

# ايتاذ ةعقوملا ةيضارتفالا ةداهشلا لادبتسإ نم هجوم ىلع ةيجراخ ةهج نم SSL ةداهشب RV34x ةلسلسلا

## ةمدقملا

حمسي اذهو. ىمسمل ةداهشلا عوضوم بسح ماع حاتفم ةيكلم ةيمقرلا ةداهشلا دمتعت  
صاخلا حاتفملا اهمدقي يتلا تاديكاتلا و اتاعيقوتلا ىلع دامتعالاب ةلوعملا فارطال  
يهو، ايتاذ ةعقوم ةداهش عاشنإ هجوملل نكمي. دمتعمل ماعلا حاتفملا عم قفاوتي يذلا  
عجارملا ىلإ تابلط لاسرا هنكمي امك. ةكبشلا لوؤسم ةطساوب اهؤاشنإ مت ةداهش  
لوصحل مامل نم. ةيمقر ةيوه ةداهش ىلع لوصحل بلطب مدقتلل (CAs) ةقدصملا  
ةثلاث فارطأ تاقببط نم ةيعرش تاداهش ىلع.

اهلالخ نم تاداهشلا ىلع ةباقرلا ةئيهل نكمي ناتقيرط كانه

1. ةصاخ حيتافم مادختساب ةداهشلا عيقوتب CA موقبي.

2. هؤاشنإ مت يذلا (CSR) ةداهشلا عيقوت بلطب مادختساب تاداهشلا عيقوتب CA موقبي.  
RV34x ةطساوب.

ةطيسولا ةداهشلا نأ امب. ةطسوتم تاداهش ةيجراحتلا تاداهشلا يعئاب مظعم مدختست  
ةداهشلا نع ةرداص ةداهش يأنف، هب قوتوملا رنجلال قدصملا عجرملا نع ةرداص  
ةثلاث ةداهش ةلسلس لثم، هب قوتوملا رنجلال ةقت ثرت ةطيسولا.

## فدهلا

ةهج نم (SSL) ةنمآلا ليصوتلا ذخأم ةقبط ةداهش بلطب ةيفيك راهظا ىلإ لاقملا اذه فدهي  
ايتاذ ةعقوملا ةداهشلا لادبتسال CA لبق نم اهرادصا متي يتلاو، اهل يمحتو ةيجراخ  
RV34x هجوم ىلع.

## قيبطتلل ةلباقلا ةزهجال

- RV340
- RV340W
- RV345
- RV345P زارطالا

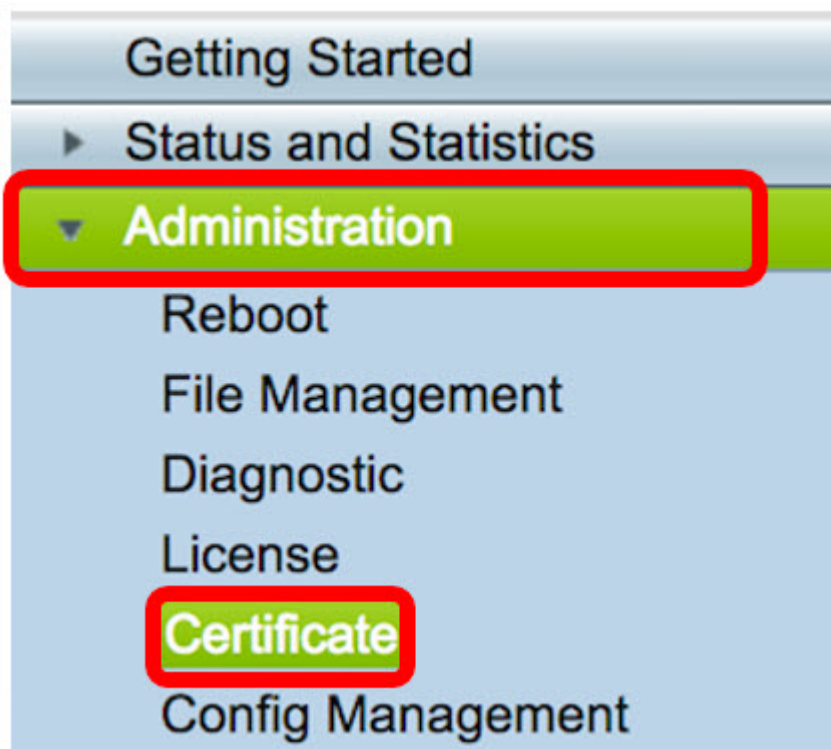
## جماربال رادصا

- 1.0.01.17

نم SSL ةداهشب ايتاذ ةعقوملا ةيضارتفالا ةداهشلا لادبتسإ  
ةيجراخ تاهج لبق

## CSR عاشنإ

هجوم الـ في بيولا إلى ةدنتسم الـ ةدعاسم الـ ةأال الـ إلى لوخدل الـ ليجستب مق 1. ةوطخل الـ صيخرت > ةراد ارتخاو.



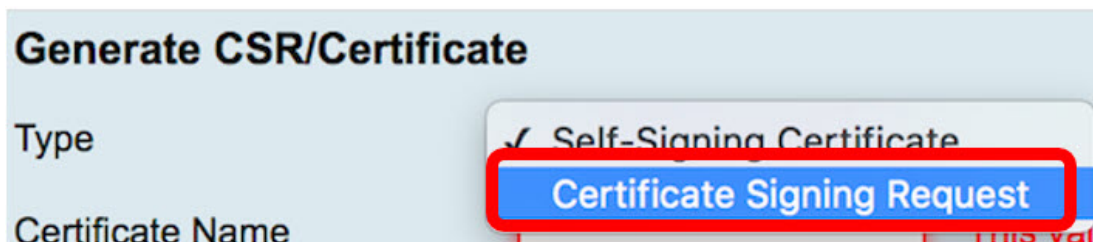
صيخرت الـ CSR ءاشن | رز رقنا ، صيخرت الـ لودج تحت 2. ةوطخل الـ

Certificate Table						
	Index	Certificate	Used By	Type	Signed By	Duration
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00

Delete Export Detail Import

Import Certificate **Generate CSR/Certificate**

بلط رتخاو ل دسنم الـ عون الـ مهس الـ ع رقنا ، ةداهش الـ CSR ءاشن | ةذفان في 3. ةوطخل الـ ةداهش الـ عيقوت.



ةداهش الـ مسا ل قح في ةداهش الـ امسا ل خدأ 4. ةوطخل الـ

## Generate CSR/Certificate

Type

Certificate Signing Request

Certificate Name

34xrouter

34xrouter هو جومل مادختسإ متي، لاثملا اذه في ةظحالم

ءاقتنا رز قوف رقنا مث عوضوملل ليدبلل مسالا لقح في اليدب امسا لخدا 5 ةوطخل نكمي يذلا لاجملا مسا وه ليدبلل مسالا نوكتسي . ةقباطم لل هل فسأ دوجوملا FQDN هو جوملا الى لوصولل ه مادختسإ

Subject Alternative Name

RVrouter.com

IP Address  FQDN  Email

RVrouter.com مادختسإ متي، لاثملا اذه في ةظحالم

كعقوم دلب رايتخال دلبلا مسا لدسنملا مهسالا قوف رقنا 6 ةوطخل

IP Address  FQDN  Email

Country Name

US - United States

ةدحتملا تايالولا رايتخإ متي، لاثملا اذه في ةظحالم

ةعطاقملا وأ ةيالولا (ST) مسا لقح في ةعطاقملا وأ ةيالولا مسا لخدا 7 ةوطخل

Country Name

US - United States

State or Province Name(ST)

California

اينروفيلك مدختست، لاثملا اذه في ةظحالم

يلحملا (L) مسا لقح في ةيلحملا تاداعإل لخدا 8 ةوطخل

State or Province Name(ST)

California

Locality Name(L)

Irvine

Irvine مادختسإ متي، لاثملا اذه في ةظحالم

رفوتملا لقحلا في ةسسؤملا (O) مسا لخدا 9 ةوطخل

Locality Name(L)	Irvine
Organization Name(O)	Cisco

ملاحظة: Cisco مادي متي، لاثملا اذه في عظمالم

رفوتل لقلل في فيميظنتل ءءولل (OU) مسلا لءءا. 10 ءوطلل

Organization Name(O)	Cisco
Organization Unit Name(OU)	SBKM

ملاحظة: SBKM مادي متي، لاثملا اذه في عظمالم

(CN) ءئاشلل مسلال لقلل في امسلا لءءا. 11 ءوطلل

Organization Unit Name(OU)	SBKM
Common Name(CN)	34xrouter

ملاحظة: 34xrouter ءوملا مادي متي، لاثملا اذه في عظمالم

لاسرا ءيرت فينورتل لءل ءيرب ناوع في أ و أفينورتل لءل ءيرب ناوع لءءا. 12 ءوطلل  
هبل ءءاهشلل

Common Name(CN)	34xrouter
Email Address(E)	@gmail.com

ملاحظة: gmail.com ناوعلا لءل فينورتل لءل ءيرب ناوع مادي متي، لاثملا اذه في عظمالم

تب ءءءو ءءل ءلءس نملل ءمءاقلل نم ءي ءافملا ريفشلل لوط رءءا. 13 ءوطلل  
512 وه فيضارءفالل لوطلل. ءءاءم في

Email Address(E)

Key Encryption Length

✓ 512  
1024  
2048

Generate Cancel

لو طأ ريف شت نأل ارظن ةدش ب كلذب ى صوي 2048 مادختسإ متي ، لا ثم لا اذه ي ف : ةط حالم  
انامأ رثكأ هل عجي امم ، رصقأ لا حيتافم لاب ةنراقم هترفش ك ف بعصلال نم نوكي

دلي ةق طقط 14. ةوطخلال

Key Encryption Length 2048

Generate Cancel

"تاداهشلا لودج" ي ف نأل هئاشنإ ب تمق يذلا ةداهشلا بلط رهظيس

Certificate Table					
	Index	Certificate	Used By	Type	Signed By
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed
<input type="checkbox"/>	3	34xRouter	-	Certificate Signing Request	-

حاجن ب CSR ءاشنإ ب نأل تمق دقل

## CSR ري دصت

قوف رقناو تاداهشلا لودج ي ف ةداهشلا بلط بناجب دوجوملا عبرملا دح 1. ةوطخلال  
ري دصت

Certificate Table				
	Index	Certificate	Used By	Type
<input type="checkbox"/>	1	Default	WebServer	Local Certificate
<input type="checkbox"/>	2	FindIT	-	Local Certificate
<input checked="" type="checkbox"/>	3	34xRouter	-	Certificate Signing Request

Delete Export Detail Import

رتوي ب مكلال لى لى لملا لى زنتل ةداهشلا ري دصت ةذفان ي ف لى زنت لى لى رقنا 2. ةوطخلال  
ب PEM قيسنتن

**Export Certificate**

Export as PEM format

Select Destination to Export:

PC

كې صاخلا رتويېمكلا زاغ ىل حاجنې CSR رېدصتې نآل تمق دقل

## ةداهشلا رفوم ىل CSR لېمحت

ف هوقصلا مث CSR خسن او Notepad مادختساپ هليزنت مت يذلا فللملحت فا. 1 ةوطخلال  
ثلاثلا فرطلاب صاخلا SSL ةداهش رفوم عقوم ف رفوتملا لقحلا

1. Copy and paste your CSR into this box:

```
STZJWoGLiyqRIPPHKREghzRfRh9WVW9KWdXzAgMI
UzBRMAkGA1UdEwQCMAAwHQYDVR0OBBYEFB24F/
A1UdDwQEAwIF4DAYBgNVHREETAPgg0zNHhyb3VC
CwUAA4IBAQA8J/x6+BL0Gr797UeHxBH8sCuBSwQ
dYGbl7qzZVVO+b/TvJii7jG52ojYzNDGFWamfYnoCrhv
x7+ooeOn9ihoOXxEFKhrn2ueaMZJKQAnFpCwapbsxf
pVBnwK74cfF8NBVivtX08SK6qn9qgsvxJcGxmlyBiffV
YZITBEWG2Q1TVIY0brOkNbir2VuGoqpsplRqMcq/yE
1WkB91P7hA6X4AB80cKZQEdDsCvrjtgI
-----END CERTIFICATE REQUEST-----
```

2. Select the server software used to generate the CSR:

Select from list:

صخيخرتلا دوزمك Comodo.com مادختساپ متي، لاثملا اذه في: ةظحالم

هجوملا نأل ارظن، ةلاحلا هذه في CSR ءاشنإل مدختسملا مداخل جامنرب ددح. 2 ةوطخلال  
رخأ زاغ رايخإ متي، ةمئاقلا في جردم ريغ RV34x

1. Copy and paste your CSR into this box:

```
STZJWoGLiyqRIPPHKREghzRfRh9WVW9KWdXzAgMI
UzBRMAkGA1UdEwQCMAAwHQYDVR0OBBYEFB24F/
A1UdDwQEAwIF4DAYBgNVHREETAPgg0zNHhyb3VC
CwUAA4IBAQA8J/x6+BL0Gr797UeHxBH8sCuBSwQ
dYGbl7qzZVVO+b/TvJii7jG52ojYzNDGFWamfYnoCrhv
x7+ooeOn9ihoOXxEFKhrn2ueaMZJKQAnFpCwapbsxf
pVBnwK74cfF8NBVivtX08SK6qn9qgsvxJcGxmlyBiffV
YZITBEWG2Q1TVIY0brOkNbir2VuGoqpsplRqMcq/yE
1WkB91P7hA6X4AB80cKZQEdDsCvrjtgI
-----END CERTIFICATE REQUEST-----
```

2. Select the server software used to generate the CSR:

رتويېمكلا ىل كتداهش ليزنتب مق. 3 ةوطخلال

## ةثلاثلا SSL ةهج ةداهش لېمحت

داريتسا رزىل عرقنا، هجوملل بيولا ىل ةدنتسملا ةدعاسملا ةادأل في. 1 ةوطخلال

ص.يخرتال لودج تحت دوجومال ص.يخرت

Certificate Table						
Index	Certificate	Used By	Type	Signed By	Duration	
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00
<input type="checkbox"/>	3	34xRouter	-	Certificate Signing Request	-	-

Buttons: Delete, Export, Detail, Import, **Import Certificate**, Generate CSR/Certificate

ةداهش رتخاو عون ةلدسنملا ةمئاقلا ىلع رقنا ،ةداهشلا داري ت سا ةذفان ي ف 2. ةوطخلال CA.

### Import Certificate

Type:  Local Certificate  
**CA Certificate**  
Certificate Name: PKCS#12 encoded file

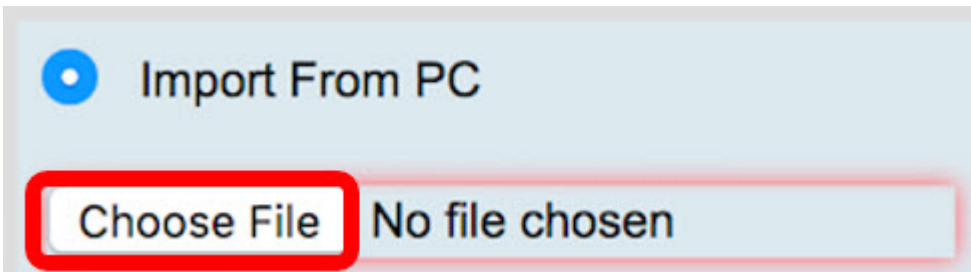
رفوتملال لقحلال ي ف ةداهش مسا لخدأ 3. ةوطخلال

### Import Certificate

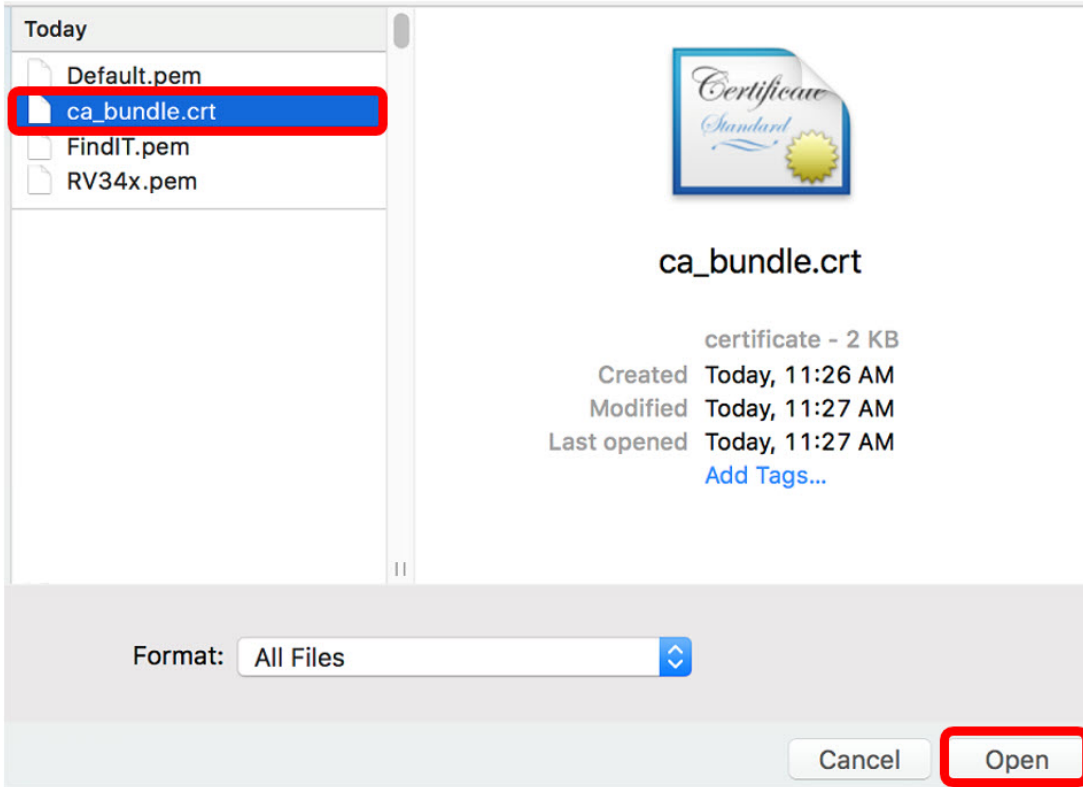
Type: CA Certificate  
Certificate Name: **RV34xCert**

مادختسا متي ،لاثملا اذه ي ف :ةظحالم RV34xCert

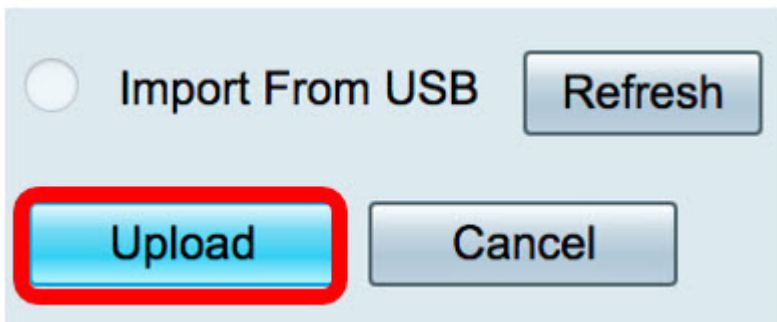
نم هليزنتب تمق يذلا ةداهشلا فلم ناكم ددحو فلم رايخا رزلا ىلع رقنا 4. ةوطخلال ق.دصملا عجرملا



جحت ف قوف رقنا م ث فلما ل قوف رقنا 5. ةوطخال



ل.محت قوف رقنا 6. ةوطخال



ةداهش ب عون ل لادب تس ن آلا متي و دي دجال ةداهش ل م سا ن آلا "تاداهش ل لودج" رهظيس  
ثلاث ل فرط ل نم قدصم ل عجرم ل ةطساوب اه ع قوت متي ل ةيمست ل ع CA



Certificate Table						
Index	Certificate	Used By	Type	Signed By	Duration	
<input type="checkbox"/> 1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00	
<input type="checkbox"/> 2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00	
<input checked="" type="checkbox"/> 3	RV34xCert	-	CA Certificate	DST Root CA X3	From 2016-03-17,00:00:00 To 2021-03-17,00:00:00	

RV34x هجوم ىلع حاجنب ةيجردك ةهج نم SSL ةداهش ليمحتب نآلا تمق دول

## ايتاذ ةعقوملا ةيضارتفالا ةداهشلا لادبتسلا

VPN > SSL VPN رتخأ، بېولا ىلى ةدنتسمل ةدعاسملا ةادألا يف 1. ةوطخل



Cisco SSL VPN مداخل نيكم تل وي دارلا ليغشت رز قوف رونا 2. ةوطخل

# SSL VPN

General Configuration

Group Policies

Cisco SSL VPN Server  On  Off

عداهش ل ف ل م ة ل د س ن م ل ا ة م ئ ا ق ل ل ا ل ع ر ق ن ا ، ة ي م ا ز ل ل ا ل ا ة ب ا و ب ل ا ت ا د ا د ع ا ت ح ت 3. ة و ط خ ل ل ا ث ي د ح ا ه ل ي م ح ت م ت ي ت ل ل S S L ة د ا ه ش ر ا ي ت خ ا ب ة ي ض ا ر ت ف ا ل ا ة د ا ه ش ل ل ل د ب ت س ا و

## Mandatory Gateway Settings

Gateway Interface WAN1

Gateway Port 8443 (Range: 1-65535)

Certificate File  Default  
 FindIT

Client Address Pool RV34xCert

ر ف و ت م ل ل ق ح ل ل ي ف ب و ل ط م ل ل ل ي م ع ل ل ل ا ج م ل خ د ا 4. ة و ط خ ل ل ا

Certificate File RV34xCert

Client Address Pool 192.168.10.0

Client Netmask 255.255.255.0

Client Domain RVrouter.com

م ا د خ ت س ا م ت ي ، ل ا ث م ل ا ا ذ ه ي ف : ة ط ح ا ل م

ق ب ط ي ة ق ط ق ط 5. ة و ط خ ل ل ا



ةصاخلا SSL ةداهشب ايتاذ ةعقوملا ةيضارتفالا ةداهشلا حاجنب نأللا تلدبتسا دقل ةيجراخ ةهجب

[ةلسلسلا هجوم لوج ةلواتملا ةلئسألا](#): تامولعملاب ةينغ ةلاقملا هذه اضيا دجت دق [RV34x](#)

مامتهالل ةريثم اهدجت دق ىرخأ تالاقم ىلا تاطابتلالا نم ديدعل عقوملا اذه رفوي [RV34x ةلسلسلا نم هجوم تاجت نم ةحفص](#)

ةمچرتل هذه لوج

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