چگونه از سرور CA مبتنی بر ویندوز سرور 2019 درخواست گواهی کنیم؟

زمانی که گواهی خود را با موفقیت در سرور CA ایجاد کرده و آماده انتشار کردیم، در مرحله بعد باید آن‌را از طریق کامپیوترهای کلاینت آزمایش کنیم تا مطمئن شویم به درستی کار می‌کند. دقت کنید روش ارائه درخواست گواهی از طریق کامپیوترهای کلاینت همیشه یکسان نیست و برخی از کاربران ترجیح می‌دهند یا مجبور هستند به جای کنسول MMC از طریق یک رابط وب درخواست دریافت گواهی را ارائه دهند. ما در این مقاله روش استفاده از هر دو روش را نشان خواهیم داد.

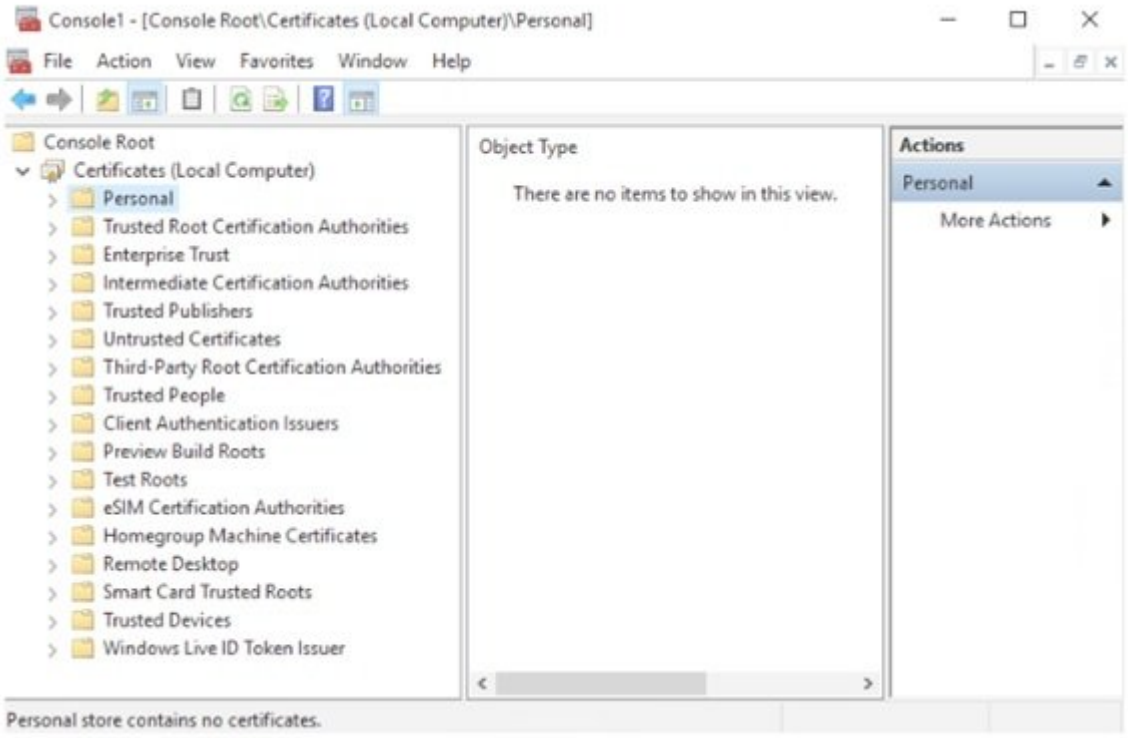
برای مطالعه قسمت قبل **آموزش رایگان ویندوز سرور 2019** اینجا کلیک کنید.

درخواست گواهی‌نامه از طریق کنسول MMC

الگوی گواهی جدید ما ایجاد شده و آن‌را با موفقیت درون کنسول CA قرار داده و به‌طور رسمی برای انتشار آماده کردیم. اکنون زمان آزمایش الگو است. برای این کار به یکی از کامپیوترهای کلاینت عادی وارد شوید. دو روش استاندارد برای درخواست گواهینامه جدید از طریق کامپیوترهای کلاینت وجود دارد. روش اول به‌کارگیری کنسول خوب و قدیمی MMC است. از طریق کامپیوتر کلاینت MMC را اجرا کرده، از منوی File گزینه Add/Remove Snap-in را انتخاب کرده و Certificate را انتخاب کنید. وقتی گواهی‌نامه‌ها را از فهرست Snap-insهای موجود انتخاب می‌کنید و روی دکمه Add کلیک می‌کنید یکسری گزینه‌های اضافی ارائه می‌شود که اجازه می‌دهد گواهی‌نامه‌ای که قصد باز کردن آن‌را دارید انتخاب کنید. شما می‌توانید از میان گواهینامه‌های باز برای حساب User، حساب Service یا حساب Computer گزینه مدنظر خود را انتخاب کنید. از آن‌جایی که ما به دنبال آن هستیم تا الگوی گواهی‌نامه جدیدی که ایجاد کرده‌ایم را آزمایش کنیم و همچنین با موفقیت توانستیم آن‌را درون کنسول CA منتشر کنیم، بنابراین آماده هستیم تا به‌طور رسمی از آن استفاده کنیم. همچنین قصد داریم گواهی‌نامه جدید که ایجاد کرده و آن‌را آماده استفاده کرده‌ایم را روی همین کامپیوتر کلاینت آزمایش کنیم، بنابراین حساب Computer را انتخاب کرده و Finish را کلیک می‌کنیم.

در صفحه بعد، دوباره روی دکمه Finish کلیک کنید تا گزینه پیش‌فرض که Local computer است انتخاب شود. با این‌کار گواهی مبتنی بر ماشین محلی درون MMC ذخیره می‌شود. در سیستم‌عامل‌های جدیدتر شبیه به ویندوز 8 و 10 و همچنین ویندوز سرورهای 2012 ، 2012R2 ، 2016 و 2019 ، میانبر MSC برای باز کردن مستقیم فروشگاه گواهی برای کامپیوتر محلی وجود دارد. اگر در دیالوگ Run فرمان CERTLM.MSC را تایپ کنید، MMC به‌طور خودکار Snap- مورد نیاز را اجرا کرده و آن‌را باز می‌کند.

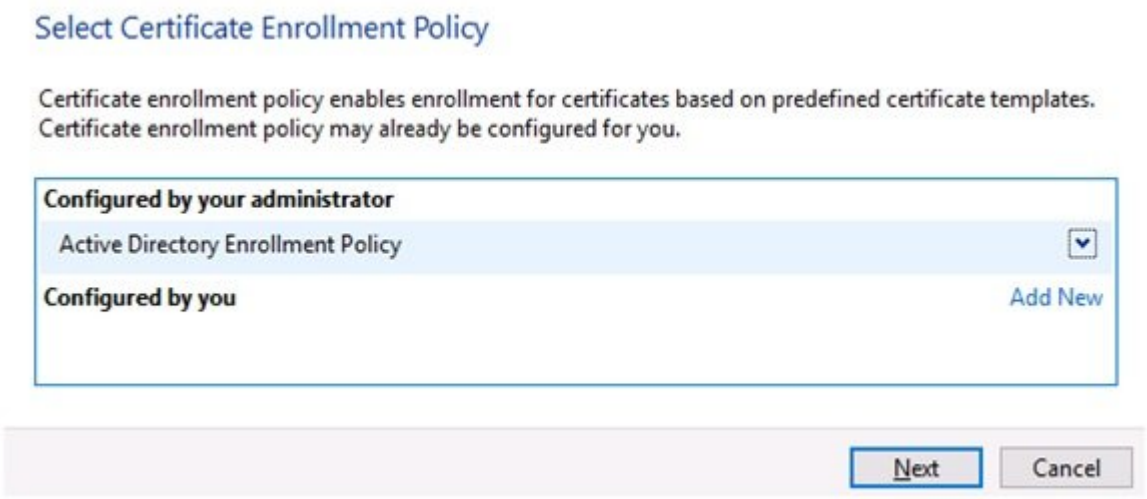
هنگام نصب گواهینامه‌ها روی یک کامپیوتر یا سرور، این همان مکانی است که باید به آن مراجعه کنید. درون فروشگاه گواهینامه، محل خاصی وجود دارد که اجازه می‌دهد گواهی‌نامه خود را درون پوشه Personal نصب کنید. درست است که شما می‌توانید یک گواهی‌نامه ماشین را در همین مکانی که ما آن‌را نصب کردیم، نصب کنید یا یک گواهی‌نامه SSL را روی یک وب‌سرور نصب کنید، اما پوشه گواهی‌نامه شخصی کامپیوتر مکان درستی برای نصب هر نوع گواهی‌نامه است. اگر روی این پوشه کلیک کنید، مشاهده می‌کنید که در حال حاضر هیچ چیزی در آن فهرست آن قرار نداده‌ایم:



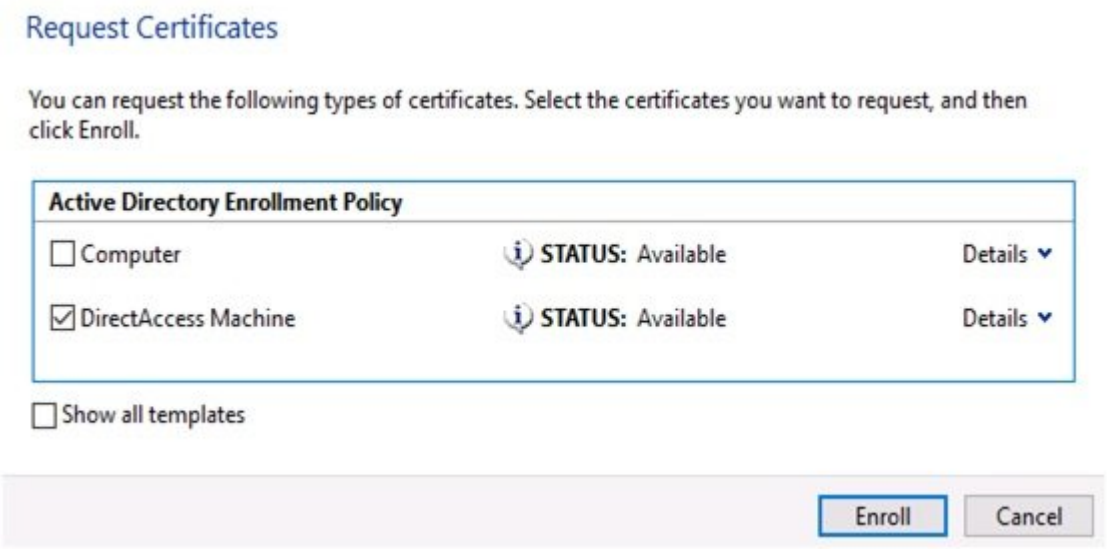
برای ارائه درخواست گواهینامه جدید به سرور CA خودمان روی پوشه Personal کلیک راست می‌کنیم و سپس به All Tasks و در نهایت Request New Certificate.... می‌رویم. در ویزاردی که باز می‌شود یکبار روی دکمه Next کلیک کنید.

اکنون صفحه‌نمایشی مشاهده می‌کنید که به نظر می‌رسد باید کاری در آن انجام شود، در بیشتر موارد ما درخواست گواهی‌نامه را برای یکی از شرکای تجاری یا ماشین‌های عضو دامنه ارسال می‌کنیم، در نتیجه کاری چندان خاصی

نداریم که در این صفحه انجام دهیم. به همین دلیل روی دکمه Next کلیک کنید. با این‌کار ویزارد پرس‌وجویی روی اکتیو دایرکتوری انجام داده و همه الگوهای گواهی موجود که برای انتشار آماده هستند را نشان می‌دهد:



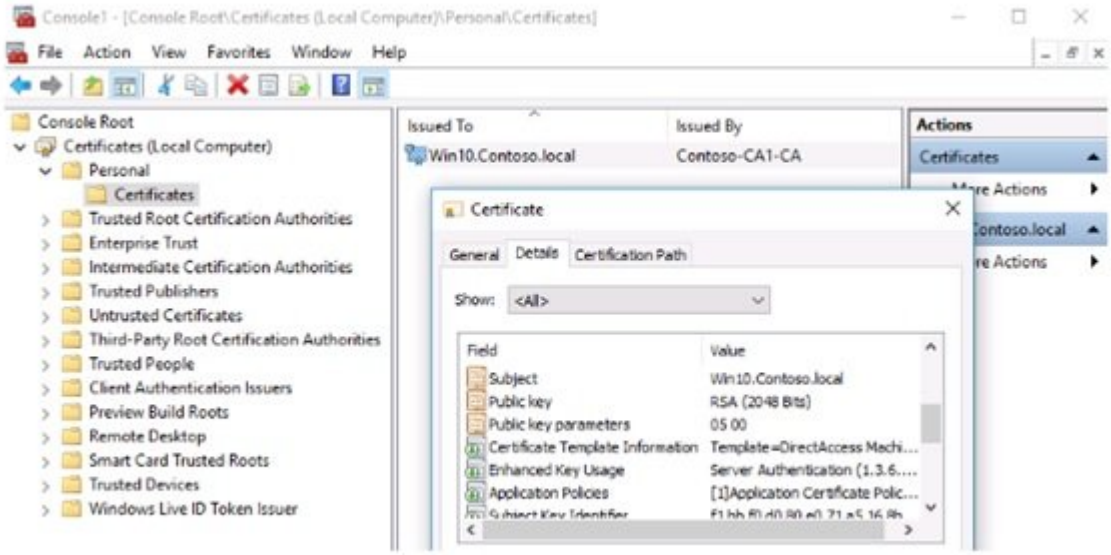
صفحه Request Certificate نشان داده می‌شود که فهرست الگوهای موجود در دسترس در آن درج شده است. این یک فهرست پویا است و محتویات درون آن به کامپیوتری که به آن وارد شده‌اید و همچنین مجوزهای حساب کاربری بستگی دارد. به یاد می‌آورید در زمان ساخت الگوی گواهی‌نامه جدید به زبانه امنیتی رفتم و آن‌را تنظیم کردیم. در زبانه تعریف کردیم که چه کسی و چه چیزی می‌تواند الگوی گواهی‌نامه جدید را دریافت کند. اگر گروه خاصی از کامپیوترهای عضو دامنه را تعریف کرده باشیم، این احتمال وجود دارد که الگوی جدید DirectAccess Machine در فهرست فوق نشان داده نشود. با این حال، از آن‌جایی که من این الگو به شکلی تعریف کردم که تمامی کامپیوترهای عضو دامنه آن‌را دریافت کنند، در نتیجه گواهی‌نامه خود را در اینجا مشاهده می‌کنم.



اگر الگوی جدید خود را در این فهرست نمی‌بینید، روی کادر تأیید نمایش همه الگوها کلیک کنید. با این‌کار فهرست کاملی از تمامی الگوهای موجود در سرور CA را مشاهده می‌کنید که برای هر یک توضیحی ارائه شده و همچنین برای گواهی‌نامه‌هایی که در دسترس نیستند، توضیحی مبنی بر دلیل عدم دسترسی ذکر شده است.

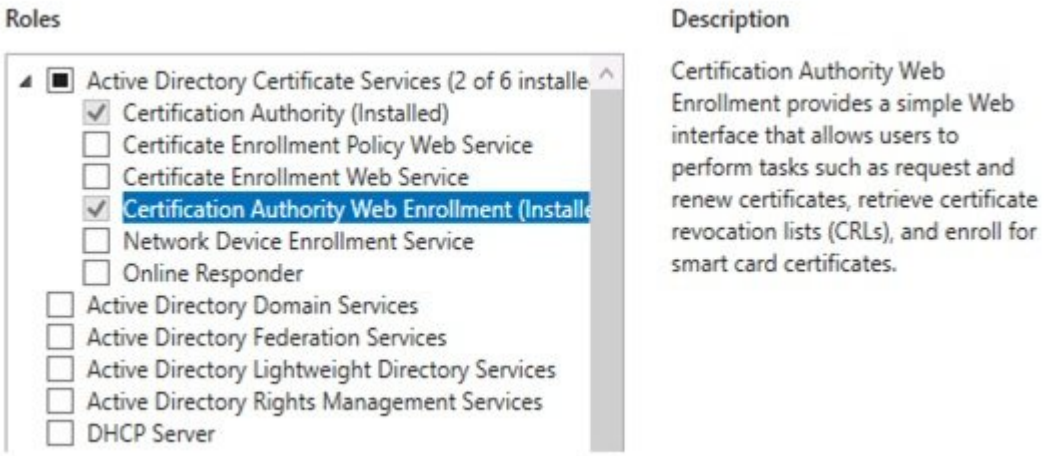
در کنار هر یک از گواهی‌نامه‌هایی که نیاز دارید یک تیک قرار داده و Enroll را کلیک کنید. اکنون کنسول برای چند ثانیه می‌چرخد، زیرا سرور CA در حال پردازش درخواست شما است تا یک گواهی‌نامه جدیدی که کامپیوتر شما به آن نیاز دارد را همراه با معیارهای مربوطه که درون گواهینامه قید شده است به آن اختصاص دهد. پس از اتمام فرآیند، مشاهده می‌کنید که گواهی ماشین جدید ما اکنون در Certificate | Personal درون MMC قرار گرفته

است. اگر روی گواهینامه دو بار کلیک کنید، قادر به بررسی خاصیت‌ها هستید تا مطمئن شوید تنظیماتی که مدنظر شما قرار دارد درون گواهی قید شده است:



درخواست گواهی از طریق رابط وب

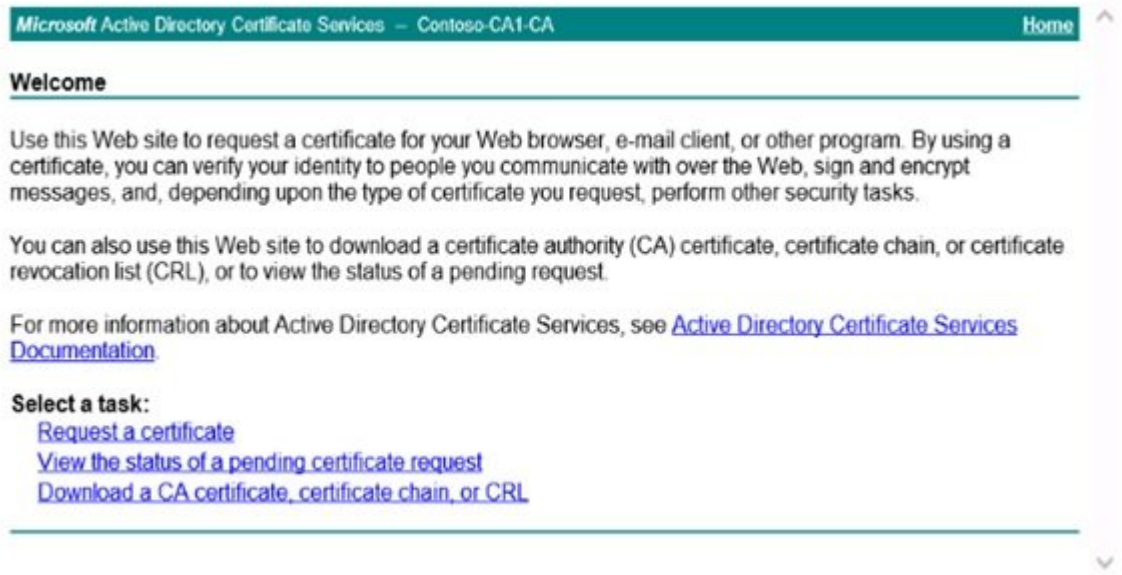
به‌طور معمول در اغلب اوقات از MMC برای درخواست گواهینامه‌ها استفاده می‌کنیم، اما بستر دیگری وجود دارد که می‌توانید از آن بستر برای ارائه درخواست و صدور گواهی استفاده کنید. البته به‌کارگیری راهکار فوق به نحوه ساخت سرور CA بستگی دارد. هنگامی که نقش AD CS را نصب کردیم، مطمئن شدیم که هر دو گزینه Certification Authority و Certification Authority Web Enrollment انتخاب شده‌اند. گزینه دوم مهم است و در ادامه به بررسی آن خواهیم پرداخت. بدون داشتن نقش Web Enrollment، ما یک رابط کاربری وب برای اجرای سرور CA خودمان نداریم و در نتیجه بخش فوق در دسترس ما قرار نمی‌گیرد. اگر سرور CA فاقد نقش فوق است، باید به Server Manager رفته و نقش موجود را به آن اضافه کنید:



زمانی‌که Certification Authority Web Enrollment روی سرور CA نصب شد، وب‌سایتی روی سرور شما اجرا می‌شود که شما از طریق یک مرورگر وب و از درون شبکه خود به آن دسترسی خواهید داشت. داشتن این وب‌سایت به ویژه زمانی مفید است که تمایل دارید کاربران از طریق رابط وب درخواست دریافت گواهی را ارائه دهند. بهتر است برای کاربران خود مستندات یا آموزش‌هایی تهیه کنید تا آن‌ها بتوانند فرآیند درخواست گواهی‌نامه را به جای آن‌که از کنسول MMC دنبال کنند از طریق وب‌سایت دنبال کنند. علاوه بر این، اگر می‌خواهید به کامپیوترهایی که درون شبکه سرور CA شما قرار ندارند، اجازه دهید درخواست گواهی بدهند، این‌کار از طریق MMC برای آن‌ها

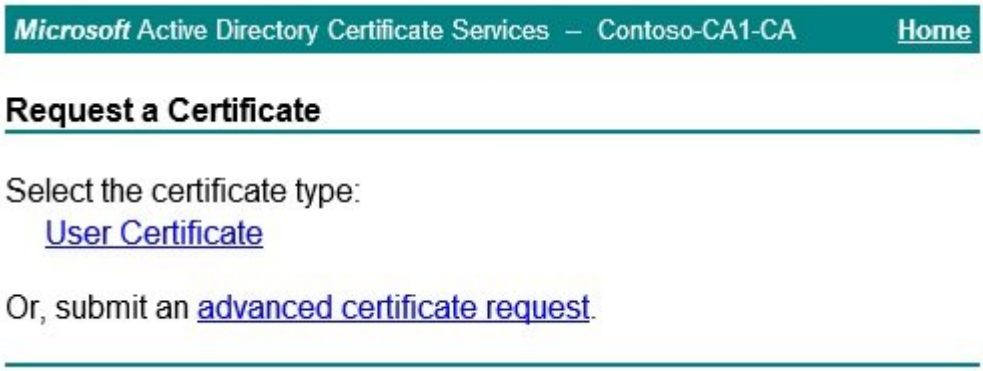
مشکل است. به‌عنوان مثال، اگر شما کاربری در خانه دارید که مجبور است درخواستی برای یک گواهی جدید بدهد، اما یک تونل وی‌پی‌ان کامل در اختیار ندارد، به احتمال زیاد کنسول MMC قادر نخواهد بود به سرور CA متصل شده و گواهی را دریافت کند. اما از آن‌جایی که ما ویژگی ثبت گواهی از طریق وب‌سایت را داریم، شما می‌توانید با استفاده از یک پروکسی معکوس یا دیوارآتش برای ایمن نگه داشتن ترافیک به کاربران خود اجازه دهید به سایت متصل شده و درخواست گواهی را از هر مکانی ارائه کرده و گواهی را دریافت کنند.

برای دسترسی و آزمایش این وب‌سایت باید دوباره از کامپیوتر کلاینت استفاده کنیم. این مرتبه به جای باز کردن MMC به سادگی مرورگر را باز کرده و آدرس https: // <CASERVER> / certsrv را درون مرورگر وارد می‌کنم. در مثال من، آدرس دقیق سایت به صورت https://CA1/certsrv: است:



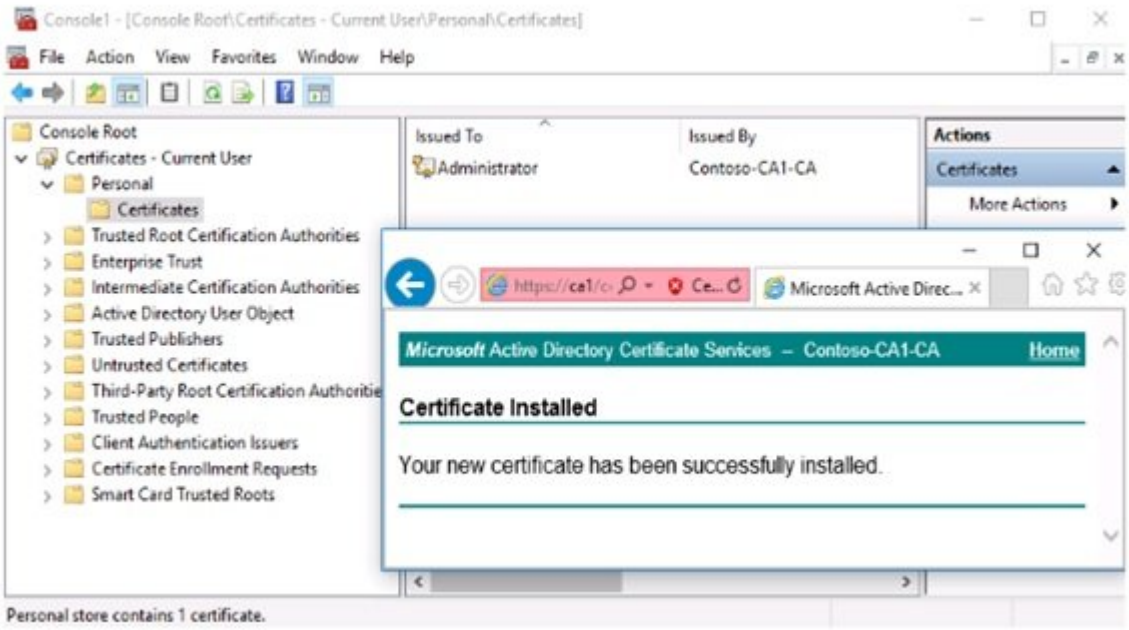
آدرس اینترنتی ما با پروتکل HTTPS آغاز می‌شود. این وب‌سایت به شکلی تنظیم می‌شود تا به جای پروتکل HTTP از پروتکل HTTPS استفاده کند تا به وب‌سایت اجازه دهد گواهی‌نامه‌ها را صادر کند. امکان صدور گواهینامه از طریق HTTP میسر نیست، زیرا این اطلاعات به صورت روشن و بدون رمزگذاری برای کلاینت ارسال می‌شوند. زمانی که وب‌سایت روی سرور CA از HTTPS استفاده می‌کند، اطمینان حاصل خواهید کرد که گواهی صادر شده هنگام ارسال رمزگذاری می‌شود.

با کلیک روی Request یک لینک گواهی نشان داده می‌شود که با استفاده از آن می‌توانید از سرور CA یک گواهی جدید درخواست کنید. زمانی‌که کاربرانی دارید که در نظر دارند از طریق رابط وب گواهی را دریافت کنند، به‌طور معمول در حال صدور گواهینامه مبتنی بر کاربر هستید، در این حالت ما راهکار خیلی ساده‌ای در اختیار داریم تا گواهی‌های سطح کامپیوتر را به‌طور خودکار و بدون آن‌که هیچ‌گونه تعاملی با کاربر داشته باشیم صادر کنیم. از آن‌جایی که ما از کاربران خود می‌خواهیم ابتدا وارد شوند و سپس یک گواهی کاربری جدید (User Certificate) را درخواست کنند، در صفحه بعد باید لینک مربوطه را انتخاب کنیم:



اگر به گواهی کاربری علاقه‌ای ندارید و می‌خواهید از رابط وب برای دریافت یک گواهی ماشین، یک گواهی وب‌سرور یا هر نوع گواهی دیگری استفاده کنید، به جای کلیک روی لینک فوق باید روی لینک advanced certificate request کلیک کرده و منطبق با دستورالعمل‌هایی که روی صفحه مشاهده می‌کنید رفتار کنید.

با کلیک روی پیوند فوق و فشار دکمه Submit، گواهی از سرور CA دریافت و تولید شده و لینکی به شما نشان داده می‌شود که می‌توانید از آن لینک برای نصب گواهی استفاده کنید. روی لینک کلیک کنید. با این‌کار گواهی که برای شما ایجاد شده روی کامپیوترتان نصب می‌شود. در تصویر زیر مشاهده می‌کنید که وب‌سایت به درخواست من پاسخ داده و اعلام می‌دارد گواهی با موفقیت نصب شده است. همچنین مشاهده می‌کنید که من گواهی کاربری فعلی را درون MMC باز کرده‌ام تا مطمئن شوم گواهی واقعا وجود دارد:



در شماره آینده آموزش رایگان **ویندوز سرور 2019** مبحث فوق را ادامه خواهیم رفت.

برای مطالعه تمام بخش‌های **آموزش ویندوز سرور 2019** روی لینک زیر کلیک کنید:

آموزش رایگان ویندوز سرور 2019

تاریخ انتشار:
13 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/tricks/network-tricks/15998/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-ca-%D9%85%D8%A8%D8%AA%D9%86%DB%8C-%D8%A8%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019-%D8%AF%D8%B1%D8%AE%D9%88%D8%A7%D8%B3%D8%AA-%DA%AF%D9%88%D8%A7%D9%87%DB%8C-%DA%A9%D9%86%DB%8C%D9%85%D8%9F