



راهاندازی و پیکربندی امن پروتکل SSL/TLS بر روی Microsoft Exchange Server 2013

APA-AMIRKABIR-1395052	شماره مستند4-1
۲۴ مرداد ۱۳۹۵	تاريخ نگارش
۲,۰	شماره نگارش
آپاي امير کبير	نگارش
عادی	طبقەبندى

فهرست مطالب

1		مقد	۱
۲ Exchang	ایط گواهی SSL برای 2013 g	شر	۲
۲	دوره اعتبار گواهی	۱-۲	
۲	اعتبار مرکز صدور گواهی	۲-۲	
۳	صحت نام سرور /دامنه	۳-۲	
۳	گامھای بعدی	4-1	
ای Exchange Server 2013	ید درخواست گواهی SSL بر	تول	٣
Exchang از CA خصوصی	ور گواهی SSL برای ge 2013	صد	۴
۱۱ Active Directory Certificate Set	نصب و پیکربندی نقش rvice	1-4	
١۶	دریافت گواهی دیجیتال	۲-۴	
نظار بررسی درخواست گواهی۲۰	ونگی کامل کردن مراحل انت	چگ	۵
هی SSL به چند سرور Exchange 2013	نخراج و وارد کردن یک گواه	اسن	۶
ویس ها در Exchange Server 2013 ویس ها در	ساب یک گواهی SSL به سرو	انتم	۷
۳۰	بع	منا	٨





۱ مقدمه

شرکتها و سازمانهای کوچک عمدتاً از شرکتهای ثالث میزبان سرویسدهنده، برای پست الکترونیک خود استفاده میکنند اما شرکتهای متوسط و بزرگ به دلیل مسائل امنیتی و حساسیت سرویس پست الکترونیک برای آنان، ناچار به استفاده از یک Mail Server اختصاصی در محل خود هستند.

برنامه Exchange Server یک نرمافزار برای مدیریت ایمیلهای سازمانی، ارسال و دریافت ایمیلها و ساماندهی ایمیلهای داخل سازمانی برای تمامی کاربران است که نسخههای مختلفی از آن توسط شرکت مایکروسافت تولید و عرضه شده است.

برای تأمین محرمانگی و جامعیت دادههای مبادله شده میتوان از پروتکلهای استانداردی که بدین منظور طراحی شده استفاده کرد. در حال حاضر مهم ترین پروتکل رمزنگاری که در سطح اینترنت برای رمزنگاری دادههای لایه کاربرد^۱ و تأمین امنیت ارتباطات استفاده میشود، پروتکل SSL/TLS است. Exchange Server 2013 ارتباطات ایمن کلاینت-سرور و سرور-سرور را با استفاده از گواهیهای SSL به منظور امن سازی پروتکلهایی مانند POP هSMTP، HTTP و IMAP و IMAP فراهم میکند. بدلیل نیازمندیهای امنیتی پیشفرض، نرمافزار مانند Exchange Server 2013 بعد از نصب، به صورت خودکار با گواهیهای Self-signed پیکربندی میشود و برای پروتکلهای نام برده فعال سازی میشود. در این گزارش مراحل نصب گواهی SSL بر روی SEV در وی 2013 2013 شرو داده شده است.

¹ Application Layer







Exchange 2013 برای SSL شرایط گواهی ۲

Exchange 2013 از فیلد خاصی در گواهیهای SSL که به نام SAN^۱ شناخته میشوند استفاده میکند. در بعضی موارد، این مورد توسط ارائه دهندگانی به نام ^۲UC نامیده میشود.

یک گواهی SAN، چندین سرور یا نام دامنه را در یک گواهی SSL دارد. این بدان معنی است که به جای گرفتن گواهی جداگانه برای هر کدام از سرورها شما میتوانید یک گواهی را برای امنسازی یک یا چند سرور Exchange 2013 استفاده کنید.

برای پیکربندی سرویسدهنده HTTPS و استفاده از این پروتکل ابتدا باید گواهینامه دیجیتال مربوطه را از مراکلی مراکلی مراکلی مراکلی مراکلی مراکلی مراکلی مراکلی است که برای اطلاعات بیشتر در این زمینه میتوانید به گزارش ارائه شده توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر که در آدرس زیر قرار دارد مراجعه کنید:

http://apa.aut.ac.ir/?p=971

برای اینکه گواهی SSL بتواند به درستی در محیط Exchange 2013 شما کار کند به سه شرط نیاز دارد:

۲-۱ دوره اعتبار گواهی

هر گواهی SSL دارای یک تاریخ انقضا است و دوره اعتبار گواهی^⁴ در واقع دوره زمانی بین صدور گواهی تا انقضای آن است. گواهی self-signed که Exchange 2013 در زمان نصب آن را صادر می کند برای پنج سال اعتبار دارد. یک گواهی صادر شده از یک مرکز صدور گواهی(CA) خصوصی⁴ ممکن است برای چندین سال معتبر باشد. یک گواهی که از یک مرکز صدور گواهی تجاری⁹ بدست آمده باشد، برای یک سال اعتبار دارد.

۲-۲ اعتبار مرکز صدور گواهی

گواهی دیجیتال سرورها باید از مراکز معتبری که در حال حاضر کلاینتها به آن اعتماد دارند گرفته شود. اگر از مرکز صدور گواهی خصوصی به منظور گرفتن گواهی SSL برای سرور Exchange 2013 استفاده می کنید و این CA یک Enterprise CA در حال حاضر برای کلاینتهایی که اعضای دامنهها در AD forest هستند مورد اعتماد خواهد بود. اعضا دامنه به CA اعتماد نخواهد داشت مگر اینکه گواهی ریشه در لیست گواهیهای مورد اعتمادشان اضافه شود.

^r Unified Communications

- ^{*} Certificate Validity Period
- ^a Private Certificate Authority
- ⁵ Commercial certificate authority



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیبپذیریها و حوادث امنیتی سایبری)

تهران - بالاتر از چهارراه وليعصر - نبش کوچه بالاور - ساختمان معاونت پژوهشی دانشگاه صنعتی اميرکبير - طبقه سوم

كد پستى: ۱۵۹۱۶۳۴۳۱۱ تلفكس: ۸۹۹۱۶<u>۳۲۱۱ autcert@aut.ac.ir</u> ۶۶۴۶۰۳۰۸ Web: <u>https://apa.aut.ac.ir</u>

[\] Subject Alternate Name

[&]quot; Certificate Authority





بیشتر مراکز صدور گواهی تجاری در حال حاضر توسط سیستمعاملها (مورد استفاده در رایانهها و گوشیهای همراه) مورد اعتماد هستند و همین طور وقتی شما گواهی خود را از این CAها دریافت کنید، این گواهی توسط کلاینتها مورد اعتماد خواهد بود.

۲-۳ صحت نام سرور/دامنه

شرط آخر این است که نام دامنه یا سروری که کلاینت به آن متصل می شود باید با یکی از نامهای داخل گواهی SSL منطبق باشد. برای مثال، اگر کلاینتها از https://mail.exchangeserverpro.net/owa برای اتصال به Outlook Web App استفاده کنند، سپس گواهی SSL روی Exchange server باید شامل نام "mail.exchangeserverpro.net" شود.

۲-۴ گامهای بعدی

گامهای بعدی در راهاندازی گواهینامه SSL برای Exchange Server 2013 به صورت زیر است:

- ۲. تولید یک درخواست امضای گواهی(CSR)^۱ برای Exchange 2013
- ۲. ارسال این درخواست به CA مورد نظر به منظور بدست آوردن گواهی SSL
 - ۳. کامل کردن انتظار برررسی "درخواست گواهی"
- ۴. استخراج و وارد کردن یک گواهی SSL به چند سرور Exchange 2013 (اختیاری)
 - ۵. اختصاص دادن گواهی SSL به سرویس های مورد نظر در Exchange 2013

در ادامه هر کدام از این مراحل را به صورت مفصل تر شرح میدهیم.

برای بررسی وضعیت امنیتی پروتکل SSL/TLS سرویس دهنده خود، می توانید به ابزاری که بدین منظور توسط پژوهشکده آپای دانشگاه صنعتی امیر کبیر طراحی شده و در آدرس زیر قرار دارد، مراجعه کنید. https://sslcheck.certcc.ir

^r Pending Certificate Request



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ / Web: <u>https://apa.aut.ac.ir</u> - Email: <u>autcert@aut.ac.ir</u>

[\] Certificate Signing Request





Exchange Server 2013 برای SSL تولید درخواست گواهی 🖇

گام اول به منظور پیکربندی یک گواهی SSL جدید برای Exchange Server 2013، تولید درخواست گواهی است. در این مثال یک درخواست گواهی SSL برای سروری به نام WIN-OQDMIIPCT5Pدر دامنه apa.local تولید شده است و این با نقشهای Client Access و rore server نصب شده است و نام Exchange Administration Center در گواهی SSL خواهند بود. درخواست گواهی می تواند توسط salbox server center تولید شود که روند کار آن را با ذکر مثالی در زیر بیان می کنیم.

با استفاده از مرورگر خود، Exchange Administration Center را باز کنید و به مسیر <- Servers با استفاده از مرورگر خود، Certificates بروید:

Exchange admin cen	iter			
recipients	servers databases database availa	bility groups virtual di	rectories <mark>certificat</mark> e	25
permissions				
compliance management	Select server: WIN-OQDMIIPCTSP.apa.local	~		
organization	+/10			
protection	NAME	STATUS	EXPIRES ON	•
mail flow	Microsoft Exchange Server Auth Certificate Microsoft Exchange	Valid Valid	7/27/2021 8/22/2021	Microsoft Exchange Server Auth Certificate
mobile	WMSVC	Valid	8/20/2026	Self-signed certificate Issuen CN=Microsoft Exchange Server Auth Certificate
public folders				Status
unified messaging				Valid Expires on: 7/27/2021
servers				Henew
hybrid				Assigned to services SMTP
tools				

شکل ۱: مدیریت گواهیها در Exchange Administration Center

روی آیکن "+" کلیک کنید و سپس گزینه "درخواست گواهی SSL" را مانند شکل زیر انتخاب کنید و روی Next به منظور ادامه کار کلیک کنید.









elect s	Exchange Certificate - Internet Explorer	_ □ X
<mark>₽</mark> .∕	new Exchange certificate	Help
Aicrosc Aicroso VMSVC	This wizard will create a new certificate or a certificate request file. You can either create a self-signed certificate or request a certificate from a certification authority. Learn more Create a request for a certificate from a certification authority Create a self-signed certificate	You can create a self- signed certificate or request a certificate from a certification authority. Learn more
		next cancel
		🔍 100% 🔻 👷

شکل ۲: شروع مراحل گواهی SSL

در قسمت بعد باید یک نام برای گواهینامه انتخاب و کلید Next را بزنید.

Select se	ê	Exchange Certificate - Internet Explorer	_ D X
+ 🖍	new Exchange certificate		Help
Microso Microso WMSVC	*Friendly name for this certificate: Exchange2013Certificate		
		back	ext cancel

شکل ۳: نام گواهینامه

یک گواهی wildcard نوعی از گواهی است که امنسازی همه زیر دامنههای مربوط به دامنه اصلی (ریشه) تنها با گرفتن یک گواهی، امکان پذیر می شود. در شکل ۴ گزینه گواهی wildcard را انتخاب نکنید. با وجود اینکه







آنها برای Exchange پشتیبانی می شوند، ولی در برخی از سرورها پشتیبانی نمی شوند و در اینجا ما این گزینه را انتخاب نمی کنیم و برای ادامه Next را انتخاب کنید.

Select se	Exchange Certificate - Internet Explorer	_ 0	x
+ 🖍	new Exchange certificate		Help
Microso Microso WMSVC	Request a wildcard certificate. A wildcard certificate can be used to secure all sub- domains under your root domain with a single certificate. Learn more *Root domain:		
	back next of	cancel	

شكل ۴: گواهی wildcard را برای Exchange 2013 درخواست ندهید.

روی Browse کلیک کنید و سپس سرور Exchange مورد نظر (همان سروری که میخواهید برای آن گواهی بگیرید) را به منظور ذخیره کردن درخواست گواهی انتخاب کنید (در اینجا WIN-OQDMIIPCT5P).

Select se	Schange Certificate - Internet Explorer	🥖 Select a Server - Internet Explorer 🗖 🗖 🗙
+ 🖍	new Exchange certificate	NAME A ROLE WIN-COODMIIPCTSP Mailbox. Client Access
Microso Microso	*Store certificate request on this server:	
WMSVC	U/UW3E	
	back	
l	-	
		ok cancel

شکل ۵: انتخاب سرور مورد نظر برای درخواست گواهی

دکمه Edit را انتخاب کنید و نام دامنهای که کلاینتها با استفاده از آن قرار است به هر سرویس متصل شوند را انتخاب کنید.

> مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ <u>web: https://apa.aut.ac.ir</u> - Email: <u>autcert@aut.ac.ir</u>







servers databases database availability groups virtual directories certificates

	6	Exchange Certificate - Internet Explorer	
Select ser	new Eychange cert	Domain Editor Webpage Dialog	x
+ NAME Microsoft WMSVC	ACCESS Outlook Web App (when Outlook Web App (when Outlook Web App (when OAB (when accessed from OAB (when accessed from Exchange Web Services (w Exchange Web Services (w Exchange ActiveSync (whe	Edit Domain Access type: Outlook Web App (when accessed from the Internet) Specify the domains for the above Access type. Ensure that these match your current configuration. Learn more appa,local	Help
		ok cancel back next Cancel @ 10%6	

شکل ۶: پیکربندی نامها به منظور اضافه کردن درخواست گواهی

اگر چندین سرویس مانند OAB، OAB، OWA، و ActiveSync قرار است با نام خارجی یکتا مورد استفاده قرار گیرند، نیاز است فقط یکبار این نام را برای یکی از سرویس ها وارد کنیم و سپس روی Next کلیک کنید.

اطلاعات سازمانی خود را وارد کرده و سپس Next را انتخاب کنید. برخی از مراکز صدور گواهی، اطلاعات وارد شده در شکل ۷ را با اطلاعات WHOIS (اطلاعات ثبت شده در دامین مورد نظر) بررسی میکنند که برای دامنههای درخواست داده شده، مطابقت داشته باشند. اگر آنها مطابقت نداشتند، ممکن است برخی روشهای خاص برای اثبات این امر قبل از صدور گواهی وجود داشته باشد.









Sector Exchange Certificate - Internet Explorer		_ □	x
new Exchange certificate			Help
Specify information about your organization. This is required by the certification authority. Learn more			
*Organization name:			
Exchange Server pro			
*Department name:			
Т			
*City/Locality:			
Tehran			
*State/Province:			
Center			
*Country/Region name:			
Iran 🗸			
back nex	xt	cancel	
		🔍 100%	•
	Exchange Certificate - Internet Explorer new Exchange certificate Specify information about your organization. This is required by the certification authority. Learn more *Organization name: Exchange Server pro *Department name: IT *City/Locality: Tehran *State/Province: Center *Country/Region name: Iran back	Exchange Certificate - Internet Explorer new Exchange certificate specify information about your organization. This is required by the certification authority. Learn more *Organization name: Exchange Server pro *Department name: [T *City/Locality: Tehran *State/Province: Center *Country/Region name: [Tran	Exchange Certificate - Internet Explorer new Exchange certificate specify information about your organization. This is required by the certification authority. Learn more *Organization name: Exchange Server pro *Department name: [T *City/Locality: Tehran *State/Province: Center *Country/Region name: Iran back next cancel

شكل ۲: وارد كردن اطلاعات سازماني

در قدم بعد باید یک مسیر ^۱UNC معتبر برای ذخیره کردن فایل درخواست گواهی وارد کرده و روی Finish کلیک کنید.

¹ Universal Naming Convention



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ / Meb: <u>https://apa.aut.ac.ir</u> - Email: <u>autcert@aut.ac.ir</u>





Select server:	🧭 Exchange Certificate - Internet Explorer 📃 🗖 🗙	ſ
+ 🖋 🖮 🗧	new Exchange certificate	
Microsoft Excha Microsoft Excha	*Save the certificate request to the following file (example: \\myservername\share\mycertrequest.REQ):	
WMSVC	\\WIN-OQDMIIPCT5P\c\$\AdminCert\mycertreq1.txt	
	You'll need to submit the contents of the file you entered to a certification authority.	
	After you receive the certificate file from the certification authority, you'll need to click Complete in the Information pane to install it on your Exchange server. Learn more	
	back finish cancel	
	🔍 100% 🔻 🛓	

شکل ۸: انتخاب مسیر برای ذخیره فایل درخواست گواهی

حال در قسمت Exchange Administration Center مشاهده می شود که درخواست در حال بررسی (Pending request) است.

+/ 🖻 🗗 …

NAME	STATUS	EXPIRES ON
Exchange2013Certificate	Pending request	8/23/2017
Microsoft Exchange Server Auth Certificate	Valid	7/27/2021
Microsoft Exchange	Valid	8/22/2021
WMSVC	Valid	8/20/2026

شكل ۹: بررسى درخواست گواهىنامه براى Exchange 2013

همان طور که مشاهده می کنید فایل درخواست گواهینامه در مسیر UNC وارد شده، قابل مشاهده است.



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ / Meb: <u>https://apa.aut.ac.ir</u> - Email: <u>autcert@aut.ac.ir</u>





Name	mycertreq1 - Notepad 📃 🗖
📄 mycertreq1	File Edit Format View HelpBEGIN NEW CERTIFICATE REQUEST
	MIIEWjCCAØICAQAwbjESMBAGA1UEAwwJYXBhLmxvY2FsMQswCQYDVQQLDAJJVDEc MBcGA1UECgwTRXhjaGFuZ2UgU2VydmVyIHBybzEPMA0GA1UEBwwGVGVocmFuMQ8w
	DQYDQQIDA2D2WS02XIXCZAJBGNVBAYTAKISMIIBIJANBGKqnKiG9W0BAQEFAAUC AQ8AMIIBCgKCAQEA6TqB1y8jdVSz/Z+6navm1GMCqjdlrOjWRfDQOP+OPRJ/eTgh b]b00y]bMk6P10bcgU7ya2seni01KbaKDKNH3eriTNmvRSKivaanzEn4bDucAkvn
	<pre>vWF5kccJOJ16pg2wKIJjV9PTyPMPMXDfySff8xcsuxlkoFv3CoWq6r9AkpS7/1Rm Wspc13iTZyrqjVWnLCA4OS13t+O0nz18pvTkASfFoqvX2LOM6CNjxS6z4H6/ZNMF</pre>
	5Gr932Ljb9nw9qNfFfp4YI83slnpuEacEVPM5czoRws1iCrpm1Sg9uP2hEfsdZVrmDlq2YUaYA2qqkR84r4yn1Kz2N5wbdnKwCUNDQIDAQABoIIBpTAaBgorBgEEAYI3
	DQIDMQwWCjYuMi45MjAwLjIwaAYJKwYBBAGCNxUUMVswWQIBBQwZV0IOLU9RRE1J SVBDVDVQLmFwYS5sb2NhbAwVQVBBMFxXSU4tT1FETU1JUENUNVAkDCJNaWNyb3Nv
	ZnQuRXhjaGFuZ2UuU2VydmljZUhvc3QuZXhIMHIGCisGAQQBgjcNAgixZDBiAgEB HloATQBpAGMAcgBvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAg
	gagGCSqGSIb3DQEJDjGBmjCBlzAOBgNVHQ8BAf8EBAMCBaAwWAYDVR0RBFEwT4IJ YXBbLmxvY2Esgbl3aW4tb3EkbWlbcGN0NXAuYXBbLmxvY2Esgb7BdXRvRGlzY292
	ZXIuYXBhLmxvY2Fsgg9XSU4tT1FETUIJUENUNVAwDAYDVR0TAQH/BAIwADAdBgNV H04E Fg0U27ux0gNvqyhPw0cf2KcyY+Awm3wwD0YJKoZIhvcNA0E FB0ADggEBAIWv
	meZie5TvOUZ7fOUKcIeClzuIOq6XgzdUSOrMrUmXDp//MN6+ad88PfyvMsjUBg0G c6abiDjUdM0YUu2jOw@mATOJjZnBxwHmZNXgsscmU6eJzCwmXrmKcUFT5jBwR81k
	pHs1XU7paw23ga+CzeXTra8Tw92S/s2znOgG5cz2FsDYQrnNDOY7Litr6w4UgQQE ZPd0DXpE8mVJGR2eMAqquHt4pQbKMRP1uxP47VBG6y+1VZt1hus/CFyCbIbudjtm
	1Ef5A4V4o7iDzocxcECdNQbcI1UxRUnd0UF2Gs8IhJ6GcUU/EEs8KBsBTgUC4AAS p06E5rDKnubM75t0jFo=
	<pre>END NEW CERTIFICATE REQUEST </pre>

شكل ١٠: فايل درخواست گواهينامه

گام بعدی این است که این درخواست گواهی به یک CA ارسال شود و سپس گواهی SSL میتواند از طرف CA صادر شود. اگر شما میخواهید از یک CA خصوصی استفاده کنید کار را در فصل مربوطه ادامه دهید.









۴ صدور گواهی SSL برای Exchange 2013 از CA خصوصی

در زمان پیکربندی گواهی SSL در Exchange Server 2013، ممکن است که مرکز صدور گواهی خصوصی را به جای تجاری انتخاب کنید. با این فرض که قسمت قبل را به درستی انجام دادهاید، حال یک درخواست گواهی برای Exchange Server 2013 در اختیار دارید و ادامه کار را در این قسمت بیان میکنیم.

Active Directory Certificate Service نصب و پیکربندی نقش ۱-۴

مراحل زیر را به منظور پیکربندی انجام دهید:

در ابتدا به Server Manager و سپس به Add Roles and Features بروید.

WELCOME TO S	ERVER MANAGER
QUICK START	 Configure this local server Add roles and features
9 🚡	Add Roles and Features Wizard
Before you begin	DESTINATION SERVER WIN-OQDMIIPCTSP.apa.local
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website. To remove roles, role services, or features: Start the Remove Roles and Features Wizard Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again. To continue, click Next.
	Skip this page by default
	< Previous Next > Install Cancel

شكل ۱۱: پنجره اضافه كردن نقشها



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ <u>autcert@aut.ac.ir</u> ها Email: <u>autcert@aut.ac.ir</u>





گزینه Active Directory Certificate Services را انتخاب کنید.



شكل ۱۲: انتخاب Active Directory Certificate Services

گزینههای Certification Authority Web Enrollment و Certification Authority Web Enrollment

B	AD CS Configuration	_ D X
Role Services		DESTINATION SERVER WIN-OQDMIIPCT5P.apa.local
Credentials Role Services Confirmation Progress Results	Select Role Services to configure Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service	
	More about AD CS Server Roles	
	< Previous Next >	Configure Cancel

شکل ۱۳: انتخاب سرویسهای مورد نظر



مرکز پژوهشی آیا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ <u>autcert@aut.ac.ir</u> ها Email: <u>autcert@aut.ac.ir</u> ها Web: <u>https://apa.aut.ac.ir</u>





گزینه Enterprise را انتخاب کنید.



شكل ۱۴: انتخاب Enterprise براى CA



شکل ۱۵: انتخاب Root CA



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور - ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ <u>aut.ac.ir</u> ۱۵۹۱۶۳۴۳۱۱ : Web: <u>https://apa.aut.ac.ir</u>





گزینه Create a new Private key را مطابق شکل زیر انتخاب کنید.



شکل ۱۶: ساخت کلید جدید

مطابق شکل زیر، موارد مورد نظر را انتخاب کنید و توصیه می شود برای امنیت بیشتر از SHA256 استفاده کنید.

2	AD CS Configuration	
Cryptography for	CA	DESTINATION SERVER WIN-OQDMIIPCT5P.apa.local
Credentials Role Services	Specify the cryptographic options	
Setup Type	Select a cryptographic provider:	Key length:
CA Type	RSA#Microsoft Software Key Storage Provider	▼ 2048 ▼
Private Key	Select the hash algorithm for signing certificates issued by this CA:	
Cryptography	SHA256	^
CA Name	SHA384	=
Validity Period	SHA512	-
Certificate Database	SHA1	
Confirmation	MD5	· _
Progress	Allow administrator interaction when the private key is accesse	d by the CA.
Results		
	More about Cryptography	
	< Previous Next >	Configure Cancel

شکل ۱۷: انتخاب موارد مربوط به رمزنگاری



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ <u>aut.ac.ir</u> ۱۵۹۱۶۳۴۳۱۱ فسطانی فال





با زدن Next به مرحله بعد بروید.



شکل ۱۸: انتخاب نامی برای CA



شکل ۱۹: تکمیل فرآیند نصب و پیکربندی

مراحل نصب و پیکربندی به پایان رسیده است.









۲-۴ دریافت گواهی دیجیتال

همانطور که در شکل زیر نشان داده شده است، با باز کردن پنجره IIS manager، صفحه "CertSrv" را می بینید.



شکل ۲۰: مشاهده CertSrv در پنجره IIS Manager



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ : Web: <u>https://apa.aut.ac.ir</u> - Email





زمانی که شما فایل درخواست گواهی را آماده کردید، ابتدا مرور گر خود را باز کنید و به صفحه ثبت نام CA خصوصی مورد نظر بروید و روی گزینه "درخواست یک گواهی" کلیک کنید.

🗲 🗇 🧭 https://localhost/certsrv/ 🔎 👻 😵 Certificate 🖉 🎑 Microsoft Active Directory 🗴 🏠 🛠
Microsoft Active Directory Certificate Services apa-WIN-OQDMIIPCT5P-CA Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> <u>Documentation</u> .
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

شکل ۲۱: درخواست گواهی جدید از مرکز صدور گواهی خصوصی







درخواست گواهیای که ایجاد کرده بودید را ارسال کنید.

🗲 🄿 🥖 https://localhost/certsrv/certrqu: 🔎 - 😵 Certificate e 🖒 🧭 Microsoft Active Directory 🗴	- □ ×
Microsoft Active Directory Certificate Services – apa-WIN-OQDMIIPCT5P-CA	Home
Request a Certificate	
Select the certificate type: User Certificate	
Or, submit an advanced certificate request.	

شکل ۲۲: ارسال درخواست گواهی

گزینه دوم را به منظور ارسال درخواست گواهی با استفاده از فایل ارسال کنید.

	_ D X
🗲 🛞 🧟 https://localhost/certsrv/certrgac 🔎 👻 😵 Certificate e 🖒 🎯 Microsoft Active Directory 🗙	☆ ★ 1
Microsoft Active Directory Certificate Services – apa-WIN-OQDMIIPCT5P-CA	Home ^
Advanced Certificate Request	
The policy of the CA determines the types of certificates you can request. Click one of the following options	to:
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal re using a base-64-encoded PKCS #7 file.	<u>equest by</u>

شكل ۲۳: ارسال فايل درخواست گواهي

فایل درخواست گواهی خود را در Notepad باز کنید و در جای مورد نظر کپی کنید و سپس قسمت نوع گواهی را به Web Server تغییر دهید.







E http	s://localhost/certsrv/certrqxt 🔎 🗝 😵 Certificate e 🖒 🥖 Microsoft Active Directory 🗴	×
Submit a Cert	ficate Request or Renewal Request	^
To submit a sav renewal reques	red request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 t generated by an external source (such as a Web server) in the Saved Request box.	ł
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	pHs1XU7paw23ga+CzeXTra8Tw92S/s2znOgG5cz2: ZPd0DXpE8mVJGR2eMAqquHt4pQbKMRP1uxP47VBG 1Ef5A4V4o7iDzocxcECdNQbcI1UxRUnd0UF2Gs8II p06E5rDKnubM75t0jFo= END NEW CERTIFICATE REQUEST	
Certificate Temp	late:	
	Web Server V	
Additional Attrib	utes:	
Attributes:		
	Submit >	~

شكل ۲۴: وارد كردن اطلاعات مربوط به فايل درخواست گواهي

در آخر، بر روی Submit کلیک کرده و بعد از آن، CA پردازشهای مورد نظر را انجام میدهد و گواهی مورد نظر را برای دانلود در اختیار شما قرار میدهد.

	File	Home	Share	View			
1	€ ⊜	т †	퉬 🕨 This	PC 🕨 Downloads	▶ Base 64	~ d) Sear
	🔶 Fav	orites		Name	•	Date modified	Туре
	💻 D	esktop		🔄 certnew.cer		8/23/2016 4:05 AM	Security
	-)@@	https://	localhost/ce	ertsrv/certfnsh 🔎 🗣	🛛 😵 Certificate e 🖒	Ø Microsoft Active Directo	iry ×

Microsoft Active Directory Certificate Services -- apa-WIN-OQDMIIPCT5P-CA

certificate Issued

he certificate you requested was issued to you.

DER encoded or

 Base 64 encoded

 <u>Download certificate</u>

 <u>Download certificate chain</u>

شکل ۲۵: دانلود گواهی SSL جدید



مرکز پژوهشی آیا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Email: autcert@aut.ac.ir ۶۶۴۶۰۳۰۸



۵ چگونگی کامل کردن مراحل انتظار بررسی درخواست گواهی

بعد از اینکه درخواست گواهی را ایجاد کردید و گواهی SSL را از مرکز مورد نظر دریافت کردید حال نیاز دارید تا مراحل "Pending certificate request" را کامل کنید.

در Exchange Administration Center (EAC) به مسیر Servers -> Certificates بروید و سپس سروری "Pending به صورت Pending" که میخواهید گواهی SSL را برای آن پیکربندی کنید، انتخاب کنید (که وضعیت آن به صورت request) (request) (توا

servers databases database availability groups virtual directories certificates

Select server: WIN-OQDMIIPCT5P.apa.local ✓ + ✓ m ♂ m ↔

NAME	STATUS	EXPIRES ON
Exchange2013Certificate	Pending request	8/23/2017
	Valid	8/23/2017
Microsoft Exchange Server Auth Certificate	Valid	7/27/2021
Microsoft Exchange	Valid	8/22/2021
	Valid	8/23/2021
WMSVC	Valid	8/20/2026

شکل ۲۶: Pending certificate request در ۲۶

به منظور کامل کردن کار، بر روی pending request مشخص شده و Complete کلیک کنید.



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ / Meb: <u>https://apa.aut.ac.ir</u> - Email: <u>autcert@aut.ac.ir</u>





Exchange2013Certificate

Certification authority-signed certificate Issuer: C=IR, S=Center, L=Tehran, O=Exchange Server pro, OU=IT, CN=apa.local

Status

Pending request Expires on: 8/23/2017

Complete

Assigned to services

NONE

شکل ۲۷: کامل کردن pending request

مسیر UNC مربوط به گواهی صادر شده توسط CA را وارد کنید و سپس روی OK کلیک کنید.

Exchange Certificate - Internet Explore	er	_ □	x
complete pending request		Н	lelp
This will import the certificate file that you received from the certification authority. After it's imported, you can assign this certificate to various Exchange services. Learn more			
*File to import from (example: \\server\folder\MyCertificate.CER):			
\\WIN-OQDMIIPCT5P\c\$\AdminCert\certnew.cer]		
	ok	cancel	
		۹ 100% م	.

شکل ۲۸: انتخاب مسیر فایل گواهی



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ <u>ettps://apa.aut.ac.ir</u> - Email: <u>autcert@aut.ac.ir</u>





زمانی که این مراحل به درستی انجام شد، با بازگشت به صفحه EAC، مشاهده میکنید که وضعیت به صورت "Valid" تغییر میکند.

servers databases database availability groups virtual directories certificates

Select server:	WIN-OQDMIIPCT5P.apa.local	\sim	
----------------	---------------------------	--------	--

+ 🖍 🖻 🗗 …

NAME	STATUS	EXPIRES ON
	Valid	8/23/2017
Exchange2013Certificate	Valid	8/23/2018
Microsoft Exchange Server Auth Certificate	Valid	7/27/2021
Microsoft Exchange	Valid	8/22/2021
	Valid	8/23/2021
WMSVC	Valid	8/20/2026

شكل ۲۹: معتبر بودن گواهي SSL

در این زمان که وضعیت به صورت "Valid" نشان داده می شود، شما می توانید گواهی SSL را به سرویس های Exchange 2013 منتصب کنید.









F استخراج و وارد کردن یک گواهی SSL به چند سرور 2013 Exchange

ممکن است بخواهید که از برخی از گواهیها بر روی چند سرور استفاده کنید. فرآیند بدست آوردن یک گواهی روی چند سرور، تقریبا شبیه به همین فرآیند برای یک سرور است. در جریان انجام فرآیند درخواست گواهی برای Exchange 2013، شما یک نام دامنه را برای دسترسی کلاینتها وارد کردید که گواهی SSL برای آن مورد استفاده قرار خواهد گرفت.

بعد از کامل کردن درخواست گواهی در سرور اول (همان جایی که درخواست گواهی تولید شده بود)، شما میتوانید گواهی را از سرور استخراج کرده و به سرورهای دیگر با گامهای زیر وارد کنید.

در Exchange Administration Center به مسیر Servers -> Certificates بروید و سروری که گواهی SSL در حال حاضر روی آن نصب است را انتخاب کنید. گواهی مورد نظر را مشخص کنید و سپس روی "..." (more) کلیک کنید و گزینه Export Exchange Certificate را انتخاب کنید.



شکل ۳۰: بیرون کشیدن گواهی Exchange

یک مسیر UNC معتبر و همچنین نامی را برای ذخیرهسازی گواهی و همچنین رمز عبور برای استخراج گواهی وارد کنید. باقی مراحل را انجام داده و کار را به اتمام برسانید.







Exchange Certificate - Internet Explorer		-		x
export Exchange certificate			H	lelp
This wizard will export the "Exchange2013Certificate" certificate to a file, along with its private key. You must protect this file with a password. Learn more				
*File to export to (example: \\server\folder\MyCertificate.PFX):	_			
\\WIN-OQDMIIPCT5P\c\$\AdminCert\certexport.pfx				
*Password:				
•••••••				
	ok	cancel		
		۹ ۱	00%	•

شکل ۳۱: انتخاب مسیر برای ذخیره سازی گواهی بیرون کشیده شده

دوباره آیکن "more" را باز کنید و این دفعه گزینه Import Exchange Certificate را انتخاب کنید.



شکل ۳۲: وارد کردن یک گواهی SSL در Exchange

سپس مسیر UNC و همچنین رمز عبوری که در زمان استخراج گواهی انتخاب نمودید را وارد کنید.









Exchange Certificate - Internet Explo	orer 📃 🗖 🗙
import Exchange certificate	Help
This wizard will import a certificate from a file. Learn more	
*File to import from (example: \\server\folder\MyCertificate.CER):	
\\WIN-OQDMIIPCT5P\c\$\AdminCert\certexport.pfx	
This file may be password protected. Password:	
•••••	
	next cancel
	🔍 100% 🔻 🔡

شکل ۳۳: وارد کردن مسیر UNC و رمز عبور گواهی

روی "+" کلیک کنید و سرورهای Exchange 2013 که میخواهید گواهی را به آن وارد کنید، انتخاب کنید.







Sector Exchange	Certificate - Internet Explorer	_ _ X
import Exchange certificate		Help
*Specify the servers you want to apply this certificate	to. Learn more	
+ -		
NAME		You can apply the
WIN-OQDMIIPCT5P.apa.local		certificate to one or more servers.
	back f	inish cancel

شکل ۳۴: انتخاب سرورهای Exchange به منظور وارد کردن گواهی SSL به آنها

بر روی **Finish** کلیک کنید تا کار به اتمام برسد.

بعد از اینکه گواهی را به سرور اضافه کردید، شما میتوانید کار را با انتصاب گواهی SSL به سرویسهای Exchange ادامه دهید.







¥ 👘 انتصاب یک گواهی SSL به سرویسها در 2013 Exchange Server

زمانی که یک گواهی SSL بر روی Exchange 2013 نصب شده است، به صورت خودکار برای سرویسهای مختلف Exchange مانند IIS (برای IIAP ،POP ،(ActiveSync etc ،Outlook Anywhere ،OWA یا SMTP فعال نمیشود و مدیر سیستم باید به صورت دستی، گواهی SSL را به سرویسهای مورد نظر منتصب کند.

در Exchange Administration Center به مسیر Servers -> Certificates بروید و سروری که مایل به اختصاص گواهی SSL به آن هستید را انتخاب کنید، در اینجا وضعیت گواهی باید Valid باشد تا بتوان باقی مراحل را انجام داد.

recipients	servers databases database availab	ility groups virtual direct	ories certificates
permissions			
compliance management	Select server: WIN-OQDMIIPCT5P.apa.local	~	
organization	+∥≣ @…		
protection	NAME	STATUS	EXPIRES ON
		Valid	8/23/2017
mail flow	Exchange2013Certificate	Valid	8/23/2018
mehila	Microsoft Exchange Server Auth Certificate	Valid	7/27/2021
mobile	Microsoft Exchange	Valid	8/22/2021
public folders		Valid	8/23/2021
	WMSVC	Valid	8/20/2026
unified messaging			
servers			
hybrid			
tools			

شكل ۳۵: مشاهده ليست گواهىهاى SSL معتبر روى Exchange 2013



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ <u>autcert@aut.ac.ir</u> ۶۶۴۶۰۳۰۸





روی آیکن edit کلیک کنید و سپس Services را انتخاب کنید.

servers databases database availability groups virtual directories certificates

	Ø	Exchange Certificate - Internet Explorer	_ [X C
Select ser + 🖍	Exchange2013Certificate			Help
NAME Exchange Microsoft WMSVC	general s	Specify the services you want to assign this certificate to. Learn more SMTP Microsoft Exchange Unified Messaging Unified Messaging Call Router IMAP POP IIS	cancel	
			🔍 100	% 👻 🔐

شکل ۳۶: ویرایش پیکربندی گواهی SSL به منظور انتصاب به سرویسهای Exchange 2013

سرویسهایی را که تمایل دارید گواهی SSL به آنها منتصب شود را انتخاب کنید و بر روی Save کلیک کنید. توجه داشته باشید که سرویسهای عمومی برای انتصاب به یک گواهی IIS «SSL و SMTP هستند.







Certificate X
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
Ensures the identity of a remote computer
Issued to: apa.local
Issued by: apa-WIN-OQDMIIPCT5P-CA
Valid from 8/23/2016 to 8/23/2018
Install Certificate Issuer Statement
OK

شکل ۳۷: مشاهده گواهی در مرورگر IE









- 1 <u>http://exchangeserverpro.com/exchange-server-2013-ssl-certificates/</u>
- 2 <u>https://support.office.com/en-us/article/Add-an-SSL-certificate-to-Exchange-2013-976c080c-fda1-400d-97f4-5b65991cdf4e#BK_Request</u>
- 3 <u>http://exchangeserverpro.com/create-ssl-certificate-request-exchange-2013/</u>
- 4 <u>http://exchangeserverpro.com/exchange-2013-ssl-certificate-private-certificate-authority/</u>
- 5 <u>http://exchangeserverpro.com/exchange-2013-complete-pending-certificate-request/</u>
- 6 <u>http://exchangeserverpro.com/exchange-2013-ssl-certificate-export-import/</u>
- 7 <u>http://exchangeserverpro.com/exchange-2013-assign-ssl-certificate-to-services/</u>
- 8 <u>http://www.careexchange.in/how-to-install-certificate-authority-on-windows-server-2012</u>

