

ةكرح مداخ ةداهش نم ققحتلا عاطخأ فاشكتسأ MRA تامدخل Expressway Traffic Server رورم اهحالصإو

تايوتحملإ

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[هب قوئوملا قدصملا عجرملا قللس](#)

[CN وأ SAN صحف](#)

[كولسلل ريغت](#)

[X14.2.0 نم لقألا تارادصلإا](#)

[شخألا تارادصلإا و X14.2.0 نم تارادصلإا](#)

[اهحالصإو تاهوي رانيسلا فاشكتسأ](#)

[هب قوئوم ريغت ديعللا ةداهشلا عي قوتب ماق يذلا قدصملا عجرملا 1.](#)

[ةداهشلا يف دوجوم ريغت \(IP وأ FQDN\) لاصتالا تاونوع 2.](#)

[ةلوهسب اهتخص نم ققحتلا ةيفيك](#)

[لحلإا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ىلعألا تارادصلإا و X14.2.0 نم Expressway تارادصلإا ىلع كولسلل ريغت دنتسملا اذه فصى
Cisco نم عاطخألا حيحصت فرع م وأ [CSCwc69661](#) Cisco نم عاطخألا حيحصت فرع م
[CSCwa25108](#).

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

- Expressway ل يساسألا نيوكتلا
- MRA يساسألا نيوكتلا

ةمدختسملا تانوكملا

X14.2 رادصلإا ىلع Cisco Expressway ىلإ دنتسملا اذه يف ةدراولا تامولعمل دنتست

ثدحأل تارادصلإاو

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجأل نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ مت تناك اذإ .(يضايرتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجأل عيمج تادب رمأ يأل لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا دي ق كتكبش

ةيساسأ تامولعم

Cisco بملعم كولسلا يف رييغتلا اذه عم [CSCwc69661](#) id قب

Cisco بملعم [CSCwa25108](#) id قب

Cisco Unified ةداهش نم ققحتلا ءارجإ Expressway ةصنم ىلع رورملا ةكرح مداخ موقى ، دقعو Cisco Unified Instant Messaging & Presence (IM&P) و Cisco Unified Communications Manager (CUCM) لشف تالاح ثودح ىلإ رييغتلا اذه يدؤي دق .(MRA) Remote Access و Mobile تامدخل Unity مداخ .يساسأل Expressway ماظن ىلع ةيقرت ءارجإ دعب MRA ىلإ لوخدلا ليچست يف

نامأ مدختسي نمأ لاصتا لوكوتورب وه (HTTPS) نمآلأ يبعشتال صنلأ لقن لوكوتورب
مادختساب ةنمآلأ ةانقلأ هذه عاشنإب موقوي وهو. لاصتالأ ريفشتل (TLS) لقنلأ ةقبط
ةفرعمل) ةقداصلأ :ضرغ نانثإ مداخ اذه. TLS ةحفاصلأ يف اهلداپت متي يتلأ TLS ةداهش
ليخدلأ تامجه ةقداصلأ يمح. (ريفشتلأ) ةيصوصخلأ (هب لصتت يذلأ ديعلل فرطلأ
تالاصتالأ اب ثبعلأ وتصنتلأ نم نيجمجاهملا ةيصوصخلأ عنمتو.

لكلأصتا نم دكأتالأب كل حمسيو ةقداصلأ ني ع يف (ةداهشلأ) TLS نم ققحتلأ عارجا متي
:نيي درف ني رصنع نم ققحتلأ فلأتيو. نميألأ ديعلل فرطلأب

1. (CA) هب قوثلأ قيديصتالأ عجرم ةلسلس
2. (CN) عئاشلأ مسالأ وأ (SAN) عوضوملل ليذلأ مسالأ

هب قوثلأ قديصملا عجرملا ةلسلس

نوكت نأ مزلي، CUCM / IM&P / Unity اهللسري يتلأ ةداهشلأ يف Expressway-C قثت يكل
قثت يذلأ (CA) يلألأ (رذجلأ) قديصملا عجرملا يلأ ةداهشلأ كلت نم طابترأ عاشنإ يلع ةرداق
ةداهشب تانايك ةداهش طبرت يتلأ تاداهشلأ نم يمره لسلست وهو، طبارلأ اذه يمس. هيف
لك يوتحت، هذه ةقثلأ ةلسلس نم ققحتلأ نم نكمتلل. ةقث ةلسلس، رذجلأ قديصم عجرم
("لجأ نم رداصلأ" وأ) عوضوملأ ("ةطساوب رداصلأ" وأ) رديصلأ : نيلقح يلع ةداهش

لقح يف Expressway-C يلأ للسري يذلأ CUCM نم دحاو لثم، مداخلأ تاداهش نمضتت
CN يف (FQDN) لمكالأب لهؤملأ لاجملأ مسا صاخ لكشب "عوضوملأ"

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

لقحل CN ةمس يف FQDN يلع يوتحي. CUCM CUCM.vngtp.lab ل مداخ ةداهش يلع لاثم
نأ ىرن نأ اننكمي امك ... (L) عقوملأ، (ST) ةلاحلأ، (C) ةلودلأ لثم ىرخأ تامس عم عوضوملأ
vngtp-active-DIR-CA. يمس يف قديصم عجرم لبق نم (اهرادصا) اهميلست متي مداخلأ ةداهش

رادصإب (رذجلأ قديصملا عجرملا) يوتسملأ ةيلال ةقديصملا عجارملا موقت نأ اضيأ نكمي
امهل عوضوملأ و رديصلأ نأ ىرن، هذه رذجلأ قديصملا عجرملا ةداهش يف. اهسفن فيرعتل ةداهش
: ةميقلا سفن

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

اهسفن فيرعتل ي رذجلأ قديصم عجرم لبق نم اهميلست متي ةداهش اهنإ

،كلذ نم الدب. ةرشابم مداخلأ تاداهش رذجلأ CA صيخارت رديصتال، ةيجزومللأ تالاحلأ يف
مسا كلذ دعب ةداحلأ يونلأ نم ىرخألأ عاونألأ هذه يلع قلطيو. ىرخأ CAS ل تاداهش رديصت اهنإف
تاداهش وأ تاداهش رادصإب اهرودب ةطيسولأ CAS موقت نأ نكمي. ةطيسوملأ ةيججرملأ يونلأ

مداخل عداش رادصا متي شيح ةلاح اني دل نوكي نأ نكمي .ىرخأال ةطيسول CAS ل ةرشابم مداخل عجرم ل لصحي ىتح .اذكهو طسوتم CA 2 نم ةداش ىلع لصحي هرودب يذل ،طسوتم CA 1 نم رذجل قدصم ل عجرم ل نم ةرشابم هتداش ىلع اريخأ طيسول قدصم ل :

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

Root CA certificate :

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

Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-C

ةرداق نوكت نأ بجي ،CUCM اهل سر ي يتل مداخل ةداش ب Expressway-C قثت نأ لجأ نم ،نآل قيقحتلو .يسيسي قدصم عجرم ةداش ىتح مداخل ةداش نم ةقثل نم ةلسلس ءانب ىلع قدصم ل عجرم ل تاداش عي مج كلذكو رذجل قدصم ل عجرم ل ةداش ليحت ىل جاتحن ،كلذ ردصأ دق رذجل قدصم ل عجرم ل ناك اذا لالحا سيل وهو ،تاداش ي أ كانه تناك اذا) ةطيسول Expressway-C ب صاخال قيثوتل نزخم ي ف (CUCM مداخل ةداش ةرشابم

 نم ةلسلس ءانب امه يلع لهسي عوضوم ل او ردصم ل يلحق نأ نم مغرل ىلع :ةظالم ي ف نيلقحل نيذه مدختست ال CUCM إف ،اهتارق نكمي ةيرشب ةقيرطب ةقثل فرعم"و" X509v3 عجرم ل جاتفم فرعم" يلحق مدختسي ه إف ،كلذ نم الدبو .ةداش ل نافرم ىلع حي تافم ل هذه يوتحت .ةقثل ةلسلس ءانب ل X509v3 عوضوم ل جاتفم كانه نوكت نأ نكمي : ردصم ل/عوضوم ل لوقح مدختست مث ةقد رثكأ نوكت تاداش ل لدحاو لازت الو امه نم ةدحاو ةيحالص تهتنا نكل ردصم ل/عوضوم ل لوقح سفنب ناتداش ثيحب X509v3 عوضوم ل حي تافم ل فلتخم فرعم ني ف رطال الك ىدل نوكتسي .ةحلاص ةحيحصل ةقثل ةلسلس ديدحت ىلع ارداق CUCM لظي

Cisco نم عاطخأل حي حصت فرعم ل اقفو كلذ مغر Expressway ةلاح تسيل هذه

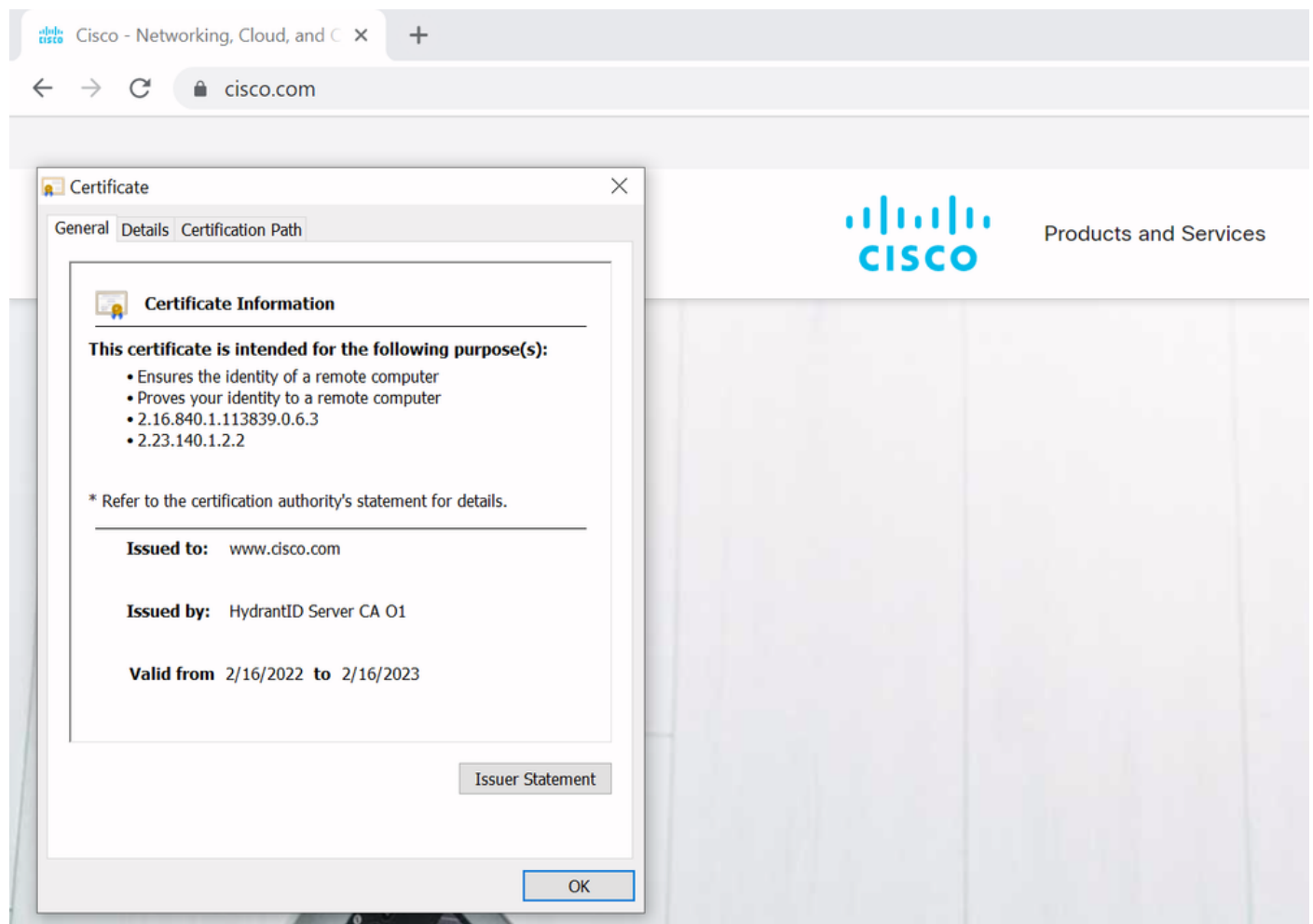
ليبس ىلع ايتاذ ةعقوم) ني تفلتخم ني تداش ليحت نكمم ل ريغ نمو [CSCwa12905](#) ةقيرطال (CN) كرتشم ل مسال س فن اهل يتل Expressway ل ةقثل نزخم ي ف (لالثم ل ةماع ءامسأ مدختست نأ وأ تاداش ل عي قوتب CA ب موقت نأ يه ،اذه ىلع حي حصت ل لزيم لالخن نم لمحتحم ل نم) ةداش ل س فن امئاد مدختست اهنأ ىرت نأ وأ هل ةفلتخم (CUCM 14) ي ف ةداش مادختسا ةداعا

CN وأ SAN صحف

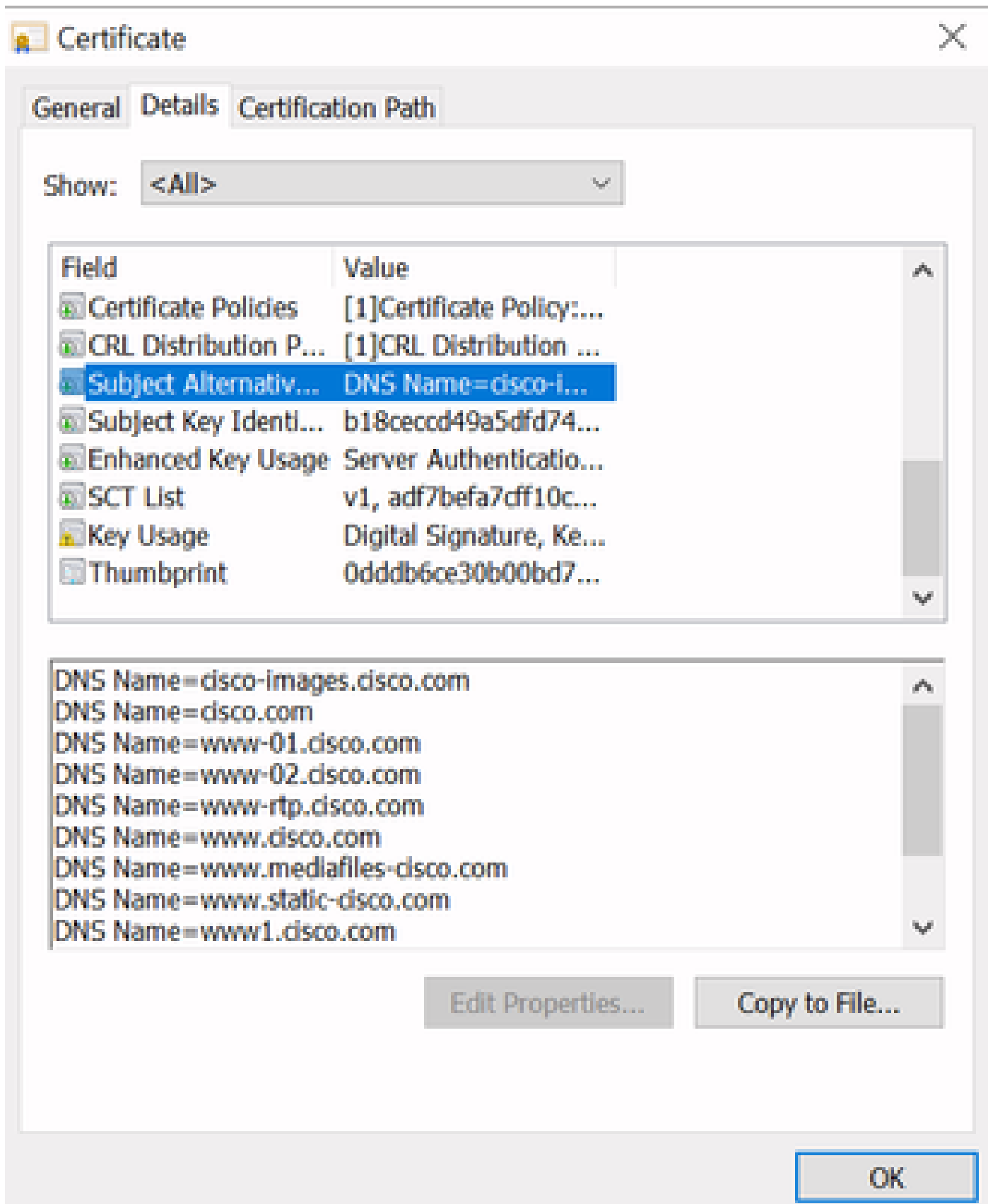
لبق نم اه عي قوت مت ةداش هي دل صخش ي إف كلذ عمو ،قيثوتل نزخم نم ققحت 1 ةوطخل فاك ريغ اذه نأ حضاولا نمو .تقولو كلذ ي ف احلاص نوكتسي قيثوتل نزخم ي ف قدصم عجرم

حيصل المداخل لعفالب وه ب لصتت يذل مداخل نا نم ققحتي يفاضل ققحت كانه ،كلذل ه.لجأ نم بلطلال مي دقت مت يذل ناو نعل الى اذانتسا كلذب موقوي.

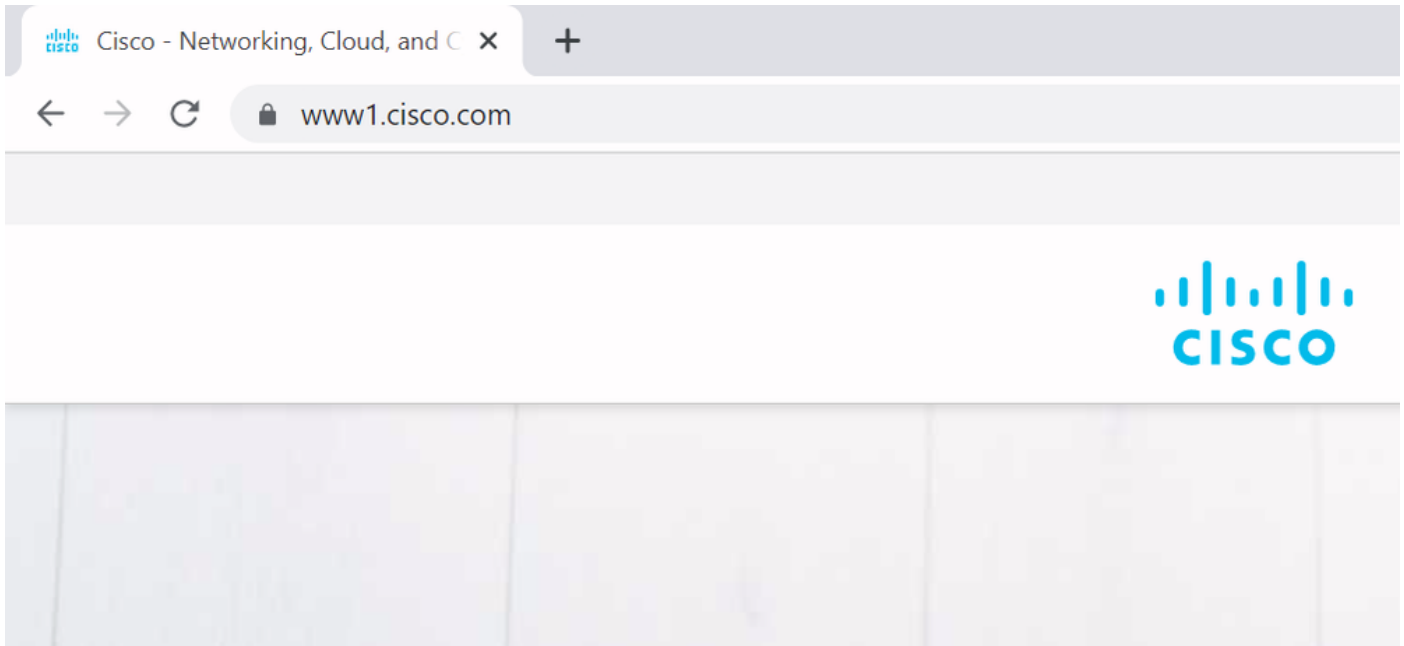
تمق اذا .لاثم لالخ نم اذه ي ف رظنن انوعد اذل ،كح ف صتم ي ف ث دحت تايلمعل نم عونل س فن ه تلخدأ يذل URL ناو نعل راو جب لف قق نوق ي أ ى رتس <https://www.cisco.com> الى ضارعت سالب (لوالا مسقلال نم) CA ة قث ة لسلس نم لك الى اذه دن تسي .ه ب قو ثوم لاصتا ه نا ينع ي امم ة نوق ي أ الى ع ر قن ب ضرعت سملال قير ط نعل) ة داهشلال انحت ف اذا . CN وأ SAN صحت ف الى كلذل و الى ع طوب ضم ('الى ه رادصا مت' لقحلال ي ف رهظي) عئاشلال مسلال نا ى رتس ،(لفقلا نكمي ة قير طلال ه ذه ب .ه ب لاصتالا ان درأ يذل ناو نعل عم امامت قفاوتي وه www.cisco.com عي قوتب ماق يذل ق دصملا عجرملا ي ف ق ثن انال) حيصلال مداخلالب انلاصتا نم دكأتلا (ة داهشلال ميلست لب ق ققحتلال عارجاب موقوي يذلاو ة داهشلال).



لكشب (SAN) نيزختلا ة قطنم ة كبش تال اخدا الى عو ة داهشلال لي صافات الى عال طالال دن ع نيزختلا ة قطنم ة كبش تال اخدا ضعب الى ة فاضالب رركتي عي شلال س فن نا طحالن ، صاخ ي:رألا (FQDN)



رهظيس ،لاثملا لىبس ىلع <https://www1.cisco.com> ب لاصتالا بلطن ام دنع هنا ينعى اذهو (SAN) نىختلا ةكبش تالخدإ ي ف 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 يذل CA يف قثي ال هنأل انمآ الاصتا رهطي ال هنإف ،(<https://72.163.4.161>) هانمدختسأ يذل (72.163.4.161) ناونع ال ىلع يوتحي الو ،انل ةمدقملا ةداهشل نكلو مداخلاب لاصلال.

TLS تالاصتا ىلع هنىكمت كنكمي ،لاح يآ ىلع ،دادعإلا اذه زواجت كنكمي ،ضرعتسملا يف ىلع كب ةصاخلا تاداهشل يوتحت نأ مهمل نم ،كلذل .فافتلالاب حامسلا متي ال ثيحب اب لاصلال اهمادختسال ديعبل فرطال ططخي يتل ةحيحصلا SAN وأ CN عامسأ.

كولسل ريغت

هاجت ةعيرسلال قرطال ربع HTTPS تالاصتا نم ديدعلا ىلع ريبك لكشب MRA تامدخ دمتعت

صاخال ءحىحصلا تامولعمل عمجل وءحىحص لكشب ءقءاصم لل CUCM / IM&P / Unity مءاوءى 6972 و 8443 ذفانم الرب ءءاع لاصءالا اءه ءءءى. لوءءلا لىءسءب موءى ىءلا لىمءلاب

X14.2.0 نم لقأل اءاراءصلا

ىءل Expressway-C لىء ءوءومل رورمل ءءرء مءاوء قءءءى مل، X14.2.0 نم لقأل اءاراءصلا ىف ءق. ءىءبل فرءلا ءطساوب اءمىءقء مء ىءلا ءءاهشل نم هءه ءنمآل HTTPS ءالاصءل ءلءاعى لالء نم TLS ءءاهش نم قءءءلل رايء لءنه، MRA نىوءء ىف. لىءءلا ءامءه ىل اءه ىءوى CUCM / IM&P / Unity اما ءفاضاوب موءء امءنع "لىءشء" ىل "TLS نم قءءءلل ءضوء" نىوءء مءاوء / ءءاوءلل ءمءء ءوءءو IM / ءءومل CM مءاوء > ءءومل ءالاصءالا > نىوءءلل ءءل ءءل رىشى امم، لاءمء ءلصل ءاءءامولعمل ءبرمو نىوءءلل رايء ضرع مءى. ءءولل لاصءا اءامو ءءاهشل ءىءالصل ىل ءفاضاوب (SAN) نىءءلل ءكبش ىف IP وأ FQDN نم قءءءى هئاً ءقء قءصم ءءرم لبق نم ءءءوم ءءاك.



Cisco Expressway-C

[Status >](#) [System >](#) [Configuration >](#) [Applications >](#) [Users >](#) [Maintenance >](#)

Unified CM servers You are here: [Configuration >](#)

Unified CM server lookup

Unified CM publisher address

cucmpub.vngtp.lab

Username

* administrator i

Password

* i

TLS verify mode

On i

Deployment

Default deployment i

AES GCM support

Off i

SIP UPDATE for session refresh

Off i

ICE Passthrough support

Off i

Save

Delete

Cancel

ىف سىل و CUCM / IM&P / Unity مءاوء فاشءءا لالء نم طقف اءه TLS ءءاهش نم قءءءلل مءى نىوءءلل اءهل لولأل ءءأمم. MRA ءانءاً مءاوءل فلءءم نع مالعءسالا هىف مءى ىءلا ءقول ءاءع ءءص نم قءءءى ال. هءفاضاوب موءء ىءلا رشانل ناوئل طقف هنم قءءءى هئاً وه ءرءشمم ءءقء ءامولعمل ءءرءسء هئاً ءىء ءىءص لكشب ءرءشمم ءقء ىل ءءاهشل ام نأ وه، اءى نىوءءلل اءه نم ىنءال بىءلاو. رشانل ءءقء ءانءب ءءاق نم (IP وأ FQDN) ىءلا رشانل ناوئل نع لاصءالا ءامولعمل فلءءم نأ نءمى ءىء MRA ءالمءل هنم نالءال مءى مءاوء > ماظن ءءل، CUCM ىف، لاءممل لىبس ىلء Expressway-C نىوءء ىف هءضوء مءمءى و (لاءممل لىبس ىلء 10.48.36.215) IP ناوئل مءاءءساوب مءاوءل نع نالءال ءنءمى ءنءمى ءلء ءمو (لىءول Expressway لاصءا ربء) MRA ءالمءل لبق نم ءلء ءعب اءه مءاءءساوب

عداهش نأ ضارتفاب cucm.steven.lab. نم FQDN مادختساب Expressway-C ىلع CUCM ةفاضإ كلذ دعب، IP ناونعك سيلاو SAN ىلا لاخداك cucm.steven.lab ىلع يوتحت CUCM نم tomcat MRA ءالمع نم ةلعلفلا تالاصتالا نكلو 'On' ىلع 'TLS Verify Mode' عم فاشتكالال حجني TLS. نم ققحتلا لشف تالالابو IP وأ فلتخم FQDN فدهتست نأ نكمي

ثدحال تارادصلال او X14.2.0 نم تارادصلال

بلط لكل TLS ةداهش نم ققحتلا ىلع Expressway مداخلمعي، ادعاصف X14.2.0 رادصلال نم متي ام دنع اضيا اذه ذفنت اهنأ ينعي اذهو. تانايبال رورم ةكرح مداخل لالخم نم هؤارج متي HTTPS ام دنع CUCM / IM&P / Unity دقع فاشتكالال ءانثأ "فاقيإ" ىلع "TLS نم ققحتلا عضو" نيينعت نأ نكمي يذال بلطلال لشفو TLS لاصتال ديكتأ متي ال، ءحصلال نم ققحتلا ةللمع حجنت ال لوخدل ليجست لشف وأ لشفال زواجت وأ راركتال لكاشم لثم فئاظولال دقف ىلا يدؤي ال، "لغشت" ىلع "TLS نم ققحتلا عضو" نيينعت عم اضيا. لاثمال ليبس ىلع لمالكال اقحال لاثمال يه هيلع صوصنم وه امك حيحص لكشب تالاصتالا عيجم لمعت نأ نمضي

وه امك CUCM / IM&P / Unity دقع نم عيبرسال قيرطال اهصحفي يتلا ةقيقدل تاداهشلال درت [MRA ليلد](#) مسق يه حضوم

ي هميدقت مت ريغت اضيا كانه، TLS نم ققحتلا ىلع يضايرتفالا دادعإلا ىلا ةفاضالاب دمتعي يذالو، ريفشتلال ةمئاول فلتخم ليضفت بئترت نع نلعي نأ نكمي يذالو X14.2 دعب ةعقوتم ريغ TLS تالاصتال ثودح يه كلذ ببست ي دق. كب صاخلا ةيقرتال راسم ىلع Cisco Tomcat وأ Cisco ةداهشل ةبولطمال ةيقرتال لبق هنأ ثدحي دق هنأل جمانربال ةيقرت نكلو (ECDSA ةيمزراوخل ةلصفنم ةداهش ىلع يوتحي رخآ جتنم يا وأ) CUCM نم Cisco CallManager (RSA نم ايلعف انام رثكالال ريفشتلال ريغتم وهو) ECDSA ريغتم بلطي هنإف ةيقرتال دعب فلتخم CA لبق نم Cisco CallManager-ECDSA وأ Cisco Tomcat-ECDSA تاداهش عيقتوت نكمي (يضايرتفالال). ايتاذ ةعقومتال لازام تاداهش وأ

ةيقرتال راسم ىلع دمتعي هنأل امئاد كب ةلص اذ اذه ريفشتلال ليضفت رمأ ريغت نوكتي ال > ةنايصلال نم ىرت نأ نكمي، راصتخاب Expressway X14.2.1 [رادصلال تاطحال](#) نم حضوم وه امك "ECDHE-RSA-AES256-GCM-SHA384" دادعإ ىلا يدؤي ناك اذا ام تاريشفشمال نم دحاو لكل تارشفشمال > نامأل ريفشت ىلع ثدحال ECDSA ريفشت لصف يهنإف، كلذك نكي مل اذالو. ال م "GCM-SHA384:." RSA. دئدنع ىلعأ ليضفت هيدل يذال RSA عم قباس كولس كيذل نوكتي سف، كلذك ناك اذا

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**).

ليصف تالاب امه تي طغت متيو، وييرانيسلا اذه يه TLS نم ققحتلا لشفل ناتقيرط كانه اقحال:

ه ب قوئوم ريغ ةديعبال ةداهشلال عيقتوتب ماق يذال قدصم العجرم ال 1.

ايتاذ ةعقومتال ةداهش أ.

فورعم ريغ قدصم العجرم لبق نم ةعقومتال ةداهشلال ب.

عداهشال ي ف (IP وأ FQDN) لاصتال ناو ن ع يوتحي ال 2.

اهالصال و تاهوي راني سلال فاشكتسا

ليجست لش ف ثيح ةيلمعم ةئي ب ي ف اهاباشم وي راني س ةيلاتال تاهوي راني سلال رهظت هبشال هجوا ي ف كرتشت ثيح X14.2 الى X14.0.7 نم Expressway ةيقرت دعب MRA الى لوخدلال ليجستال ةطساوب طقف تالجلال عي مجت متي .ةقدلال فالتخا نم مغرلا يلع ،تالجلال ي ف ادب مت يذلا (ي صيخششتال ليجستال > تاصيخششتال > ةنايصال نم) ي صيخششتال مل MRA الى لوخدلال ليجست لش ف دعب هفاقي متو MRA الى لوخدلال ليجست لش ف هليغشت هل ي فاضا اعاطخا حي حصت ليجست ي ا ني كمت متي .

ه ب قو ثوم ريغ ةديعبال عداهشال عي قوتب ماق يذلا قدصم ال عجرم ال 1.

ه ب قو ثومال نزخمال ي ف نمضم ريغ قدصم عجرم لش ف نم دعب نع عداهشال عي قوت نكمي ال (اضي ا قدصم عجرم اهرهوج ي ف) ايتاذ ةعقوم عداهش نوكت نا نكمي وا Expressway-C مداخلل Expressway-C مداخل صاخال قي ثوتال نزخم ي ف اهتفاضل مت

ف CUCM (10.48.36.215 - cucm.steven.lab) 8443 ذفنمال يلع حي حص لكشب اهعم لماعتال متي (200 OK ةباجتسا) 6972 ذفنمال يلع (502 ةباجتسا) اطخا ثودح ي ف ببستت اهنكلو TFTP لاصتال

<#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 ققحتل نم Expressway-C نكمت مدع ققح ىلإ "ةداهشل ةحص نم ققحتل" أطخ ريشي ايتاذ ةعقوم ةداهش ىلإ ريشي هنأل ريذحتل رطس يف رهظي كلذب بسو. TLS ةحفاصم ةحص 0، نم ىلعأ قمعلل نوكي امدنع. ايتاذ ةعقوم ةداهش اهنإف، 0 ةئيه ىلع حصوص قمعلل ناك اذا فورعم ريغ قدصم عجرم لبق نم هعيقوت متي يلاتلابو تاداهش ةلسلس هل نأ ينعي اذهف (Expressway-C روظنم نم).

تالچس نم ةروكذمل ةينمزلل عباوطلال يف هعيجت مت يذل PCAP فلم يف رظنن امدنع و) cucm.ms.steven.lab CUCM- ةئيه ىلع CN عم ةداهشل مدقي CUCM نأ ىرت نأ كنكمي، صنلل ىلع Expressway-C ىلإ Steven-DC-CA لبق نم ةعقوم (SAN ةئيه ىلع cucm.steven.lab 8443 ذفنمل).

eth0_diagnostic_logging_tcpdump00_vscs_2022-07-11_16_55_44.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Top pane=0402

No.	Time	Source	Sr 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	C50		74	35622 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=878578435 TSecr=0 WS=128
4692	2022-07-11 16:55:25.916953	10.40.36.215	8443	10.40.36.46	35622	TCP	C50		74	8443 → 35622 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=343633238 TSecr=878578435 WS=128
4693	2022-07-11 16:55:25.916973	10.40.36.46	35622	10.40.36.215	8443	TCP	C50		66	35622 → 8443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=878578435 TSecr=343633238
4694	2022-07-11 16:55:25.917032	10.40.36.46	35622	10.40.36.215	8443	TLSv1.2	C50		583	Client Hello
4695	2022-07-11 16:55:25.918356	10.40.36.215	8443	10.40.36.46	35622	TLSv1.2	C50		1514	Server Hello
4696	2022-07-11 16:55:25.918390	10.40.36.46	35622	10.40.36.215	8443	TCP	C50		66	35622 → 8443 [ACK] Seq=518 Ack=1449 Win=64128 Len=0 TSval=878578457 TSecr=343633251
4697	2022-07-11 16:55:25.930409	10.40.36.215	8443	10.40.36.46	35622	TLSv1.2	C50		1478	Certificate, Server Key Exchange, Server Hello Done
4698	2022-07-11 16:55:25.930419	10.40.36.46	35622	10.40.36.215	8443	TCP	C50		66	35622 → 8443 [ACK] Seq=518 Ack=1853 Win=63488 Len=0 TSval=878578457 TSecr=343633251
4699	2022-07-11 16:55:25.940807	10.40.36.46	35622	10.40.36.215	8443	TLSv1.2	C50		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	C50		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	C50		66	35622 → 8443 [ACK] Seq=444 Ack=3095 Win=64128 Len=0 TSval=878578461 TSecr=343633256
4702	2022-07-11 16:55:25.943277	10.40.36.46	35622	10.40.36.215	8443	TLSv1.2	C50		2543	Application Data
4703	2022-07-11 16:55:25.943476	10.40.36.215	8443	10.40.36.46	35622	TCP	C50		66	8443 → 35622 [ACK] Seq=3095 Ack=3121 Win=35072 Len=0 TSval=343633256 TSecr=878578462
4707	2022-07-11 16:55:25.954796	10.40.36.215	8443	10.40.36.46	35622	TCP	C50		1514	8443 → 35622 [ACK] Seq=3095 Ack=3121 Win=35072 Len=1440 TSval=343633260 TSecr=878578462 [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	C50		66	35622 → 8443 [ACK] Seq=3121 Ack=4543 Win=64128 Len=0 TSval=878578473 TSecr=343633268
4709	2022-07-11 16:55:25.954861	10.40.36.215	8443	10.40.36.46	35622	TLSv1.2	C50		1257	Application Data
4710	2022-07-11 16:55:25.954873	10.40.36.46	35622	10.40.36.215	8443	TCP	C50		66	35622 → 8443 [ACK] Seq=3121 Ack=5734 Win=63488 Len=0 TSval=878578473 TSecr=343633268
4711	2022-07-11 16:55:25.955712	10.40.36.46	35622	10.40.36.215	8443	TLSv1.2	C50		97	Encrypted Alert
4712	2022-07-11 16:55:25.955750	10.40.36.46	35622	10.40.36.215	8443	TCP	C50		66	35622 → 8443 [FIN, ACK] Seq=3152 Ack=5734 Win=64128 Len=0 TSval=878578474 TSecr=343633268
4714	2022-07-11 16:55:25.956123	10.40.36.215	8443	10.40.36.46	35622	TLSv1.2	C50		97	Encrypted Alert
4715	2022-07-11 16:55:25.956170	10.40.36.46	35622	10.40.36.215	8443	TCP	C50		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	C50		66	8443 → 35622 [FIN, ACK] Seq=5765 Ack=3153 Win=35072 Len=0 TSval=343633269 TSecr=878578474
4717	2022-07-11 16:55:25.956252	10.40.36.46	35622	10.40.36.215	8443	TCP	C50		54	35622 → 8443 [RST] Seq=3153 Win=0 Len=0

Certificates (2423 bytes)

Certificate Length: 1587

Certificate: 308208030202728003020102013450000012205060503... (id-at-commonName=cucm.ms.steven.lab, id-at-organizationalUnitName=TAC, id-at-organizationName=Cisco, id-at-localityName=Olegien, id-at-stateOrProvinceName=Belgium, id-at-countryName=)

version: v3 (2)

serialNumber: 0x4500000122050605034608442000200000122

signature (sha1withRSAEncryption)

issuer: rdnsSequence (0)

validity

subject: rdnsSequence (0)

subjectPublicKeyInfo

extensions: 9 items

Extension (id-ce-extKeyUsage)

Extension (id-ce-keyUsage)

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: 9fba7f0741637a2a92071efb68f227b9cccf7c4a487822b...

Certificate Length: 910

Certificate: 30820803020272800302010201062170f3fc2939a004... (id-at-commonName=Steven-DC-CA, dc=steven, dc=lab)

Secure Sockets Layer

ةعقوم ةداهش اهنأ ىرت نأ كنكمي، 6972 ذفنمل ىلع ةمدقملا ةداهشل صحن امدنع نكلو ةراش EC- دادتما يطعي. CUCM-EC.Steven.lab ةئيه ىلع CN دادعا عم (هسفن رخصملا) ايتاذ CUCM ىلع اهدادعا مت يتلا ECDSA ةداهش يه هذه نأ ىلإ

No.	Time	Source	Srv port	Destination	Dest port	Protocol	OS	Length	Info
4730	2022-07-11 16:55:26.006608	10.40.36.46		11576 10.40.36.215	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	10.40.36.215		6972 10.40.36.46	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	10.40.36.46		31576 10.40.36.215	6972 TCP	C50		66	31576 → 6972 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=878578525 TSecr=343633320
4733	2022-07-11 16:55:26.007190	10.40.36.46		31576 10.40.36.215	6972 TLSv1.2	C50		583	Client Hello
4734	2022-07-11 16:55:26.016350	10.40.36.215		6972 10.40.36.46	31576 TLSv1.2	C50		1514	Server Hello, Certificate, Server Key Exchange
4735	2022-07-11 16:55:26.016391	10.40.36.46		31576 10.40.36.215	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	10.40.36.215		6972 10.40.36.46	31576 TLSv1.2	C50		499	Certificate Request, Server Hello Done
4737	2022-07-11 16:55:26.016419	10.40.36.46		31576 10.40.36.215	6972 TCP	C50		66	31576 → 6972 [ACK] Seq=518 Ack=1882 Win=63744 Len=0 TSval=878578535 TSecr=343633329
4738	2022-07-11 16:55:26.016793	10.40.36.46		31576 10.40.36.215	6972 TCP	C50		73	Alert (Level: Fatal, Description: Unknown CA)
4739	2022-07-11 16:55:26.016821	10.40.36.46		31576 10.40.36.215	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	10.40.36.46		31576 10.40.36.215	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	10.40.36.215		6972 10.40.36.46	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	10.40.36.46		31576 10.40.36.215	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	10.40.36.215		6972 10.40.36.46	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 16:55:26.017121	10.40.36.46		31576 10.40.36.215	6972 TCP	C50		54	31576 → 6972 [RST] Seq=525 Win=0 Len=0
4745	2022-07-11 16:55:26.017118	10.40.36.46		31576 10.40.36.215	6972 TLSv1.2	C50		583	Client Hello
4746	2022-07-11 16:55:26.024226	10.40.36.215		6972 10.40.36.46	31576 TLSv1.2	C50		1514	Server Hello, Certificate, Server Key Exchange
4747	2022-07-11 16:55:26.024265	10.40.36.46		31576 10.40.36.215	6972 TCP	C50		66	31576 → 6972 [ACK] Seq=518 Ack=1449 Win=64128 Len=0 TSval=878578543 TSecr=343633337
4748	2022-07-11 16:55:26.024298	10.40.36.215		6972 10.40.36.46	31576 TLSv1.2	C50		500	Certificate Request, Server Hello Done
4749	2022-07-11 16:55:26.024389	10.40.36.46		31576 10.40.36.215	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	10.40.36.46		31576 10.40.36.215	6972 TLSv1.2	C50		73	Alert (Level: Fatal, Description: Unknown CA)
4751	2022-07-11 16:55:26.024647	10.40.36.46		31576 10.40.36.215	6972 TCP	C50		66	31576 → 6972 [RST, ACK] Seq=525 Ack=1883 Win=64128 Len=0 TSval=878578543 TSecr=343633337
4752	2022-07-11 16:55:26.025159	10.40.36.46		31508 10.40.36.215	6972 TCP	C50		74	31508 → 6972 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=878578543 TSecr=0 WS=128

Secure Sockets Layer

- TLSv1.2 Record Layer: Handshake Protocol: Server Hello
- TLSv1.2 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
 - Certificate Length: 660
 - Certificates (600 bytes)
 - Certificate #1: 657
 - Certificate: 30820203082021480830202107470ee62271e3d1346... (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)
 - signedCertificate
 - version: v3 (2)
 - serialNumber: 02470ee62271e3d13461d09946f8a30f5d
 - signature (ecdsa-with-sha384)
 - signature (ecdsa-with-sha384)
 - issuer: rdnSequence (8)
 - rdnSequence: 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: rdnSequence (8)
 - subjectPublicKeyInfo
 - extensions: 5 items
 - Extension (id-ce-keyUsage)
 - Extension (id-ce-extKeyUsage)
 - Extension (id-ce-subjectKeyIdentifier)
 - Extension (id-ce-basicConstraints)
 - Extension (id-ce-subjectAltName)
 - Extension Id: 2.5.29.17 (id-ce-subjectAltName)
 - GeneralNames: 1 item
 - GeneralName: dnName (2)
 - dnName: cucm.steven.lab
 - algorithmIdentifier (ecdsa-with-sha384)
 - padding: 0
 - encrypted: 3064023021480830202107470ee62271e3d1346... (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)
 - TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange

> نبيم أتل تحت ةحضورم ل تاداهش ل إ رظن ل كنكمي ، Cisco Unified OS ةراد تحت ف و Tomcat ل ةفلتخم ةداهش رهظت . ل اثل م ل لبس ل ع انه حضورم وه امك تاداهش ل ةراد امن ب (Expressway-C ل ب ق نم ه ب ق و ثوم و) ع قوم Tomcat CA نو كي ثي ح Tomcat-ECDSA انه Expressway-C ل ب ق نم ه ب ق و ثوم ريغو اي اذ ة ع قوم Tomcat-ECDSA ةداهش

| Cisco Unified Operating System Administration | | | | | | | | | |
|--|-------------------|-----------------------------|-------------|----------|-----------------------------|----------------------------|------------|--|----------|
| For Cisco Unified Communications Solutions | | | | | | | | | |
| Navigation: Cisco Unified OS Administration | | | | | | | | | |
| Show 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 | | | | | | | | | |
| Certificate List (43 of 43) | | | | | | | | | |
| Find Certificate List where | Certificate | Common Name | Type | Key Type | Distribution | Issued By | Expiration | Description | Rows per |
| | authZ | AUTHZ_cucm.steven.lab | Self-signed | RSA | cucm.steven.lab | AUTHZ_cucm.steven.lab | 07/21/2038 | Self-signed certificate generated by system | |
| | CallManager | cucm.steven.lab | CA-signed | RSA | cucm.steven.lab | stevens-DC-CA | 07/13/2022 | Certificate Signed by steven-DC-CA | |
| | CallManager-ECDSA | cucm-ec.steven.lab | Self-signed | EC | cucm.steven.lab | cucm-ec.steven.lab | 02/18/2024 | Self-signed certificate generated by system | |
| | CallManager-trust | stevens-DC-CA | Self-signed | RSA | stevens-DC-CA | stevens-DC-CA | 06/01/2023 | Signed Certificate | |
| | CallManager-trust | NOMAT-AD-CA | Self-signed | RSA | NOMAT-AD-CA | NOMAT-AD-CA | 04/23/2028 | Signed Certificate | |
| | CallManager-trust | CAP-RTT-002 | Self-signed | RSA | CAP-RTT-002 | CAP-RTT-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-eb206408 | Self-signed | RSA | CAPF-eb206408 | CAPF-eb206408 | 04/12/2020 | Self-signed certificate generated by system | |
| | CallManager-trust | ms-AD2-CA-1 | Self-signed | RSA | ms-AD2-CA-1 | ms-AD2-CA-1 | 09/11/2024 | vnpq-CA | |
| | CallManager-trust | CAP-RTT-001 | Self-signed | RSA | CAP-RTT-001 | CAP-RTT-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 | NOMAT-CA-10 | 08/11/2027 | Signed Certificate | |
| | CallManager-trust | Cisco_Root_CA_H2 | Self-signed | RSA | Cisco_Root_CA_H2 | Cisco_Root_CA_H2 | 11/12/2027 | 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_SU01_CA | CA-signed | RSA | ACT2_SU01_CA | 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 | vnpq-ACTIVE-ORR-CA | Self-signed | RSA | vnpq-ACTIVE-ORR-CA | vnpq-ACTIVE-ORR-CA | 02/10/2024 | VNPQ-CA | |
| | CallManager-trust | Cisco_Root_CA_2048 | Self-signed | RSA | Cisco_Root_CA_2048 | 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 | 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 | dcomics-WONDERWOMAN-CA | Self-signed | RSA | dcomics-WONDERWOMAN-CA | Cisco_Root_CA_H2 | 11/12/2027 | 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 | dcomics-WONDERWOMAN-CA | 09/19/2027 | CA-bvntum | |
| | CallManager-trust | CAPF-6184213c | Self-signed | RSA | CAPF-6184213c | CAPF-6184213c | 07/12/2025 | Self-signed certificate generated by system | |
| | CAPF | CAPF-6184213c | Self-signed | RSA | cucm.steven.lab | CAPF-6184213c | 07/12/2025 | Self-signed certificate generated by system | |
| | CAPF-trust | CAP-RTT-002 | Self-signed | RSA | CAP-RTT-002 | CAP-RTT-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. | |
| | CAPF-trust | CAPF-eb206408 | Self-signed | RSA | CAPF-eb206408 | CAPF-eb206408 | 04/12/2020 | Self-signed certificate generated by system | |
| | CAPF-trust | CAP-RTT-001 | Self-signed | RSA | CAP-RTT-001 | CAP-RTT-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. | |
| | CAPF-trust | Cisco_Root_CA_H2 | Self-signed | RSA | Cisco_Root_CA_H2 | Cisco_Root_CA_H2 | 11/12/2027 | 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. | |
| | CAPF-trust | ACT2_SU01_CA | CA-signed | RSA | ACT2_SU01_CA | 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. | |
| | CAPF-trust | Cisco_Root_CA_2048 | Self-signed | RSA | Cisco_Root_CA_2048 | 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. | |
| | CAPF-trust | Cisco_Manufacturing_CA_SHA2 | CA-signed | RSA | Cisco_Manufacturing_CA_SHA2 | 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. | |
| | CAPF-trust | Cisco_Manufacturing_CA_SHA2 | CA-signed | RSA | Cisco_Manufacturing_CA_SHA2 | Cisco_Root_CA_H2 | 11/12/2027 | 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. | |
| | CAPF-trust | CAPF-6184213c | Self-signed | RSA | CAPF-6184213c | CAPF-6184213c | 07/12/2025 | Self-signed certificate generated by system | |
| | spec-trust | cucm.steven.lab | Self-signed | RSA | cucm.steven.lab | cucm.steven.lab | 07/12/2025 | Self-signed certificate generated by system | |
| | spec-trust | cucm.steven.lab | Self-signed | RSA | cucm.steven.lab | cucm.steven.lab | 07/12/2025 | Trust Certificate | |
| | TLREcovery | TLRECOVERY_cucm.steven.lab | Self-signed | RSA | cucm.steven.lab | TLRECOVERY_cucm.steven.lab | 02/14/2039 | Self-signed certificate generated by system | |
| | tomcat | stevens-DC-CA | CA-signed | RSA | stevens-DC-CA | stevens-DC-CA | 07/10/2024 | Certificate Signed by steven-DC-CA | |
| | tomcat-ECDSA | cucm-ec.steven.lab | CSF Only | EC | cucm.steven.lab | --- | --- | --- | |
| | tomcat-ECDSA | cucm-ec.steven.lab | Self-signed | EC | cucm.steven.lab | cucm-ec.steven.lab | 07/25/2023 | Self-signed certificate generated by system | |
| | tomcat-trust | stevens-DC-CA | Self-signed | RSA | stevens-DC-CA | stevens-DC-CA | 06/01/2023 | Trust Certificate | |
| | tomcat-trust | NOMAT-AD-CA | Self-signed | RSA | NOMAT-AD-CA | NOMAT-AD-CA | 04/23/2028 | Signed Certificate | |
| | tomcat-trust | cucm-ec.steven.lab | Self-signed | EC | cucm.steven.lab | cucm-ec.steven.lab | 07/25/2023 | Trust Certificate | |
| | tomcat-trust | cucm.steven.lab | CA-signed | RSA | cucm.steven.lab | stevens-DC-CA | 07/10/2024 | Trust Certificate | |
| | tomcat-trust | Cisco_Root_CA_H2 | Self-signed | EC | cucm.steven.lab | cucm-ec.steven.lab | 07/25/2023 | Trust Certificate | |
| | tomcat-trust | NOMAT-CA-10 | Self-signed | RSA | NOMAT-CA-10 | NOMAT-CA-10 | 08/11/2027 | Signed Certificate | |
| | tomcat-trust | vnpq-ACTIVE-ORR-CA | Self-signed | RSA | vnpq-ACTIVE-ORR-CA | vnpq-ACTIVE-ORR-CA | 02/10/2024 | Trust Certificate | |
| | tomcat-trust | dcomics-WONDERWOMAN-CA | Self-signed | RSA | dcomics-WONDERWOMAN-CA | CA-bvntum | 09/19/2027 | Trust Certificate | |
| | TVS | cucm.steven.lab | Self-signed | RSA | cucm.steven.lab | cucm.steven.lab | 07/12/2025 | Self-signed certificate generated by system | |

2. ةداهش ل ا ف دوجوم ريغ (IP وأ FQDN) لاصت ل ا ناونع

يذل ل لاصت ل ا ناونع نم اضي ا تاناي ب ل رورم ة ك ر م د خ ق ق ح ت ي ، ة ق ث ل ن ز خ م ل ا فاض ل ا ب

مما ظننا أن مضمون CUCM قد أعاد، لا، لم يلبي سببى. هلجأنا لمبدأ MRA لمجمع موقى
> كذا ن Expressway-C نلعي، (10.48.36.215) IP ناونع مادتساب كبا صاخال CUCM مداخ
اذب (Expressway-C لال خنا لم ليكول) لم ليعملنا نم ققخال تابلل طال فادهتسا متيولي عمل
ناونعل.

متيولي كذا TLS نم ققخال لشفي، مداخل ادهاش نمضا اذلا لاصلتالنا ناونع نوكي ال امدنع
لا، لم يلبي سببى MRA لى لوخدلا ليجست في لشف هنع جتنى 502 أطخا لى.

<#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/em
...
```

```
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

لى (base64) c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw ممتت ثيح
10.48.36.215 ون لاصلتالاب موقى نا بجى هنا رهظي يذلاو، steven.lab/https/10.48.36.215/8443،
ادهاش يوتحتال، طاقتلال مزح في حضوم وه امك. cucm.steven.lab. نم الدب لاصلتالنا ناونعك
أطخا لى متي مثنو (SAN) نيزختال اكبش في IP ناونع لى CUCM TOMCAT.

ةلوهسب اهتحص نم ققخال لى فيك

ةللاتال تاوطخال مادتساب ةلوهسب كولسلا اذلا ريغت دىرت تنك اذا امم ققخال كنكمي

1. نيكم عم ايجزومن) C و Expressway-E (مداوخ) مداخ لى صيخششتال ليجستال ادب.
ةومجم ماظن ةلاح في) صيخششتال ليجستال > تاصيخششتال > ةنايصلال نم (TCPDumps،
(ةيساسال ةدقعلال نم هليغشتل ايفاك نوكي)

2. ةيقرتلال دعب ةلطمعلال ةفيظولال رابتخا و MRA لى لوخدلا ليجستال لواح.

مق م ث C و Expressway-E (مداوخ) مداخ يل ع يصيخش التال ليجستال لش في ى تح رظتنا 3.
نم ةدق ع لك نم تال جسال ع م ح نم دكأت ، ةعوم ج ةلا ح في ف) يصيخش التال ليجستال فاق ياب
(ي در ف لك شب ةعوم جال

اهل ليحت و نواع تال لولح للحم ةادا يل ع ةدوج وول تال جسال ليجحت 4.

ري غتال اذ ب ةقل عت مال ا طخال و ري ذحتال طوط خ ث دحأ طقت لت ا ه نإ ف ، ةلك ش مال ه ذه ته جا و اذ 5.
ةرثأت مال مداوخال نم مداخ لك ل

Diagnostic overview

Issues found No issue Not applicable Missing information Potential problem

Click on any of the below to see details or [continue to analysis](#).

diagnostic_log_vcsoc_2022-07-11_17_33 18-DifferentCA-8443.tar.gz

- Duplicate search rule for same protocol which may trigger 2 invites on the targets Configuration
- Detected alarms in Expressway Configuration
- Server failed to verify certificate causing TLS issues Configuration
- Certificates expired causing TLS failures and service issues Configuration
- defect** Traffic Server Enforces Certificate Validation of UCM/IMP/Unity nodes for MRA services [CSOwc69661] MRA

Related documentation Related defect(s)
CSOwc69661

Description
The tomcat(-ECDSA) certificate of the following CUCM / IMP / 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 CSOwc69661), the Expressway-C traffic server will do a TLS certificate check on the CUCM / IMP / Unity tomcat(-ECDSA) certificates irrespective of the configuration of TLS Verify Mode set when discovering each of those servers.

Action
1. Update the Expressway-C trust store with the CA certificates that signed the tomcat(-ECDSA) certificates of CUCM / IMP / Unity nodes.
2. 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 vcsoc_traffic_server[3926]: [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 vcsoc_traffic_server[3926]: [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 vcsoc_traffic_server[3926]: [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=1
2022-07-11T19:33:06.160+02:00 vcsoc_traffic_server[3926]: [ET_NET 1] ERROR: SSL connection failed for "cucm.steven.lab": error:1416F080:SSL routines:tls_process_server_certificate:certificate verify failed
```

CA صيخش ت عي قوت

Diagnostic overview

Issues found No issue Not applicable Missing information Potential problem

Click on any of the below to see details or [continue to analysis](#).

diagnostic_log_vcsoc_2022-07-11_17_49 11-ConnectCAButwithPonCUCM.tar.gz

- Duplicate search rule for same protocol which may trigger 2 invites on the targets Configuration
- Detected alarms in Expressway Configuration
- Server failed to verify certificate causing TLS issues Configuration
- Certificates expired causing TLS failures and service issues Configuration
- defect** Traffic Server Enforces Certificate Validation of UCM/IMP/Unity nodes for MRA services [CSOwc69661] MRA

Related documentation Related defect(s)
CSOwc69661

Description
The tomcat(-ECDSA) certificate of the following CUCM / IMP / 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 CSOwc69661), the Expressway-C traffic server will do a TLS certificate check on the CUCM / IMP / Unity tomcat(-ECDSA) certificates irrespective of the configuration of TLS Verify Mode set when discovering each of those servers.

Action
1. Update the Expressway-C trust store with the CA certificates that signed the tomcat(-ECDSA) certificates of CUCM / IMP / Unity nodes.
2. 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

```
2022-07-11T19:49:01.513+02:00 vcsoc_traffic_server[3926]: [ET_NET 2] WARNING: SAN (10.48.36.215) not in certificate. Action=Terminate server=10.48.36.215(10.48.36.215)
2022-07-11T19:49:01.513+02:00 vcsoc_traffic_server[3926]: [ET_NET 2] ERROR: SSL connection failed for "10.48.36.215": error:1416F080:SSL routines:tls_process_server_certificate:certificate verify failed
```

لحل

يذل عارج ال دمت عي. ديچ لكش ب لمعي TLS نم ققحت ال نأ نم دكأت ال وه يدم ال ليوط ل حل. عضور عم ال ريذحت ال ة لاسر يلع هذيفنت متيس

(<server-FQDN-or-IP>) ل يساس ال مداخل ة داهش نم ققحت ال لش ف: ريذحت ال نوطحات ام دن ع message، اما. كلذل اق فو Expressway-C مداوخ يلع ة قث ال نزخم ثيذحت يلى جاتحت م، م ادختساب و (0 > قمع ال) ة داهش ال هذه يلع تعقو يتي ال قدصم ال عجرم ال ة لس لس م ادختساب دكأت. ة قث ال قدصم ال عجرم ال داهش > ني مأت ال > ة نا يصل ال نم (0 = قمع ال) ايتاذ ة ققوم ة داهش دع ب نع ة داهش ال عي قوت وه رخأ را ي خ. ة وموم ال ماظن ي ف مداخل لك يلع عارج ال اذه ذيفنت نم Expressway-C ة قث نزخم ي ف فور عم قدصم عجرم ة طساوب

 يلع ايتاذ ة ققوم) ني تفل تخم ني ت داهش لي محتب Expressway حمست ال: ة طحال م اق فو (CN) كرتشم ال مسال س فن امهل ة قث لل Expressway نزخم يلى (لا ثم ال لي بس ت ا داهش ال يلى لقتنا، كلذ حي حصت ل [CSCwa12905](#) Cisco نم عا طخال ا حي حصت فرع م لس فن م ادختسا ة داهش كنكمي شي ح 14 رادصال يلى CUCM ة ققرتب مق و CA نم ة ققوم ال س فن م ادختسا ة داهش كنكمي شي ح 14 رادصال يلى CUCM ة ققرتب مق و CA نم ة ققوم ال Tomcat و CallManager ل (ايتاذ ة ققوم) ة داهش ال

ريشي م، ة داهش ال ة لاسر ي ف دوجوم ريغ (<server-FQDN-or-IP>) SNI: ريذحت ال نوطحات ام دن ع في فيكت اما كنكمي. اهم يدقت مت يتي ال ة داهش ال ي ف دوجوم ريغ مداخل اذه IP و FQDN نأ يلى > ماظن ال يلى CUCM لثم) ني وكت ال لي دعت كنكمي و ا تامول عم ال هذه ني مضت ل ة داهش ال ي تحت Expressway-C مداخل يلع ني وكت ال ثيذحت م (مداخل ة داهش ي ف دوجوم عيش يلى مداخل رابتع ال ي ف هعضو متي

ة ل ص تاذ تامول عم

ل ب ق قباس ال كولس ال يلى عوچر لل قثوم وه امك لي دبل ل حل ق يبطت وه يدم ال ري صق ل حل Expressway-C مداخل دق يلع (رم اوأل رطس ة هجاو) CLI لال خ نم كلذ ذيفنت كنكمي X14.2.0: اتي دح هم يدقت مت يذل رم ال م ادختساب

xConfiguration EdgeConfigServer VerifyOriginServer: Off

تامول عم ال ة ينقت

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا