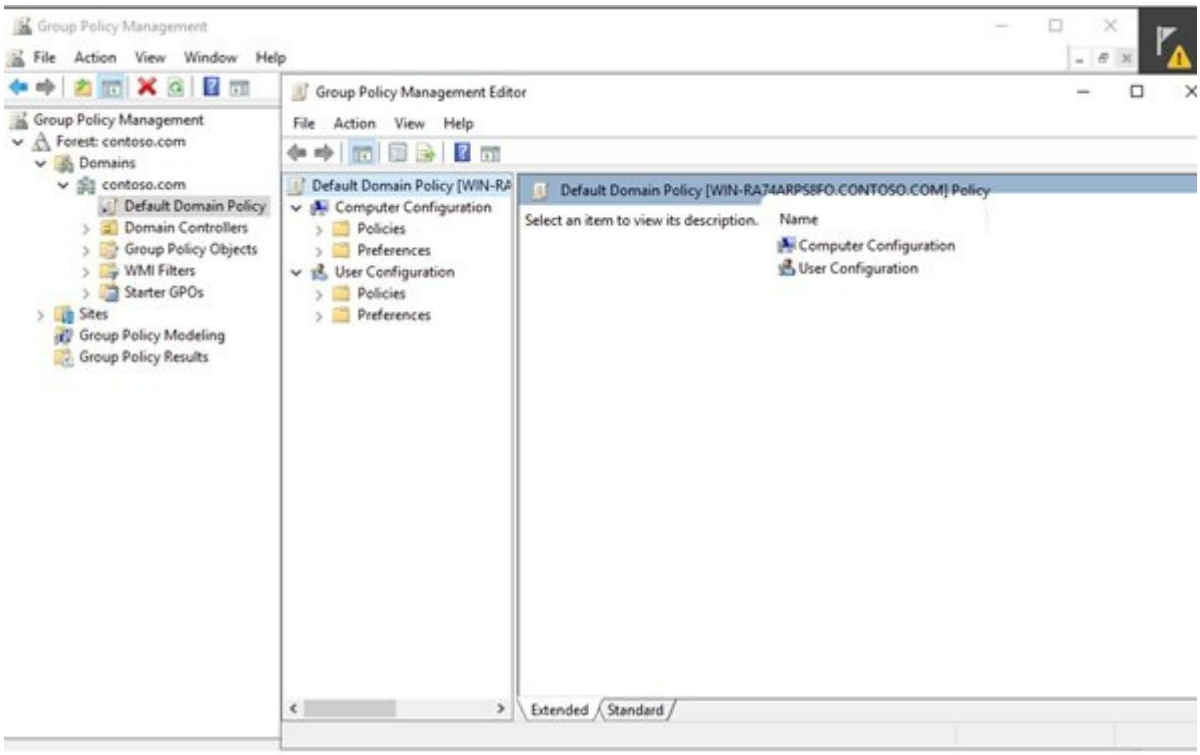
آموزش به‌کارگیری Group Policy در ویندوز سرور 2019 برای ساخت GPO

Group Policy یکی از مولفه‌های کلیدی ویندوز سرور 2019 است که به ما کمک می‌کند خط‌مشی‌های درستی در ارتباط با کاربران و کامپیوترها اعمال کنیم. خط‌مشی‌هایی که در اغلب موارد به شکل خودکار اعمال شده و مدیران شبکه نیازی ندارند به‌طور دستی این خط‌مشی‌ها را روی تک‌تک کامپیوترها اعمال کنند. اما چگونه می‌توانیم خط‌مشی‌های پیش‌فرض را مشاهده کرده یا آن‌ها را ویرایش کنیم؟

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

خط‌مشی پیش‌فرض دامنه

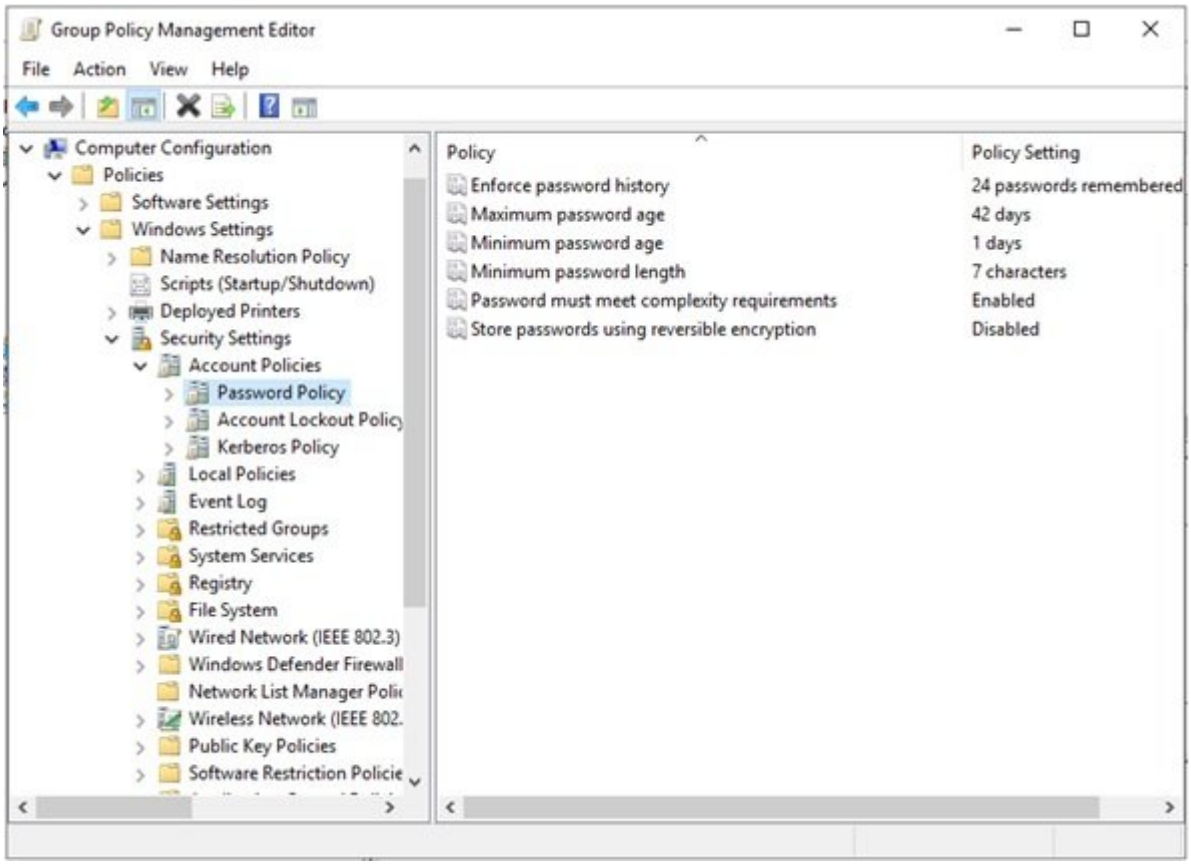
یاد گرفتیم که چگونه کنسول Group Policy Management را اجرا کرده و خط‌مشی پیش‌فرض دامنه را مشاهده کنیم. اگر روی هر خط‌مشی پیش‌فرض دامنه (GPO) که در کنسول مدیریت مشاهده می‌کنید کلیک راست کرده و گزینه ویرایش (Edit) را انتخاب کنید، پنجره جدیدی باز می‌شود که ویرایشگر GPO بوده و همه مولفه‌های داخلی مرتبط با خط‌مشی انتخاب شده را نشان می‌دهد.



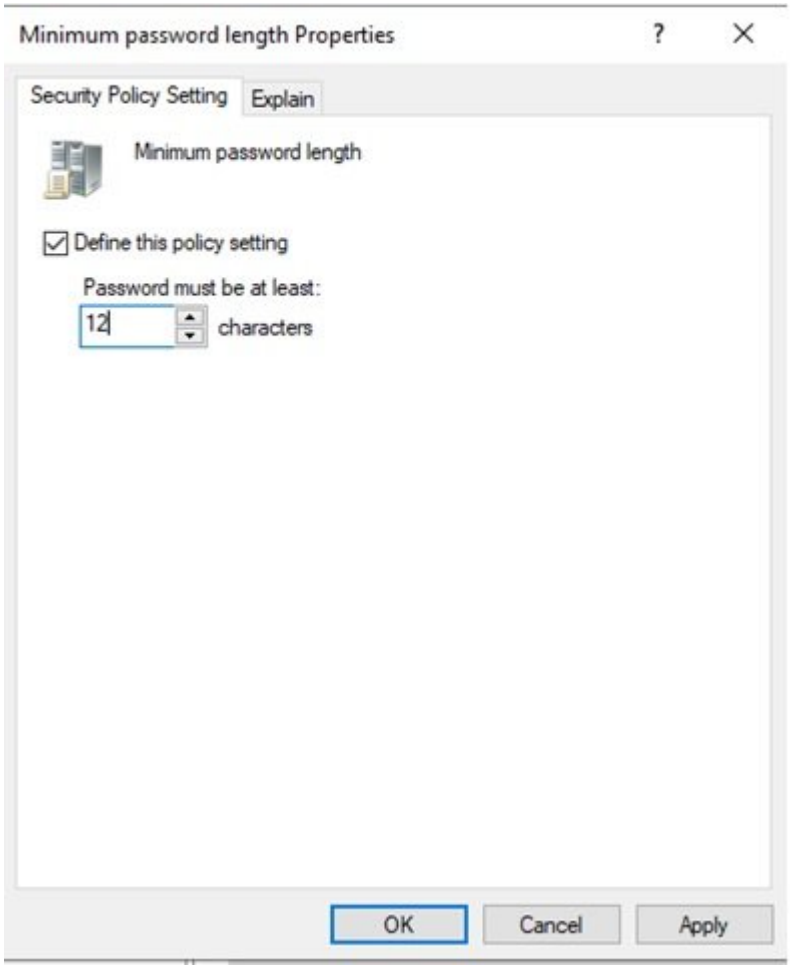
این پنجره، همان مکانی است که شما می‌توانید تنظیمات یا پیکربندی‌هایی را که قرار است بخشی از یک GPO خاص باشند را اعمال کنید. فرض کنید قصد داریم خط‌مشی‌های مربوط به ویرایش گذرواژه‌ها را تغییر دهیم. برای این منظور به مسیر زیر می‌رویم.

Computer Configuration | Policies | Windows Settings | Security Settings | Account Policies | Password Policy

در این بخش، فهرستی از گزینه‌های مختلف موجود برای پیکربندی خط‌مشی گذرواژه مرتبط با دامنه را مشاهده می‌کنید.



با دوبار کلیک روی هر یک از تنظیماتی که در پنل سمت راست مشاهده می‌کنید، ویرایش پارامترها امکان‌پذیر می‌شود. به محض آن‌که دکمه Ok را کلیک کردید، تنظیمات روی همه کامپیوترهای عضو دامنه اعمال می‌شود. به‌طور مثال، شما می‌توانید حداقل طول گذرواژه 7 کاراکتری را مشاهده کنید. بسیاری از شرکت‌ها در زمینه تعیین حداقل طول گذرواژه‌ها سخت‌گیری‌های خاصی را اعمال می‌کنند تا حداقل طول کاراکترهای گذرواژه‌ها بیشتر از مقدار پیش‌فرض باشد. با دوبار کلیک روی گزینه Minimum password length پنجره‌ای همانند شکل زیر ظاهر می‌شود که امکان ویرایش پارامتر فوق را ممکن می‌کند. اگر این مقدار تغییر پیدا کند، همه کاربران عضو دامنه در مراجعه بعدی و لاگین کردن به کامپیوتر خود ملزم هستند تا گذرواژه خود را تغییر داده و طول آن را مطابق با مقدار تعیین شده مشخص کنند.



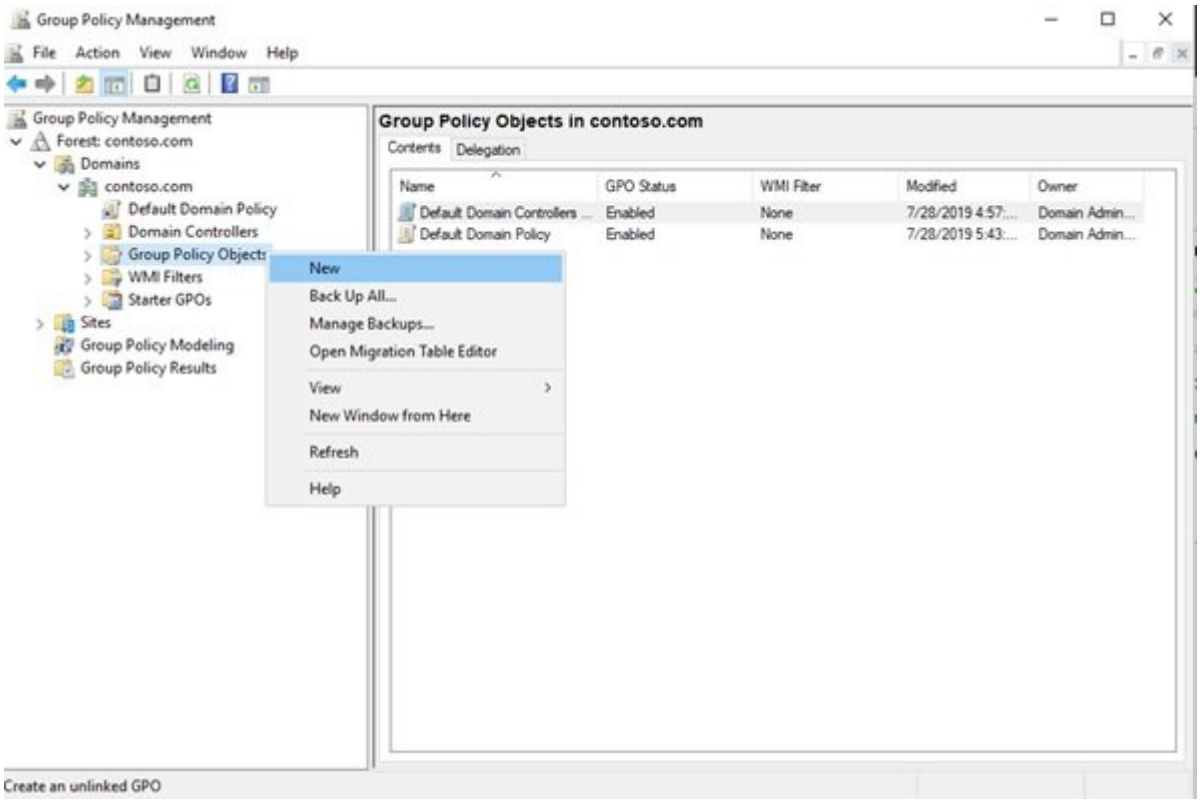
اگر به سمت چپ ابزار Group Policy Management نگاه کنید، طیف گسترده‌ای از تنظیمات و پیکربندی‌هایی را مشاهده می‌کنید که همگی از طریق Group Policy قابل ویرایش هستند. در حالی که خط‌مشی پیش‌فرض دامنه یک راهکار سریع و آسان برای پیکربندی همه تنظیماتی که قرار است روی همه کاربران اعمال شود در اختیارتان قرار می‌دهد، اما در برخی موارد مجبور هستید خط‌مشی‌های پیش‌فرض را تغییر داده و مطابق با اصول شرکت یا سازمان این تنظیمات را ویرایش کنید. به خاطر داشته باشید، هربار که تغییری در تنظیمات اعمال می‌کنید، این تنظیمات روی هر کاربری که عضو دامنه است، حتا کامپیوتری که خودتان از آن استفاده می‌کنید اعمال می‌شود. در بسیاری از موارد، خط‌مشی‌هایی ایجاد می‌کنید که قرار نیست روی همه حساب‌های کاربری اعمال شود، در چنین شرایطی پیشنهاد می‌کنیم از Default Group Policy دوری کرده و به جای آن، GPO خودتان را ایجاد و پیکربندی کنید. در حقیقت ، برخی از مدیران توصیه می‌کنند که هیچ‌گاه خط‌مشی پیش‌فرض دامنه را تغییر نداده و همواره خط‌مشی خاص خود را ایجاد کرده و آن‌را ویرایش کنید. اما چگونه می‌توانیم خط‌مشی پیش‌فرض دامنه خود را ایجاد کنیم؟

ایجاد یک GPO جدید و مرتبط کردن آن با دامنه

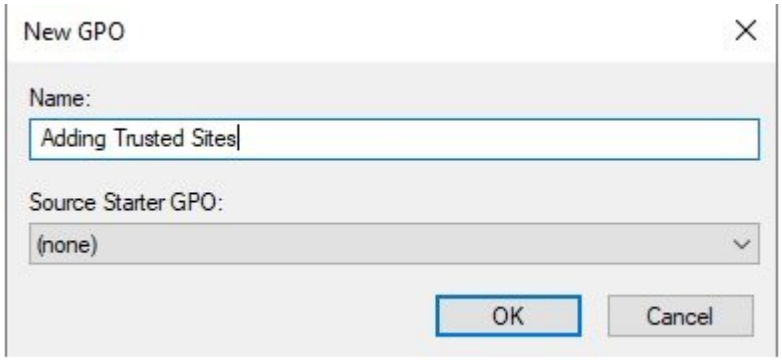
بهترین راه آشنایی و درک بهتر عملکرد GPO، ایجاد و پیکربندی آن است. انجام این‌کار چند دقیقه از وقت شما را می‌گیرد، اما در مقابل اجازه می‌دهد روی همه تنظیمات و پیکربندی‌ها نظارت دقیقی اعمال کنید. به‌طور مثال، ما می‌خواهیم یک GPO جدید ایجاد کنیم که فهرستی از سایت‌های قابل اعتماد را به مرورگر اینترنت اکسپلورر معرفی کند. اگر یک برنامه تحت وب را در شبکه خود اجرا کنید که نیاز دارد تا کنترل‌های اکتیوایکس یا جاوااسکریپت را اجرا کرده یا کاری شبیه به آن‌را انجام دهد، مجبور هستید آن وب‌سایت را به عنوان یک مولفه قابل اعتماد در بخش سایت‌های قابل اعتماد درون اینترنت اکسپلورر معرفی کنید تا مشکلی در اجرای برنامه تحت وب رخ ندهد. در این حالت شما دو گزینه پیش رو دارید، اول آن‌که فهرستی ایجاد کرده و در قالب یک دستورالعمل نحوه انجام این‌کار را برای هر کامپیوتر مشخص کرده و سپس به هر کاربر نشان دهید که چگونه این‌کار را انجام دهد تا کاربر بتواند به برنامه دسترسی پیدا کند. راهکاری که سخت و طاق‌فرسا است. اما در مقابل می‌توانید یک GPO ساده ایجاد کرده و این تغییرات را درون آن درج کنید تا به‌طور خودکار روی هر ایستگاه کاری اعمال شود. موردی که به آن اشاره کردیم، تنها یک نمونه ساده از توانایی‌هایی است که Group Policy در اختیارتان قرار می‌دهد. برای انجام این‌کار

مراحل زیر را دنبال کنید.

داخل کنسول Group Policy Management، روی پوشه‌ای به‌نام Group Policy Objects کلیک راست کرده و New را انتخاب کنید.

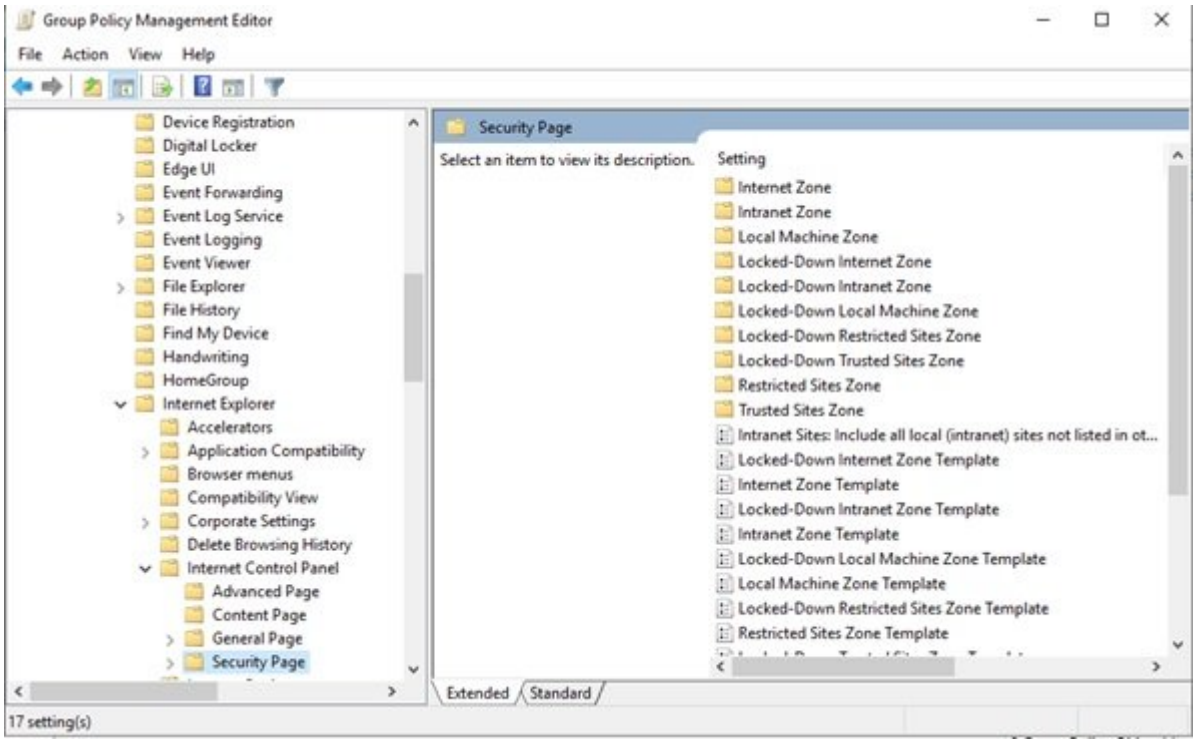


نامی شبیه به Adding Trusted Sites برای GPO خود انتخاب کرده و سپس روی OK کلیک کنید.

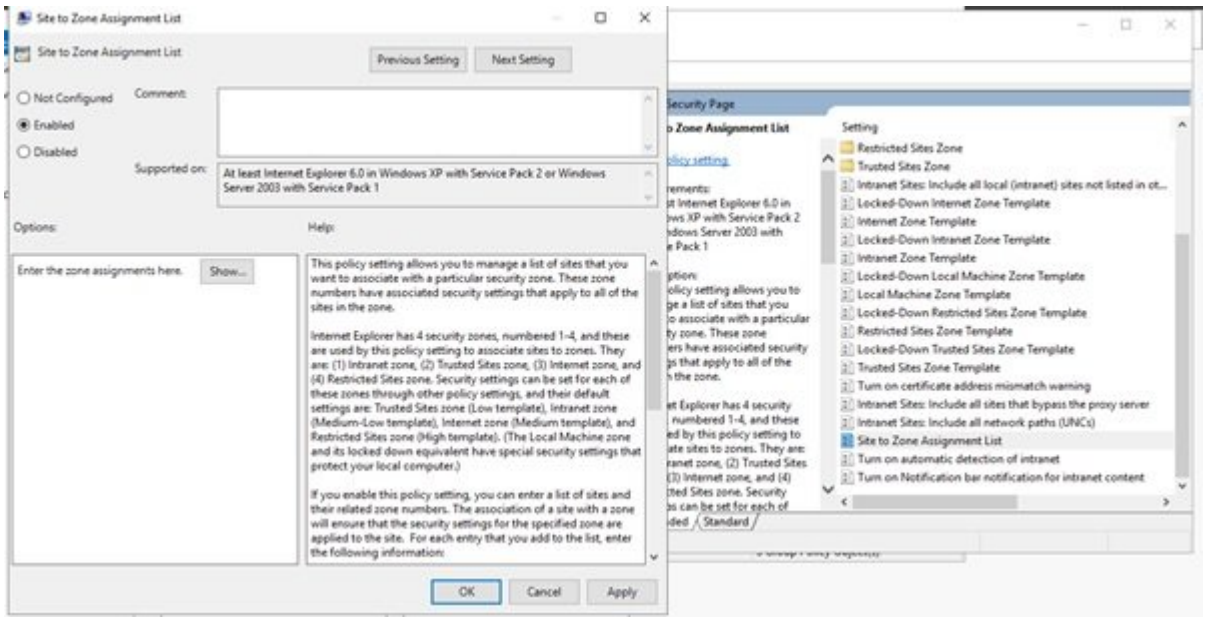


GPO جدید شما اکنون در فهرست GPOهای موجود قرار دارد، اما هنوز این قابلیت را ندارد تا روی هیچ حساب کاربری یا کامپیوتری تاثیرگذار باشد. قبل از این‌که GPO جدید را فعال کنیم، ابتدا باید فهرستی از سایت‌های قابل اعتماد که شامل اطلاعات پیکربندی می‌شود را درون آن وارد کنیم. دقت کنید در حال حاضر ما یک خط‌مشی جدید داریم، اما فاقد تنظیمات است. روی GPO جدید کلیک راست کرده و گزینه Edit را انتخاب کنید. اکنون به مسیر بروید.

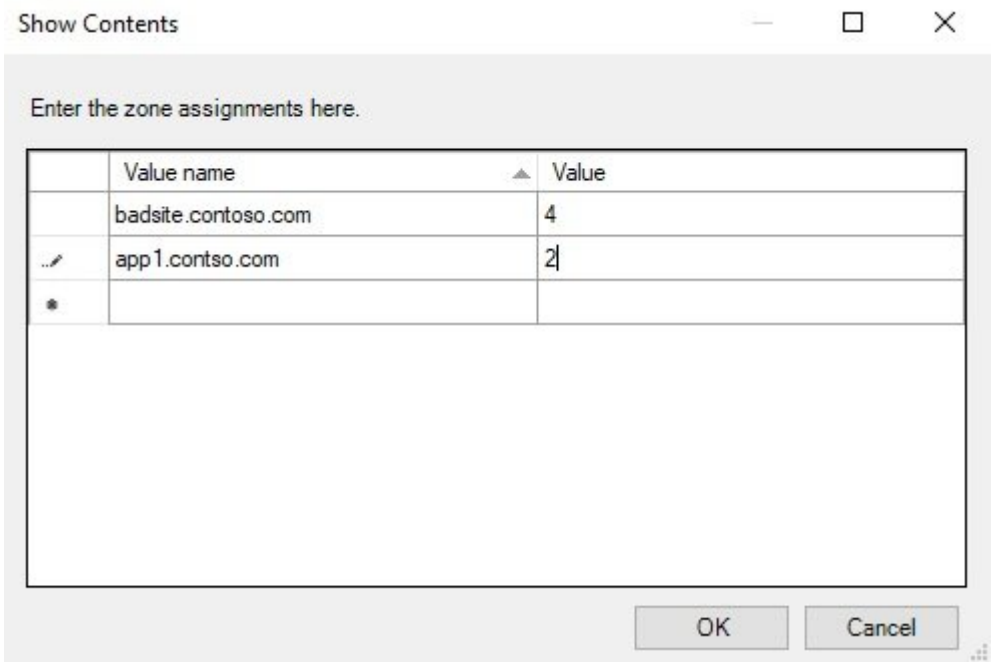
Computer Configuration | Policies | Administrative Templates | Windows Components | Internet Explorer | Internet Control Panel | Security Page



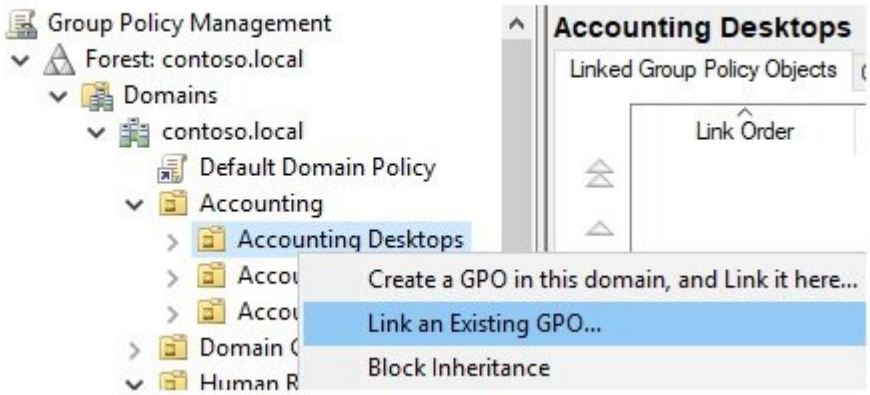
اکنون روی Site to Zone Assignment List دو بار کلیک کرده و گزینه Enabled را کلیک کنید.



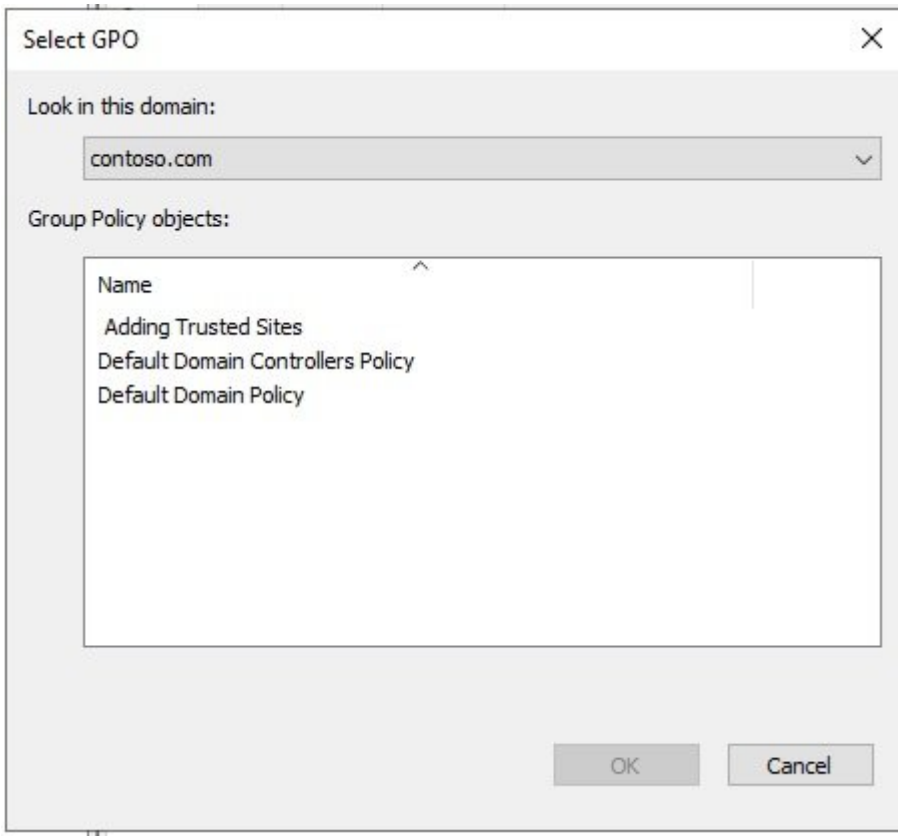
روی پیغامی که مشاهده می‌کنید کلیک کنید. اکنون دکمه Show در همین پنجره را کلیک کنید تا بتوانید وب‌سایت‌هایی که مجاز هستند را درج کنید. هر GPO یک توصیف متنی مخصوص به خود را دارد که به ما اعلام می‌کند که این تنظیمات دقیقا چه هستند و هر یک از گزینه‌ها چه معنایی می‌دهند. همان‌گونه که مشاهده می‌کنید برای وب‌سایت‌های قابل اعتمادی که قرار است مشخص کنیم، مقدار 2 در نظر گرفته شده است. به‌طور مثال، می‌خواهم سایتی که تمایل ندارم کاربران به آن دسترسی داشته باشند را مشخص کرده و مقدار 4 را به آن اختصاص می‌دهم. به‌طور مثال سایت badsite.contoso.com را وارد کرده و مقدار 4 را همانند شکل زیر در فیلد Value آن وارد می‌کنم.



آیا کارمان تمام شد؟ تقریبا. به محض این‌که روی دکمه OK کلیک کنیم، تنظیمات در Group Policy Object ذخیره شده و آماده اعمال شدن است، اما ما هنوز مشخص نکرده‌ایم که GPO جدید قرار است به چه موجودیتی در شبکه اعمال شود. اکنون باید به پنجره کنسول Group Policy Management باز گردیم و مکانی که قرار است GPO جدید با آن مرتبط شود را مشخص کنیم. شما می‌توانید GPO را به بالای دامنه تخصیص داده و مرتبط کنیم تا GPO جدید روی هر چیزی که در زیر آن قرار دارد اعمال شود. به عبارت دقیق‌تر، GPO جدید به هر ماشینی که درون دامنه قرار دارد متصل خواهد شد. در این‌جا ما قصد نداریم تا GPO جدید به شکل سراسری اجرایی شود و قصد داریم آن‌را به واحد سازمانی خاصی شبیه به دپارتمان حساب‌داری مرتبط کنیم. برای این منظور کافی است روی واحد سازمانی (OU) مدنظر خود کلیک راست کرده و گزینه Link an Existing GPO را انتخاب کنیم.



پنجره‌ای همانند شکل زیر ظاهر می‌شود که اجازه می‌دهد GPO جدید تنها به ماشین‌هایی که درون واحد سازمانی ذخیره‌سازی شده‌اند اعمال شود.



نکته: واحد سازمانی (OU) که در اوایل آموزش به آن اشاره کردیم، در چنین شرایطی به یاری ما آماده و اجازه می‌دهد تنظیمات را به درستی روی کامپیوترهای موردنظر خود اجرا کنید.

دقت کنید که شما می‌توانید GPO را به بیش از یک واحد سازمانی اختصاص دهید. کافی است مراحل بالا را تکرار کرده و هر GPO که ایجاد کردید را روی واحد سازمانی مربوطه اعمال کنید.

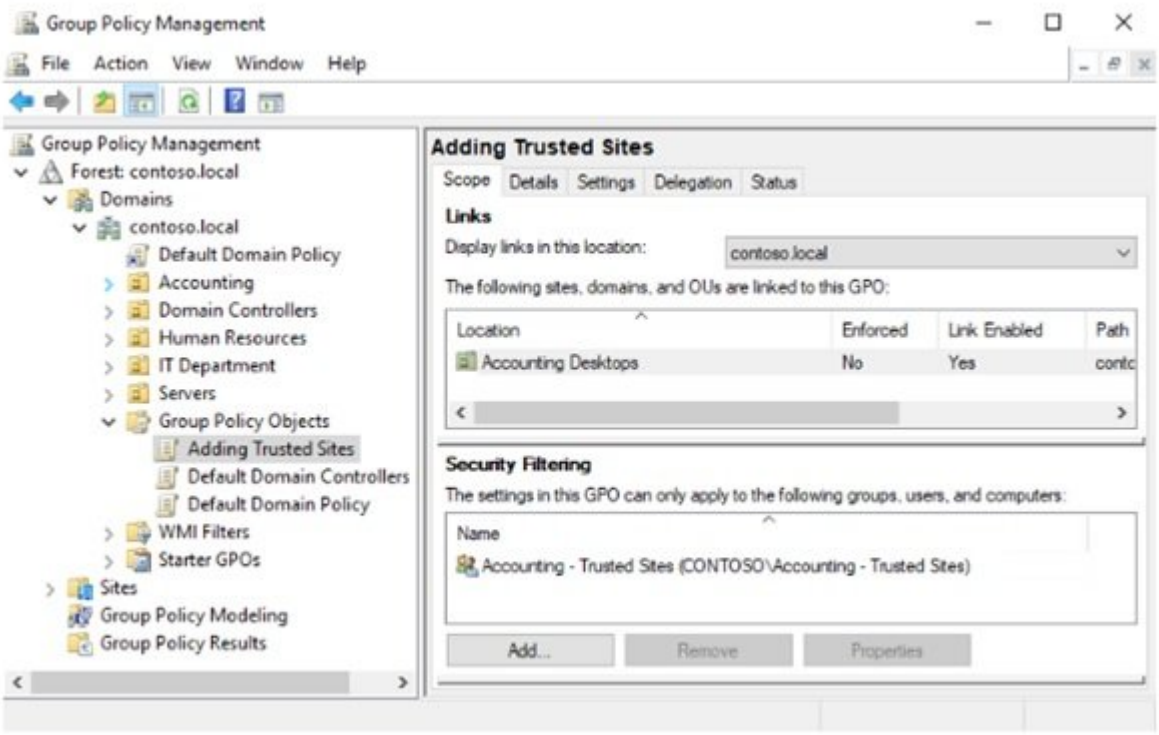
فیلتر کردنGPO برای دستگاه‌های خاص

اکنون که یک GPO ایجاد کرده و آن‌را به واحد سازمانی خاصی متصل کردید، این دانش را پیدا کرده‌اید که در محیط واقعی از Group Policy استفاده کنید. مرتبط کردن GPO با ماشین‌ها و کاربرانی که قرار است خط‌مشی‌ها را دریافت کنند، رایج‌ترین کاری است که مدیران شبکه انجام می‌دهند. اما در برخی موارد مجبور هستید یک کار بیشتر انجام دهید. اگر یک GPO جدید دارید و آن‌را به واحد سازمانی متصل کردید که شامل تمامی کامپیوترهای دسکتاپی است و پس از مدتی تصمیم گرفتید که برخی از ماشین‌ها باید از خط‌مشی جدید جدا شوند چه کاری انجام می‌دهید؟ این یک سردرد بزرگ است، زیرا مجبور خواهید شد دو واحد سازمانی جدید برای این خط‌مشی ایجاد کنید. **ویندوز سرور 2019** برای حل این مشکل ویژگی GPO Security Filtering را در اختیارتان قرار می‌دهد.

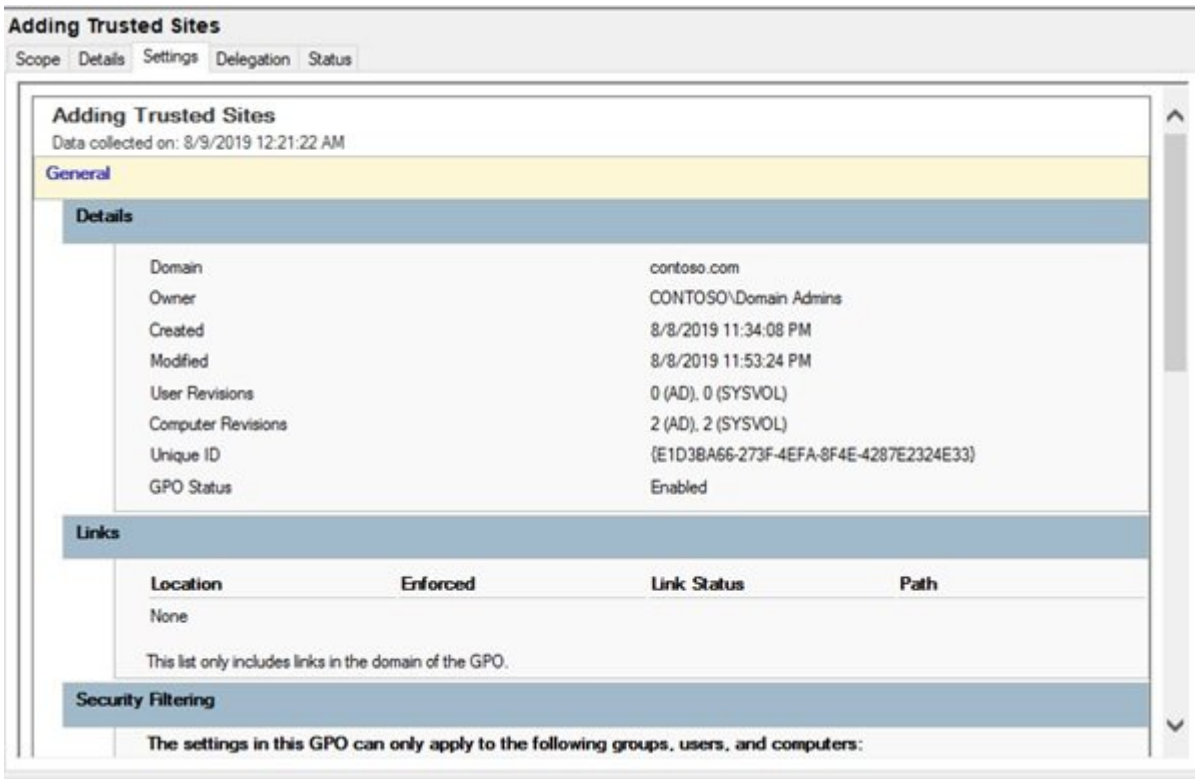
فیلترکردن امنیتی قابلیتی است که اجازه می‌دهد GPO روی اشیا خاصی در اکتیو دایرکتوری اعمال شوند. در مورد هر GPO که درون دایرکتوری خود دارید، شما می‌توانید فیلترهایی را تنظیم کنید تا GPO فقط روی کاربران، کامپیوترها یا حتا گروه‌های خاصی از کاربران یا کامپیوترها اعمال شود. به نظرم استفاده از گروه‌ها خیلی مفید است. بنابراین، در ارتباط با مثال قبلی ما یک خط‌مشی داریم که باید تنها روی کامپیوترهای دسکتاپی اعمال شود. برای این منظور باید یک Security group جدید درون اکتیو دایرکتوری ایجاد کنیم و فقط کامپیوترهای مدنظرمان را به آن گروه اضافه کنیم. هنگامی که GPO با آن گروه فیلتر شد، خط‌مشی فقط روی کامپیوترهایی که بخشی از آن گروه هستند اعمال می‌شود. راهکار فوق به شما اجازه می‌دهد در آینده، اگر نیاز داشتید تا خط‌مشی‌ها را از روی برخی از کامپیوترها بردارید، به راحتی کامپیوترها را به گروه مربوطه اضافه کرده یا از آن حذف کنید بدون آن‌که نیازی داشته باشید GPO را اصلاح کنید.

بخش Security Filtering هنگام کلیک روی هر GPO از داخل کنسول مدیریت Group Policy نمایش داده می‌شود. روی GPO که پیش‌تر ساختید کلیک کنید. در سمت راست پنجره و در بخش بالا پیوندهایی که در حال حاضر روی

خط‌مشی فعال هستند و در نیمه پایین صفحه بخش Security Filtering را مشاهده می‌کنید. در این‌جا مشاهده می‌کنید که GPO ما به واحد سازمانی Accounting Desktops متصل شده است، اکنون قصد داریم یک فیلتر امنیتی اضافی را برای آن تنظیم کنید تا فقط ماشین‌هایی که بخشی از Accounting - Trusted Sites group هستند، GPO ساخته شده را دریافت کنند.



برای این منظور باید روی دکمه Add در پایین بخش Security Filtering کلیک کرده و گروه موردنظر را مشخص کنید تا GPO جدید روی آن اعمال شود. اگر در همین پنجره روی دکمه Settings کلیک کنید، همه اطلاعات پیکربندی GPO که ایجاد کرده‌اید را مشاهده می‌کنید. اطلاعات این زبانه به ویژه زمانی مفید است که GPO توسط فردی دیگری ساخته شده و تمایل دارید اطلاعاتی در مورد آن به دست آورید.



در شماره آینده آموزش رایگان **ویندوز سرور 2019** به سراغ سامانه نام دامنه خواهیم رفت.

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

آموزش رایگان ویندوز سرور 2019

تاریخ انتشار:
19 مرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15886/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%A8%D9%87%E2%80%8C%DA%A9%D8%A7%D8%B1%DA%AF%DB%8C%D8%B1%DB%8C-group-policy-%D8%AF%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%B3%D8%A7%D8%AE%D8%AA-gpo