ت ن ك م ي
(ي ض ا ر ت ف ا ل ا) ا ي ت ا ذ ة ع ق و م ت ل ا ز ا م ت ا د ا ه ش و

ة ي ق ر ت ل ا ر ا س م ىل ع د م ت ع ي ه ن ا ل ا م ئ ا د ك ب ة ل ص ا ذ ا ذ ه ر ي ف ش ت ل ا ل ي ض ف ت ر م ا ر ي ي غ ت ن و ك ي ال
> ة ن ا ي ص ل ا نم ى ر ت ن ا ن ك ن ك م ي ، ر ا ص ت خ ا ب . Expressway X14.2.1 ر ا د ص ا ت ا ط ح ا ل م نم ح ض و م وه ا م ك
"ECDHE-RSA-AES256-GCM-SHA384" د ا د ع ا ىل ا ي د و ي ن ا ك ا ذ ا ا م ت ا ر ي ف ش م ل ا نم د ح ا و ل ك ل ت ا ر ف ش م ل ا > ن ا م ا ل ا
ر ي ف ش ت ىل ع ث د ح ا ل ا ECDSA ر ي ف ش ت ل ص ف ي ه ن ا ف ، ك ل ذ ك ن ك ي م ل ا ذ ا و . ال م ا " :GCM-SHA384-
ذ ي د ن ع ىل ع ا ل ي ض ف ت ه ي د ل ي ذ ل ا RSA عم ق ب ا س ك و ل س ك ي د ل ن و ك ي س ف ، ك ل ذ ك ن ا ك ا ذ ا RSA.

Cipher Preferences - ECDSA Cipher Preference Over RSA

ECDSA certificates are preferred over RSA.



Important

The following points lists the various upgrade path(s) that are mandatory for upgrading ciphers.

1. When upgrading from version lower than 14.0 to 14.2, the ECDSA would be preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with "ECDHE-RSA-AES256-GCM-SHA384:" using either Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers).
2. When upgrading from version equal or higher than 14.0 to 14.2 or higher version, you have appended "ECDHE-RSA-AES256-GCM-SHA384:" to the default Ciphers List to prefer RSA certificates over ECDSA. If you prefer ECDSA certificates over RSA, then remove "ECDHE-RSA-AES256-GCM-SHA384:" from the cipher string using Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers).
3. Any customer has a fresh install X14.2 image, ECDSA is being preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with "ECDHE-RSA-AES256-GCM-SHA384:" using either Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers).

ل ي ص ف ت ل ا ب ا م ه ت ي ط غ ت م ت ي و ، و ي ر ا ن ي س ل ا ا ذ ه ي ف TLS نم ق ق ح ت ال ا ل ش ف ل ن ا ت ق ي ر ط ك ا ن ه
ا ق ح ا ل :

1. ه ب ق و ث و م ر ي غ ة د ي ع ب ل ا ة د ا ه ش ل ا ع ي ق و ت ب م ا ق ي ذ ل ا ق د ص م ل ا ع ج ر م ل ا

ا ي ت ا ذ ة ع ق و م ة د ا ه ش - ا

ب ف و ر ع م ر ي غ ق د ص م ع ج ر م ل ب ق نم ة ع ق و م ل ا ة د ا ه ش ل ا .

ةداهشلالي في (IP وأ FQDN) لاصتالاناونع يوتحي ال 2.

اهحالصإوتاهوييرانيسالافاشكتسأ

ليجست لشف شح ةيلعم ةئيبي في اهابشم وييرانيس ةيلاتال تاهوييرانيسالارفظت، تالجالسالي في نوهباشتي. X14.2 إلى X14.0.7 نم Expressway ةيقرت دعب MRA إلى لوخدلاليجستالاةطساوب طقف تالجالسالي عيمجت متي. ةفلتخم ةقدلانا نم مغرلالي ع دعب متي ذلالي (يصيخششتالاليجستالاةصايخششتالاةنايصالانم) يصيخششتالال MRA إلى لوخدلاليجست لشف دعب هفاقيإ متو MRA إلى لوخدلاليجست لبق هليغشت هل في اضاإ اءاطخأ حيحصت ليجست لي أني كمت متي.

1. هب قوثوم ريغ ةديعبالاةداهشلاليعيقوتب ماق يذلالي قدصم ال اعجرم ال 1.

هب قوثوم ال نزم ال في نمضم ريغ قدصم اعجرم لبق نم دعب نع ةداهشلاليعيقوت نكمي ال (اضيأ قدصم اعجرم اهرهوج في) ايتاذةعقوم ةداهش نوكت نا نكمي وأ Expressway-C مداخلل Expressway-C مداخل صاخال قيثوتال نزم في اهتفاضا متت

في CUCM (10.48.36.215 - cucm.steven.lab) إلى لقتنت يتي تابل لطلانا ةظحال مكنكمي، انه لاثمالي في (200 OK ةباجتسإ) 8443 ذفنمالي إلى عحيحص لكشب اهعم لماعتال متي (502 ةباجتسإ) أءطخ ثودح في ببستت اهنكلو TFTP لاصتال 6972 ذفنمالي إلى ع

<#root>

===Success connection on 8443===

2022-07-11T18:55:25.910+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,910" Module="net

2022-07-11T18:55:25.917+02:00 vcsc traffic_server[18242]: Event="Request Allowed" Detail="Access allow

2022-07-11T18:55:25.917+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,916" Module="net

2022-07-11T18:55:25.955+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,955" Module="net

2022-07-11T18:55:25.956+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,955" Module="net

200

"

===Failed connection on 6972===

2022-07-11T18:55:26.000+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,000" Module="net

2022-07-11T18:55:26.006+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,006" Module="net

2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,016" Module="net

2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: [ET_NET 0]

WARNING: Core server certificate verification failed for

(cucm.steven.lab).

Action=Terminate Error=self signed certificate server=cucm.steven.lab(10.48.36.215)

depth=0

2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: [ET_NET 0]

ERROR: SSL connection failed for

'cucm.steven.lab': error:1416F086:

SSL routines:tls_process_server_certificate:certificate verify failed

2022-07-11T18:55:26.024+02:00 vscs traffic_server[18242]: UTCTime="2022-07-11 16:55:26,024" Module="net

502 connect failed

"

نم ققحتلا نم Expressway-C نكمت مدع ققح ىلإ "ةداهشلا ةحص نم ققحتلا" أطخ ريشي ايتاذ ةعقوم ةداهش ىلإ ريشي هنأل ريذحتلا رطس يف رهظي كلذ ببسو. TLS ةحفاصم ةحص 0، نم ىلعأ قمعلل نوكي امدنع. ايتاذ ةعقوم ةداهش اهنإف، 0 ةئيه ىلع حضوم قمعلل ناك اذا فورعم ريغ قدصم عجرم لبق نم هعيقوت متي يلاتلابو تاداهش ةلسلس هل نأ ينعي اذف (Expressway-C روظنم نم).

تالجس نم ةروكذملا ةينمزللا عباوطلال يف هعيجمت مت يذلا PCAP فلم يف رظنن امدنع (و cucm.ms.steven.lab CUCM-MS ةئيه ىلع CN عم ةداهشلا مدقي CUCM نأ ىرت نأ كنكمي، صنلا ىلع Expressway-C ىلإ Steven-DC-CA لبق نم ةعقوم SAN ةئيه ىلع cucm.steven.lab 8443 ذفنملا).

No.	Time	Source	Src port	Destination	Dest port	Protocol	DSCP	VLAN	Length	Info
4691	2022-07-11 16:55:25.916680	10.40.36.46	35622	10.40.36.215	8443	TCP	CS0		74	35622 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=878570435 TSecr=0 WS=128
4692	2022-07-11 16:55:25.916993	10.40.36.215	8443	10.40.36.46	35622	TCP	CS0		74	8443 → 35622 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=343633230 TSecr=878570435 WS=128
4693	2022-07-11 16:55:25.916993	10.40.36.46	35622	10.40.36.215	8443	TCP	CS0		66	35622 → 8443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=878570435 TSecr=343633230
4694	2022-07-11 16:55:25.917032	10.40.36.46	35622	10.40.36.215	8443	TLSv1.2	CS0		583	Client Hello
4695	2022-07-11 16:55:25.938356	10.40.36.215	8443	10.40.36.46	35622	TLSv1.2	CS0		1514	Server Hello
4696	2022-07-11 16:55:25.938390	10.40.36.46	35622	10.40.36.215	8443	TCP	CS0		66	35622 → 8443 [ACK] Seq=518 Ack=1449 Win=64128 Len=0 TSval=878570457 TSecr=343633251
4697	2022-07-11 16:55:25.938409	10.40.36.215	8443	10.40.36.46	35622	TLSv1.2	CS0		1478	Certificate, Server Key Exchange, Server Hello Done
4698	2022-07-11 16:55:25.938419	10.40.36.46	35622	10.40.36.215	8443	TCP	CS0		66	35622 → 8443 [ACK] Seq=518 Ack=353 Win=63488 Len=0 TSval=878570457 TSecr=343633251
4699	2022-07-11 16:55:25.940804	10.40.36.46	35622	10.40.36.215	8443	TLSv1.2	CS0		192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4700	2022-07-11 16:55:25.943004	10.40.36.215	8443	10.40.36.46	35622	TLSv1.2	CS0		308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
4701	2022-07-11 16:55:25.943051	10.40.36.46	35622	10.40.36.215	8443	TCP	CS0		66	35622 → 8443 [ACK] Seq=644 Ack=3095 Win=64128 Len=0 TSval=878570461 TSecr=343633256
4702	2022-07-11 16:55:25.943277	10.40.36.46	35622	10.40.36.215	8443	TLSv1.2	CS0		2543	Application Data
4703	2022-07-11 16:55:25.943476	10.40.36.215	8443	10.40.36.46	35622	TCP	CS0		66	8443 → 35622 [ACK] Seq=3095 Ack=3121 Win=35072 Len=0 TSval=343633256 TSecr=878570462
4707	2022-07-11 16:55:25.954796	10.40.36.215	8443	10.40.36.46	35622	TCP	CS0		1514	8443 → 35622 [ACK] Seq=3095 Ack=3121 Win=35072 Len=1448 TSval=343633260 TSecr=878570462 [TCP segment of a reassembled PDU]
4708	2022-07-11 16:55:25.954842	10.40.36.46	35622	10.40.36.215	8443	TCP	CS0		66	35622 → 8443 [ACK] Seq=3121 Ack=4543 Win=64128 Len=0 TSval=878570473 TSecr=343633260
4709	2022-07-11 16:55:25.954861	10.40.36.215	8443	10.40.36.46	35622	TLSv1.2	CS0		1257	Application Data
4710	2022-07-11 16:55:25.954873	10.40.36.46	35622	10.40.36.215	8443	TCP	CS0		66	35622 → 8443 [ACK] Seq=3121 Ack=5734 Win=63488 Len=0 TSval=878570473 TSecr=343633260
4711	2022-07-11 16:55:25.955712	10.40.36.46	35622	10.40.36.215	8443	TLSv1.2	CS0		97	Encrypted Alert
4712	2022-07-11 16:55:25.955750	10.40.36.46	35622	10.40.36.215	8443	TCP	CS0		66	35622 → 8443 [FIN, ACK] Seq=3152 Ack=5734 Win=64128 Len=0 TSval=878570474 TSecr=343633260
4713	2022-07-11 16:55:25.956123	10.40.36.215	8443	10.40.36.46	35622	TLSv1.2	CS0		97	Encrypted Alert
4714	2022-07-11 16:55:25.956170	10.40.36.46	35622	10.40.36.215	8443	TCP	CS0		54	35622 → 8443 [RST] Seq=3153 Win=0 Len=0
4716	2022-07-11 16:55:25.956232	10.40.36.215	8443	10.40.36.46	35622	TCP	CS0		66	8443 → 35622 [FIN, ACK] Seq=5765 Ack=3153 Win=35072 Len=0 TSval=343633269 TSecr=878570474
4717	2022-07-11 16:55:25.956252	10.40.36.46	35622	10.40.36.215	8443	TCP	CS0		54	35622 → 8443 [RST] Seq=3153 Win=0 Len=0

```

Certificates (2423 bytes)
Certificate Length: 918
Certificate: 30822030820227200302010201120500001220500505... (id-at-commonName=cucm.ms.steven.lab,id-at-organizationalUnitName=TAC,id-at-organizationName=Cisco,id-at-localityName=Oiegen,id-at-stateOrProvinceName=Belgium,id-at-countryName=BE)
  signedCertificate
    version: v3 (2)
    serialNumber: 0x490000012205005050348608442000200000122
    signature (sha1WithRSAEncryption)
    issuer: rdnsSequence (0)
    validity
    subject: rdnsSequence (0)
    subjectPublicKeyInfo
    extensions: 9 items
      Extension (id-ce-ekusage)
      Extension (id-ce-keyusage)
      Extension (id-ce-subjectAltName)
      Extension (id-ce-subjectAltName)
        Extension Id: 2.5.29.17 (id-ce-subjectAltName)
          critical: True
          GeneralNames: 3 items
            GeneralName: dNSName (2)
              dNSName: cucm.steven.lab
            GeneralName: dNSName (2)
              dNSName: steven.lab
            GeneralName: dNSName (1)
              dNSName: cucm.steven.lab
      Extension (id-ce-subjectKeyIdentifier)
      Extension (id-ce-authorityKeyIdentifier)
      Extension (id-ce-cRLDistributionPoints)
      Extension (id-pe-authorityInfoAccessSyntax)
      Extension (id-ms-certificate-template)
      Extension (id-ms-application-certificate-policies)
    algorithmIdentifier (sha1WithRSAEncryption)
    padding: 0
    encrypted: 9fba7f0741637a2a82071ef08f2270ccc7c4470c82b...
    Certificate Length: 918
Certificate: 30822030820227200302010201120500001220500505... (id-at-commonName=steven-DC-CA,dc=steven,dc=lab)
  > Secure Sockets Layer
  
```

ةعقوم ةداهش اهنأ ىرت نأ كنكمي، 6972 ذفنملا ىلع ةمدقملا ةداهشلا صحفن امدنع نكلو ةراشإ EC- دادتما يطعي cucm-ec.steven.lab ةئيه ىلع CN دادع عم (هسفن رصملا) ايتاذ CUCM ىلع اهدادع مت يتي ECDSA ةداهش يه هذه نأ ىلإ

eth0_diagnostic_logging_tcpdump00_vsc_2022-07-11_16_55_44.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcpdump4872

No.	Time	Source	Seq port	Destination	Dest port	Protocol	OS	Length	Info
4730	2022-07-11 16:55:26.006408	10.48.36.46		15756 10.48.36.215	6972 TCP	C50	74	31576 → 6972 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=878578525 TSecr=0 WS=128	
4731	2022-07-11 16:55:26.006851	10.48.36.215		6972 10.48.36.46	31576 TCP	C50	74	6972 → 31576 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=343633320 TSecr=878578525 WS=128	
4732	2022-07-11 16:55:26.006892	10.48.36.46		31576 10.48.36.215	6972 TCP	C50	66	31576 → 6972 [ACK] Seq=1 Win=64256 Len=0 TSval=878578525 TSecr=343633320	
4733	2022-07-11 16:55:26.007380	10.48.36.46		31576 10.48.36.215	6972 TLSv1.2	C50	583	Client Hello	
4734	2022-07-11 16:55:26.013050	10.48.36.215		6972 10.48.36.46	31576 TLSv1.2	C50	1514	Server Hello, Certificate, Server Key Exchange	
4735	2022-07-11 16:55:26.013911	10.48.36.46		31576 10.48.36.215	6972 TCP	C50	66	31576 → 6972 [ACK] Seq=518 Ack=1449 Win=64128 Len=0 TSval=878578535 TSecr=343633329	
4736	2022-07-11 16:55:26.016408	10.48.36.215		6972 10.48.36.46	31576 TLSv1.2	C50	499	Certificate Request, Server Hello Done	
4737	2022-07-11 16:55:26.016419	10.48.36.46		31576 10.48.36.215	6972 TCP	C50	66	31576 → 6972 [ACK] Seq=518 Ack=1882 Win=63744 Len=0 TSval=878578535 TSecr=343633329	
4738	2022-07-11 16:55:26.016703	10.48.36.46		31576 10.48.36.215	6972 TLSv1.2	C50	73	Alert (Level: Fatal, Description: Unknown CA)	
4739	2022-07-11 16:55:26.016821	10.48.36.46		31576 10.48.36.215	6972 TCP	C50	74	31576 → 6972 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=878578535 TSecr=0 WS=128	
4740	2022-07-11 16:55:26.016965	10.48.36.46		31576 10.48.36.215	6972 TCP	C50	66	31576 → 6972 [RST, ACK] Seq=525 Ack=1882 Win=64128 Len=0 TSval=878578535 TSecr=343633329	
4741	2022-07-11 16:55:26.016984	10.48.36.215		6972 10.48.36.46	31576 TCP	C50	74	6972 → 31576 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=343633330 TSecr=878578535 WS=128	
4742	2022-07-11 16:55:26.017009	10.48.36.46		31576 10.48.36.215	6972 TCP	C50	66	31576 → 6972 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=878578535 TSecr=343633330	
4743	2022-07-11 16:55:26.017181	10.48.36.215		6972 10.48.36.46	31576 TCP	C50	66	6972 → 31576 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=343633330 TSecr=878578535 WS=128	
4744	2022-07-11 16:55:26.017212	10.48.36.46		31576 10.48.36.215	6972 TCP	C50	54	31576 → 6972 [RST] Seq=525 Win=0 Len=0	
4745	2022-07-11 16:55:26.017218	10.48.36.46		31576 10.48.36.215	6972 TLSv1.2	C50	583	Client Hello	
4746	2022-07-11 16:55:26.024226	10.48.36.215		6972 10.48.36.46	31576 TLSv1.2	C50	1514	Server Hello, Certificate, Server Key Exchange	
4747	2022-07-11 16:55:26.024265	10.48.36.46		31576 10.48.36.215	6972 TCP	C50	66	31576 → 6972 [ACK] Seq=518 Ack=1449 Win=64128 Len=0 TSval=878578543 TSecr=343633337	
4748	2022-07-11 16:55:26.024295	10.48.36.215		6972 10.48.36.46	31576 TLSv1.2	C50	590	Certificate Request, Server Hello Done	
4749	2022-07-11 16:55:26.024309	10.48.36.46		31576 10.48.36.215	6972 TCP	C50	66	31576 → 6972 [ACK] Seq=518 Ack=1883 Win=63744 Len=0 TSval=878578543 TSecr=343633337	
4750	2022-07-11 16:55:26.024548	10.48.36.46		31576 10.48.36.215	6972 TLSv1.2	C50	73	Alert (Level: Fatal, Description: Unknown CA)	
4751	2022-07-11 16:55:26.024647	10.48.36.46		31576 10.48.36.215	6972 TCP	C50	66	31576 → 6972 [RST, ACK] Seq=525 Ack=1883 Win=64128 Len=0 TSval=878578543 TSecr=343633337	
4757	2022-07-11 16:55:26.030159	10.48.36.46		31500 10.48.36.215	6972 TCP	C50	74	31500 → 6972 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=878578061 TSecr=0 WS=128	

Secure Sockets Layer

- TLV1.2 Record Layer: Handshake Protocol: Server Hello
- TLV1.2 Record Layer: Handshake Protocol: Certificate
- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 667
- Handshake Protocol: Certificate
- Handshake type: Certificate (11)
- Length: 663
- Certificates length: 660
- Certificates (600 bytes)
- Certificate Length: 657
- Certificate: 3082028202021480830202107470e6271e1d1346... (id-at-localityName=diegem, id-at-stateOrProvinceName=Belgium, id-at-commonName=cucm-ec.steven.lab, id-at-organizationalUnitName=TAC, id-at-organizationName=Cisco, id-at-countryName)
- signedCertificate
 - version: v3 (2)
 - serialNumber: 02740e6271e1d13461099460a30f5fd
 - signature (ecdsa-with-SHA384)
 - issuer: rdmsession (8)
 - consequence: 6 items (id-at-localityName=diegem, id-at-stateOrProvinceName=Belgium, id-at-commonName=cucm-ec.steven.lab, id-at-organizationalUnitName=TAC, id-at-organizationName=Cisco, id-at-countryName=BE)
 - validity
 - subject: rdmsession (8)
 - subjectPublicKeyInfo
 - extensions: 5 items
 - Extension (id-ce-keyUsage)
 - Extension (id-ce-extendedKeyUsage)
 - Extension (id-ce-subjectKeyIdentifier)
 - Extension (id-ce-basicConstraints)
 - Extension (id-ce-subjectAltName)
 - GeneralNames: 1 item
 - GeneralName: rdmsession (2)
 - rdmsession: cucm.steven.lab
 - algorithmIdentifier (ecdsa-with-SHA384)
 - padding: 0
 - encrypted: 30640282021480830202107470e6271e1d1346... (id-at-localityName=diegem, id-at-stateOrProvinceName=Belgium, id-at-commonName=cucm-ec.steven.lab, id-at-organizationalUnitName=TAC, id-at-organizationName=Cisco, id-at-countryName=BE)
- TLV1.2 Record Layer: Handshake Protocol: Server Key Exchange

نم أتال تحت حضورم اتاداش لى ل رظنلا كنكمي ، Cisco Unified OS قراذ تحت في
 و Tomcat لة فل تخم قدهاش رهظت . لاثم ل لى بس لى انه حضورم وه امك اتاداش لى قراذ
 ام نى ب (Expressway-C لى بى نم هب قو ثوم و) ع قوم Tomcat CA نو كى شى ح Tomcat-ECDSA
 انه Expressway-C لى بى نم هب قو ثوم و اى تاذة ع قوم Tomcat-ECDSA قدهاش

Cisco Unified Operating System Administration

Navigation Cisco Unified OS Administration

Home Settings Security Software Updates Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR Download CSR

Status

43 records found

Find Certificate List where	Certificate	begins with	Find	Clear Filter	Rows per	
Common Name	Type	Key Type	Distribution	Issued by	Expiration	Description
authZ	AUTHZ_cucm.steven.lab	Self-signed	RSA	cucm.steven.lab	07/21/2038	Self-signed certificate generated by system
CallManager	cucm.steven.lab	CA-signed	RSA	steven-DC-CA	07/13/2022	Certificate Signed by steven-DC-CA
CallManager-ECDSA	cucm-ec.steven.lab	Self-signed	EC	cucm.steven.lab	02/18/2024	Self-signed certificate generated by system
CallManager-trust	steven-DC-CA	Self-signed	RSA	steven-DC-CA	06/01/2023	Signed Certificate
CallManager-trust	NOMAT-AD-CA	Self-signed	RSA	NOMAT-AD-CA	04/23/2028	Signed Certificate
CallManager-trust	CAP-RTP-002	Self-signed	RSA	CAP-RTP-002	10/10/2023	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	CAPF-eb20648	Self-signed	RSA	CAPF-eb20648	04/12/2020	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	ms-AD2-CA-1	Self-signed	RSA	ms-AD2-CA-1	09/11/2024	vngtp-CA
CallManager-trust	CAP-RTP-001	Self-signed	RSA	CAP-RTP-001	02/07/2023	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	NOMAT-CA-10	Self-signed	RSA	NOMAT-CA-10	08/11/2027	Signed Certificate
CallManager-trust	Cisco_Root_CA_H2	Self-signed	RSA	Cisco_Root_CA_H2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	ACT2_SU02_CA	CA-signed	RSA	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	vngtp-ACTIVE-DIR-CA	Self-signed	RSA	vngtp-ACTIVE-DIR-CA	02/10/2024	VNGTP-CA
CallManager-trust	Cisco_Root_CA_2048	Self-signed	RSA	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	Cisco_Manufacturing_CA_SHA2	CA-signed	RSA	Cisco_Manufacturing_CA_SHA2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	dcomics-WONDERWOMAN-CA	Self-signed	RSA	dcomics-WONDERWOMAN-CA	09/19/2037	CA-bantam
CallManager-trust	CAMP-6164210c	Self-signed	RSA	CAMP-6164210c	07/12/2025	Self-signed certificate generated by system
CallManager-trust	CAMP-6164210c	Self-signed	RSA	CAMP-6164210c	07/12/2025	Self-signed certificate generated by system
CallManager-trust	CAP-RTP-002	Self-signed	RSA	CAP-RTP-002	10/10/2023	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	CAPF-eb20648	Self-signed	RSA	CAPF-eb20648	04/12/2020	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	CAP-RTP-001	Self-signed	RSA	CAP-RTP-001	02/07/2023	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	Cisco_Root_CA_H2	Self-signed	RSA	Cisco_Root_CA_H2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	ACT2_SU02_CA	CA-signed	RSA	ACT2_SU02_CA	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	Cisco_Root_CA_2048	Self-signed	RSA	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	Cisco_Manufacturing_CA_SHA2	CA-signed	RSA	Cisco_Manufacturing_CA_SHA2	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	Cisco_Manufacturing_CA_SHA2	CA-signed	RSA	Cisco_Manufacturing_CA_SHA2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	CAMP-6164210c	Self-signed	RSA	CAMP-6164210c	07/12/2025	Self-signed certificate generated by system
CallManager-trust	Cisco.steven.lab	Self-signed	RSA	cucm.steven.lab	07/12/2025	Trust Certificate
CallManager-trust	Cisco.steven.lab	Self-signed	RSA	cucm.steven.lab	07/12/2025	Trust Certificate
CallManager-trust	TLRECOVERY_cucm.steven.lab	Self-signed	RSA	TLRECOVERY_cucm.steven.lab	02/14/2039	Self-signed certificate generated by system
CallManager-trust	steven-DC-CA	Self-signed	RSA	steven-DC-CA	07/10/2024	Certificate Signed by steven-DC-CA
CallManager-trust	CSR Only	EC	EC	cucm.steven.lab
CallManager-trust	ECDSA	Self-signed	EC	cucm.steven.lab	07/25/2023	Self-signed certificate generated by system
CallManager-trust	steven-DC-CA	Self-signed	RSA	steven-DC-CA	06/01/2023	Trust Certificate
CallManager-trust	NOMAT-AD-CA	Self-signed	RSA	NOMAT-AD-CA	04/23/2028	Signed Certificate
CallManager-trust	cucm.steven.lab	Self-signed	EC	cucm.steven.lab	07/25/2023	Trust Certificate
CallManager-trust	steven-DC-CA	CA-signed	RSA	steven-DC-CA	07/10/2024	Trust Certificate
CallManager-trust	cucm.steven.lab	Self-signed	EC	cucm.steven.lab	07/25/2023	Trust Certificate
CallManager-trust	NOMAT-CA-10	Self-signed	RSA	NOMAT-CA-10	08/11/2027	Signed Certificate
CallManager-trust	vngtp-ACTIVE-DIR-CA	Self-signed	RSA	vngtp-ACTIVE-DIR-CA	02/10/2024	Trust Certificate
CallManager-trust	dcomics-WONDERWOMAN-CA	Self-signed	RSA	dcomics-WONDERWOMAN-CA	09/19/2037	CA-bantam
CallManager-trust	Cisco.steven.lab	Self-signed	RSA	cucm.steven.lab	07/12/2025	Self-signed certificate generated by system

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR Download CSR

قدهاش لى ف دوجوم رىغ (FQDN و IP) لاصتال ناوع 2.
 لذلا لاصتال ناوع نم اضيأ تاناي ب ل رورم ة ك ر م داخ ق قحتي ، ة ق ث ل نا زخم لى ة فاض ال اب

مماظنلا نمض CUCM دادع| دنع ، لاثملا ليلبس ىلع . هلعأ نم بلطلال ميققتب MRA ليلمع موقيل
> كلذ نع Expressway-C نلعي ، IP (10.48.36.215) ناونع مادختساب كب صاخلا CUCM مداخ
اذهب (Expressway-C لالخنم ليلكولا) ليلمعلال نم ةقحلال تابطلال فادهتسا لمثيوليلمعلال
ناونعلال .

مميوكلكلذك TLS نم ققحتلال لشفيل ، مداخلا ةداهش نمض اذهل لاصلتالا ناونع نوكلال ام دنع
لالثملا ليلبس ىلع MRA لىل لوخدلال ليجستيف لشفل هنع جتنيل 502 أطخلاقلا

<#root>

```
2022-07-11T19:49:01.472+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,472" Module="network"
HTTPMSG:
|GET http://vcs_control.steven.lab:8443/c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw/cucm-uds/user/emusk/
...
```

```
2022-07-11T19:49:01.478+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,478" Module="network"
2022-07-11T19:49:01.478+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,478" Module="network"
HTTPMSG:
|GET /cucm-uds/user/emusk/devices?max=100 HTTP/1.1
...
```

```
2022-07-11T19:49:01.491+02:00 vcsc traffic_server[3916]: [ET_NET 2]
```

WARNING: SNI (

10.48.36.215

) not in certificate

. Action=Terminate server=10.48.36.215(10.48.36.215)

```
2022-07-11T19:49:01.491+02:00 vcsc traffic_server[3916]: [ET_NET 2]
```

ERROR: SSL connection failed for

'10.48.36.215': error:1416F086:

SSL routines:tls_process_server_certificate:certificate verify failed

لىل c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw (base64) ةمچرت ممتت شيل
10.48.36.215 وحن لاصلتالاب موقيل نا بجيل هناعظي يذلاو . steven.lab/https/10.48.36.215/8443
ةداهش يوتحتال ، طاقتلال مزحيف حضوم وه امك . cucm.steven.lab نم اللب لاصلتالا ناونعك
أطخاللاقلا لمثيوليلمعلال (SAN) نيلختلال ةكبش يليل IP ناونع ىلع CUCM TOMCAT .

ةلوهسب اهتحص نم ققحتلال ةيفيل

ةليلتاللا تاوطخال مادختساب ةلوهسب كولسلا اذهل ريلغيت ديرت تنك اذا ام ققحتلال كنكميل :

1. نيلم عم ايلجذومن) C و Expressway-E (مداوخ) مداخ ىلع يصيخشتلال ليلجستلال ادب .
ةومجم ماظن ةلاح يليل (صيصيخشتلال ليلجستلال > تاصيخشتلال > ةنايصلال نم TCPDumps)
(ةيساسال ةدقعلال نم هللغشتلال ايلفانوكيل

2. ةيلقرتلال دعب ةلطمعلال ةليلظولال رابلخال وأ MRA لىل لوخدلال ليلجستلال لواح .

3. مق م ث C و Expressway-E (مداوخ) مداخ لى ع يصيخ شت ل ليجست ل ل ش في ى تح رطت نا 3. نم ةدق لك نم تال ج س ل ا عمج نم دكأت ، ةومجم ةلا ح في) يصيخ شت ل ل ليجست ل ل ا فاق ي ا ب (ي در ف لك شب ةومجم ل

4. اه ل ل ح ت و نواع ت ل ل لولج ل ل لجم ةا د ا لى ع ةدوجوم ل ل تال ج س ل ل ليجست ل ل

5. ر ي غ ت ل ل ا ذب ةق ل ع ت م ل ل ا ط خ ل ل ا و ر ي ذ ح ت ل ل ا ط و ط خ ل ل ا ط ق ت ل ل ا ه ن ا ف ، ةك ل ش م ل ل ا ه ذ ه ت ه ج ا و ا ذ ا ل ل ا ق ر ث ا ت م ل ل ا م دا و خ ل ل ا نم م دا خ ل ل ا ل

The screenshot shows the Cisco Collaboration Solutions Analyzer Log Analyzer interface. The main content area displays a 'Diagnostic overview' with a list of 'Issues found'. The selected issue is 'Traffic Server Enforces Certificate Validation of UCM/IMSP/Unity nodes for MRA services [CSCw69661]'. The detailed view for this issue includes:

- Description:** The tomcat(-ECDSA) certificate of the following CUCM / IMSP / Unity nodes is not trusted by the Expressway-C: cucm.steven.lab, 10.48.36.215. This leads to MRA login issues.
- Condition:** Expressway-C X14.2 and higher versions running MRA services are affected.
- Further information:** Starting with version X14.2 and higher (due to CSCw69661), the Expressway-C traffic server will do a TLS certificate check on the CUCM / IMSP / Unity tomcat(-ECDSA) certificates irrespective of the configuration of TLS Verify Mode set when discovering each of those servers.
- Action:**
 - Update the Expressway-C trust store with the CA certificates that signed the tomcat(-ECDSA) certificates of CUCM / IMSP / Unity nodes.
 - Make sure that the SAN entries of the tomcat certificates contain the IP or FQDN (as shown from the log snippet below) of the respective servers how they are announced over.

If you are not able to update the certificates or trust store immediately, you can also apply the workaround on the CLI of the Expressway-C with the following command:
`xConfiguration EdgeConfigServer VerifyOriginServer: Off`
- Snippet:**

```

2022-07-11T19:33:06.740+02:00 vscs:traffic_server[3936]: [ET_NET 0] WARNING: Core server certificate verification failed for (10.48.36.215). Action:Terminate Error=self signed certificate in certificate chain server=10.48.36.215(10.48.36.215) depth=1
2022-07-11T19:33:06.740+02:00 vscs:traffic_server[3936]: [ET_NET 0] ERROR: SSL connection failed for "10.48.36.215": error:1416F080:SSL routines:tls_process_server_certificate:certificate verify failed
2022-07-11T19:33:06.160+02:00 vscs:traffic_server[3936]: [ET_NET 1] WARNING: Core server certificate verification failed for (cucm.steven.lab). Action:Terminate Error=self signed certificate in certificate chain server=cucm.steven.lab(10.48.36.215) depth=0
2022-07-11T19:33:06.160+02:00 vscs:traffic_server[3936]: [ET_NET 1] ERROR: SSL connection failed for "cucm.steven.lab": error:1416F080:SSL routines:tls_process_server_certificate:certificate verify failed

```

CA صيخ شت عي قوت

The screenshot shows the Cisco Collaboration Solutions Analyzer Log Analyzer interface. The main content area displays a 'Diagnostic overview' with a list of 'Issues found'. The selected issue is 'Traffic Server Enforces Certificate Validation of UCM/IMSP/Unity nodes for MRA services [CSCw69661]'. The detailed view for this issue includes:

- Description:** The tomcat(-ECDSA) certificate of the following CUCM / IMSP / Unity nodes is not trusted by the Expressway-C: 10.48.36.215. This leads to MRA login issues.
- Condition:** Expressway-C X14.2 and higher versions running MRA services are affected.
- Further information:** Starting with version X14.2 and higher (due to CSCw69661), the Expressway-C traffic server will do a TLS certificate check on the CUCM / IMSP / Unity tomcat(-ECDSA) certificates irrespective of the configuration of TLS Verify Mode set when discovering each of those servers.
- Action:**
 - Update the Expressway-C trust store with the CA certificates that signed the tomcat(-ECDSA) certificates of CUCM / IMSP / Unity nodes.
 - Make sure that the SAN entries of the tomcat certificates contain the IP or FQDN (as shown from the log snippet below) of the respective servers how they are announced over.

If you are not able to update the certificates or trust store immediately, you can also apply the workaround on the CLI of the Expressway-C with the following command:
`xConfiguration EdgeConfigServer VerifyOriginServer: Off`
- Snippet:**

```


2022-07-11T19:49:01.533+02:00 vscs:traffic_server[3936]: [ET_NET 2] WARNING: SAN (10.48.36.215) not in certificate. Action:Terminate server=10.48.36.215(10.48.36.215)
2022-07-11T19:49:01.533+02:00 vscs:traffic_server[3936]: [ET_NET 2] ERROR: SSL connection failed for "10.48.36.215": error:1416F080:SSL routines:tls_process_server_certificate:certificate verify failed

```

لحل

يذلا عارج ال دم تعي .ديج لكشب لم تعي TLS نم ققحت ال نأ نم دكأ ال وه يدم ال ليوط ل حل
ة.ضور عم ال ريذحت ال ة لاسر يلع هذيفنت متيس

ل يس اساس ال مداخل ة داهش نم ققحت ال لشف :ريذحت ال ة طحال م دنع (<server-FQDN-or-IP>).
إلإ =End Error=Self Signed Certificate Server=cucm.steven.lab(10.48.36.215) depth=x
إم .كلذل اق فو Expressway-C مداوخ يلع ة قث ال نزخم شيذحت يلى جاتحت م ث ،
مادختساب وأ (0 > قمع ال) ة داهش ال هذه يلع تعقو وي تلل ق دصم ال عجرم ال ة لس لس مادختساب
دكأ .ة قث ال ق دصم ال عجرم ال ة داهش > ني مأل ال > ة نا يصل ال نم (0 = قمع ال) ايتا ذة ة قوم ة داهش
دعب نع ة داهش ال عي قوت وه رخأ را يخ .ة ومجرم ال ماظن ي ف مداخل لك يلع عارج ال اذ هذيفنت نم
Expressway-C ة قث نزخم ي ف فور عم ق دصم عجرم ة طساوب

 يلع ايتا ذة ة قوم) ني تفلتخم ني ت داهش لي محتب Expressway حمست ال :ة طحال م
(CN) كرتشم ال مس ال س فن امه ي دل Expressway ل نامض ال نزخم يلى (لا ثم ال لي بس
لاق ت ال اب مق ،رم ال اذ ه حي حصت ل [CSCwa12905](#) Cisco نم اطاخ ال ا حي حصت فر عم ل اق ب ط
ة داء | كنكم ي شي 14 رادص ال ال CUCM ة قرت وأ CA نم ة قوم ال ا داهش ال يلى
CallManager و Tomcat ل (ايتا ذة ة قوم ال) ة داهش ال س فن مادختسا

ريشي هنإف ،ة داهش ال ة لاسر ي ف دوجوم ريغ (<server-FQDN-or-IP> SNI :ريذحت ال طحالت ام دنع
في يكت ام | كنكم ي .اهم ي دقت مت ي تلل ة داهش ال ي ف دوجوم ريغ مداخل اذ ه IP وأ FQDN نأ يلى
> ماظن ال يلع CUCM لثم) ني وكت ال لي دعت كنكم ي وأ تامول عم ال هذه ني مضت ل ة داهش ال
يحت Expressway-C مداخل يلع ني وكت ال شيذحت م ث (مداخل ة داهش ي ف دوجوم عي ش يلى مداخل
رابتع ال ي ف هعضو متي

ة ل ص تا ذ تامول عم

X14.2.0 ل بق ق باس ال كولس ال يلى عوجرل قثوم وه امك ل حل ق ي ب طت وه ل ج ال ري صق ل حل
مادختساب Expressway-C مداخل دق يلع (رم او ال رطس ة ه جاو) CLI لال خ نم كلذ ذيفنت كنكم ي
اثيذح هم ي دقت مت يذلا رم ال

xConfiguration EdgeConfigServer VerifyOriginServer: Off

تامول عم ال ة ينقت

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد وء مء مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظءالم ءرء. ةصاءل مءءب
Cisco ءلءت. فرءم مچرت مءم دقء ءلءل ةءفارتءال ةمچرتل عم لءل او
ءل ءمءءءء ءوچرلاب ءصوء وءءامچرتل هذه ةقءن ءءءل وءءس م
Systems (رفوتم طبارل) ءلصأل ءزءلءنءل دن تسمل