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

شماره مستند APA-AMIRKABIR-13950524-1

تاریخ نگارش ..... ۲۴ مرداد ۱۳۹۵

شماره نگارش ۲,۰

نگارش ..... آپای امیرکبیر

طبقه‌بندی ..... عادی

فهرست مطالب

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 مهم‌ترین 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 امن‌سازی پروتکل‌هایی مانند HTTP، SMTP، POP و IMAP فراهم می‌کند. بدلیل نیازمندی‌های امنیتی پیش‌فرض، نرم‌افزار Exchange Server 2013 بعد از نصب، به‌صورت خودکار با گواهی‌های self-signed پیکربندی می‌شود و برای پروتکل‌های نام برده فعال‌سازی می‌شود. در این گزارش مراحل نصب گواهی SSL بر روی Exchange Server 2013 شرح داده شده است.

[۱] Application Layer

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

۲ شرایط گواهی SSL برای Exchange 2013

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 UC[۲] 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 مراکز صدور گواهی (CA)[۳] معتبر دریافت کرد (یا گواهی خود-امضا را تولید کرد). گرفتن گواهی دارای مراحلی 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[۴] در واقع دوره زمانی بین صدور گواهی تا انقضای آن است. گواهی self-signed که Exchange 2013 در زمان نصب آن را صادر می‌کند برای پنج سال اعتبار دارد. یک گواهی صادر شده از یک مرکز صدور گواهی(CA) خصوصی[۵] ممکن است برای چندین سال معتبر باشد. یک گواهی که از یک مرکز صدور گواهی تجاری[۶] 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 می‌کنید و این CA یک Enterprise CA در AD forest شما است، پس 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.

---

۱ Subject Alternate Name
۲ Unified Communications
۳ Certificate Authority
۴ Certificate Validity Period
۵ Private Certificate Authority
۶ Commercial certificate authority

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

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 می‌شود 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:

۱. 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"[۲]
۴. استخراج و وارد کردن یک گواهی SSL به چند سرور Exchange 2013 (اختیاری)
۵. اختصاص دادن گواهی SSL به سرویس‌های مورد نظر در Exchange 2013

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

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

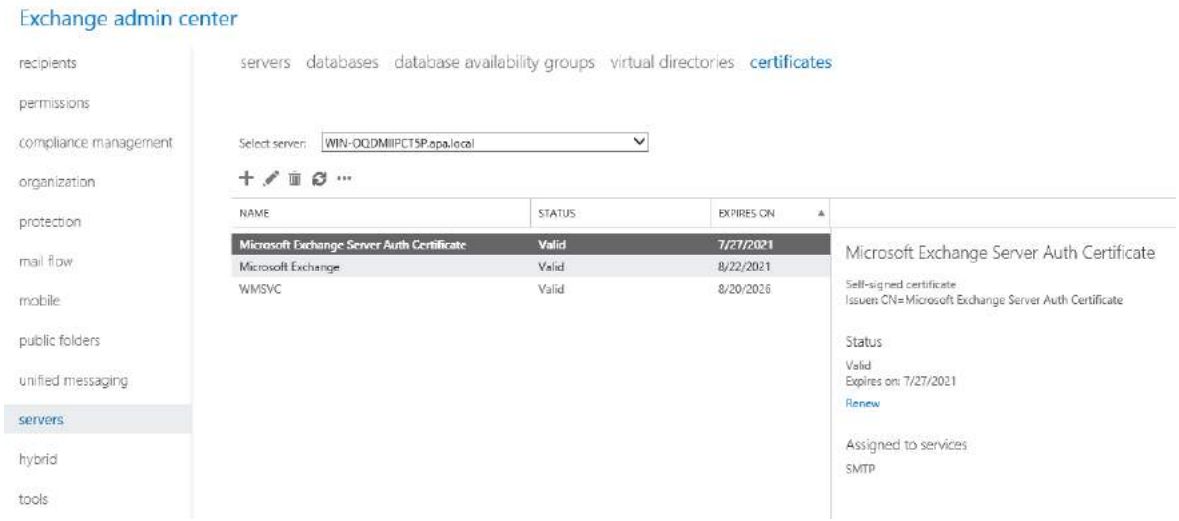
[۱] Certificate Signing Request
[۲] Pending Certificate Request

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

۳ تولید درخواست گواهی SSL برای Exchange Server 2013

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 Mailbox server نصب شده است و نام apa.local در گواهی SSL خواهند بود. درخواست گواهی می‌تواند توسط Exchange Administration Center تولید شود که روند کار آن را با ذکر مثالی در زیر بیان می‌کنیم.

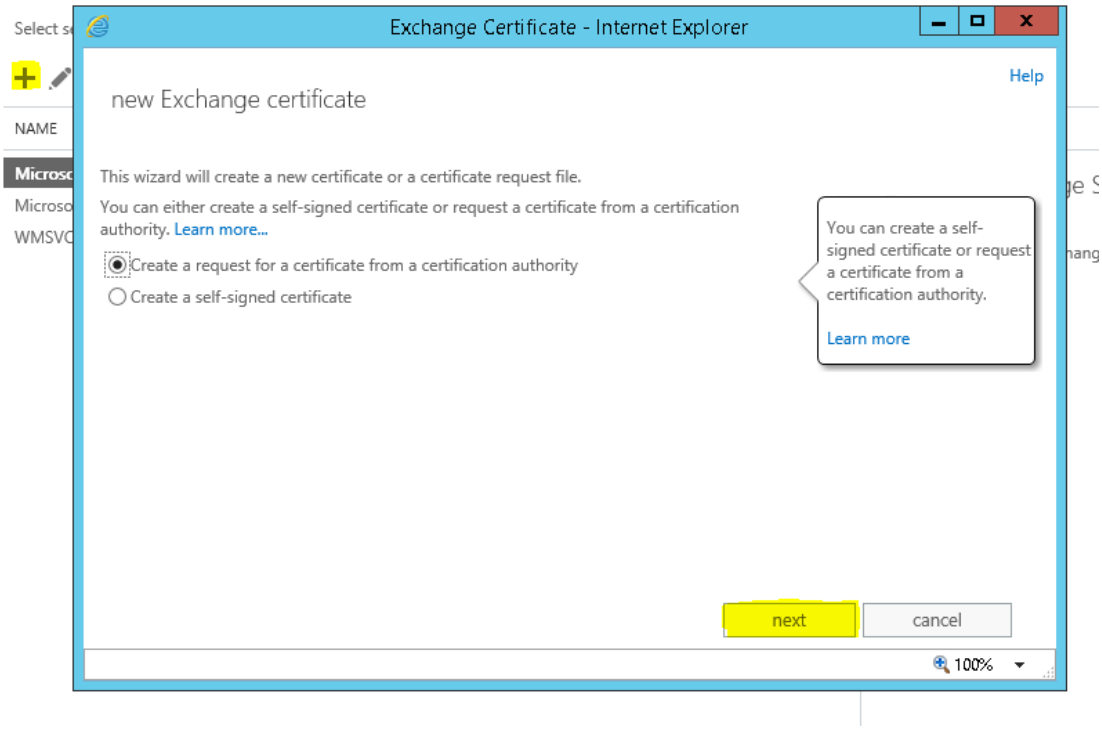
با استفاده از مرورگر خود، Exchange Administration Center را باز کنید و به مسیر -> **Servers** **Certificates** بروید:



شکل ۱: مدیریت گواهی‌ها در Exchange Administration Center

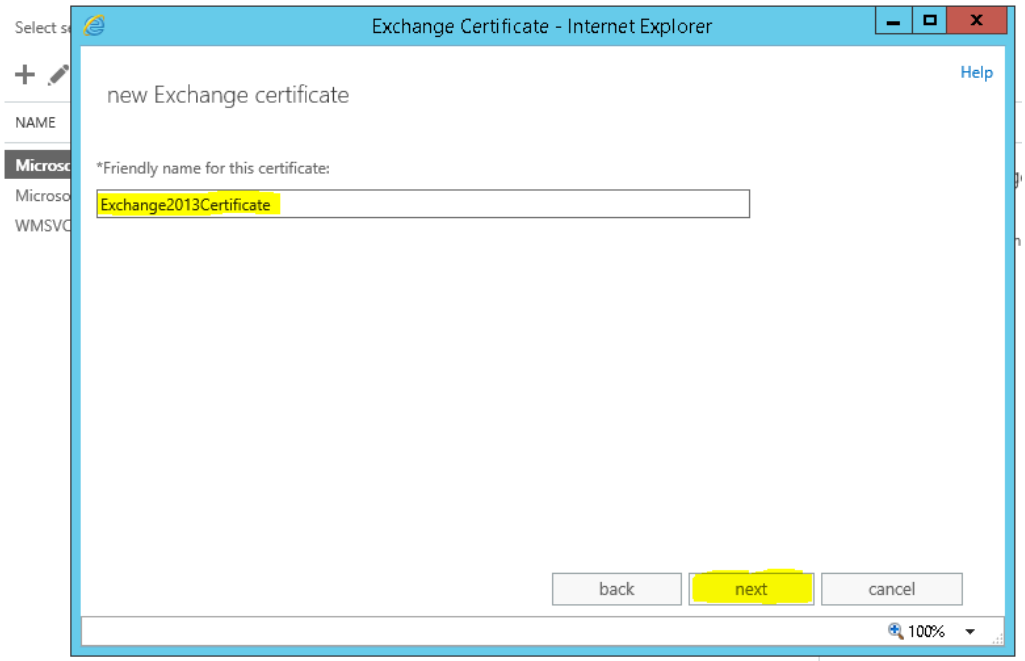
روی آیکن "+" کلیک کنید و سپس گزینه "درخواست گواهی SSL" را مانند شکل زیر انتخاب کنید و روی **Next** به منظور ادامه کار کلیک کنید.

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir



شکل ۲: شروع مراحل گواهی SSL

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

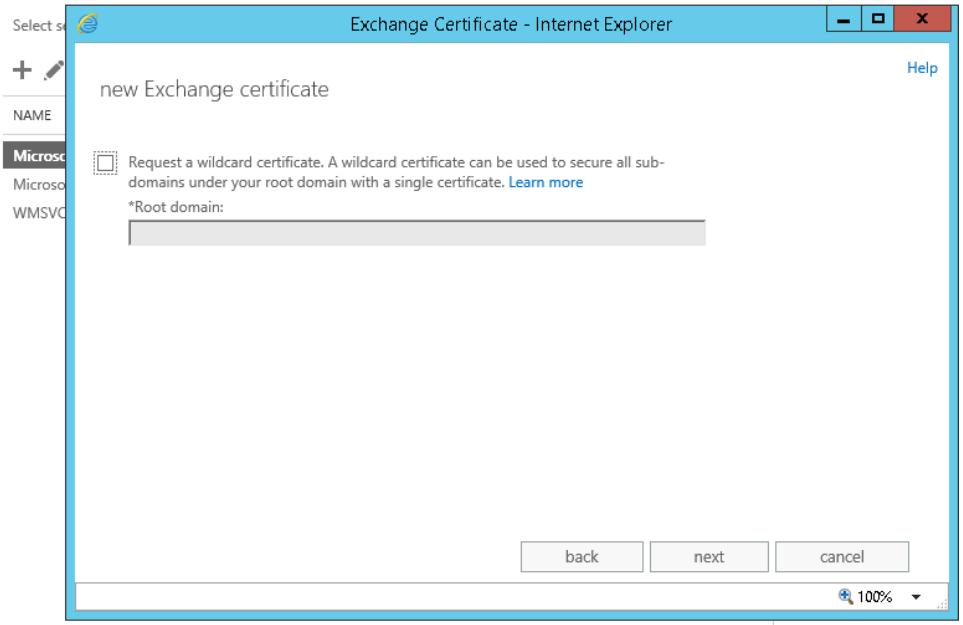


شکل ۳: نام گواهی‌نامه

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

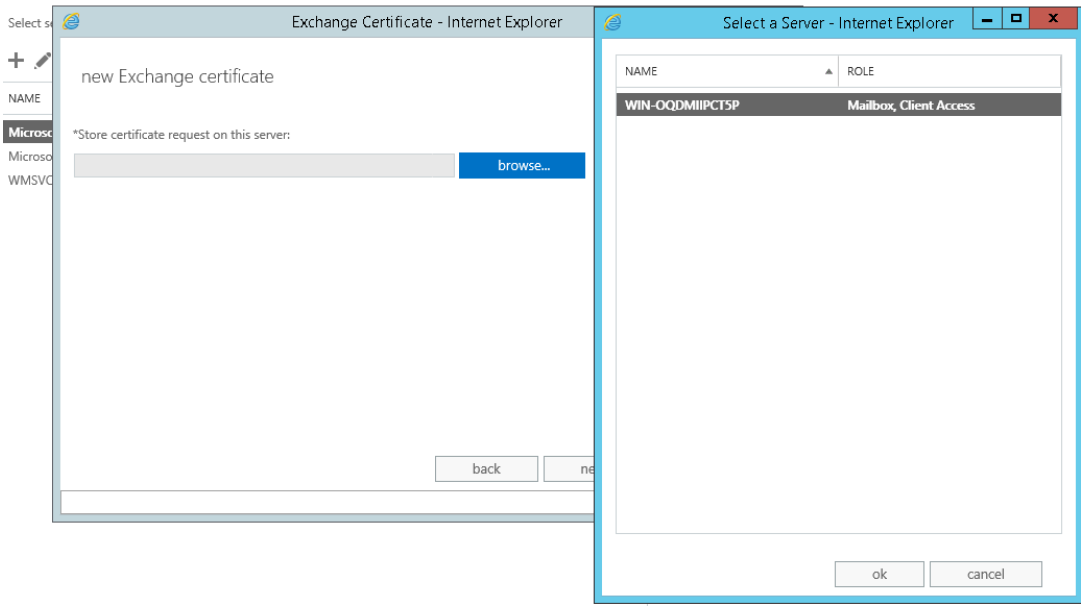
مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

آنها برای Exchange پشتیبانی می‌شوند، ولی در برخی از سرورها پشتیبانی نمی‌شوند و در اینجا ما این گزینه را انتخاب نمی‌کنیم و برای ادامه **Next** را انتخاب کنید.



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

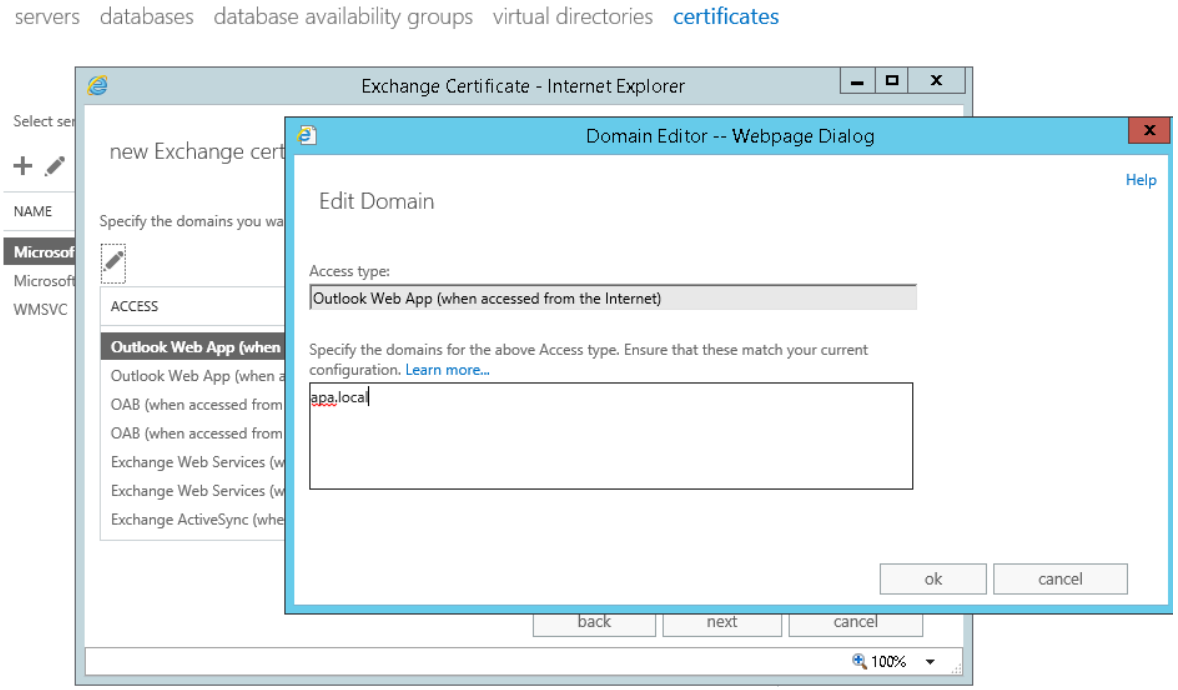
روی **Browse** کلیک کنید و سپس سرور Exchange مورد نظر (همان سروری که می‌خواهید برای آن گواهی بگیرید) را به منظور ذخیره کردن درخواست گواهی انتخاب کنید (در اینجا WIN-OQDMIIPCT5P).



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 آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

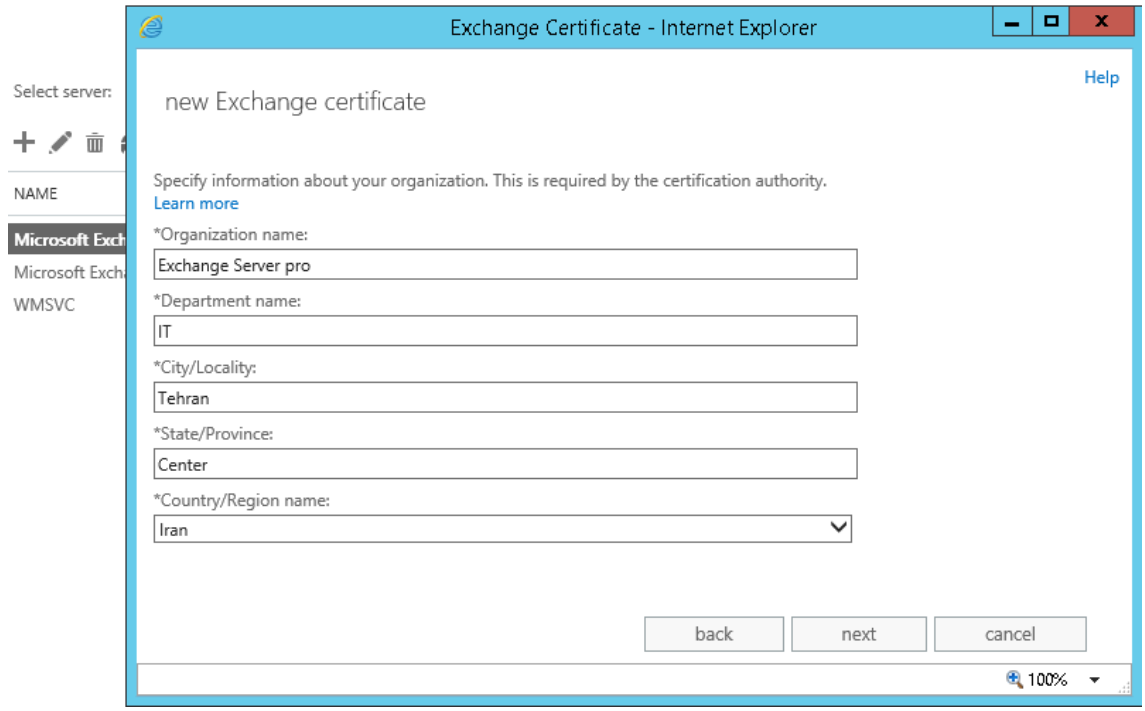


شکل ۶: پیکربندی نام‌ها به منظور اضافه کردن درخواست گواهی

اگر چندین سرویس مانند OWA، OAB، OA، EWS و ActiveSync قرار است با نام خارجی یکتا مورد استفاده قرار گیرند، نیاز است فقط یکبار این نام را برای یکی از سرویس‌ها 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.

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

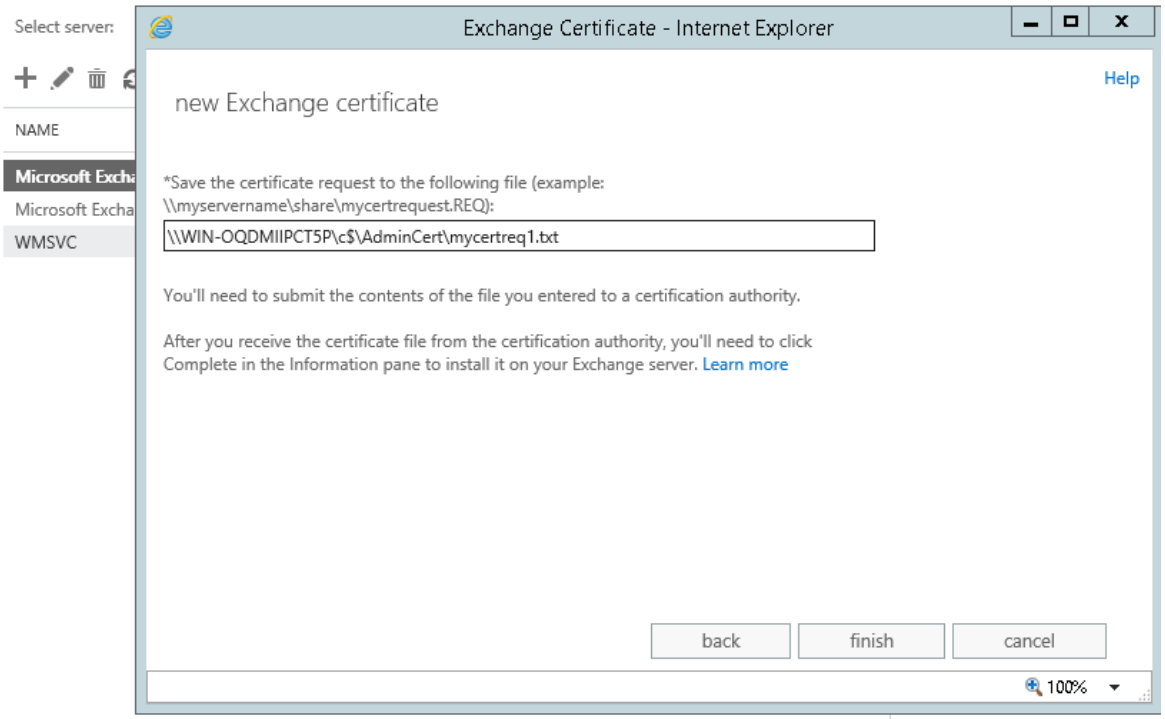


شکل ۷: وارد کردن اطلاعات سازمانی

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

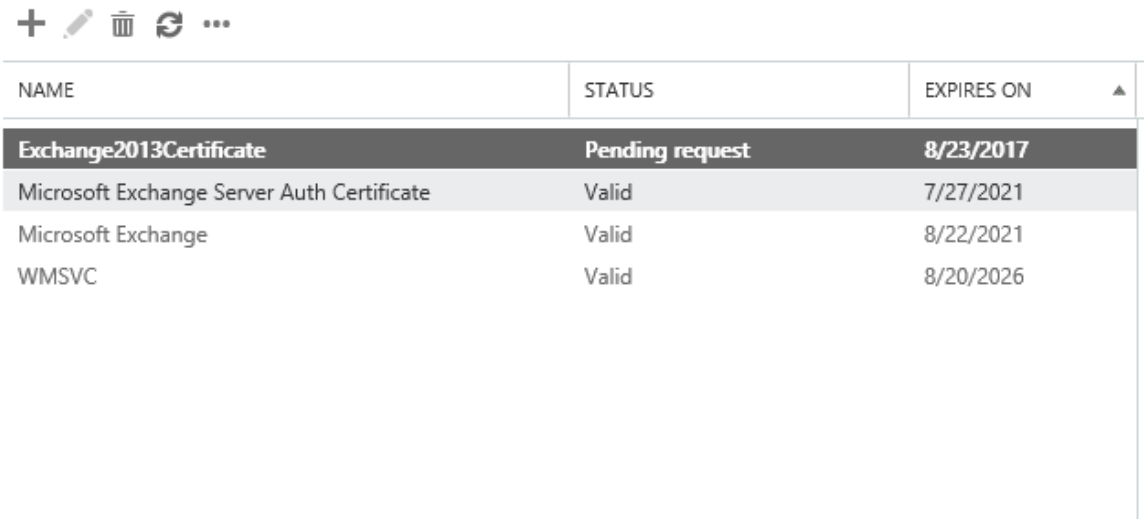
[۱] Universal Naming Convention

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir



شکل ۸: انتخاب مسیر برای ذخیره فایل درخواست گواهی

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

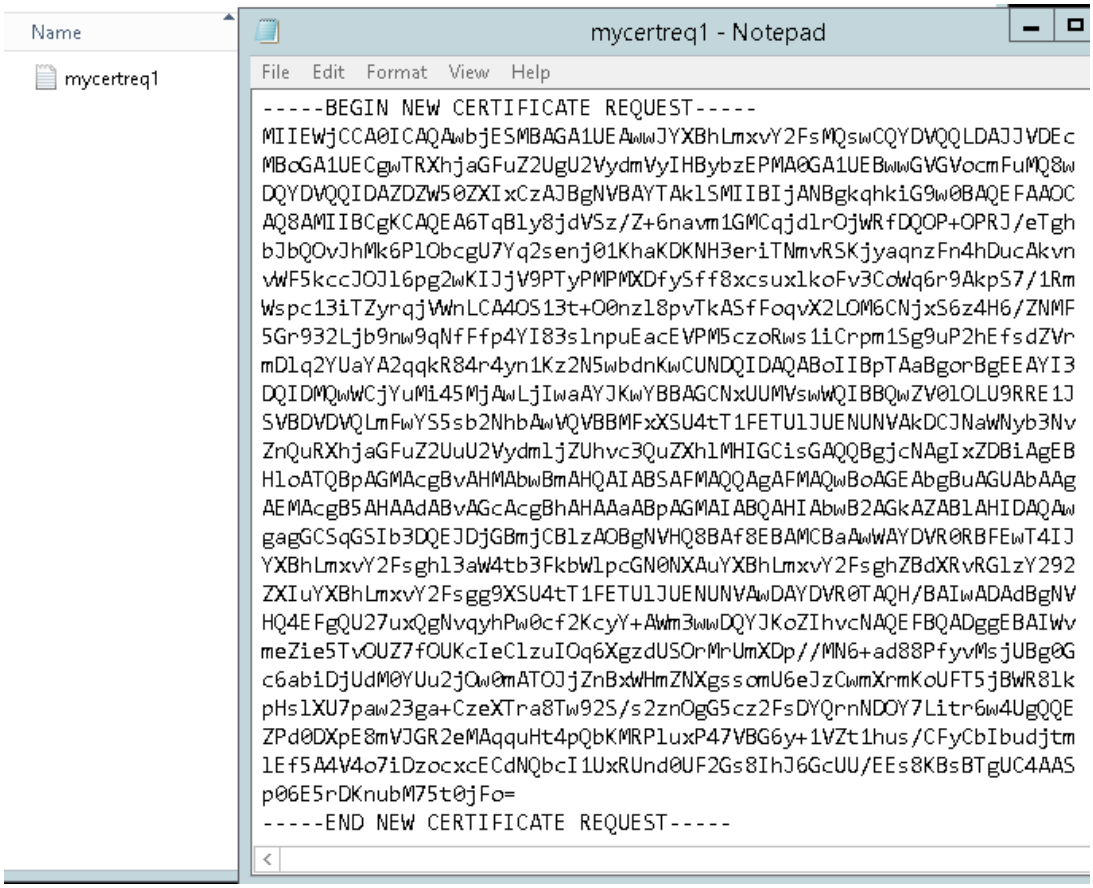


NAME	STATUS	EXPIRES ON
Exchange2013Certificate	**Pending request**	**8/23/2017**
Microsoft Exchange Server Auth Certificate	Valid	7/27/2021
Microsoft Exchange	Valid	8/22/2021
WMSVC	Valid	8/20/2026

شکل ۹: بررسی درخواست گواهی‌نامه برای Exchange 2013

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

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir



شکل ۱۰: فایل درخواست گواهی‌نامه

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.

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

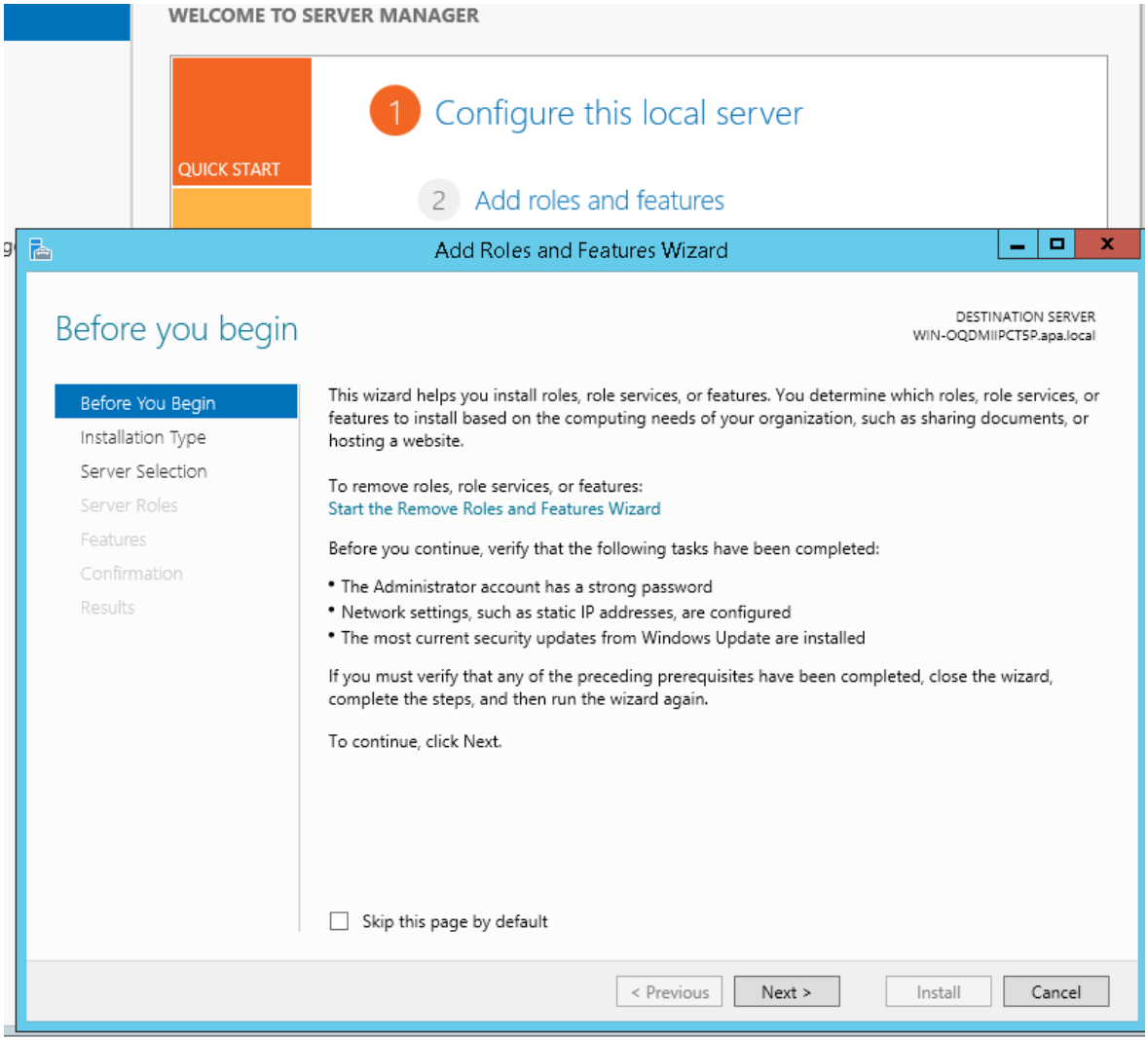
۴ صدور گواهی SSL برای Exchange 2013 از CA خصوصی

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.

۴–۱ نصب و پیکربندی نقش Active Directory Certificate Service

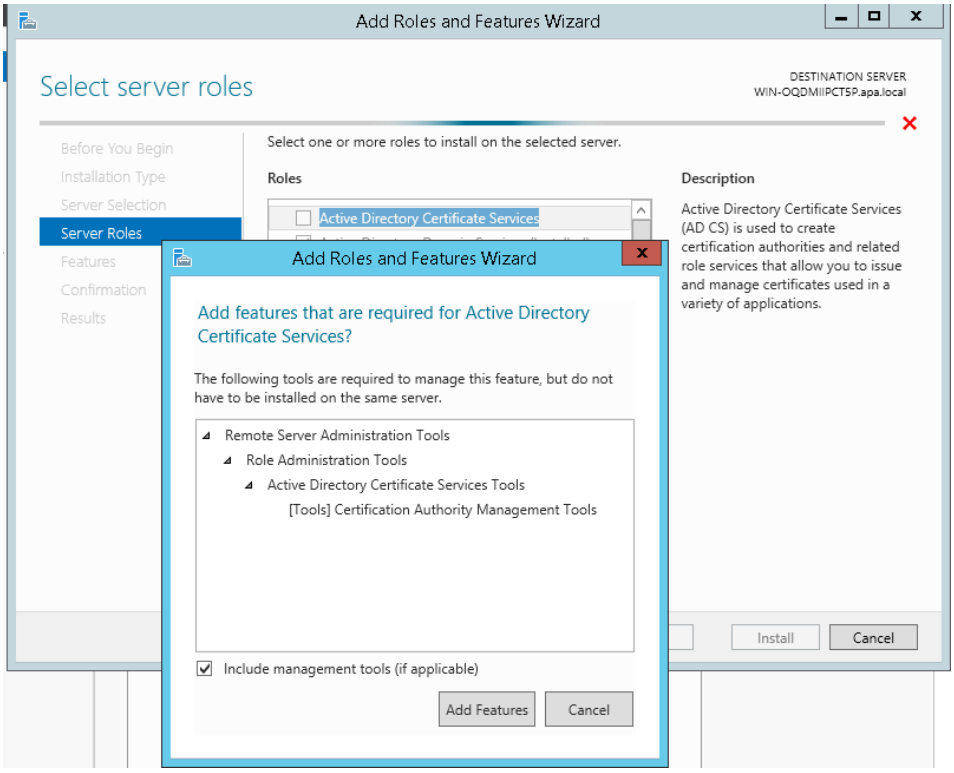
مراحل زیر را به منظور پیکربندی انجام دهید:

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



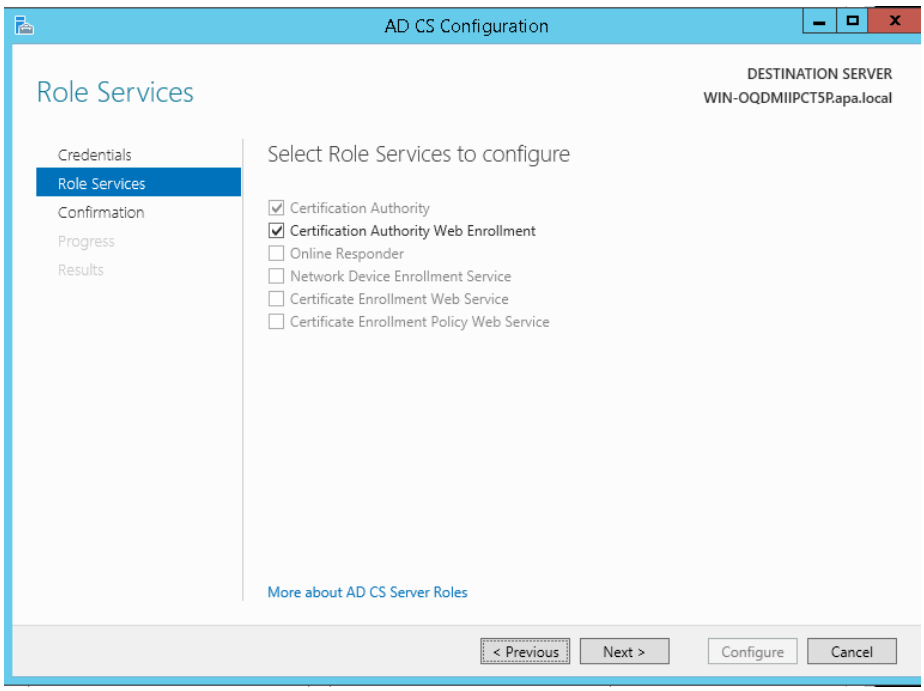
شکل ۱۱: پنجره اضافه کردن نقش‌ها

گزینه Active Directory Certificate Services را انتخاب کنید.



شکل ۱۲: انتخاب Active Directory Certificate Services

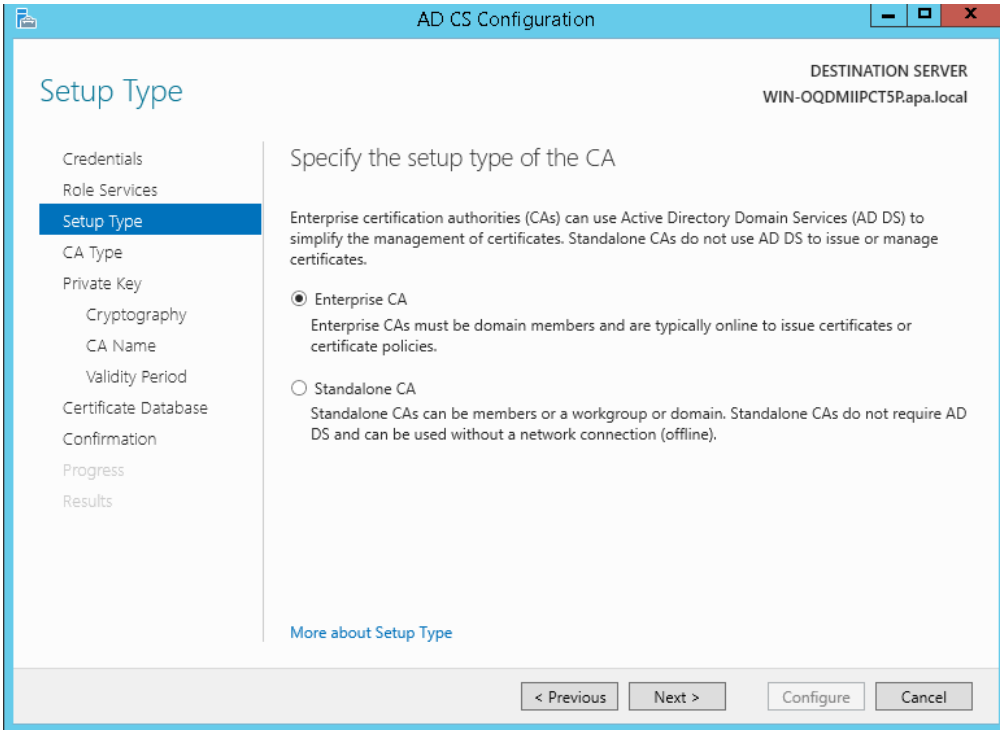
گزینه‌های Certification Authority و Certification Authority Web Enrollment را انتخاب کنید.



شکل ۱۳: انتخاب سرویس‌های مورد نظر

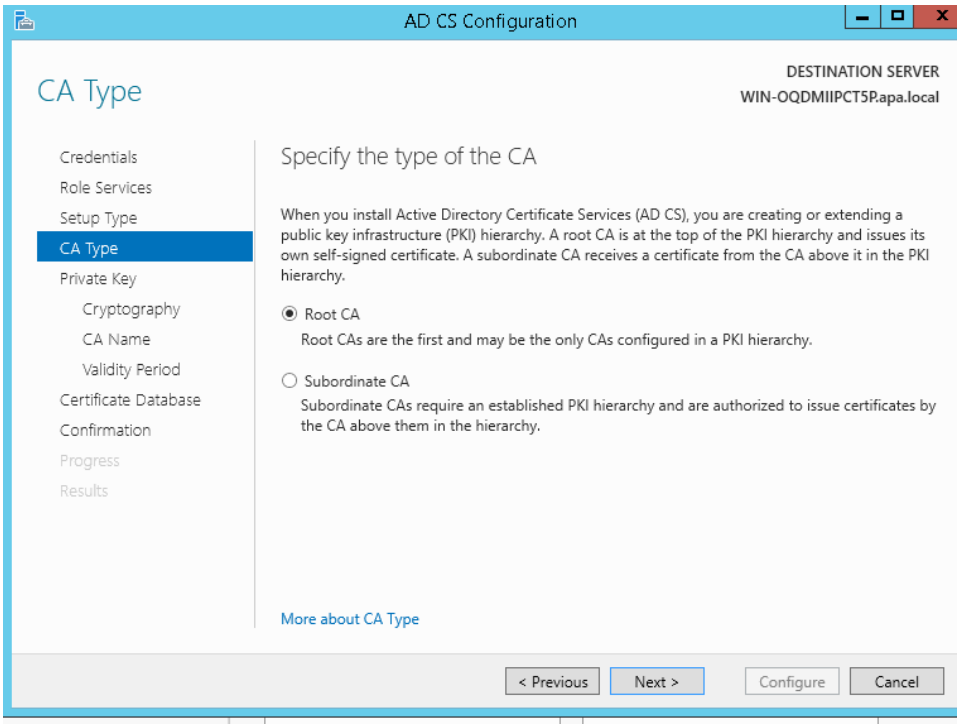
مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸
Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

گزینه Enterprise را انتخاب کنید.



شکل ۱۴: انتخاب Enterprise برای CA

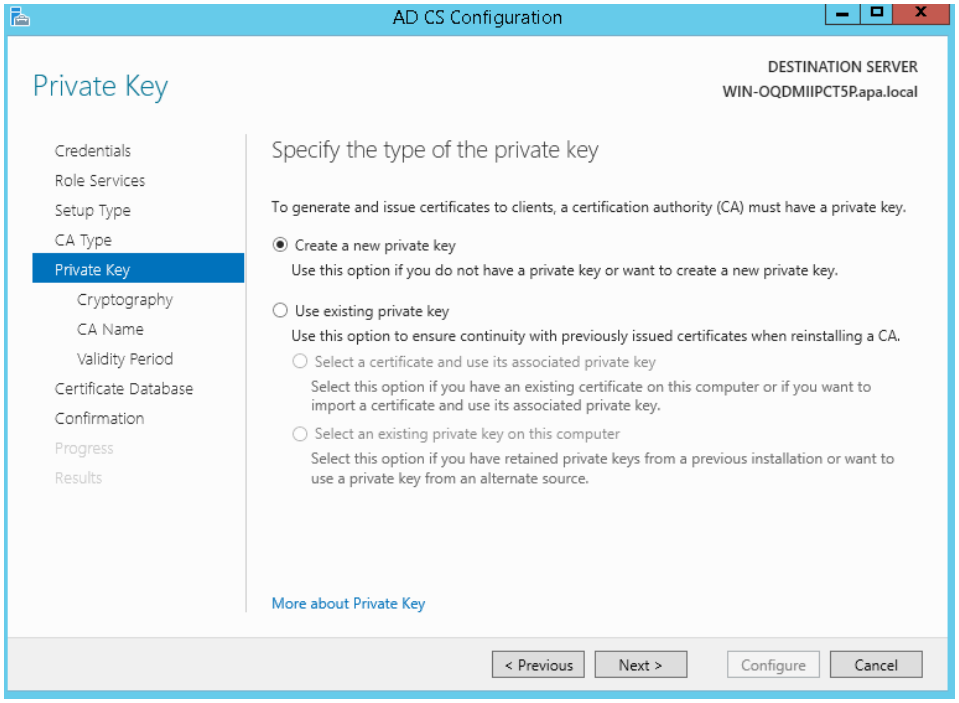
گزینه Root CA را انتخاب کنید.



شکل ۱۵: انتخاب Root CA

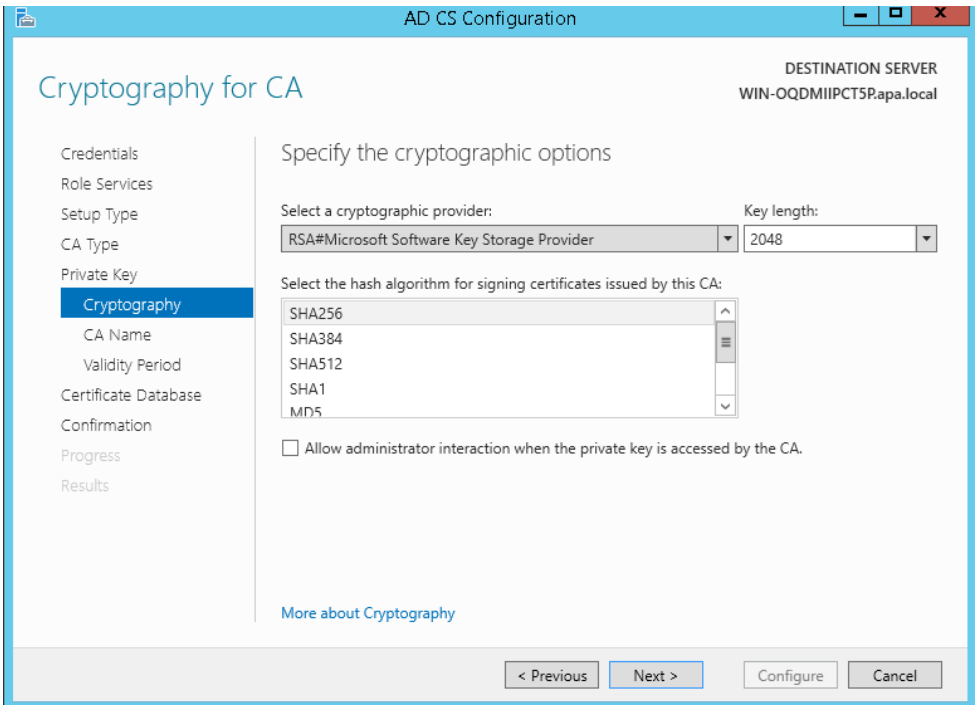
مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

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



شکل ۱۶: ساخت کلید جدید

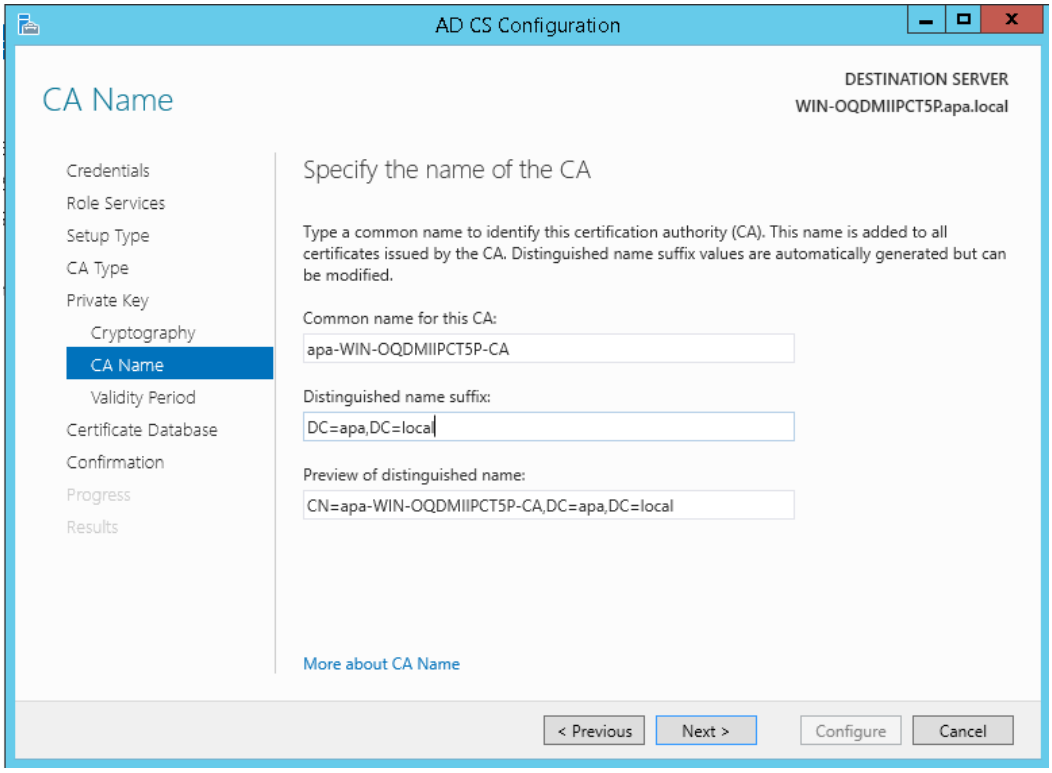
مطابق شکل زیر، موارد مورد نظر را انتخاب کنید و توصیه می‌شود برای امنیت بیشتر از SHA256 استفاده کنید.



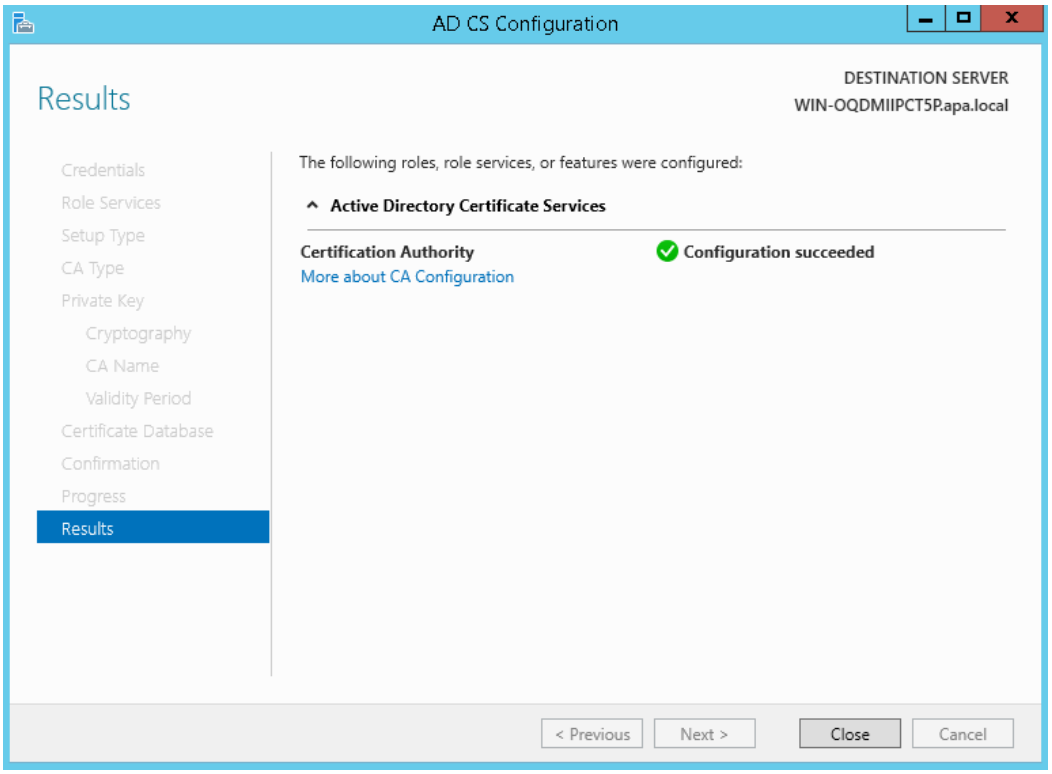
شکل ۱۷: انتخاب موارد مربوط به رمزنگاری

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

با زدن Next به مرحله بعد بروید.



شکل ۱۸: انتخاب نامی برای CA



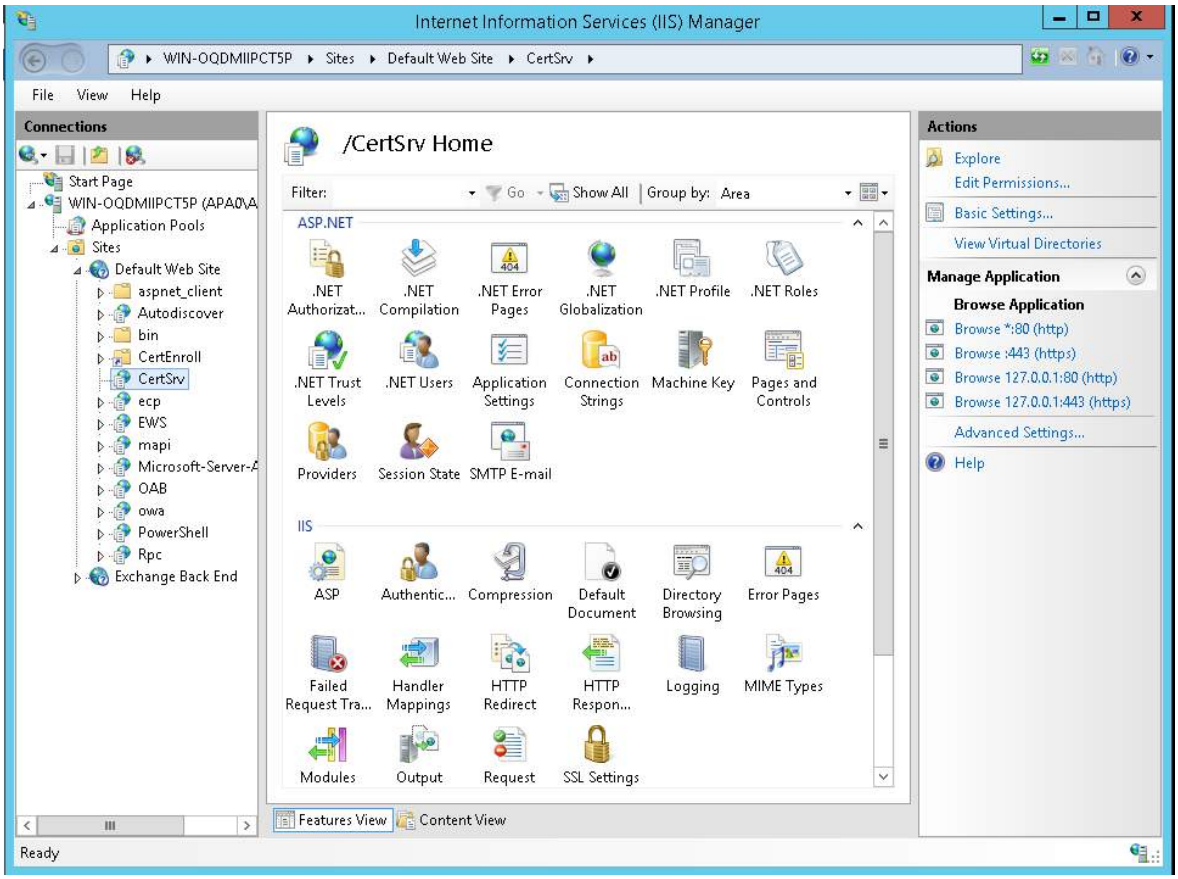
شکل ۱۹: تکمیل فرآیند نصب و پیکربندی

مراحل نصب و پیکربندی به پایان رسیده است.

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

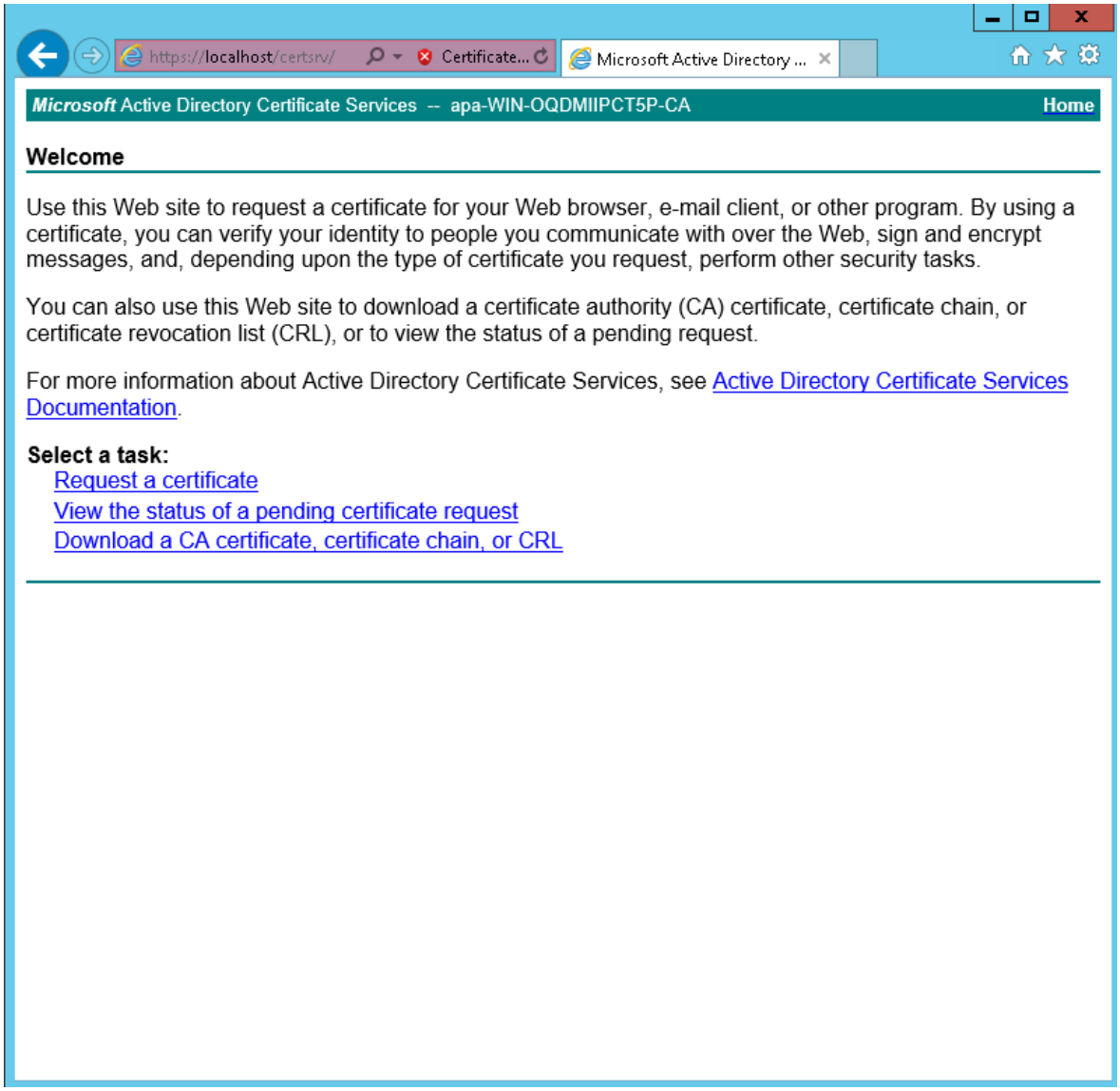
۲-۴ دریافت گواهی دیجیتال

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



شکل ۲۰: مشاهده CertSrv در پنجره IIS Manager

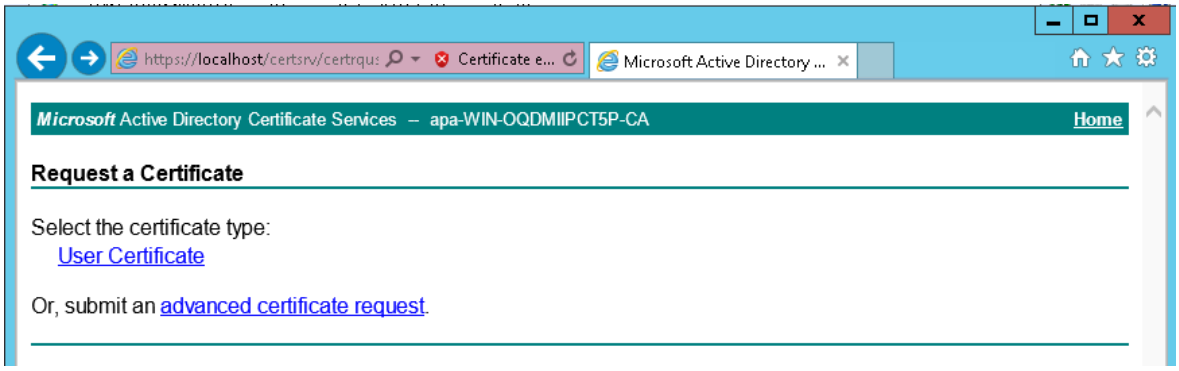
زمانی که شما فایل درخواست گواهی را آماده کردید، ابتدا مرورگر خود را باز کنید و به صفحه ثبت نام CA خصوصی مورد نظر بروید و روی گزینه "درخواست یک گواهی" کلیک کنید.



شکل ۲۱: درخواست گواهی جدید از مرکز صدور گواهی خصوصی

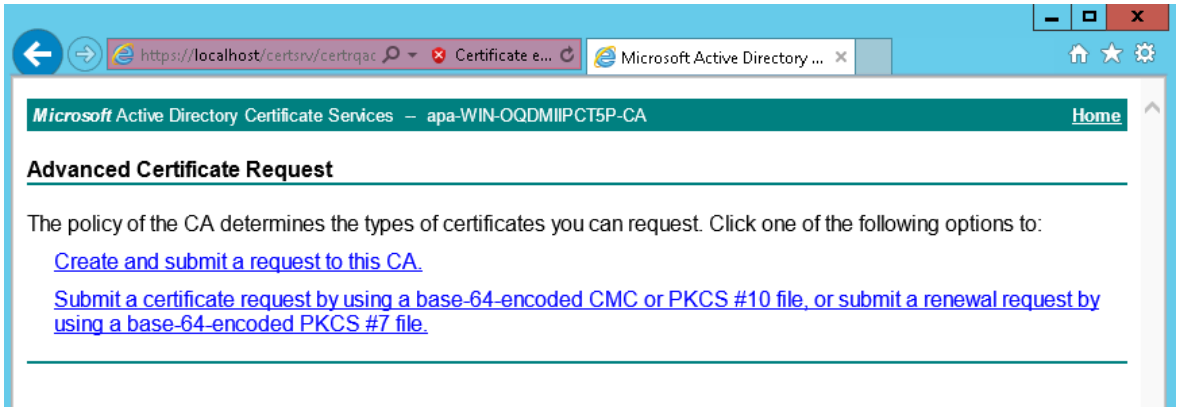
مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

درخواست گواهی‌ای که ایجاد کرده بودید را ارسال کنید.



شکل ۲۲: ارسال درخواست گواهی

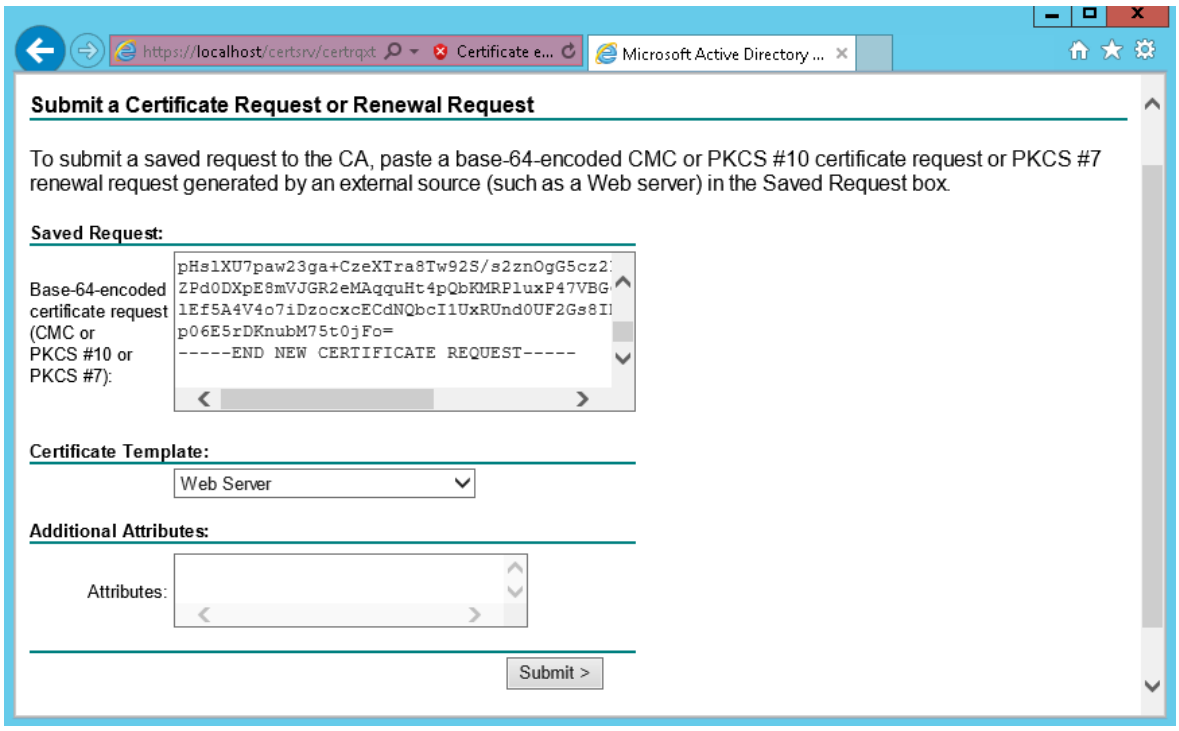
گزینه دوم را به منظور ارسال درخواست گواهی با استفاده از فایل ارسال کنید.



شکل ۲۳: ارسال فایل درخواست گواهی

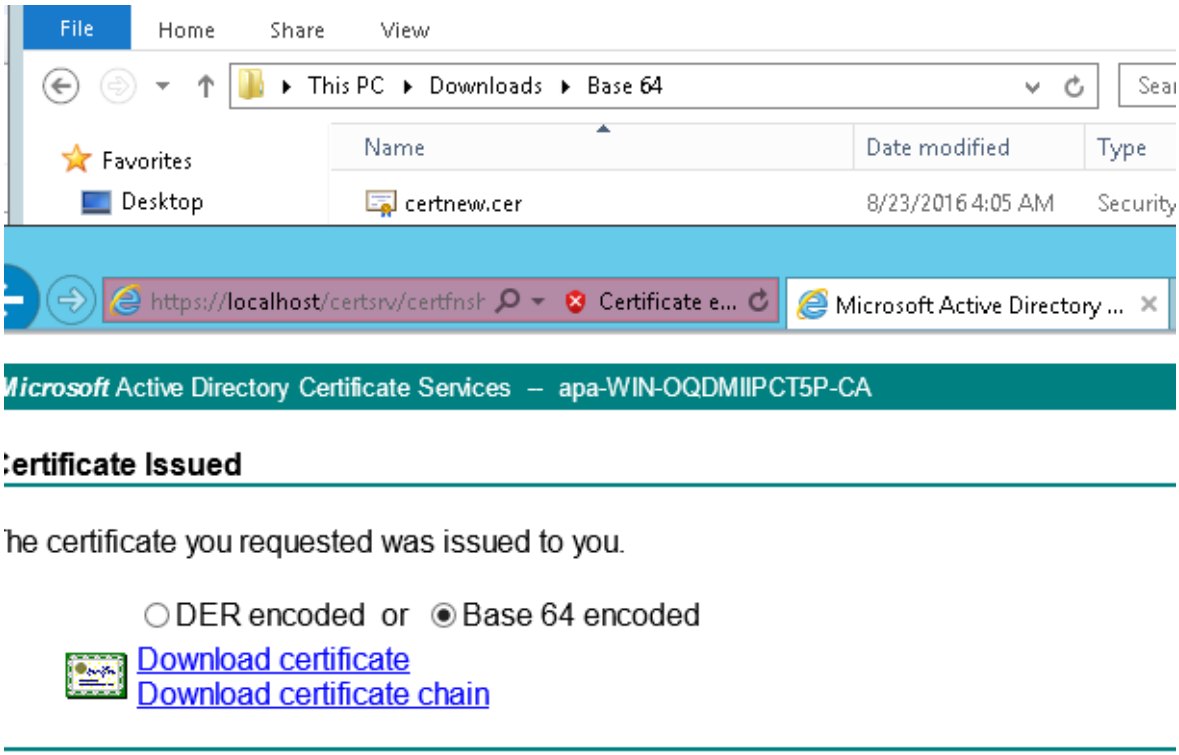
فایل درخواست گواهی خود را در Notepad باز کنید و در جای مورد نظر کپی کنید و سپس قسمت نوع گواهی را به Web Server تغییر دهید.

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir



شکل ۲۴: وارد کردن اطلاعات مربوط به فایل درخواست گواهی

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.



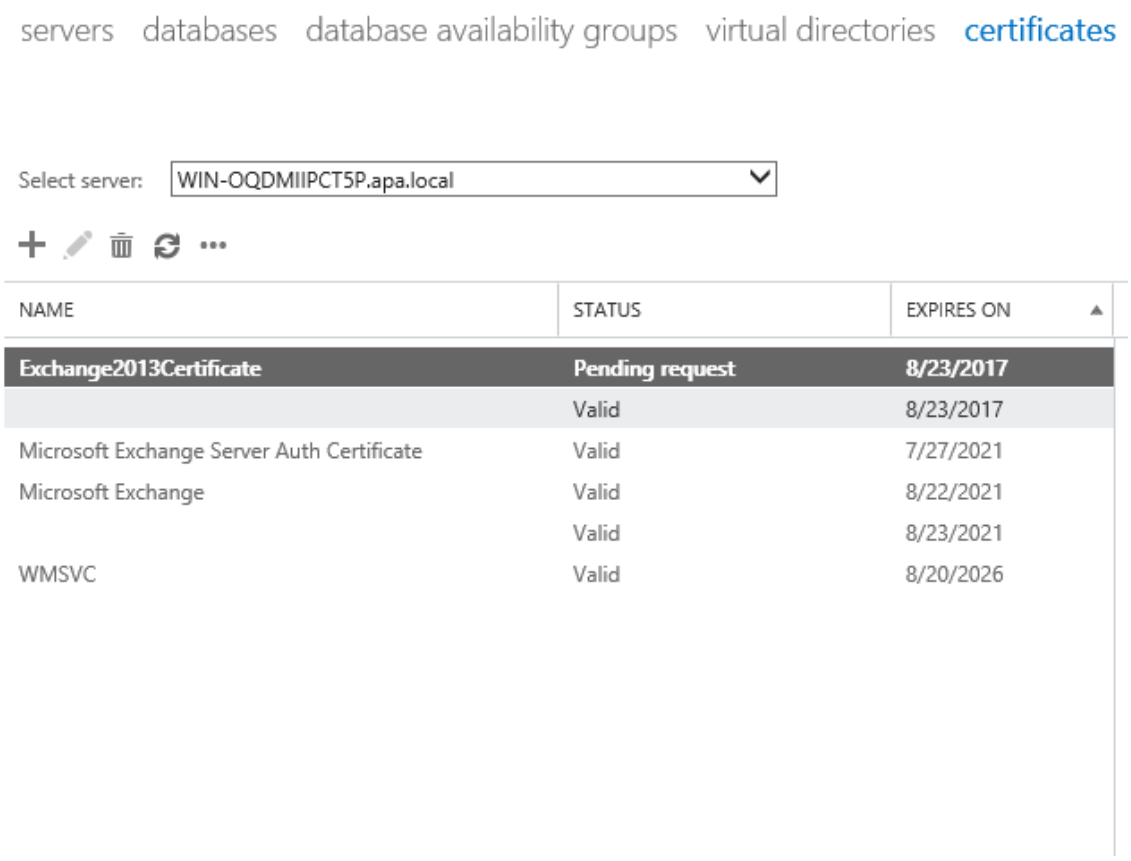
شکل ۲۵: دانلود گواهی SSL جدید

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

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.

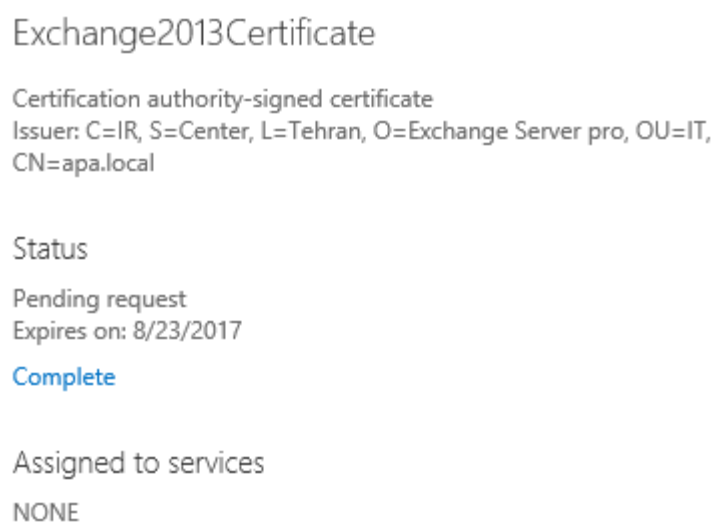
در Exchange Administration Center (EAC) به مسیر Servers -> Certificates بروید و سپس سروری که می‌خواهید گواهی SSL را برای آن پیکربندی کنید، انتخاب کنید (که وضعیت آن به صورت "Pending request" است).



شکل ۲۶: Pending certificate request در Exchange 2013

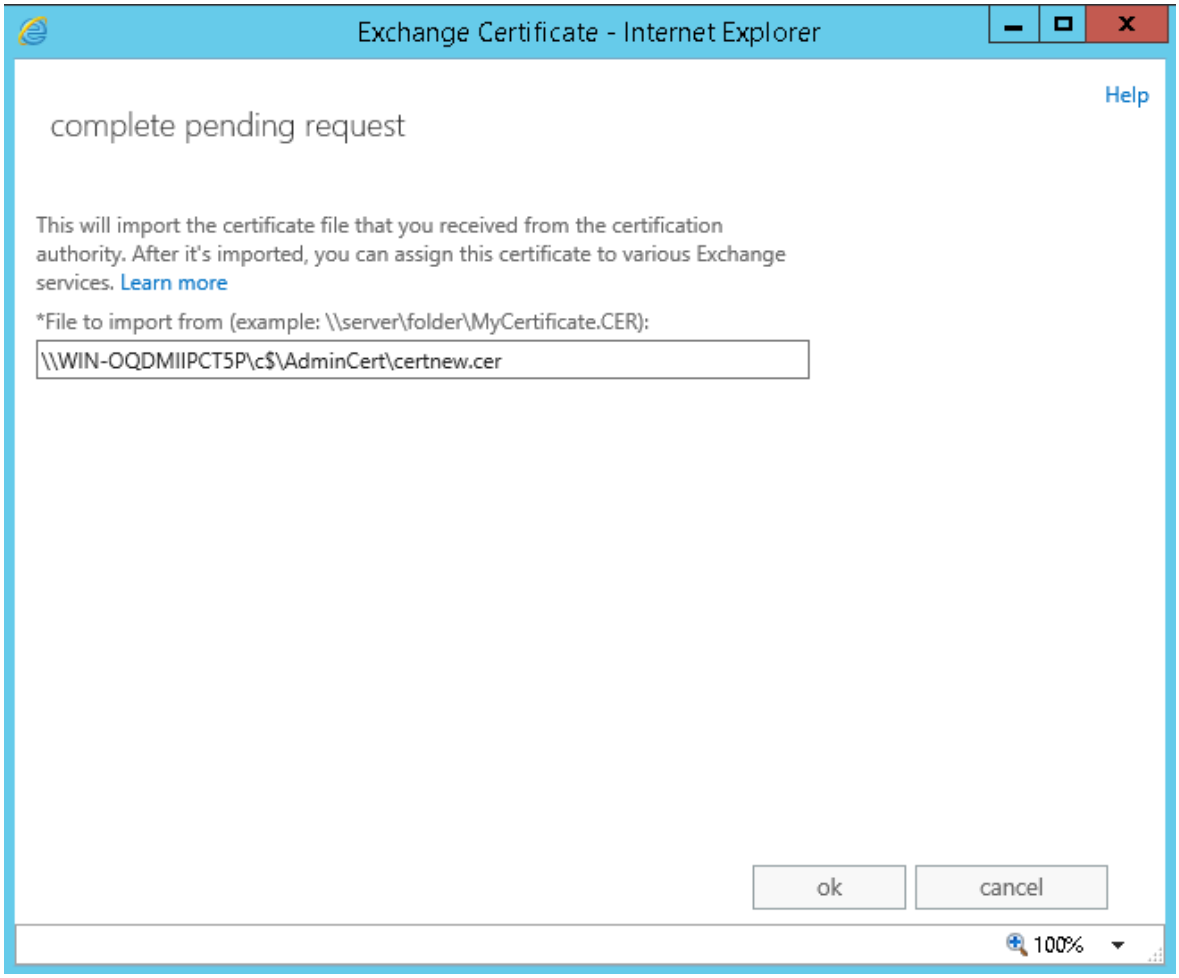
به منظور کامل کردن کار، بر روی pending request مشخص شده و Complete کلیک کنید.

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir



شکل ۲۷: کامل کردن pending request

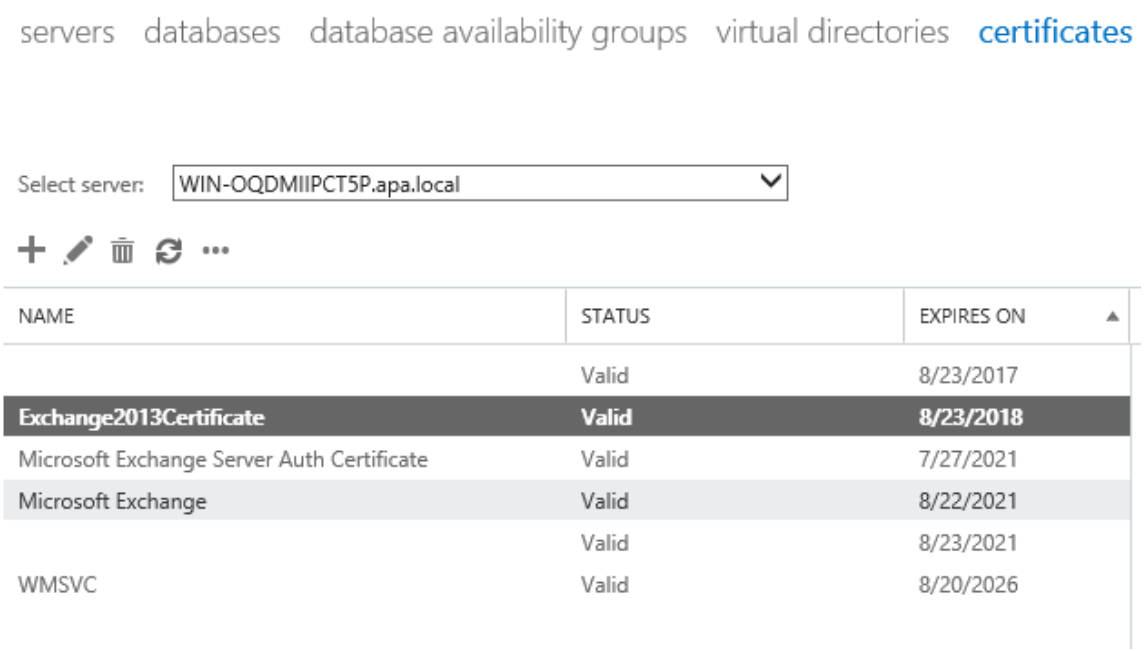
مسیر UNC مربوط به گواهی صادر شده توسط CA را وارد کنید و سپس روی OK کلیک کنید.



شکل ۲۸: انتخاب مسیر فایل گواهی

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

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



شکل ۲۹: معتبر بودن گواهی SSL

در این زمان که وضعیت به صورت "Valid" نشان داده می‌شود، شما می‌توانید گواهی SSL را به سرویس‌های Exchange 2013 منتصب کنید.

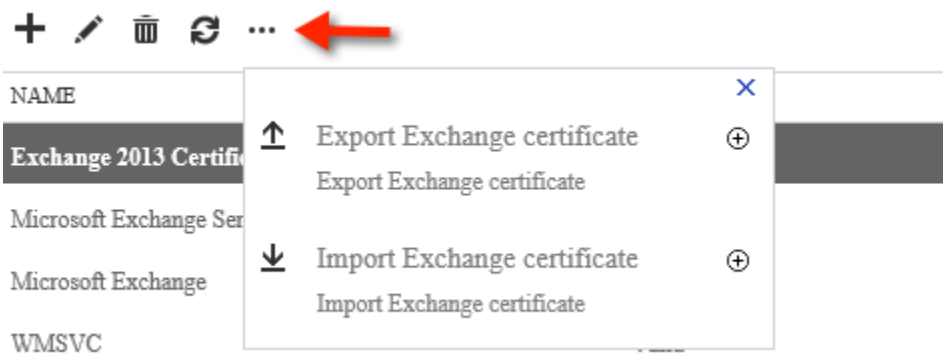
مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

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

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.

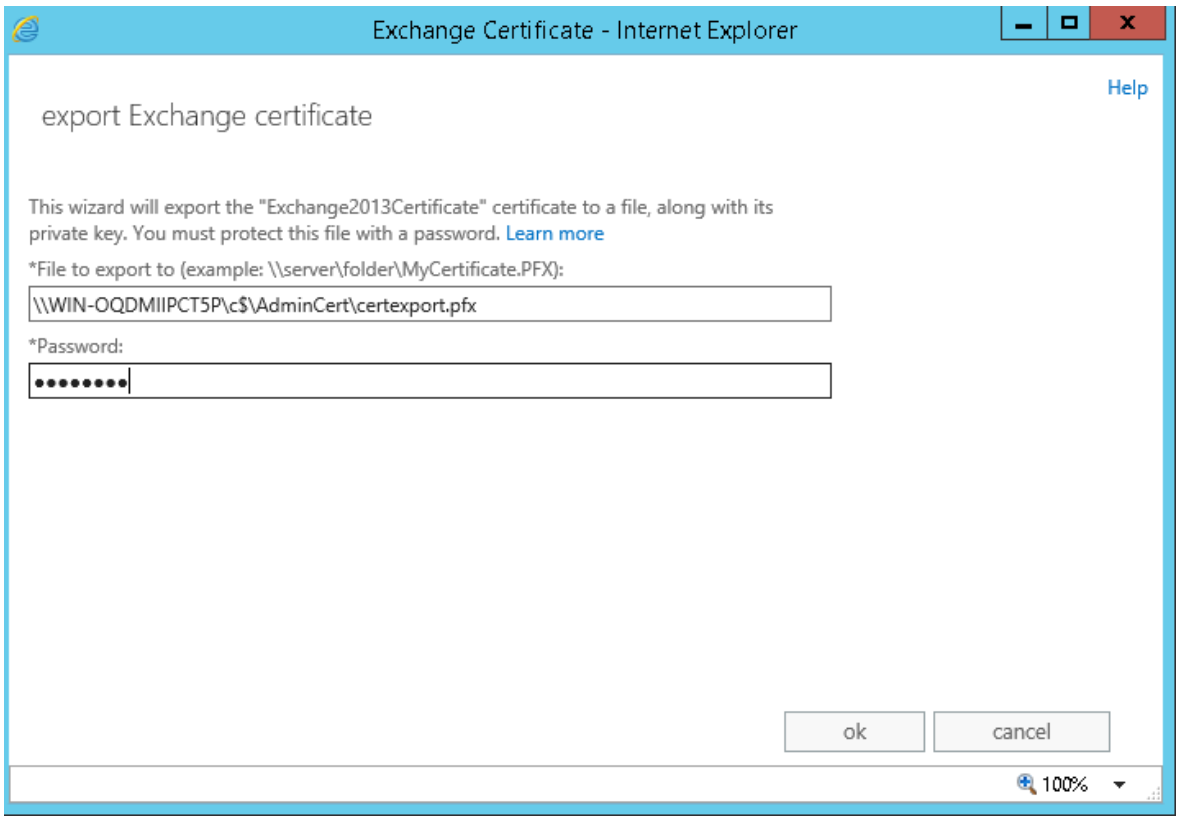
بعد از کامل کردن درخواست گواهی در سرور اول (همان جایی که درخواست گواهی تولید شده بود)، شما می‌توانید گواهی را از سرور استخراج کرده و به سرورهای دیگر با گام‌های زیر وارد کنید.

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.



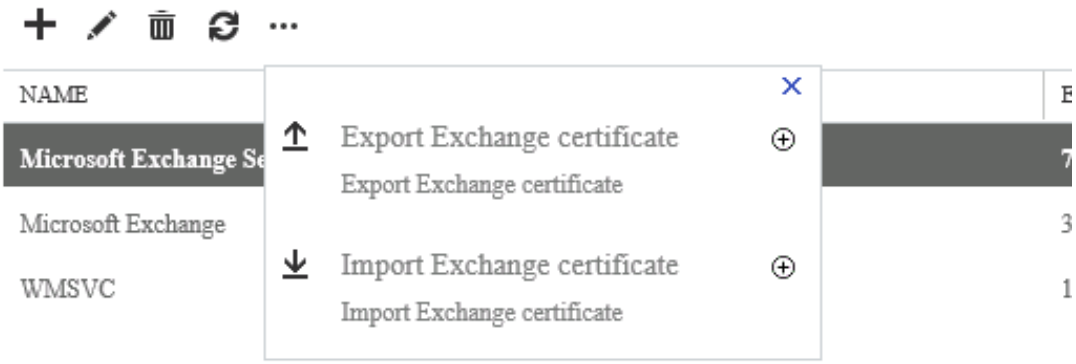
شکل ۳۰: بیرون کشیدن گواهی Exchange

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.



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

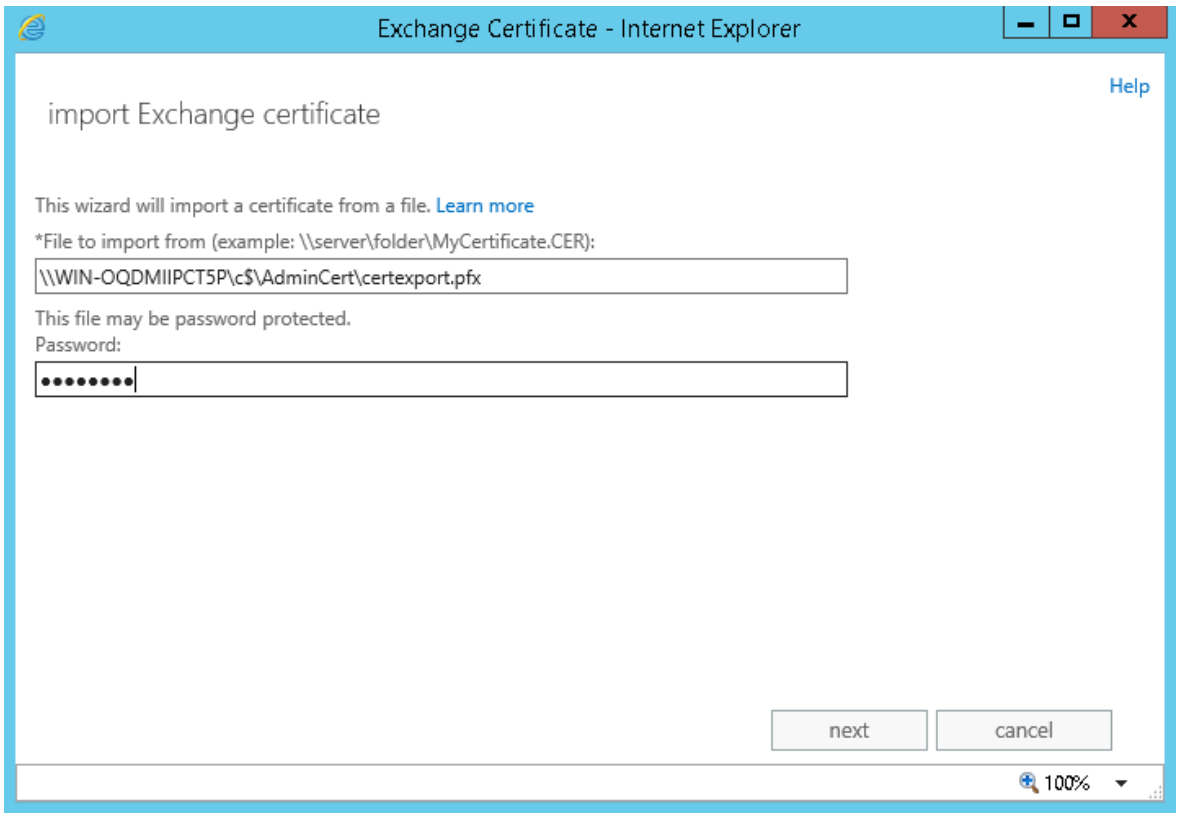
دوباره آیکن "more" را باز کنید و این دفعه گزینه **Import Exchange Certificate** را انتخاب کنید.



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.

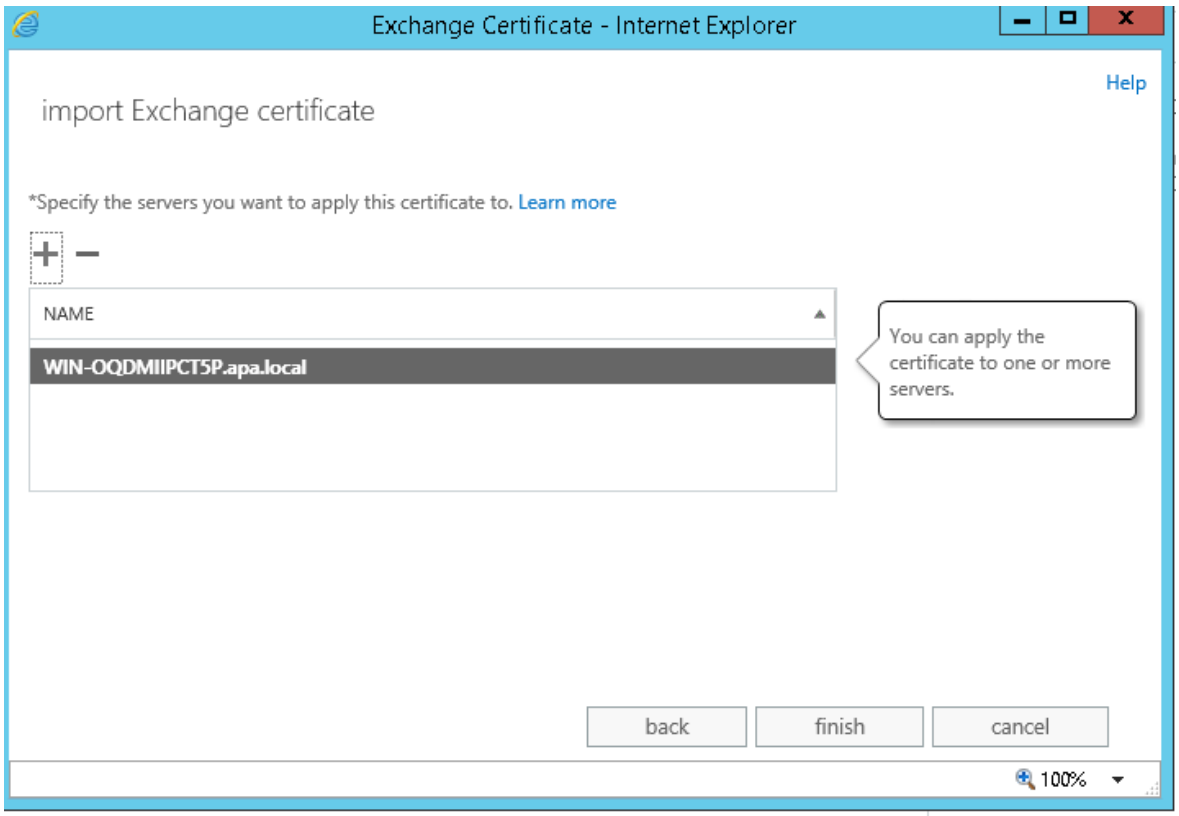
مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir



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.

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir



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

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

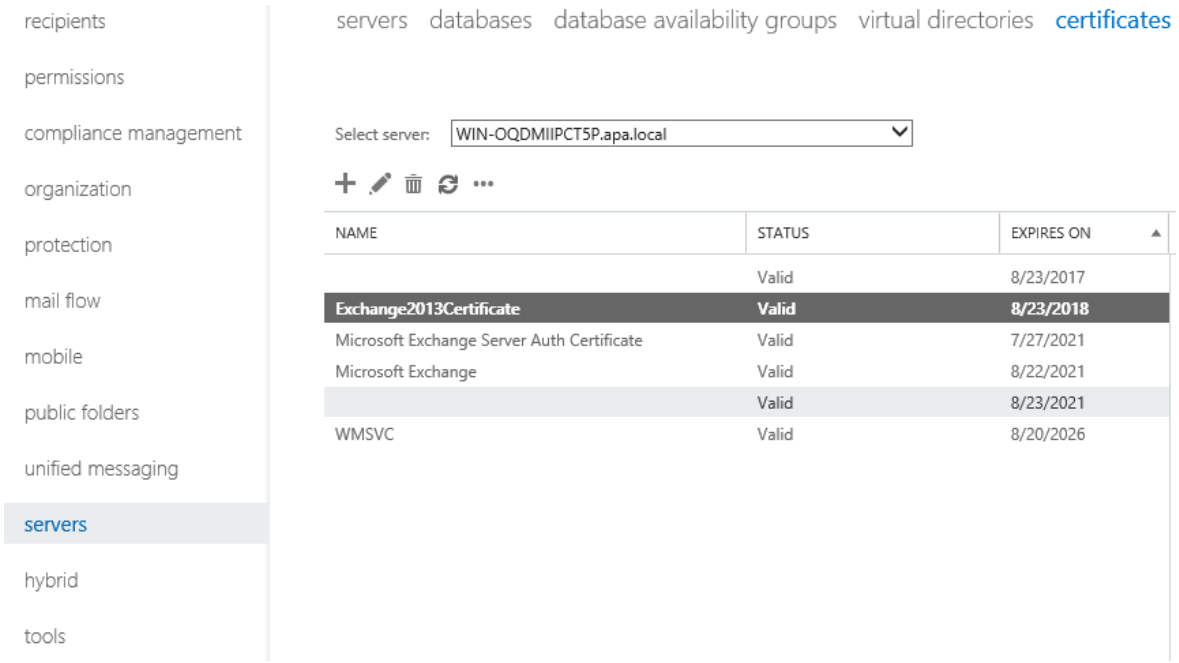
بعد از اینکه گواهی را به سرور اضافه کردید، شما می‌توانید کار را با انتصاب گواهی SSL به سرویس‌های Exchange ادامه دهید.

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

۷ انتصاب یک گواهی SSL به سرویس‌ها در Exchange Server 2013

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

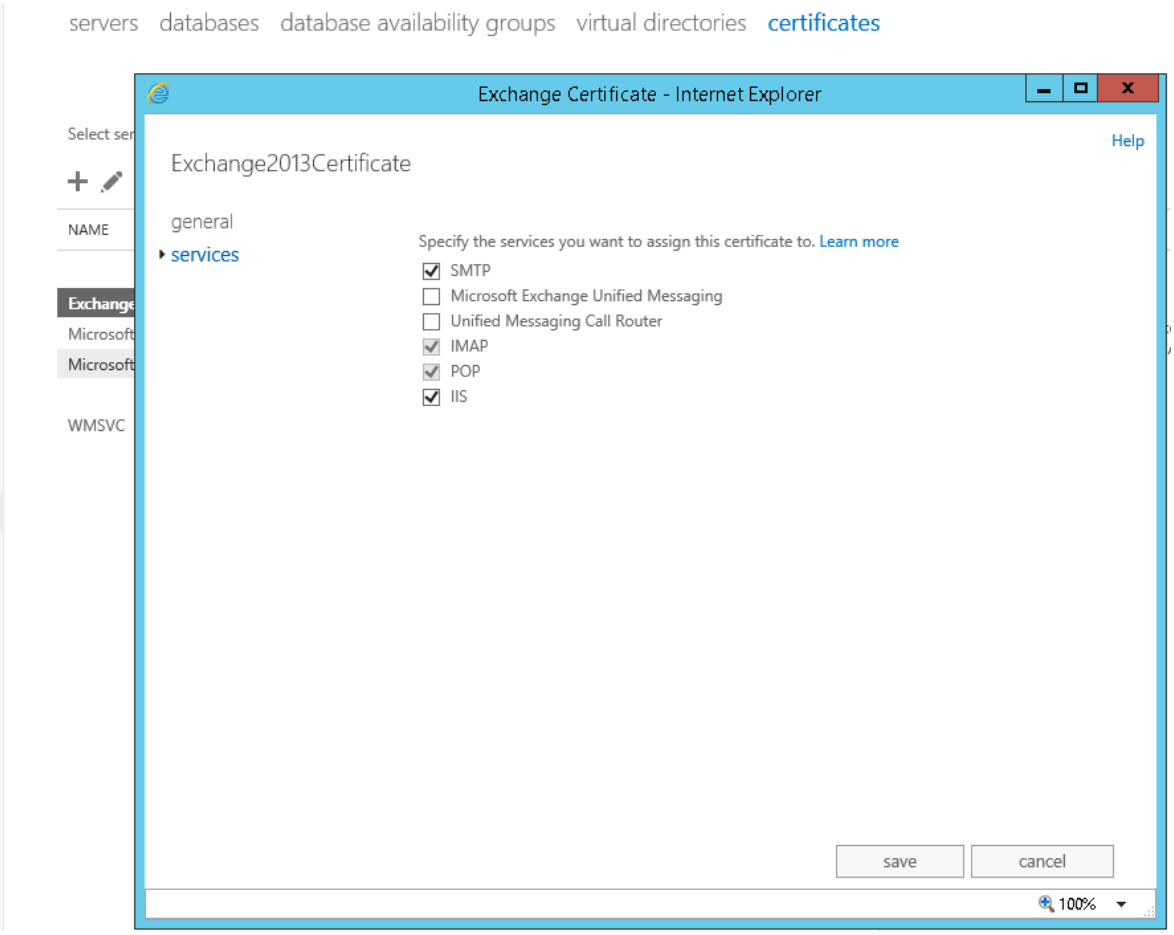
در Exchange Administration Center به مسیر Servers -> Certificates بروید و سروری که مایل به اختصاص گواهی SSL به آن هستید را انتخاب کنید، در اینجا وضعیت گواهی باید Valid باشد تا بتوان باقی مراحل را انجام داد.



شکل ۳۵: مشاهده لیست گواهی‌های SSL معتبر روی Exchange 2013

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

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

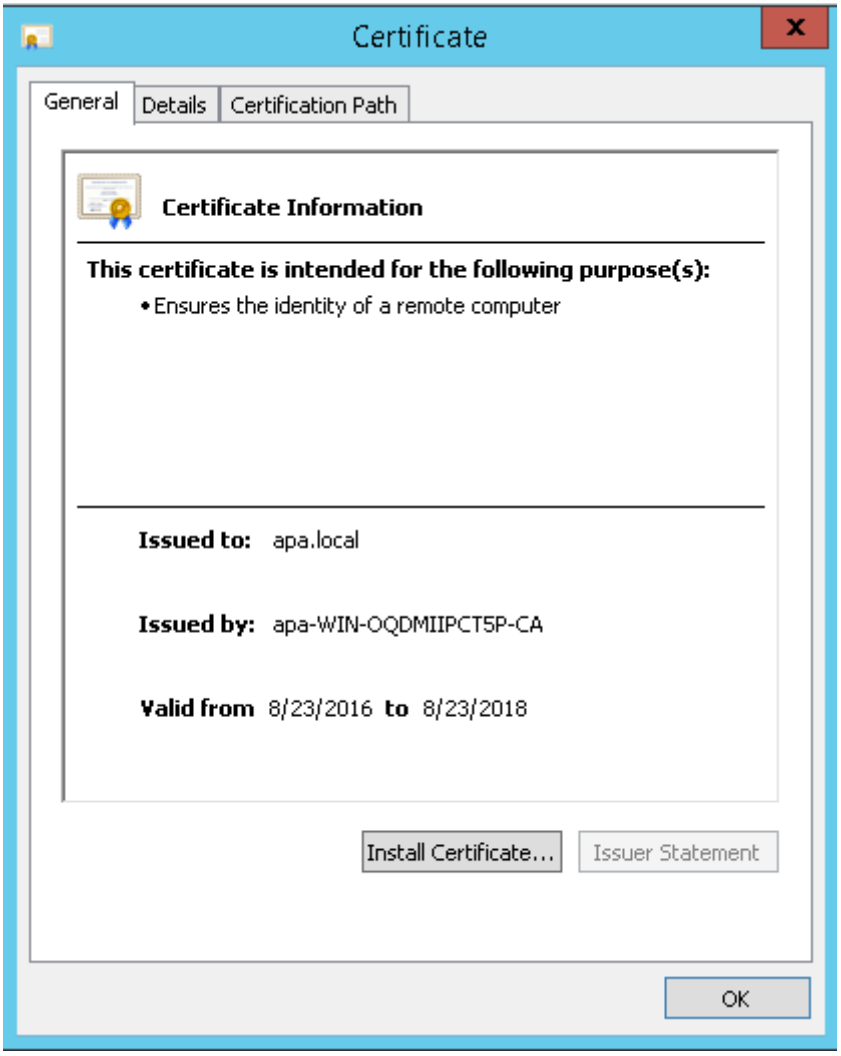


شکل ۳۶: ویرایش پیکربندی گواهی SSL به منظور انتصاب به سرویس‌های Exchange 2013

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 SSL، IIS و SMTP هستند.

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir



شکل ۳۷: مشاهده گواهی در مرورگر IE

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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 - Web: https://apa.aut.ac.ir

۸ منابع

1 http://exchangeserverpro.com/exchange-server-2013-ssl-certificates/

2 https://support.office.com/en-us/article/Add-an-SSL-certificate-to-Exchange-2013-976c080c-fda1-400d-97f4-5b65991cdf4e#BK_Request

3 http://exchangeserverpro.com/create-ssl-certificate-request-exchange-2013/

4 http://exchangeserverpro.com/exchange-2013-ssl-certificate-private-certificate-authority/

5 http://exchangeserverpro.com/exchange-2013-complete-pending-certificate-request/

6 http://exchangeserverpro.com/exchange-2013-ssl-certificate-export-import/

7 http://exchangeserverpro.com/exchange-2013-assign-ssl-certificate-to-services/

8 http://www.careexchange.in/how-to-install-certificate-authority-on-windows-server-2012

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir