« فصل ۸ »

ایجاد و مدیریت سیاست‌های گروهی

Creating and Managing

Group Policies

زمانی که صحبت از اکتیو دایرکتوری به میان می‌آید، لازم است که در مورد Group Policy (GP) نیز صحبت شود. Group Policy در واقع به سیاست‌هایی گفته می‌شود که برروی اشیاء اکتیو دایرکتوری اعمال شده و نحوه عملکرد آنها را در شبکه تعیین می‌کند. Group Policy یک فناوری جدید برای اکتیو دایرکتوری در ویندوز سرور 2008R2 به شمار نمی آید زیرا از زمان ویندوز 2000 وجود داشته است، اما با انتشار هر نسخه یا Service Pack جدید از ویندوز سرور (و اکتیو دایرکتوری) این فناوری نیز دستخوش پیشرفت‌ها و بهبودهای قابل توجهی شده است. این پیشرفت‌ها به ویژه از زمان ویندوز سرور 2008 در مواردی همچون مدیریت Group Policy (با استفاده از ابزارهایی همچون Group Policy Management Console و Group Policy Management Editor)، مدیریت تنظیمات (بیش از ۵۰۰۰ مشخصه قابل تنظیم)، کنترل اشیاء و همچنین عیب‌یابی زیرساخت Group Policy حاصل شده است. پیکربندی و توسعه Group Policy به کمک **Group Policy objects (GPOs)** انجام می‌شود. GPOها کانتینترها یا گروه‌هایی از تنظیمات (Policy Setting) هستند که می‌توانند به حساب‌های کاربری و کامپیوترهای یک اکتیو دایرکتوری در طول شبکه اعمال شوند. اشیاء Policy با استفاده از Group Policy Management Editor یا به اختصار GPME ایجاد می‌شوند و در این ابزار قابل ویرایش می‌باشند. با استفاده از GPOها می‌توان اعمالی مانند مشخص نمودن تعدادی برنامه برای نصب برروی Desktop کاربران، تعیین نحوه انتخاب رمز عبور کاربران، محدود کردن سهمیه[1] استفاده از دیسک برای کاربران و ... را انجام داد. امکان ایجاد یک GPO همه جانبه به منظور اعمال تعدادی از سیاست‌ها و یا ایجاد تعدادی GPO هریک برای یک عمل خاص وجود دارد.

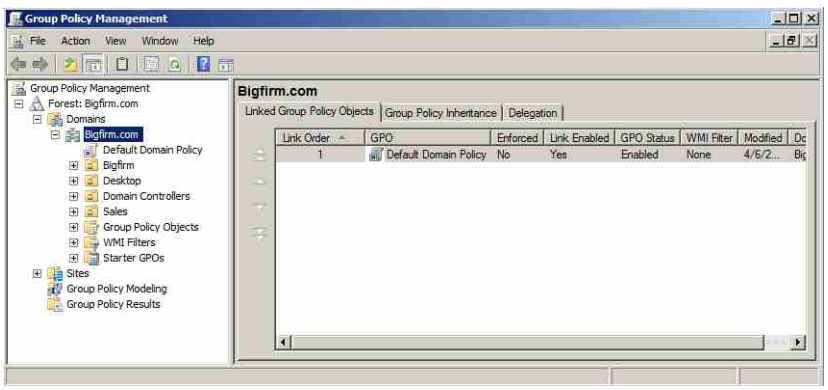
در این فصل قصد داریم به نحوه ایجاد و مدیریت Group Policyها با استفاده از ابزارهای مدیریتی آن بپردازیم. بطور کلی مهمترین مباحثی که در این فصل مورد بررسی قرار می‌گیرند عبارتند از:

- آشنایی با سیاست‌های Local و اشیاء Group Policy[2] (GPO)
- ایجاد GPOها
- مدیریت و عیب‌یابی Group Policyها

۸-۱ ایجاد GPOها

برای ایجاد Group Policy مبتنی بر دامنه لازم است ابزاری به نام Group Policy Management را اجرا کنید. این ابزار از مسیر Start » Administrative Tools » Group Policy Management و یا از طریق کنسول Server Manager قابل دسترسی می‌باشد.

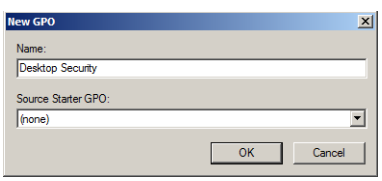
1. Quota
2. Group Policy Objects



شکل ۸-۱

جهت ایجاد یک GPO ابتدا برروی نام جنگل (Forest: Bigfirm.com) کلیک کرده تا آیتم‌های زیرمجموعه آن نشان داده شوند. سپس از زیر نام دامنه (Bigfirm.com) آیتم Group Policy Objects را پیدا نموده و مراحل زیر را دنبال کنید:

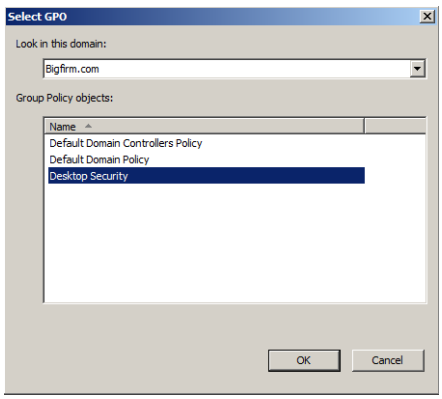
۱. برروی Group Policy Objects کلیک‌راست نموده و New را انتخاب کنید.
۲. در پنجره "New GPO" نام انتخابی برای GPO (در اینجا Desktop Security) را وارد نموده و برروی OK کلیک کنید.



شکل ۸-۲

پس از انجام مراحل بالا، GPOای با نام Desktop Security ایجاد می‌شود ولی این GPO به هیچ کانتینری در دامنه پیوند نشده است، بنابراین شاید قصد داشته باشید که تنظیماتی را برای این GPO پیکربندی نموده و آنرا به یک سایت، دامنه و یا OU پیوند دهید. برای انجام این کار (با فرض اینکه قبلاً یک OU با نام Desktop در ADUC ایجاد کرده‌اید)، مراحل زیر را دنبال کنید:

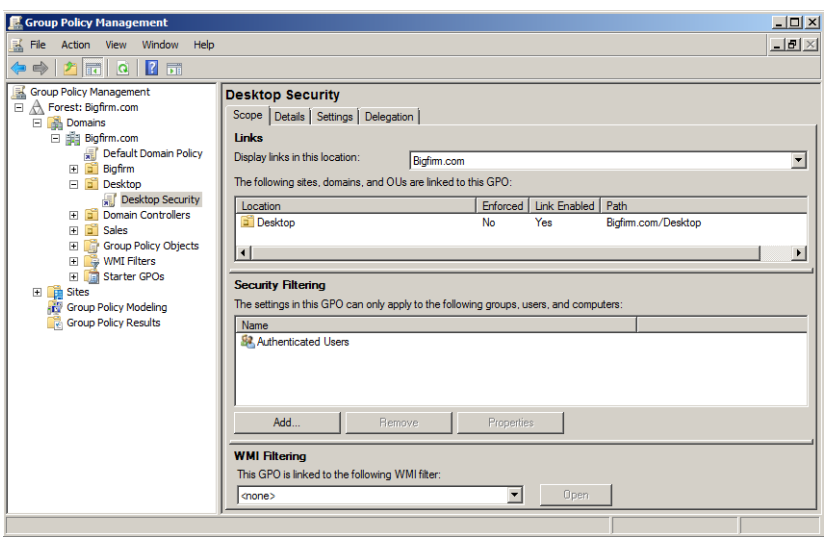
۱. برروی Desktop OU کلیک‌راست نموده و گزینه Link an Existing GPO را انتخاب کنید.
۲. در پنجره "Select GPO" لیستی از GPOهای موجود نشان داده می‌شود. GPO با نام Desktop Security را انتخاب نموده و برروی OK کلیک کنید.



شکل ۸-۳

۳. برای ایجاد و پیوند دادن GPO به یک دامنه نیز کافی است برروی نام آن دامنه کلیک‌راست نمـوده و گزینه "Create a GPO in this domain, and link it here" را انتخاب کنید.

پس از ایجاد GPO و پیوند آن به Desktop OU، برروی OU کلیک کنید. در پنل سمت راست تعدادی تب ظاهر می‌شود. این تب‌ها عبارتند از: Scope، Details، Settings و Delegation.



شکل ۸-۴

تب Scope

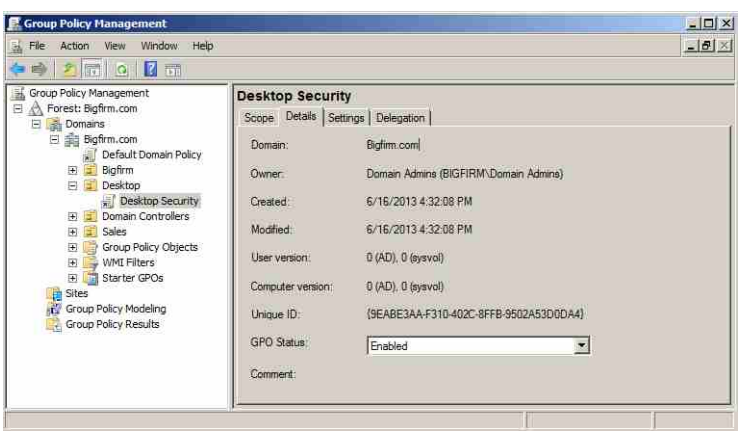
تب Scope کمک می‌کند تـا بسـیاری از جنبـه‌هـای GPO را پیگیـری کنیـد. مهمتـرین جزئیـات قابـل

مشاهده در این تب، نام گره‌ای از اکتیو دایرکتوری است که GPO به آن پیوند شده است.

- در قسمت **Link** می‌توان نام OU، دامنه و یا سایتی که GPOبه آن پیوند شده را مشاهده نمود.
- قسمت **Security Filtering** مشخص می‌کند که کدام کاربران و یا گروه‌ها می‌توانند تنظیمات را برروی GPO اعمال کنند. انجام فیلترینگ برای دادن مجوز یا حذف آن تنها با اضافه کردن و یا حذف کردن کاربران و گروه‌ها از این لیست قابل انجام می‌باشد.
- سومین قسمت موجود در این تب، **WMI Filtering**[1] می‌باشد. WMI یک زیرساخت مدیریتی است که مدیران شبکه را قادر می‌سازد تا بتوانند اشیاء روی یک شبکه را نظارت و کنترل کنند. برای خودکار کردن فرایندهای امنیتی، می‌توان یک برنامه یا اسکریپت WMI نوشت و آن را به صورت Remote یا Local به کار برد. با یک WMI Query می‌توان سیستم‌های موجود در شبکه را بر حسب مشخصه خاصی از آنها فیلتر نمود، مانند مقدار فضای RAM آزاد آنها، سیستم عامل، Service Pack، نرم افزارهای نصب شده و تنظیمات پرینتر. جهت کسب اطلاعات بیشتر در این زمینه به آدرس http://technet microsoft.com/en-us/library/cc779036(v=ws.10).aspx مراجعه کنید.

تب Details

در این تب اطلاعاتی راجع به GPO و وضعیت آن ارائه شده است. همچنین امکان فعال یا غیر فعال کردن تنظیمات GPO برای کامپیوترها یا کاربران نیز در این تب امکان پذیر می‌باشد.

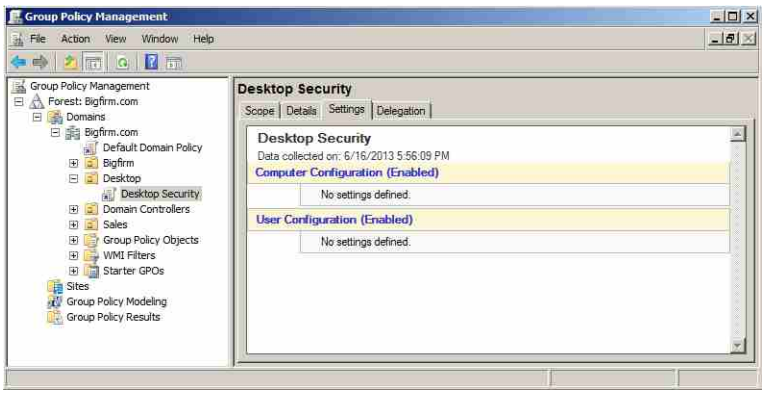


شکل ۸-۵

تب Settings

این تب شامل داده‌های پویای مرتبط با تنظیمات پیکربندی شده برای GPO می‌باشد.

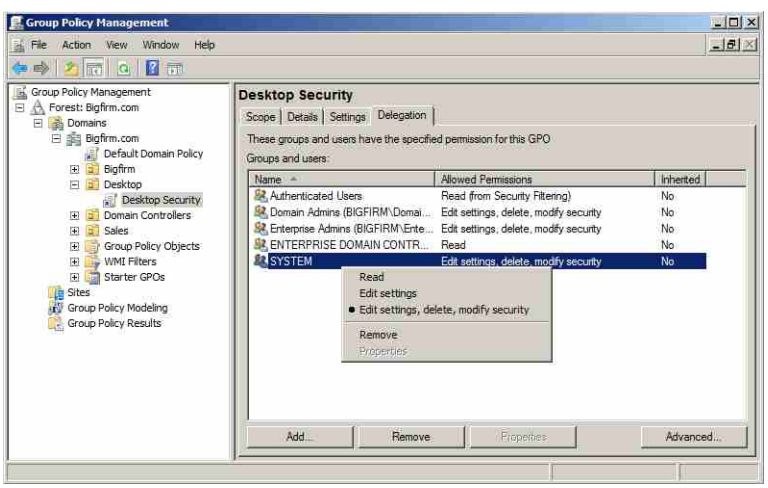
1. Windows Management Instrumentation Filters



شکل ۸-۶

تب Delegation

در این تب لیست افراد و یا گروه‌های مجاز جهت مدیریت GPO آورده شده است. سه سطح مدیریتی برای GPO تعریف شده است که سطح اول (Read) تنها مجوز خواندن و دو سطح بعدی مجوز ویرایش GPO را به کاربران و یا گروه‌ها واگذار می‌کنند. در شکل زیر این سطوح قابل مشاهده هستند.

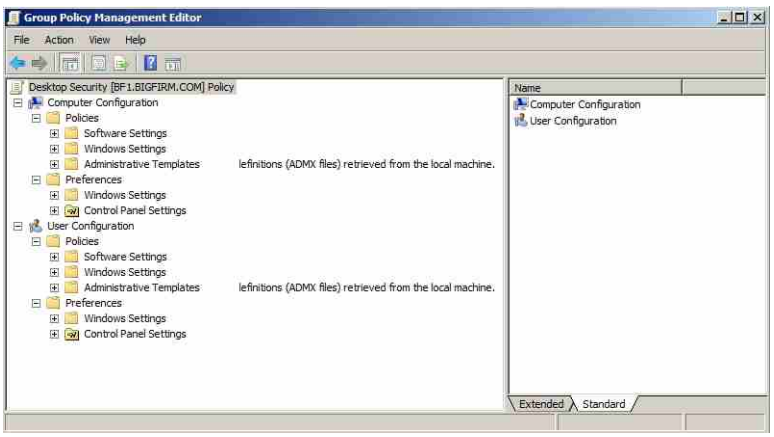


شکل ۸-۷

تنظیمات GPO

پس از ایجاد GPO اجازه دهید نحوه ایجاد تغییرات در آن را نیز مورد بحث قرار دهیم. به گره

Group Policy Objects در GPMC باز گشته و برروی GPO کلیک‌راست کنید. با انتخاب گزینه Edit پنجره GPME اجرا می‌شود.



شکل ۸-۸

دو دسته کلی از تنظیمات در این پنجره قابل انجام هستند. دسته اول **Computer Configuration** است که مربوط به تنظیمات حساب‌های کامپیوتری و دسته دوم **User Configuration** تنظیمات مربوط به حساب‌های کاربری می‌باشد. در این قسمت تعدادی تنظیمات قابل اعمال برروی حساب‌ها را معرفی نموده و در قسمت‌های بعد مثال‌هایی در این زمینه ارائه می‌دهیم.

- برای مشخص کردن یک بسته نرم افزاری (جهت نصب از طریق Group Policy) پوشه Policies\Software Settings\Software Installation را انتخاب نموده و برروی آن کلیک‌راست کنید. گزینه «New» Package را انتخاب نموده و در پنجره باز شده مسیر برنامه مورد نظر را تعیین و سپس آنرا نصب کنید. پس از نصب می‌توانید مشخصات آنرا تنظیم کنید.
- برای تنظیم مدت زمانی که کاربران باید برای تغییر رمز عبور خود منتظر بمانند، به مسیر Computer Configuration\Policies\ Windows Settings\Security Settings\Account Policies\Password Policy رفته و سپس با دابل کلیک برروی هر یک از گزینه‌ها، تنظیمات مربوط به رمز عبور کاربران را مشخص کنید.
- برای تنظیم سیاستی که اعضای یک گروه را محدود می‌کند، به مسیر Computer Configuration\Policies\ Windows Settings\ Security Settings رفته و Restricted Groups را انتخاب کنید. برروی این آیتم کلیک‌راست نموده و Add Group را انتخاب کنید. پس از انتخاب گروه برروی نام آن دابل کلیک نموده و کاربران یا گروه‌هایی که در این گروه باید قرار گیرند را تعیین

نمایید.

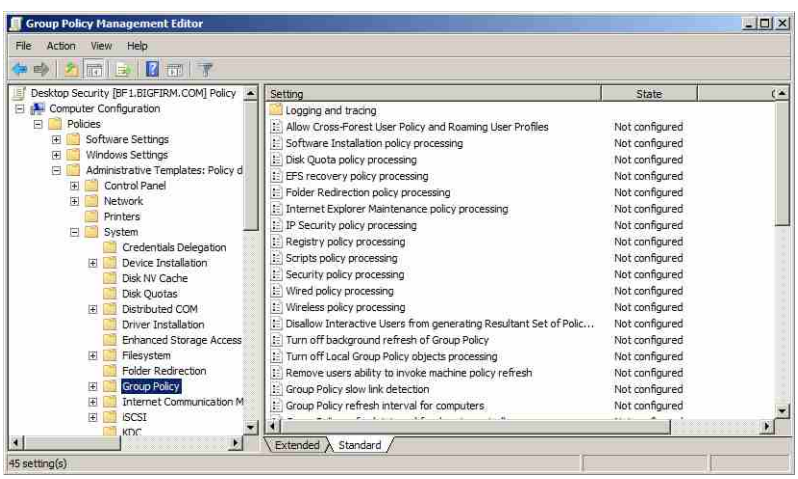
- برای تنظیم تغییر مسیر یک پوشه، به مسیر User Configuration \Policies\ Windows Settings \ Folder Redirection رفته و سپس یک پوشه (به عنوان مثال Start Menu) را انتخاب کنید. در پنل سمت راست، کلیک‌راست نموده و Properties را انتخاب کنید. در صفحه باز شده می‌توانید تنظیمات مربوط به محل قرار گیری محتویات پوشه مورد نظر را انجام دهید.

۸-۲ تغییر عملکرد پیش‌فرض Group Policy

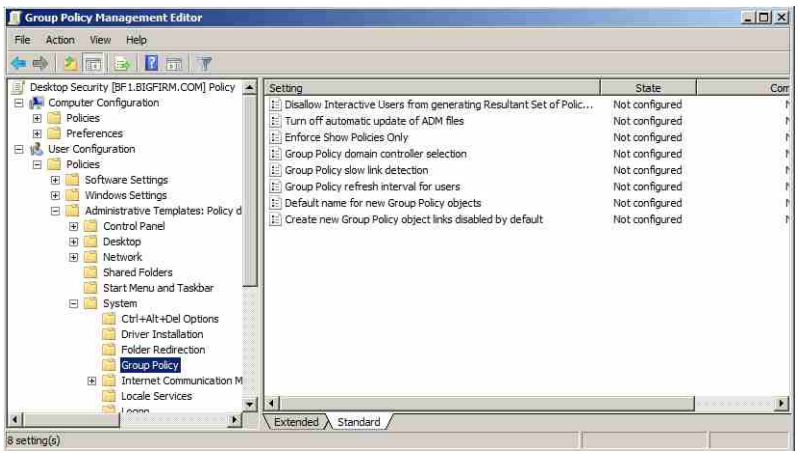
Group Policy بطور ذاتی یک امکان فوق‌العاده به شمار می‌آید اما برخی عملکردها در آن وجود دارند که ممکن است بخواهید تغییر دهید و یا کنترل کنید. تغییر این عملکردها با استفاده از GPOها و تنظیمات آنها قابل انجام است. بسیاری از این تنظیمات نیازی به پیکربندی ندارند اما در مواردی که نیازمند ایجاد برخی از تنظیمات جزئی هستید، این کار لازم است.

۸-۲-۱ سیاست‌های Group Policy

تنظیمات GPO از زیرمجموعه Administrative Templates در گره‌های User Configuration و Computer Configuration قابل دسترسی می‌باشد. (Policies\AdministrativeTemplates\System\Group Policy). در شکل‌های ۸-۹ و ۸-۱۰ به ترتیب آپشن‌های Group Policy برای هر دوگره Computer Configuration و User Configuration نشان داده شده است. در ادامه مهمترین آپشن‌های پیکربندی را مورد بررسی قرار می‌دهیم.



شکل ۸-۹: آپشن‌های Computer Configuration

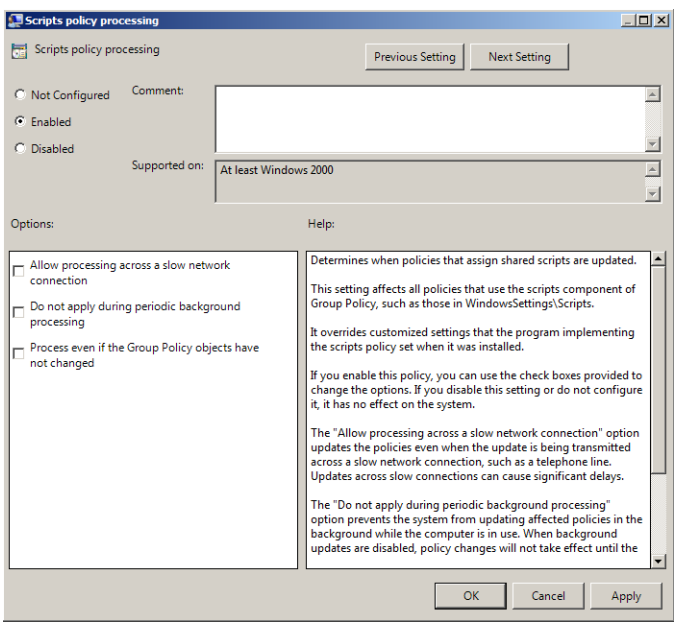


شکل ۸-۱۰: آپشن‌های User Configuration

- **Group Policy refresh intervals for users/computers/domain controller**: این سیاست‌ها چگونگی Refresh شدن GPOها را زمانی که کاربران و کامپیوترها در حال کارکردن هستند مشخص می‌کند. این پارامترها اجازه تغییر Refresh شدن پیش‌فرض و تنظیم بازه‌های زمانی برای Refresh شدن را مشخص می‌کنند.
- **Turn off background refresh of Group Policy**: چنانچه این گزینه را فعال کرده باشید، سیاست‌ها تنها در زمان راه اندازی سیستم و logon کردن کاربران Refresh می‌شوند. این امکان برای دلایل بهبود کارایی در شعبه‌های سازمان زمانی که دارای ۱۵۰۰ کامپیوتر که هر ۹۰ دقیقه Refresh شده و باعث ایجاد ازدحام در یک ارتباط WAN می‌شوند مفید است.
- **Policy processing options**: این سیاست‌ها با نام‌هایی مثل **Policy Processing** Registry و Folder **Policy Processing** Redirection به منظور شخصی‌سازی عملکرد GPOهای مختلف در دسترس هستند. این تنظیمات در زیرمجموعه گره Computer Configuration موجود بوده و هر سیاست حداقل دو مورد از سه آپشن زیر را ارائه می‌دهند:
  - **Allow processing across a slow network connection**: در ارتباطات کند تعدادی از سیاست‌ها به منظور افزایش کارایی می‌توانند غیرفعال شوند.(امکان تعریف ارتباط کند از طریق سیاست Group Policy Slow Link Detection امکان‌پذیر می‌باشد). البته دقت داشته باشید که تنظیمات امنیتی و Registry Policy Processing همیشه اعمال شده و امکان خاموش کردن آنها وجود ندارد.
  - **Do not apply during periodic background processing**: این گزینه تعیین می‌کند چنانچه

کامپیوتر در حال اجرا است، سیاست‌هایی که آپدیت شده و قرار است در عملکرد سیستم تغییری ایجاد کنند نتوانند برروی کامپیوتر اعمال شوند. اعمال تغییرات ایجاد شده در زمان ورود بعدی کاربر و یا Restart شدن کامپیوتر انجام خواهد شد.

- **Process even if the Group Policy objects have not changed:** برای افزایش امنیت و جلوگیری از ایجاد تغییر در تنظیمات Policy توسط یک کابر، فعال‌سازی این سیاست اطمینان می‌دهد که در هر بار Refresh شدن، تمام تنظیمات مجدداً تکرار می‌شوند. دقت داشته باشید که فعال‌سازی این سیاست ممکن است بطور قابل توجهی باعث کاهش کارایی گردد.

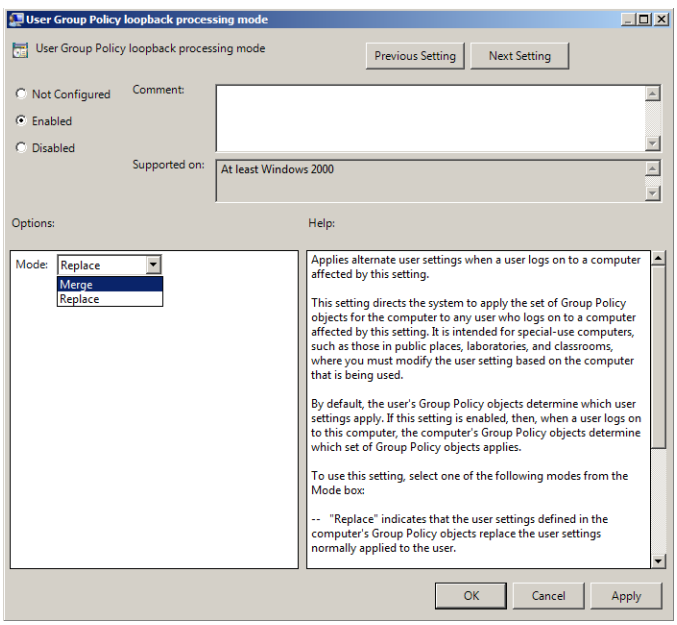


شکل ۸-۱۱

- **Loopback processing mode:** بطور پیش‌فرض تنظیمات User Policy بعد از سیاست‌های Computer Configuration پردازش می‌شوند. همچنین کاربران تنظیمات Policy را بدون در نظر گرفتن ماشینی که به آن وارد می‌شوند دریافت می‌کنند. به عنوان مثال فرض کنید که با استفاده از User Policy تعریف شده است که در هنگام ورود کاربران به دامنه، تعدادی برنامه کاربردی برای آنها نصب شود. زمانی که شما به منظور انجام اقدامات مدیریتی به سرور وارد می‌شوید، دیگر نیازی به نصب شدن این برنامه‌ها نخواهید داشت بنابراین لازم است که این Policyها بجای کاربر، مطابق با کامپیوتری که به آن وارد می‌شوید اعمال شوند (Loopback processing). به عنوان مثالی دیگر می‌توان حالتی را در نظر گرفت که لازم است سیاست‌های کامپیوتر،

سیاست‌های مربوط به کاربران را نادیده بگیرند. این حالت زمانی است که از کامپیوتر در مکان‌های عمومی مانند کتابخانه‌ها، آزمایشگاه‌های کامپیوتر در دانشگاه‌ها، و ... استفاده می‌شود. دو حالت برای کنترل عملکرد این سیاست وجود دارد:

- **Merge mode:** این گزینه تنظیمات معمولی کاربر و تنظیمات GPOهای کامپیوتر را با یکدیگر ترکیب می‌کند. چنانچه در این تنظیمات تضادی وجود داشته باشد، تنظیمات کاربر در GPOهای کامپیوتر نسبت به تنظیمات معمولی کاربر اولویت پیدا می‌کنند.
- **Replace mode:** این گزینه تنظیمات GPOهای کامپیوتر را جایگزین تنظیمات معمولی کاربر می‌نماید.

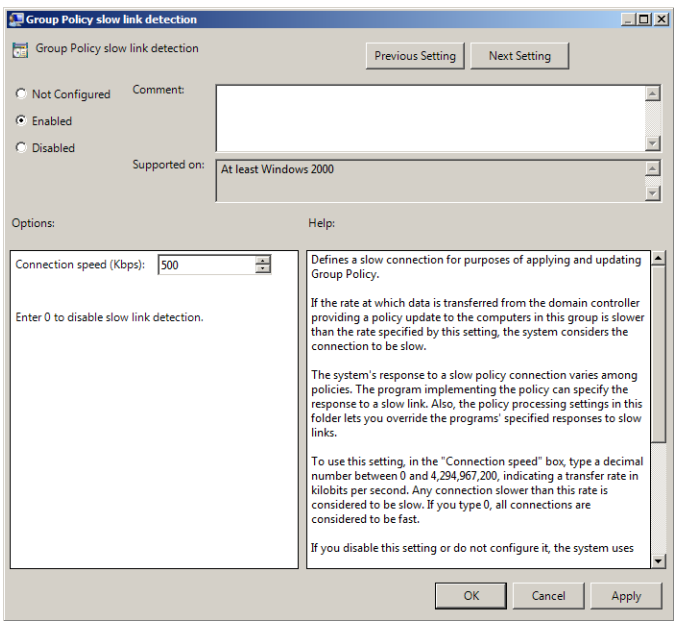


شکل ۸-۱۲

۸-۲-۲ Group Policy برروی لینک‌های کم سرعت

Group Policy هنوز هم در طول لینک‌های کم سرعتی مانند Dial_Up عمل می‌کنند (این لینک‌ها ممکن است در بین سایت‌هایی که شعبه‌های سازمان را به یکدیگر و یا شعبه مرکزی متصل می‌کنند برقرار باشد). به دلیل اینکه استفاده از لینک‌های کم سرعت باعث ایجاد مسائل کارایی می‌شود، در Group policy برای آنها تنظیماتی جهت تعریف سرعت لینک و همچنین چگونگی اعمال سیاست‌ها برروی این لینک‌ها وجود دارد. برای انجام تنظیمات لینک‌های کم سرعت می‌توانید از مسیر

سیاست Group Policy slow link detection را پیدا نموده و با فعال‌سازی آن، سرعت مورد نظر برای لینک کم سرعت را تعیین کنید. زمانی که این Policy را فعال می‌کنید بطور پیش‌فرض عدد ۵۰۰ در آن درج شده است که می‌توانید با توجه به نوع ارتباط خود آنرا تغییر دهید. (به عنوان مثال سرعت ٥٦ کیلو بیت/ثانیه برای ارتباط Dial_Up).



شکل ۸-۱۳

توجه داشته باشید که پس از تعریف لینک کم سرعت باید امکان ارتباط از طریق این لینک را فعال کنید. این کار با فعال کردن گزینه "Allow processing across a slow network connection" در Policyها امکان‌پذیر می‌باشد.

۸-۳ استفاده از Group Policy

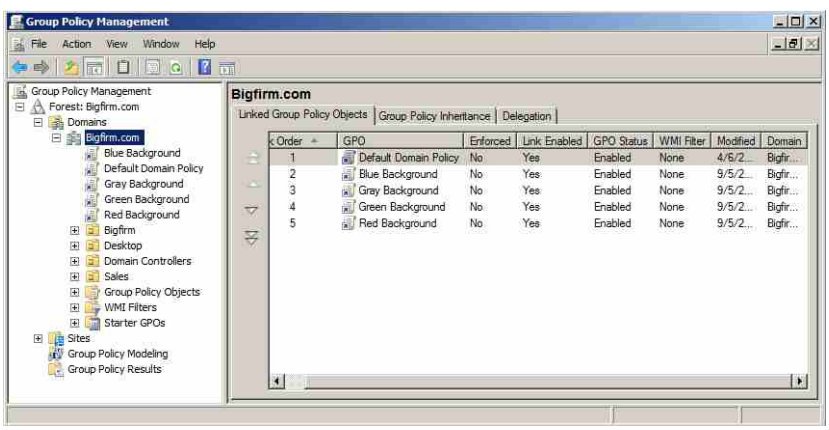
هنگام استفاده از Group Policy باید مطمئن شوید که سیاست‌ها به روش قابل اطمینانی اعمال می‌شوند. بیشتر اوقات استفاده از Group Policy ساده است و تنها زمانی که در هنگام استفاده از آن با تضاد مواجه می‌شوید یا قصد دارید عملکرد پیش‌فرض آنرا تغییر دهید ممکن است کار برایتان کمی پیچیده‌تر شود. با این وجود زمانی که در حال طراحی و پیاده‌سازی تنظیمات Policy هستید باید درک کاملی از نتیجه اجرای آنها برروی کاربران و کامپیوترها داشته باشید.

۸-۳-۱ Group policy چگونه اعمال می‌شود

اکنون با داشتن یک یا دو GPO بزودی با بخش دردسر ساز Group policy مواجه می‌شوید: دانستن این مطلب که نتیجه نهایی برای کاربران و کامپیوترها چه خواهد بود. به عنوان مثال فرض کنید یک کاربر سؤال می‌کند که "چرا پس زمینه[1] من بنفش است؟"، بعد از آن متوجه می‌شوید که سیستم این کاربر از جاهای زیادی سیاست‌های خود را دریافت می‌کند و ممکن است این سیاست‌ها در مسائلی مانند رنگ پس زمینه متفاوت باشند. بنابراین کدامیک سیاست دارای اولویت خواهد بود؟

سیاست‌ها از پایین به بالا در GUI اجرا می‌شوند

اجازه دهید کار را با یک وضعیت ساده آغاز کنیم: حالتی که Policyها تنها از یک دامنه دریافت می‌شوند. فرض کنید که در حال جستجوی یک گره در پنجره GPMC هستید و پس از پیدا کردن آن مشاهده می‌کنید که تعدادی GPO به آن پیوند شده است. این وضعیت در شکل ۸-۱٤ نشان داده شده است.



شکل ۸-۱۴

در این وضعیت (مسلماً خیالی) دامنه دارای پنج Group policy است که چهارتای آن برای تنظیم رنگ پس زمینه ایستگاه‌های کاری به خاکستری، سبز، قرمز یا آبی است. برای مشاهده اینکه کدامیک از GPOها دارای اولویت است، برروی گره دامنه (Bigfirm.com) کلیک نموده و در پنل سمت راست تب Linked Group Policy Objects را انتخاب کنید. با توجه به Policyهای موجود در این تب حدس می‌زنید کدامیک برنده خواهند شد؟ خاکستری، قرمز، سبز یا آبی؟

پاسخ به این سوال در دو قاعده برای حل تعارض GPOها نهفته است:

1. Background

- قاعده اول: توجه به آخرین سیاستی که برروی گره اعمال شده است.
- قاعده دوم: اجرای سیاست‌ها از پایین به بالا انجام می‌شود همانگونه که در GUI (منظور همان پنجره گرافیکی است) ظاهر شده‌اند.

با خواندن سیاست‌ها از پایین صفحه به بالای آن مشاهده می‌کنید که سیستم ابتدا به Policy که رنگ پس زمینه را به قرمز تنظیم می‌کند توجه می‌نماید. پس از آن به سیاستی که رنگ را به سبز، پس از آن سیاست تنظیم رنگ به خاکستری و در آخر نیز به سیاست رنگ آبی نگاه می‌کند. از آنجایی که آبی آخرین سیاست اعمال شده است بنابراین برنده است و تاثیر رنگ سه سیاست قبلی را خنثی می‌نماید.

چنانچه قصد داشته باشید اولویت این سیاست‌ها را تغییر دهید، می‌توانید از دکمه‌های جهتی که در این تب تعبیه شده است استفاده کنید. دقت داشته باشید که هر سیاستی که به بالا انتقال داده شود اولویت بالاتری اتخاذ می‌کند و تأثیر سیاست‌های پایین‌تر از خود را خنثی می‌نماید.

ترتیب استفاده از Group Policy

مثالی که در قسمت قبل ارائه شد، تنها حالتی را در نظر گرفته بود که GPOها به دامنه پیوند شده‌اند، اما می‌توانید GPOها را به سایر گره‌ها در اکتیو دایرکتوری نیز پیوند دهید:

- GPOها می‌توانند به سایت‌ها نیز پیوند شده بدون اینکه به ماشین‌ها و کاربرانی که در آن قرار گرفته‌اند توجهی داشته باشند.
- OUها نیز می‌توانند شامل پیوندهای GPO باشند. توجه داشته باشید که هر OU می‌تواند شامل تعدادی OU دیگر باشد، بنابراین هر یک از OUهای موجود در طی این زنجیره (OUهای داخل سایر OUها) می‌توانند شامل GPOهایی باشند که به آنها پیوند شده است.
- Policyها به صورت Local نیز قابل اعمال برروی ماشین‌ها و کاربران می‌باشند.

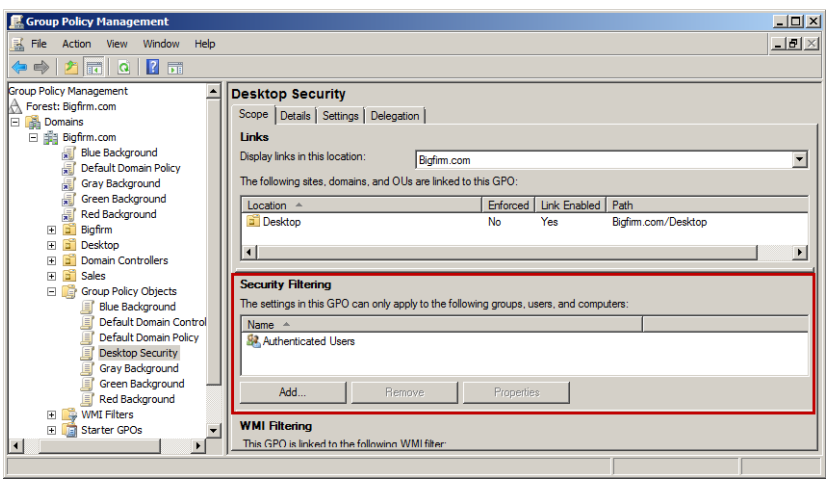
با توجه به موارد بالا چنانچه مجدداً بخواهید سوال "کدام Policy برنده است؟" را پاسخ دهید باید ترتیب زیر را دنبال کنید:

- Policyهای Local
- Policyهای اعمال شده برروی سایت‌ها
- Policyهای اعمال شده برروی دامنه‌ها
- Policyهای اعمال شده برروی OUها
- Policyهای اعمال شده برروی Child OUها

اگر سیاست دامنه بگوید که "قبل از خاموش کردن سیستم باید به آن Login کنید" و سیاست OU بگوید که "اجازه خاموش کردن سیستم را قبل از Login کردن دارید" سیاست OU دارای اولویت خواهد بود زیرا آخر از همه اعمال شده است. اگر یک Policy بگوید که "آنرا قفل کن" و سیاست بعدی بگوید "پیکربندی نشده"، تنظیمات پیکربندی نشده باقی می‌ماند. بر عکس، زمانی که یک سیاست "پیکربندی نشده" است و سیاست بعدی "قفل کردن باشد" تنظیمات به صورت قفل کردن باقی خواهد ماند. به همین ترتیب اگر چندین سیاست به صورت متوالی آورده شده باشند، آن سیاستی برنده خواهد بود که آخر از همه (از پایین به بالا) خوانده می‌شود.

۸-۳-۲ فیلتر کردن Group policy با استفاده از ACL

لیست کنترل دسترسی[1] (ACL) به فهرستی از کاربران گفته می‌شود که برای خواندن و یا ایجاد تغییر در GPOها مجوزدهی می‌شوند. برای دسترسی به این لیست، برروی یکی از GPOها در GPMC کلیک نموده (به عنوان مثال GPO با نام Desktop Security) و سپس تب Scope را از پنل سمت راست مشاهده کنید. در قسمت Security Filtering لیست ACL برای GPO قابل مشاهده می‌باشد.

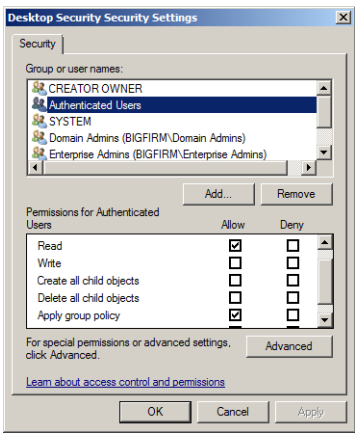


شکل ۸-۱۵

مدیران دامنه[2] و مدیران سازمانی[3] باید مجوز خواندن و ایجاد تغییر، و کاربران مجاز[4] باید مجوز خواندن و اعمال Group policyها را داشته باشند. با این وجود، در شکل ۸-۱۶ شما تنها کاربران مجاز را در لیست مشاهده خواهید نمود. علت این است که این لیست تنها برای کاربران، کامپیوترها و

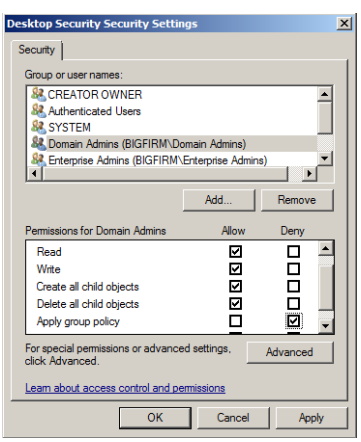
1. Access Control List
2. Domain Admins
3. Enterprise Admins
4. Authenticated Users

گروه‌هایی است که دارای مجوز اعمال تنظیمات GPO می‌باشد. برای مشاهده لیست کامل ACL به تب Delegation بروید. در این تب برروی دکمه Advanced کلیک کنید تا پنجره زیر نمایش داده شود.



شکل ۸-۱۶

ممکن است اتفاق افتد که شما یک GPO برای محدود کردن Desktop کاربران ایجاد نموده و نخواهید که برروی گروه خاصی از افراد اعمال شود. گروه Authenticated Users (کاربران مجاز) شامل همه افراد (حساب‌های کاربری و کامپیوتری) بجز مهمانان (guests) می‌باشد. بنابراین بطور پیش‌فرض GPO برروی تمام افراد به غیر از مهمانان اعمال می‌شود. این بدین معناست که Domain Admins و Enterprise Admins نیز تنظیمات Policy را دریافت می‌کنند. برای اجتناب از دریافت این تنظیمات توسط Domain Admins و Enterprise Admins، باید گزینه Apply Group Policy را برای آنها با Deny تنظیم کنید. در شکل ۸-۱۷ این وضعیت قابل مشاهده می‌باشد.



شکل ۸-۱۷

چنانچه قصد دارید افراد دیگری را نیز از این تنظیمات معاف کنید، می‌توانید آنها را به صورت تک تک اضافه نموده (با استفاده از دکمه Add) و یا یک گروه (به عنوان مثال Security Group) ایجاد نموده و این افراد را در آن قرار دهید. سپس گروه مورد نظر را به لیست ACL اضافه کنید. چون این گروه جزء Authenticated Users به شمار می‌رود، پس مجوزهای Read و Apply Group Policy به آنها داده شده است. اما لازم است برای معاف کردن آنها از دریافت تنظیمات Policy، گزینه Apply Group Policy را برای آنها با Deny تنظیم کنید.

جهت حذف کاربران یا گروه‌ها از لیست ACL نیز می‌توانید ابتدا آن کاربر و یا گروه را انتخاب نموده و سپس برروی دکمه Remove کلیک کنید.

۸-۳-۳ استفاده از فیلترهای WMI به همراه Group policy

ویندوز سرور 2003، سرور 2008 و سرور 2008R2 نوعی از فیلترینگ به نام WMI را ارائه می‌کنند که در ویندوز 2000 وجود ندارد. فیلترهای WMI پرس و جوهایی[1] که به زبان WQL[2] ایجاد شده‌اند را اجرا نموده و از آنها به منظور تعیین اینکه همه تنظیمات در یک GPO اعمال شوند استفاده می‌کنند. در این فیلترها امکان انتخاب تنظیمات Policy از میان سایر تنظیمات وجود ندارد.

برای استفاده از فیلترهای WMI ابتدا برروی GPO کلیک نموده و سپس از تب Scope به قسمت WMI Filtering مراجعه کنید. با استفاه از drop-down لیستی که در این قسمت قرار دارد می‌توانید فیلترهای مورد نظر را انتخاب نموده و به GPO پیوند دهید.

امکان انتخاب از میان هزاران فیلتر WMI وجود دارد. به عنوان مثال فرض کنید که قصد دارید تنظیمات Policy شما تنها برروی لپ‌تاپ‌ها اعمال شوند. برای انجام این کار ابتدا باید ساخت و مدل لپ‌تاپ‌ها را مشخص نموده و سپس Query شبیه زیر ایجاد کنید:

```
Root\CimV2; Select * from Win32_ComputerSystem where manufacturer = "Toshiba"
and Model = "Tecra 800" OR Model = "Tecra 810"
```

سایر شرایطی که برای WMI (در این مثال) می‌تواند تعیین شود، فضای دیسک و نسخه سیستم عامل است که در دو Query زیر آورده شده‌اند:

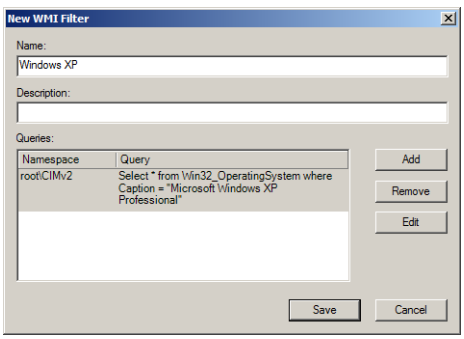
```
Root\CimV2; Select * from Win32_LogicalDisk where FreeSpace > 629145600 AND
FileSystem = " NTFS"

Root\CimV2; Select * from Win32_OperatingSystem where Caption = "Microsoft
Windows XP Professional"
```

قبل از اقدام به استفاده از فیلترهای WMI ابتدا باید آنها را ایجاد کنید. برای انجام این کار، در

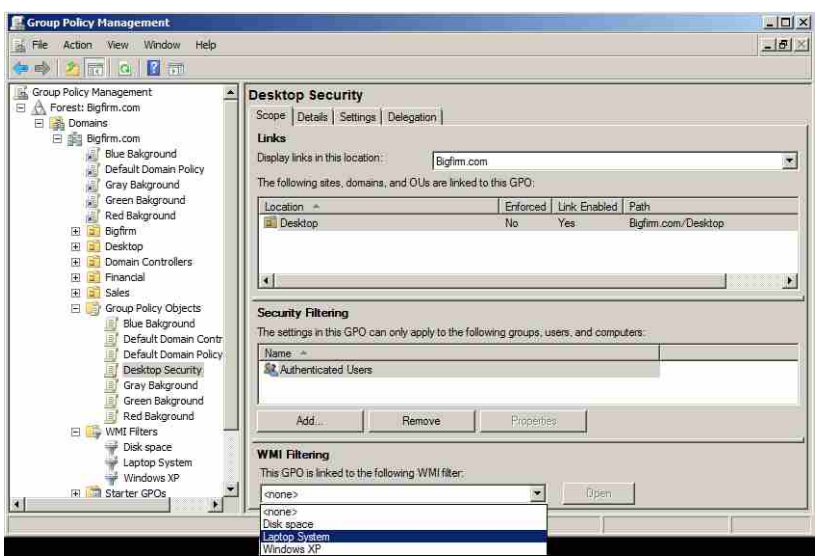
1. Query
2. WMI Query Language

پنجره GPMC برروی گره WMI Filters کلیک‌راست نموده و گزینه New را انتخاب کنید. در پنجره "New WMI Filter" نام فیلتر را وارد نموده و سپس با کلیک برروی Add، نوع فیلتر و Query آن را وارد کنید.



شکل ۸-۱۸

به عنوان مثال سه Query که در صفحه قبل آورده شده است را به صورت جداگانه وارد نموده و سه فیلتر ایجاد کنید. سپس با مراجعه به قسمت WMI Filtering زمانی‌که برروی GPO کلیک می‌کنید، فیلترها را انتخاب نموده و به GPO پیوند دهید.



شکل ۸-۱۹

جهت کسب اطلاعات بیشتر در زمینه استفاده از فیلترهای WMI می‌توانید به آدرس

http://technet.microsoft.com مراجعه نموده و سپس عبارت WMI Filters را جستجو کنید.

۸-۳-۴ مثال Group policy : انتخاب Passwordهای پیچیده

اکنون پس از توضیحات بالا، قصد داریم مثالی در رابطه با ایجاد Group Policy برای رمز عبور کاربران ارائه دهیم. اما قبل از آن لازم است فاکتورهایی را که در برنده شدن یک policy مؤثر است بیان کنیم:

- آزمودن Policyها به ترتیب روبرو می‌باشد: GPOهای Local، GPOهای سایت، GPOهای دامنه، GPOهای OU، GPOهای Child OU و به همین ترتیب.
- برای هر گره در اکتیو دایرکتوری (سایت، دامنه، OU) ترتیب آزمودن Policyها از پایین به بالای GUI می‌باشد.
- در صورت مشاهده تضاد در Policyها، باید آخرین GPO آزموده شده را مورد بررسی قرار دهید، مگر اینکه اجرای یک Policy به صورت اجباری باشد که در این صورت باید تناقض را نادیده گرفت.
- قبل از اعمال کردن یک GPO، لیست ACL آن را بررسی کنید. اگر کاربران و کامپیوترهای این لیست دارای مجوز Read و Apply Group Policy نباشند، GPO قابل اعمال برروی آنها نیست.

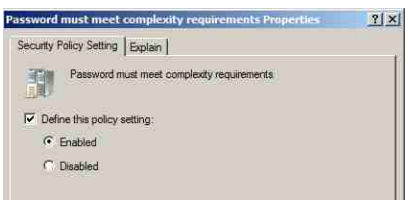
اکنون به مثال رمز عبور باز می‌گردیم. فرض کنید قصد ایجاد یک سیاست رمز عبور بسیار امن برای کاربران دامنه دارید بطوری که GPO ایجاد شده برای این کار از دو شرایط زیر برخوردار باشد:

- وجود پیچیدگی در رمز عبور.
- وجود حداقل ۱۲ کاراکتر در رمز عبور.

برای پیاده‌سازی این سیاست مراحل زیر را دنبال کنید:

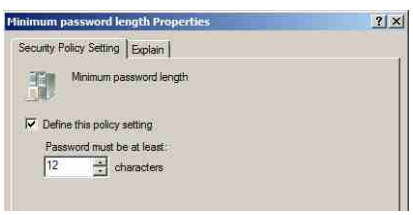
۱. کنسول Group Policy Management را اجرا کنید.
۲. برروی گره دامنه (در اینجا Bigfirm.com) کلیک‌راست نموده و گزینه Create a GPO in this domain, and Link it here را انتخاب کنید.
۳. نام GPO را New Password Policy قرار داده و برروی OK کلیک کنید.
٤. برروی GPO ایحاد شده (New Password Policy) کلیک‌راست نموده و Edit را انتخاب کنید.
٥. در پنجره GPME به مسیر \Computer Configuration\Policies\Windows Settings\Security Settings\ Account Policies\ Password Policy بروید.
٦. برروی سیاست Password must meet complexity requirements دابل‌کلیک نموده و آنرا در

وضعیت Enable (فعال) قرار دهید.



شکل ۸-۲۰

۷. سیاست Minimum password length را نیز فعال نموده و آنرا با عدد ۱۲ پیکربندی کنید.



شکل ۸-۲۱

۸. پنجره GPME را ببندید.

اکنون Policy ایجاد شده است ولی به سرعت برروی حساب‌ها اعمال نخواهد شد. Domain Controllerها، بطور پیش‌فرض تغییرات ایجاد شده در Policy را هر ۱۵ ثانیه یکبار و در صورتی که نسبت به این تغییرات آگاه باشند اعمال خواهند نمود، بنابراین چنانچه در دامنه چندین DC وجود داشته باشد باید منظر بمانید تا اطلاعات Policy به سایر DCها ارسال شود (واضح است که اگر تنها یک DC داشته باشید با مسئله انتظار روبرو نخواهید بود).

اکنون سعی کنید یک حساب کاربری با رمز عبور ۷ کاراکتری ایجاد کنید، احتمالاً منتظر دریافت پیغام خطایی خواهید بود اما هیچ پیغامی دریافت نخواهید کرد. سیستم رمز عبور ۷ کاراکتری شما را برخلاف GPO که ایجاد نمودید (New Password Policy) می‌پذیرد. حتی اگر از دستور `gpupdate` در خط فرمان نیز استفاده کنید (این دستور جهت آپدیت سریع Policyها می‌باشد)، باز هم رمز عبور ۷ کاراکتری شما پذیرفته می‌شود. شاید بپرسید که علت این امر چیست؟ اگر بخاطر داشته باشید در قسمت‌های قبل گفتیم که GPOها به ترتیب از پایین به بالا در GUI اجرا می‌شوند. زمانی‌که شما GPO مورد نظر (New Password Policy) را ایجاد می‌کنید، این GPO در زیر Default Domain Policy قرار می‌گیرد. Default Domain Policy بطور پیش‌فرض همراه اکتیو دایرکتوری قرار دارد بنابراین تا زمانی که در بالای GPO شما قرار داشته باشد، سیاست‌های موجود در آن نسبت به سیاست‌های شما

اولویت خواهد داشت. راه حل این مشکل، انتقال GPOهای ایجاد شده بـه بـالای Default Domain Policy می‌باشد. پس از انجام این انتقال اگر بار دیگر اقـدام بـه ایجـاد یـک حسـاب کـاربری بـا رمـز عبـور ۷ کاراکتری نمایید پیغامی ظاهر شده و به شما اعلام می‌کند که رمز عبوری بـا حـداقل ۱۲ کـاراکتر وارد کنید.

نکته‌ای که در این زمینه نباید فراموش کنید اولویت GPOها در سطوح مختلف می‌باشـد. بـه عنـوان مثال فرض کنید که GPO بالا را ایجاد نموده‌اید تا به کاربران یک OU اعمال شوند. اما مشاهده می‌کنید که مشکلی در این روند وجود دارد. علت این است که این GPO به دامنـه پیونـد شـده اسـت و چنانچـه GPO دیگری به OU مورد نظر شما پیوند شده باشد، سیاست‌های GPO دامنه را نادیده می‌گیرد.

۸-۴ تنظیمات Group Policy

با استفاده از تنظیمات Group policy امکان انجام بسیاری از اقـدامات پیکربنـدی بـرای سیسـتم‌هـا وجود دارد. تعدادی از این اقدامات عبارتند از:

- **استقرار نرم افزار**: می‌توانید تمام فایل‌های مورد نیاز برای نصب یـک نـرم افـزار را بـا یکـدیگر بـه صورت یک بسته (Package) در آورده و سپس این بسته را در جایی از سرور قرار داده و نصـب کنید. سپس با استفاده از Group Policy، Desktop کاربران را به آن اشاره دهید. مشـاهده خواهیـد نمود با وجود اینکه این نرم افزار تنها برروی سـرور قـرار دارد و همانجـا نیـز نصـب شـده، امـا برروی Desktop تمام کاربران نیز موجود است. زمانی که کاربر برای اولین بار سـعی در اجـرای این برنامه می‌کند، نرم افزار بطور خودکار شروع به نصب شدن نموده بدون اینکـه کـاربر در آن دخالتی داشته باشد.
- **تنظیم حقوق کاربر**: احتمالاً می‌دانید که کلمه "Right" اشاره بـه حقـوق و یـا توانـایی کـاربر بـرای انجام عملکردهای خاص می‌باشد. این عملکردهـا شـامل Logon شـدن بـه صـورت Local و یـا از طریق سرویس‌های Terminal (در ویندوز NT4) و ماننـد اینهـا مـی‌باشـد. بـا اسـتفاده از GPOهـا می‌توان این حقوق را برای کابران و یا ماشین‌ها به راحتی تعریف نمـوده و دیگـر نگرانـی در ایـن زمینه وجود نخواهد داشت.
- **محدود کردن برنامه‌هایی که کاربر می‌تواند اجرا نماید**: با استفاده از GPOها مـی‌توانیـد برنامـه‌هـا و قابلیت‌هایی که یک کاربر می‌تواند به آنها دسترسی داشته باشد را مشخص کنید. به عنـوان مثـال برنامه‌هایی مانند Word، Outlook، Internet Explorer.
- **کنترل تنظیمات سیستم**: یک روش آسـان بـرای کنتـرل سـهمیه‌بنـدی فضـای دیسـک، اسـتفاده از GPOها است. بسیاری از سیستم‌های ویندوز به آسانی توسط تنظیمات Policyها کنترل می‌شـوند.

برای برخی از سیستم‌ها، استفاده از Policyها تنها روش کنترل تنظیمات سیستم است.

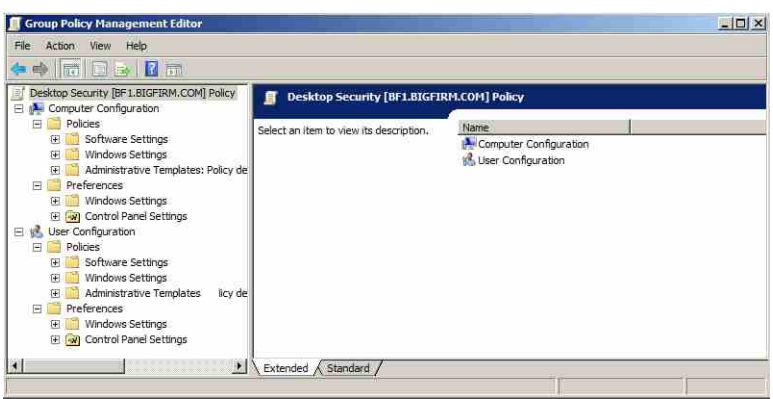
- **تنظیم اسکریپت‌های Logon، Logoff، Startup و Shutdown**: GPOها اجازه می‌دهند که همه این چهار رویداد به صورت اسکریپت ایجاد نموده و تعیین کنید که کدام اسکریپت اجرا گردد.
- **ساده سازی و محدود کردن برنامه‌ها**: با استفاده از GPOها امکان حذف بسیاری از ویژگی‌ها از برنامه‌هایی مثل Internet Explorer، Windows Explorer و سایر برنامه‌ها وجود دارد.
- **محدود کردن Desktop**: با استفاده از GPOها می‌توانید همه یا بخشی از آیتم‌های منوی Start کاربران را حذف نموده، مانع از اضافه کردن پرینتر توسط آنها شده، و یا به آنها اجازه خروج از سیستم و تغییر پیکربندی Desktop را ندهید.

اقدامات قابل انجام بسیاری توسط Policyها وجود دارد، اما در اینجا تنها مقدمه‌ای برای شروع کار آوردیم.

۸-۴-۱ تنظیمات Computer/User Configuration

ویندوز سرور 2008، سرور 2008R2، ویندوز ویستا SP1 و بعد از آن با یک نگاه کاملاً جدید نسبت به تنظیمات Computer/User Configuration در GPME آمده‌اند. مایکروسافت در این سیستم عامل‌ها بیش از ۳۰۰۰ تنظیم GPO معرفی نموده است که به منظور انجام بهتر تنظیمات توسط مدیران Group Policy است.

در شکل ۸-۲۳ دو گره اصلی در واسط GPME قابل مشاهده هستند: User Configuration و Computer Configuration. هر دوی این گره‌ها دارای زیرگره‌های Policies و Preferences می‌باشند. زیرگره policies خود به سه زیر گره Software Settings، Windows Settings و Administrative Templates شکسته می‌شود. زیرگره Preferences نیز به زیرگره‌های Control Panel و Windows Settings تقسیم می‌شود.



شکل ۸-۲۲

تفاوت میان این گره‌های اصلی در این است که تنظیمات User Configuration برروی حساب‌های کاربری و تنظیمات Computer Configuration برروی حساب‌های کامپیوتر اعمال می‌شوند. به عنوان مثال تنظیمات Registry را در نظر بگیرید. تنظیمات Registry برای Computer Configuration در کلیدی به نام HKEY_LOCAL_MACHINE و تنظیمات User Configuration در کلیدی به نام HKEY_ CURRENT_USER (HKCU) ذخیره می‌شوند. چنانچه دو GPO یکی در Computer Configuration و دیگری در User Configuration ایجاد نموده و تنظیمات یکسانی را در آن قرار دهید، تنظیمات Computer Configuration نسبت به تنظیمات User Configuration دارای اولویت خواهند بود.

بیشتر از ۵۰۰۰ تنظیم برای GPO در ویندوز سرور 2008 موجود است که در زمینه‌های مختلفی تدوین شده‌اند. در ادامه تعدادی از مفیدترین این سیاست‌ها را مورد بررسی قرار می‌دهیم.

مشخص کردن اسکریپت‌ها با استفاده از Group Policy

اسکریپت‌ها کدهایی هستند که در زمان Logon یا Logoff شدن کاربران و همچنین در زمان Startup یا Shutdown شدن سیستم اجرا می‌شوند. این اسکریپت‌ها می‌توانند به هر زبان ActiveX Scirpt مانند VBScript، MicrosoftJScript و یا در قالب فایل‌های Batch (*.bat یا *.cmd) می‌توانند مورد استفاده قرار گیرند. به عنوان مثال با استفاده از اسکریپ زیر که به زبان Visual Basic نوشته شده است می‌توانید یک پیغام در هنگام ورود کاربر به سرور ایجاد کنید:

```
MsgBox "Welcome to your server!", vbExclamation, "Logon Script"
```

برای استفاده از اسکریپت‌ها ابتدا باید آنها برروی سرور ایجاد شوند. بدین منظور می‌توانید مراحل زیر را دنبال کنید:

۱. کنسول GPMC را اجرا کنید.
۲. برروی یکی از GPOها کلیک‌راست نموده و Edit را انتخاب کنید تا پنجره GPME اجرا شود.
۳. به مسیر User Configuration\Policies\Windows Settings\Scripts(Logon/Logoff) بروید.
٤. در پنل سمت راست برروی Logon کلیک‌راست نموده و Properties را انتخاب کنید.
۵. در پنجره "Logon Properties" برروی Show Files کلیک کنید.
٦. کد زیر را در برنامه Notepad وارد نموده و آنرا با نام و پسوند LogonMsg.vbs ذخیره کنید:

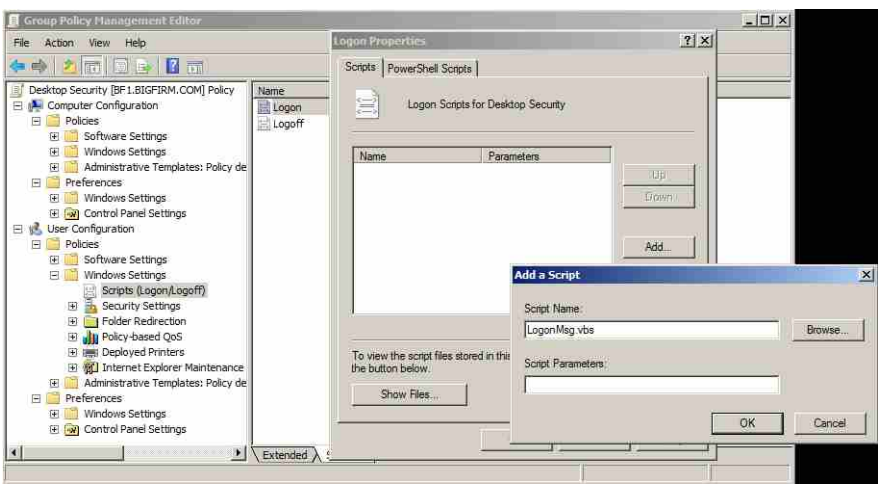
```
MsgBox "Welcome to your server!", vbExclamation, "Logon Script"
```

۷. فایل ذخیره شده را در محلی که با کلیک برروی Show Files باز می‌شود کپی نموده و پنجره را ببندید.

۸. اکنون برروی دکمه Add کلیک کنید.

۹. در پنجره "Add a Script" نام LogonMsg.vbs را وارد نموده و برروی Ok کلیک کنید. اکنون زمانی که کاربران به سیستم وارد می‌شوند، پیغام "Welcome to your server!" در یک پنجره پیغام به آنها نشان داده می‌شود.

۱۰. ایجاد اسکریپت‌ها برای Shutdown، Startup و Logoff نیز به همین صورت می‌باشد.



شکل ۸-۲۳

برای دسترسی به محل ذخیره سازی فایل‌های اسکریپت می‌توانید به مسیر زیر مراجعه کنید:

C:\Windows\SYSVOL\sysvol\Bigfirm.com\Policies\{GUID for example: 366FADC5-051F-4C97-965A-8E0F62958FB3}

در این مسیر دو پوشه با نام های Machine و User قابل مشاهده است که اسکریپت‌های Computer Configuration و User Configuration در آن ذخیره می‌شوند.

Folder Redirection

یکی از موارد پر اهمیت در تنظیمات User Configuration در Group policy، امکان تعیین مکانی مشخص در شبکه جهت قرارگیری پوشه‌هایی همچون AppData، Desktop، Start Menu، Documents، Favorites و سایر پوشه‌های پر اهمیت برای کاربر است. این پوشه‌ها از این نظر مورد اهمیت کاربران هستند که محیط عملکرد آنها به این پوشه‌ها وابسته می‌باشد. پوشه AppData محل نگهداری اطلاعات مرتبط با برنامه‌ها مانند Internet Explorer، Desktop محل نگهداری پوشه‌های مهم و میانبرهایی[1] است

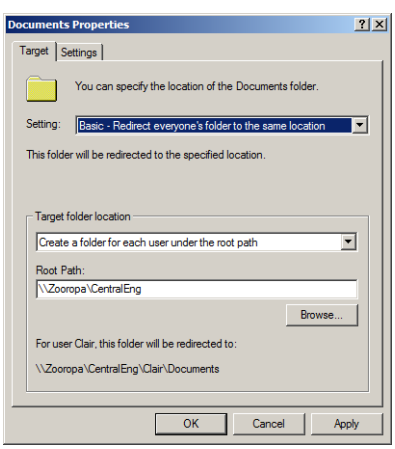
1. Shortcuts

که تنها با یک کلیک قابل دسترسی هستند، پوشه Start Menu شامل گروه‌هایی از برنامه‌ها و میانبرهای آنها است، My Documents محل پیش‌فرض ذخیره و بازیابی اطلاعات کاربران است و ... .

دلایل زیادی برای استفاده از Folder Redirection (تغییر مسیر پوشه‌ها) وجود دارد. یکی از این دلایل، راحتی کاربرانی است که از چندین کامپیوتر در شبکه استفاده می‌کنند. زمانی که این کاربران دارای مکان مشخصی در شبکه جهت نگهداری برنامه‌ها و اطلاعات خود باشند، بدون نیاز به داشتن برنامه‌ها برروی همه این ماشین‌ها می‌توانند به داده‌های خود دسترسی پیدا کنند.

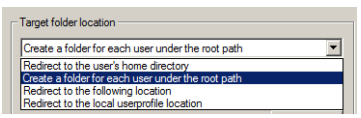
برای تنظیم مکانی از شبکه برای پوشه‌ها، به مسیر User Configuration\Policies\Windows Settings\Folder Redirection بروید. لیستی از پوشه‌های قابل انتقال نمایش داده می‌شود. برای تغییر مسیر هر یک می‌توانید برروی آن پوشه کلیک‌راست نموده و Properties را انتخاب کنید. سپس با تعیین مسیری جهت قرار گیری پوشه، مسیر آنرا برای کاربران در شبکه تغییر دهید. به عنوان مثال برای تغییر مسیر پوشه Documents در Group Policy، مراحل زیر را دنبال کنید:

۱. به مسیر User Configuration\Policies\Windows Settings\Folder Redirection\Documents رفته و برروی پوشه Documents کلیک‌راست کنید.
۲. پس از انتخاب گزینه Properties، مشاهده می‌کنید که این تنظیمات بطور پیش‌فرض برروی Not Configured قرار دارد. از داخل لیست Drop-Down، گزینه Basic را انتخاب کنید.
۳. فیلدهایی جهت تعیین محل قرار گیری پوشه و ریشه آن (سرور شبکه) ظاهر می‌شود. از لیست Target folder location گزینه Create a folder for each user و در قسمت Root patch آدرس سروری که پوشه در آن قرار می‌گیرد (در اینجا سروری با نام Zooropa) را وارد کنید.
٤. با استفاده از دکمه Browse می‌توانید هر مکان از سرور فعلی یا سروری در شبکه را جستجو نموده و انتخاب کنید.



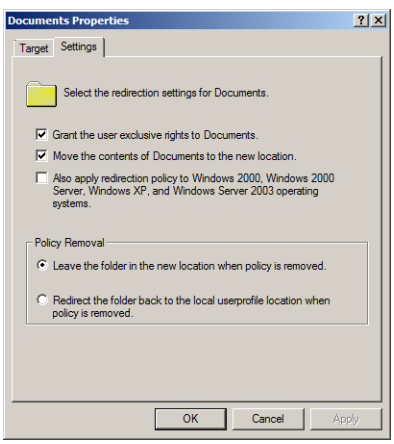
شکل ۸-۲۴

۵. دقت داشته باشید که در قسمت Target folder location گزینه‌های دیگری نیز وجود دارد. می‌توانید با توجه به مکانی که جهت تغییر مسیر در نظر گرفته‌اید، یکی از این گزینه ها را انتخاب کنید.



شکل ۸-۲۵

علاوه بر تب Target در این پنجره، تب دیگری نیز با نام Settings وجود دارد. در این تب تنظیماتی پیرامون انتقال فایل به مکان جدید وجود دارد. می‌توانید این تنظیمات را با فعال/غیر فعال کردن هر گزینه تغییر دهید.



شکل ۸-۲۶

Security Settings

Security Settings به همراه Administrative Templates بخش قابل توجهی از Group policy را تشکیل می‌دهند. تنظیمات پیش‌فرض در این دو گره به منظور راحتی کار در نظر گرفته شده‌اند. افزایش امنیت به معنی افزایش محدودیت‌ها بوده و دارای رابطه‌ای معکوس با راحتی می‌باشد. تنظیمات امنیتی در چند گروه دسته بندی شده و از مسیر Computer Configuration\Policies\Windows Settings\Security Settings قابل دسترسی می‌باشند. عمده‌ترین دسته از این تنظیمات عبارتند از:

- **Account Policies**: این سیاست‌ها محدودیت‌های رمزعبور، سیاست‌های قفل شدن سیستم و سیاست‌های Kerberos را مشخص می‌کنند.
- **Local Policies**: این سیاست‌ها مربوط به حقوق کاربران و حسابرسی آنها می‌باشد.

- **Event Log**: متمرکز نمودن پیکربندی‌ها برای ثبت وقایع سیستم.
- **Restricted Groups**: وادار نمودن و کنترل کردن کاربران گروه‌ها برای گروه‌های خاصی مانند Administrators group.
- **System Services**: استانداردسازی پیکربندی سیستم و جلوگیری از ایجاد تغییر در آن.
- **Registry**: ایجاد قالب‌های امنیتی برای Keyهای رجیستری به منظور کنترل Keyهایی که می‌توانند تغییر کنند و همچنین کنترل دسترسی به بخش‌های رجیستری.
- **File System**: ایجاد قالب‌های امنیتی برای مجوزهای فایل‌ها و پوشه‌ها به منظور اطمینان از اینکه فایل‌ها و مسیرها دارای مجوزهای مورد نظر می‌باشند.
- **Public Key Policies**: مدیریت تنظیمات برای سازمان‌ها با استفاده از زیرساخت‌های کلید عمومی[1]
- **Software Restrictions Policies**: قرار دادن محدودیت برای اجرای برنامه‌ها برروی سیستم. این یکی از ویژگی‌های جدید است که مانع از اجرای ویروس‌ها و نرم افزارهای مخرب برروی سیستم می‌شود.

کار با Templateها

Templateها قالب‌های امنیتی هستند که توسط مدیران ایجاد شده و می‌توان تنظیمات دلخواه را برای همیشه در آن جای داد. برای آشنایی با طرز کار Templateها اجازه دهید مثالی ارائه دهیم. قصد داریم Template ای برای انجام سه اقدام زیر ایجاد کنیم:

- حصول اطمینان از اینکه فردی در گروه محلی Power users قرار ندارد.
- تنظیم مجوز NTFS برای مسیر C:\SECRET که تنها توسط گروه محلی Administrators قابل دسترسی است.
- خاموش کردن سرویس IIS[2] که به نظر می‌رسد برروی هر سیستم عامل مایکروسافت خود را نصب نموده و برای Web server ایجاد مزاحمت می‌کند.

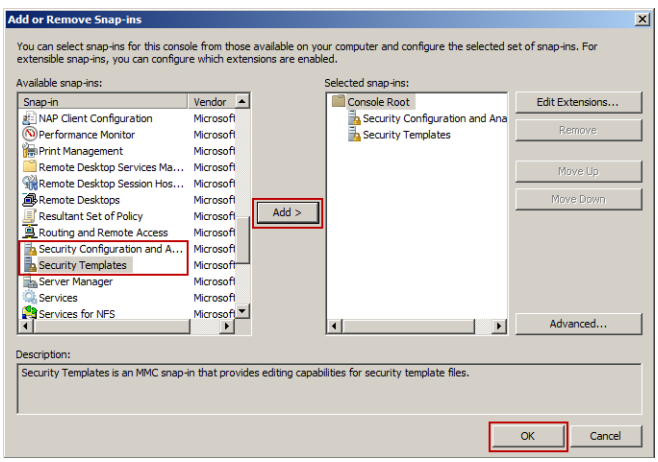
در ابتدا به تعدادی ابزار نیازمندید. یکی از این ابزارها کنسول MMC[3] می‌باشد. در این کنسول به دو Snap-in با نام‌های Security Templates و Security Configuration and Analysis نیاز است. این ابزار را به صورت زیر راه اندازی نمایید:

۱. در قسمت Search از منوی Start، عبارت mmc /a را وارد نموده و Enter را فشار دهید تا کنسول MMC اجرا گردد.

1. Public Key infrastuctures
2. Internet Information Service
3. Microsoft Management Console

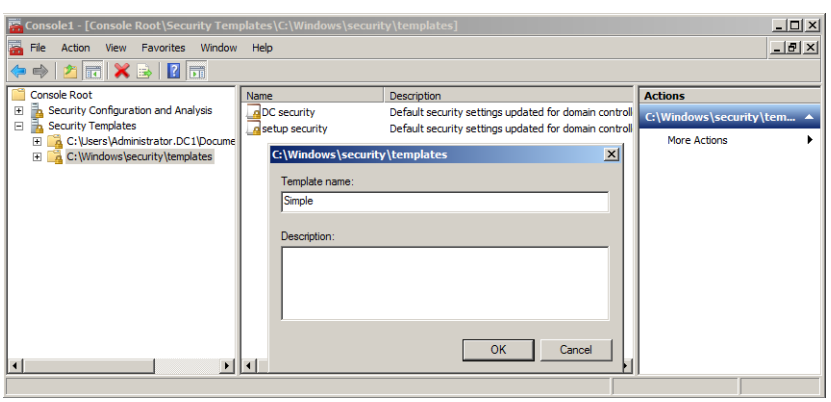
۲. از منوی File گزینه Add/Remove Snap-in را انتخاب کنید.

۳. در صفحه "Add or Remove Snap-ins" گزینه‌های Security Configuration and Analysis و Security Templates را انتخاب نموده و برروی Add کلیک کنید تا به فهرست Selected snap-ins اضافه شوند. در نهایت برروی Ok کلیک کنید.



شکل ۸-۲۷

٤. اکنون به منظور اضافه کردن یک مسیر برای Template (در کنسول MMC) برروی گره Security Templates کلیک‌راست نموده و گزینه New Template Search Path را انتخاب کنید. مسیری که باید اضافه شود به صورت C:\Windows\Security\Templates خواهد بود. این مسیر شامل Template از پیش ساخته‌ای به نام DC Security می‌باشد، اما در اینجا قصد داریم یک Template را از ابتدا ایجاد کنیم بنابراین برروی مسیری که اضافه نمودید کلیک‌راست نموده و New Template را انتخاب کنید. سپس نام آنرا (در اینجا Simple) را وارد نمایید.



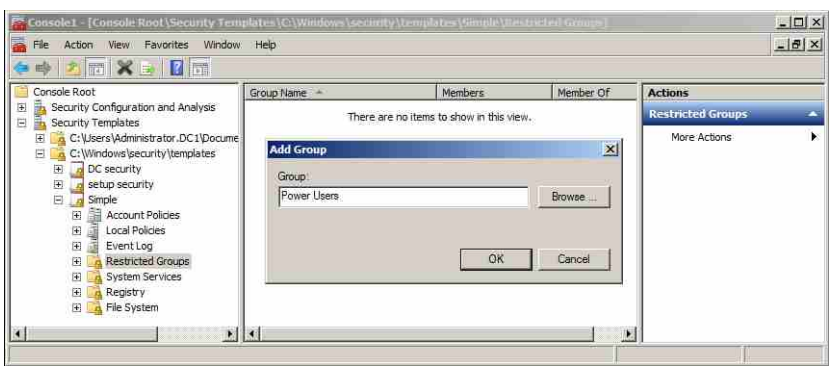
شکل ۸-۲۸

هر Security Templates شامل تعدادی زیرمجموعه است که عبارتند از:

- Account Policies: برای تنظیم Passwordها، قفل کردن حساب‌ها و سیاست‌های Kerberos استفاده می‌شود.
- Local Policies: جهت کنترل تنظیمات حسابرسی، حقوق کاربر و تنظیمات امنیتی می‌باشد.
- Event Log settings: پارامترهای مربوط به نحوه ذخیره‌سازی وقایع سیستم را ذخیره می‌نماید.
- Restricted Groups: اعضای وارد شده و خارج شده از یک گروه Local را کنترل می‌نماید.
- System Services: روشن و خاموش کردن سرویس‌ها و کنترل افرادی که مجوز انجام این کار را دارند.
- Registry security: تنظیم و کنترل مجوزها برای مشاهده و تغییر Keyهای رجیستری.
- File System: کنترل مجوزهای NTFS برای فایل‌ها و پوشه‌ها.

اکنون به سراغ **گروه Power Users** (اقدام اول) رفته و آنرا تشریح می‌کنیم:

۱. Simple (Template ایجاد شده) را باز کنید.
۲. از زیرگره‌های آن برروی Restricted Groups کلیک‌راست نموده Add Group را انتخاب کنید.
۳. نام Power Users را وارد نموده و یا با استفاده از دکمه Browse آنرا جستجو کنید (به شرطی که از قبل این گروه را ایجاد کرده باشید).

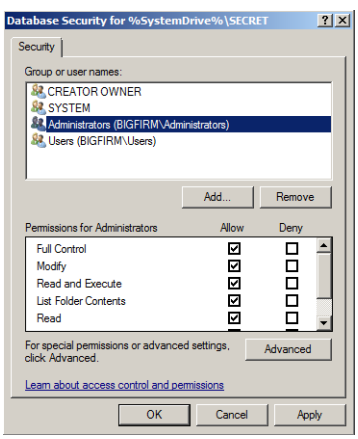


شکل ۸-۲۹

بطور پیش‌فرض، اگر گروهی در Security Template قرار گیرد اعضای آن از گروه حذف می‌شوند. بنابراین چنانچه با پنجره‌ای تحت این موضوع مواجه شدید، برروی Ok کلیک کنید. چنانچه تمایل دارید افرادی را در این گروه قرار دهید می‌توانید برروی گروه کلیک‌راست نموده و با ورود به بخش Properties، افراد مورد نظر را به آن اضافه کنید.

اکنون قصد داریم **برای مسیر C:\SECRET مجوز NTFS تنظیم نموده** (اقدام دوم) بطوری که تنها توسط گروه محلی Administrators قابل دسترسی باشد. برای انجام این کار مراحل زیر را دنبال کنید:

۱. به پنل سمت چپ باز گردید. برروی File System کلیک‌راست نموده و Add Files را انتخاب کنید.
۲. در پنجره "Add a File or Folder" مسیر مورد نظر (C:\SECRET) را وارد نموده و یا با استفاده از دکمه Browse آنرا تعیین کنید.
۳. پس از کلیک برروی Ok، پنجره مجوز NTFS ظاهر می‌شود. مجوزهای داده شده به تمام گروه‌ها و کاربران را به غیر از گروه Administrators حذف نموده و مجوز Full Control را برای گروه Administrators فعال کنید.



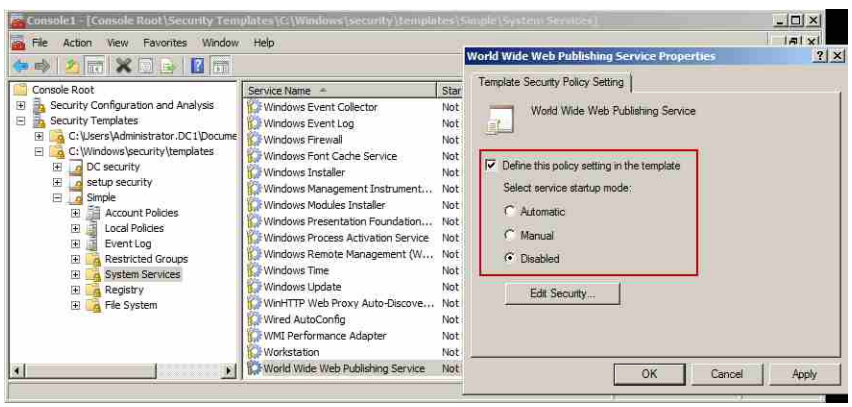
شکل ۸-۳۰

٤. پنجره "Add Object" ظاهر شده و از شما می‌پرسد که این مجوز تنها برروی همین پوشه اعمال شود یا زیر پوشه‌های آنرا نیز شامل شود. با توجه به نظر خود آنرا تنظیم نموده و برروی Ok کلیک کنید.

شکل ۸-۳۱

سرانجام نوبت به **خاموش نمودن IIS** (اقدام سوم) می‌رسد.

۱. برروی System Services کلیک کنید.
۲. در پنل سمت راست برروی World Wide Web Publishing Services کلیک‌راست نموده و Properties را انتخاب کنید.
۳. گزینه Define This Policy Setting in the Template را فعال نموده و Disabled را انتخاب کنید.
٤. برروی Ok کلیک کنید.



شکل ۸-۳۲

اکنون می‌توانید Template ایجاد شده را ذخیره کنید. برای انجام این کار برروی Simple کلیک راست نموده و Save را انتخاب کنید. اکنون شما یک فایل با نام Simple.inf در مسیر \Windows\Security\Templates در اختیار دارید.

ایجاد یک Security Database

پس از ایجاد Template، برای اینکه ببینید چگونه این Template سیستم را مورد تغییر قرار می‌دهد و یا برای آگاهی از اینکه چگونه تنظیمات آن با استفاده از Snap-in های MMC اعمال می‌شوند، باید یک Security Database ایجاد کنید. در واقع باید Template را از فرم ASCII به فرم Binary که Database نامیده می‌شود کامپایل (ترجمه) کنید. این کار با استفاده از Snap-in اول یعنی Security Configuration and Analysis قابل انجام است.

۱. در کنسول MMC برروی Security Configuration and Analysis کلیک‌راست نموده و Open Database را انتخاب کنید.
۲. در پنجره "Open Database" باید یک Database جدید ایجاد کنید اما آپشنی برای این کار وجود

ندارد. بنابراین می‌توانید در قسمت File name نام Database جدید را وارد کنید. در این مثال نام Simple را وارد نموده و Enter را فشار دهید.

۳. در پنجره باز شده از شما خواسته می‌شود که فایلی با پسوند inf. را باز کنید. می‌توانید از مسیر C:\Windows\Security\Templates فایل Simple.inf را انتخاب نموده و برروی Open کلیک کنید.

٤. برروی Security Configuration and Analysis کلیک‌راست کنید. دو گزینه قابل مشاهده است: Analyze Computer Now و Configure Computer Now. Analyze در کامپیوتر تغییری ایجاد نمی‌کند و فقط نشان می‌دهد که سیستم شما چگونه تغییر خواهد کرد. با اجرای این گزینه یک فایل log در مسیر \Documents\Security\Logs\ ایجاد می‌شود.

٥. گزینه Analyze Computer Now را انتخاب نموده تا سیستم شما با تنظیمات Database سنجیده شود. چنانچه تصمیم به اعمال این تنظیمات گرفتید، گزینه Configure Computer Now را انتخاب نموده (از منوی کلیک‌راست) تا تغییرات برروی سیستم شما اعمال گردد.

این عمل عالی به نظر می‌رسد. اما اگر بخواهید آنرا برروی ده‌ها کامپیوتر اعمال کنید چطور؟ راه حل ساده است. می‌توانید با استفاده از ابزاری به نام `secedit.exe` در خط فرمان ابتدا Template را به یک Database تبدیل نموده و سپس Database را اعمال کنید. برای خواندن یک Template، اعمال نمودن آن و سپس ایجاد Database از قالب دستوری زیر استفاده کنید:

```
Secedit /configure /cfg templatefilename /db databasefilename/
overwrite /log logfilename
```

برای اعمال این دستور برروی ایستگاه‌های کاری مختلف می‌توانید آنرا با استفاده از Logon Scripts یا فایل های Batch تعریف نموده تا در هر بار ورود به سیستم مجدداً اعمال گردد.

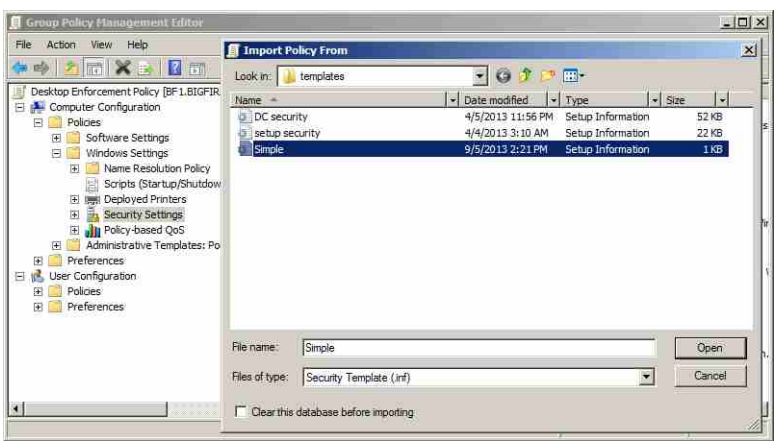
استفاده از Group policyهای مبتنی بر دامنه برای اعمال Templateها

اگرچه استفاده از Logon Scriptها برای اعمال Templateها مناسب است اما باید توجه داشته باشید که این اسکریپت‌ها تنها در زمان وارد شدن کاربر قادر به اجرا هستند و در بقیه موارد نمی‌توان آنها را اجرا نمود. برای حل این مشکل می‌توان از GPOهای مبتنی بر دامنه استفاده نمود. GPOهای مبتنی بر دامنه در طول روز قابل اعمال هستند و کنترل کردن آنها نیز نسبت به فایل‌های Batch ساده‌تر است.

Import کردن Security Templates

Template ایجاد شده در قسمت قبل (Simple.inf) را در نظر بگیرید. قصد داریم آنرا با استفاده از GPO برروی سیستم مستقر کنیم. مراحل زیر را برای Import کردن Templateها دنبال کنید:

۱. کنسول GPMC را اجرا کنید.
۲. OUای که شامل کامپیوترهای مورد نظر جهت اعمال تنظیمات امنیتی است را انتخاب کنید (به عنوان مثال Desktop).
۳. برروی OU کلیک‌راست نموده و گزینه Create a GPO in this domain, and Link it here را انتخاب کنید.
٤. نام GPO را وارد نمایید. در اینجا ما از نام Desktop Enforcement Policy استفاده کرده‌ایم.
٥. برروی GPO ایجاد شده کلیک‌راست نموده و Edit را انتخاب کنید.
٦. در پنجره GPME به مسیر Computer Configuration\Policies\Windows Settings رفته و گره Security Settings را انتخاب کنید.
۷. برروی Security Settings کلیک‌راست نموده و گزینه Import Policy را انتخاب کنید.
۸. Template مورد نظر (Simple.inf) را انتخاب نموده و برروی Open کلیک کنید.



شکل ۸-۳۳

۹. به گره Security Settings و سپس Restricted Groups بروید و مطمئن شوید که سیاست Power Users در آن قرار دارد.

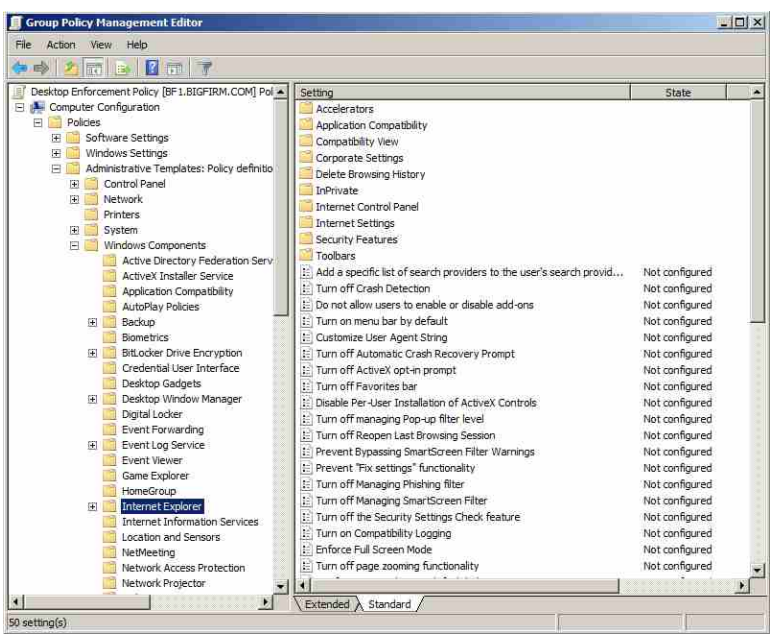
شاید این سؤال برایتان پیش آمده باشد که در حال حاضر باید چه اقدامی انجام دهید؟ پاسخ انتظار به مدت ۹۰ دقیقه است. نیاز به انجام کار خاصی نیست فقط اجازه دهید تا سیاست‌ها Refresh شده و تنظیمات شما برروی تمام کاربران موجود در Desktop OU اعمال شوند (البته فراموش نشود که با استفاده از دستور `gpupdate` می‌توانید عملیات Refresh شدن را در هر زمان انجام دهید).

(ADMX /ADML) Administrative Templates

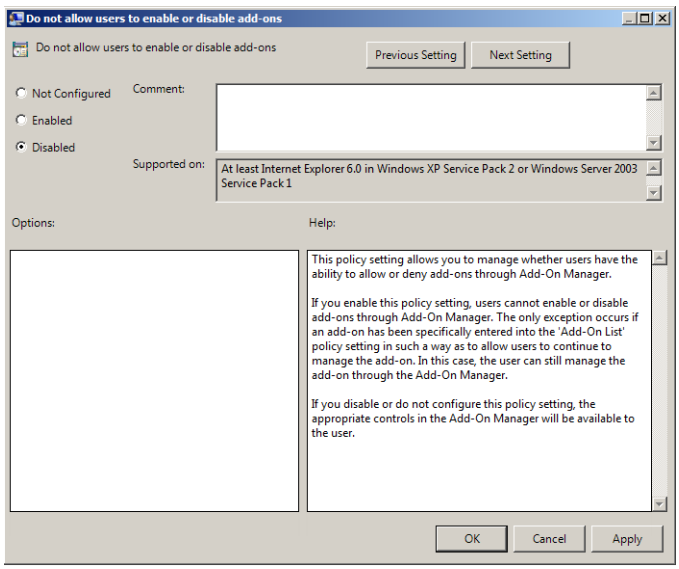
Administrative Templates تنظیماتی هستند که بسیاری از جنبه‌های محیط عملکرد کاربر و پیکربندی ماشین‌ها را مشخص می‌کنند. از معروف‌ترین این تنظیمات می‌توان محدود کردن Desktop کاربران برای اجرای محدوده‌ای از برنامه ها می‌باشد. این تنظیمات برای کاربران در مسیر HKEY_CURRENT_USER\Software\Policies و برای ماشین‌ها در مسیر HKEY_LOCAL_MACHINE\Software\Policies نوشته می‌شوند. در ادامه تعدادی از عملکردهای این Templateها را ارائه می‌دهیم.

محدودکردن Internet Explorer

به نظر می‌رسد برای هر امکان در Internet Explorer یک Policy به منظور غیر فعال کردن آن امکان در نظر گرفته شده است. برای دسترسی به این Policyها می‌توانید به مسیر Computer Configuration/Policies/Administrative Templates/ Windows Components/Internet Explorer مراجعه نموده و سپس از میان Policyهای موجود، آنهایی را که در نظر دارید انتخاب نموده و با کلیک‌راست برروی آن و انتخاب گزینه Edit، امکان استفاده از آنرا توسط کاربران فعال/غیر فعال کنید. در شکل ۸-۳۵ Policyهای مربوط به Internet Explorer و در شکل ۸-۳۶ نمونه‌ای از این Policyها که غیر فعال شده نشان داده شده است.



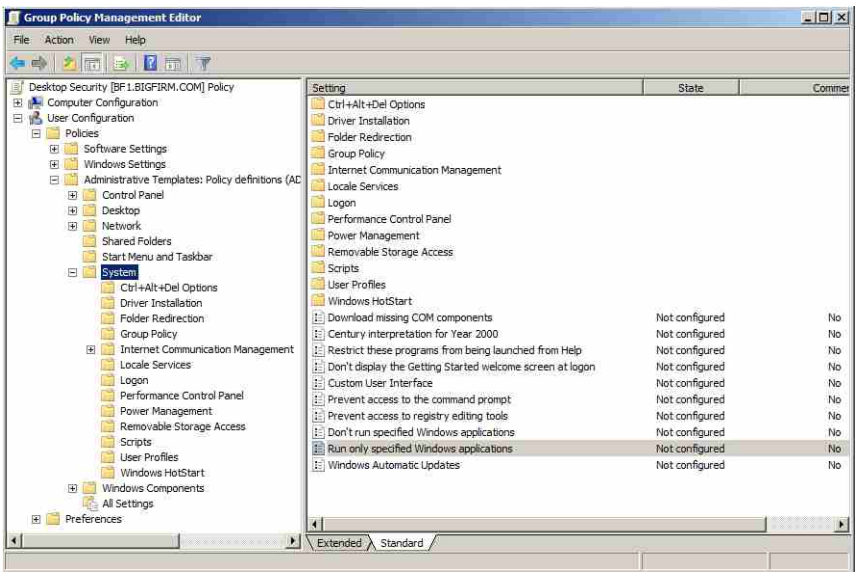
شکل ۸-۳۴



شکل ۸-۳۵

ممنوعیت کاربران از نصب و اجرای نرم افزارهای غیر مجاز

برای جلوگیری از انجام نصب نرم افزارها توسط کاربران باید Policy به نام "Prevent Removable Media Source for Any Install" که در مسیر User Configuration/.../ Windows Components/Windows Installer قرار دارد را فعال کنید. با فعال‌سازی این Policy کاربران قادر نخواهند بود با استفاده از رسانه‌هایی مانند CD-ROM یا Floppyها فرایند نصب نرم افزارها را راه‌اندازی کنند. همچنین باید Policy دیگری به نام "Add a Program from CD-ROM or floppy disk" را نیز در مسیر User Configuration/.../Control Panel/Add or Remove Programs فعال کنید. در گره Control Panel تعدادی از آپشن‌ها به منظور غیرفعال کردن و یا حذف قسمت‌هایی از اَپلت‌های Add/Remove Programs در نظر گرفته شده است. دقت داشته باشید که تنها استفاده از این سیاست‌ها جهت جلوگیری از نصب برنامه‌ها توسط کاربران کافی نیست زیرا امکان انجام آن با استفاده از خط فرمان نیز امکان‌پذیر است. بنابراین دسترسی به Command Line نیز باید غیر فعال گردد. این کار با فعال نمودن سیاست "Prevent access to the command prompt" امکان‌پذیر می‌باشد. البته توجه داشته باشید که Policy دیگری برای اجرای برنامه‌ها وجود دارد که نام آن "Run only specified windows application" می‌باشد. در هنگام استفاده از این Policy باید مراقب باشید زیرا فعال‌سازی آن باعث اجرای تنها برنامه‌های مشخصی خواهد شد. می‌توانید لیست این برنامه‌های قابل اجرا را در این سیاست مشخص کنید. در شکل ۸-۳٦ محل قرارگیری این Policyها نشان داده شده است.



شکل ۸-۳۶

به عنوان آخرین نکته در رابطه با اجرای برنامه‌ها اشاره می‌کنیم که کاربران می‌توانند برنامه‌ها را از طریق Task Manager نیز اجرا کنند، بنابراین لازم است که سیاست Ctrl+Alt+Delete را نیز غیرفعال نمایید.

استفاده از Group Policy به منظور تنظیم سیاست Password و Account Lockout

شاید یکی از مهمترین کاربردهای Group policy، استفاده از آن به منظور تعیین سیاست‌های رمز عبور برای کاربران می‌باشد. به همین دلیل در این قسمت سیاست‌های مرتبط با رمز عبور را مورد بررسی قرار می‌دهیم. قبل از شروع کار لازم است بار دیگر محل قرارگیری این سیاست‌ها را یاد آور شویم. سیاست‌های مرتبط با رمز عبور و حساب‌های کاربران در مسیر Computer Configuration/ Policies/Windows Settings/Security Settings قرار دارند. اکنون به بررسی هریک از آپشن‌های موجود در این مسیر می‌پردازیم.

سیاست‌های Password

این سیاست‌ها مرتبط با رمز عبور کاربران هستند:

- **Enforce password history**: فعال‌سازی این گزینه، تعداد دفعاتی را که باید رمزهای عبور متمایز برای یک حساب کاربری وارد شده تا بتوان مجدداً یک رمز عبور را مورد استفاده قرار داد مشخص می‌نماید.

- **Maximum password age:** حداکثر مدت زمانی را که یک رمز عبور قبل از اینکه کاربر بتواند آنرا تغییر دهد مشخص می‌نماید.
- **Minimum password age:** مدت زمانی است که یک رمز عبور باید استفاده شود تا کاربر بتواند آنرا مجدداً تغییر دهد.
- **Minimum password length**: حداقل تعداد کاراکترهای استفاده شده در رمز عبور را مشخص می‌نماید. تعداد ۷ یا ۸ کاراکتر برای این آپشن مناسب می‌باشد. تنظیم این گزینه مانع از انتخاب رمز عبور خالی می‌شود.
- **Passwords must meet complexity requirements:** این آپشن تعیین می‌کند که رمز عبور باید دارای پیچیدگی باشد. پیچیدگی رمز عبور شامل سه مورد می‌باشد:
  - حداقل دارای ٦ کاراکتر باشد.
  - نباید شامل نام کاربری یا قسمتی از آن باشد.
  - باید شامل سه دسته از ٦ نوع کاراکتر روبرو باشد: حروف بزرگ (A-Z)، حروف کوچک (a-z)، اعداد (0-9)، کاراکترهای ویژه (@، %، &، #)
- **Store passwords using reversible encryption:** این آپشن باعث می‌شود که اکتیو دایرکتوری رمز عبور را با استفاده از روش رمزگذاری بازگشتی ذخیره نماید. فعال‌سازی این گزینه برای دسترسی‌های Remote و سرویس‌های Internet Authentication Services مناسب است.

سیاست‌های Account Lockout

سیاست‌های مرتبط با قفل شدن حساب کاربری به دلیل وارد نمودن تعداد مشخصی از رمزهای عبور نادرست در این قسمت قرار دارند:

- **Account lockout duration**: مدت زمانی است که کاربر پس از قفل شدن یک حساب کاربری باید منتظر مانده تا بتواند مجدداً رمز عبور خود را وارد کند. اگر این آپشن فعال شود ولی فیلد minutes با صفر تنظیم گردد، حساب کاربری باید توسط مدیر از حالت Lokout خارج گردد. بنابراین منتظر ماندن برای مدت مشخص بی‌فایده خواهد بود.
- **Account lockout threshold**: این آپشن تعداد دفعات مجاز تا لحظه وارد نمودن رمز عبور صحیح جهت ورود به سیستم را قبل از قفل شدن آن مشخص می‌نماید. چنانچه این گزینه با صفر تنظیم گردد حساب کاربری هرگز قفل نخواهد شد.
- **Reset account lockout counter after**: این گزینه تعیین می‌کند که قبل از آخرین تلاش برای وارد نمودن رمز عبور صحیح (در صورتی که رمزهای وارد شده در دفعات قبلی اشتباه باشند) چه

مدت باید منتظر مانده تا شمارنده مجدداً به صفر بازگردد. به عنوان مثال اگر Reset account lockout counter را برروی ۲ دقیقه و Account lockout threshold را برروی ۳ بار تنظیم نموده باشید، اگر دوبار رمز عبور را اشتباه وارد کنید، باید دو دقیقه منتظر مانده تا بتوانید مجدداً از سه فرصت خود استفاده کنید.

۸-۴-۲ Group Policy Preferences

Group Policy Preferences (GPP) یکی از جنبه‌های تاثیرگذار در ویندوز سرور 2008 است که بیش از ۳۰۰۰ تنظیم Policy به GPOها اضافه می‌نماید. در ادامه با این تنظیمات بیشتر آشنا خواهید شد.

تنظیمات GPP

تنظیمات GPP کمی متفات‌تر از سایر تنظیمات Group Plicy هستند. در درجه اول به این دلیل که آنها در هر دو محیط Computer Configuration و User Configuration از GPO قرار دارند. این امکان قدرت و انعطاف‌پذیری بیشتری به منظور انجام تنظیمات برروی Desktopها و کاربران در اختیار شما قرار می‌دهد. در جدول ۸-۱ لیستی از تنظیمات GPP آورده شده است.

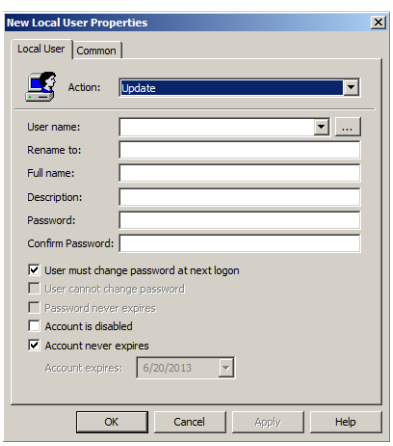
جدول ۸-۱ تنظیمات GPP

تنظیمات	قابل دسترسی در	
Group Policy Preferences	**Computer Configuration**	**User Configuration**
Applications	No	Yes
Drive Maps	No	Yes
Environment	Yes	Yes
Files	Yes	Yes
Folders	Yes	Yes
Ini Files	Yes	Yes
Network Shares	Yes	No
Registry	Yes	Yes
Shortcuts	Yes	Yes
Data Sources	Yes	Yes
Devices	Yes	Yes
Folder Options	Yes	Yes
Internet Settings	No	Yes
Local Users and Groups	Yes	Yes
Network Options	Yes	Yes
Power Options	Yes	Yes

Yes	Yes	Printers
Yes	No	Regional Options
Yes	Yes	Scheduled Tasks
No	Yes	Services
Yes	No	Start Menu

بیشتر تنظیمات موجود در جدول ۸-۱ واضح بوده و نیاز به توضیح ندارند. با این وجود نحوه کار با تعدادی از این تنظیمات را که ممکن است مورد استفاده قرار گیرند شرح می‌دهیم.

همواره امنیت یکی از مسائل مهم در ذهن مدیران IT بوده است اما همیشه زمان کافی برای اعمال آن وجود ندارد. به عنوان مثال بازنشانی رمز عبور برای مدیر Local (Local Administrator) در هر کامپیوتر رومیزی سازمان را در نظر بگیرید. آخرین باری که این رمز عبورها را تغییر داده‌اید چه زمانی بوده است؟ زمان نصب؟ دو سال پیش؟ شاید هر کدام از شما پاسخ‌هایی در این زمینه داشته باشید، اما استفاده از GPP شما را قادر می‌سازد تا این کار را هر زمان که تمایل داشته باشید انجام دهید. برای انجام این کار لازم است یک GPO ایجاد نموده و آنرا به یک OU که شامل تمام کامپیوترهای رومیزی سازمان شما می‌باشد پیوند دهید. زمانی که GPME را برای این GPO اجرا می‌کنید، به مسیر Computer Configuration\Preferences\Control Panel\Local Users and Groups رفته و برروی گره Local Users and Groups کلیک‌راست کنید. گزینه New » Local User را انتخاب نموده تا پنجره "New Local User Properties" اجرا گردد.



شکل ۸-۳۷

در قسمت User name، نام کاربری که قصد کنترل کردن آنرا دارید (در اینجا Administrator) وارد

کنید. سپس در فیلدهای Password و Confirm Password نیز رمز عبور جدیدی جهت بازنشانی وارد نمایید. اکنون رمز عبور کاربر Administrator در هر کامپیوتر که به دامنه و شبکه متصل است پس از مدت ۲ ساعت بازنشانی خواهد شد.

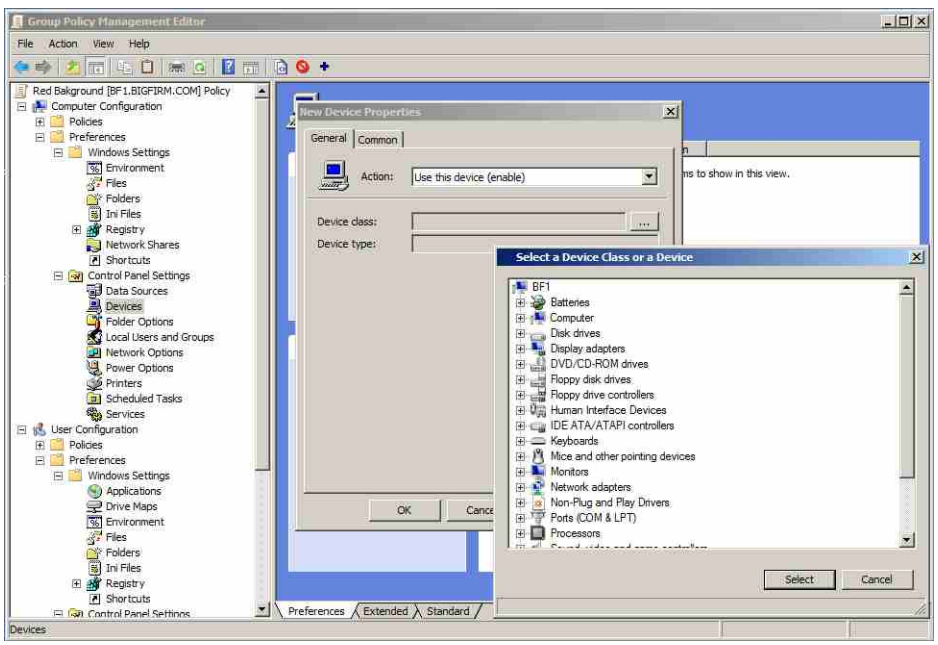
مشاهده نمودید که استفاده از GPPها بسیار ساده است. برای درک چگونگی عملکرد سایر GPPها، اعمالی که توسط آنها قابل انجام است را شرح می‌دهیم:

- **Applications**: انجام اقداماتی مانند فعال‌سازی غلط یاب املایی (spell checker) برای Microsoft Word، پیکربندی قابلیت بایگانی خودکار برنامه Outlook، پیکربندی امضاء "company-approved and consistent" برای ایمیل‌های Outlook.
- **Drive maps**: جایگزینی تمام نگاشت‌های درایو تعریف شده در logon script با تنظیمات Group Policy preferences
- **Environment**: ایجاد متغیرهای محیطی جهت استفاده با سایر تنظیمات Group Policy preferences (به عنوان مثال تعریف فضای مشخصی از RAM یا سرعت مشخصی از CPU به منظور استفاده یک برنامه)
- **Files**: استقرار فایل‌های پیکربندی برنامه‌ها روی کامپیوترهای رومیزی.
- **Folders**: ایجاد پوشه‌ها به منظور استفاده سایر برنامه‌های کاربردی، و یا حذف محتویات از پوشه‌ها و ... .
- **Network shares**: کنترل اشتراک گذاری‌های شبکه برروی سرور.
- **Registry**: ایجاد و کنترل تنظیمات مربوط به Registry.
- **Data sources**: ایجاد یک منبع داده متمرکز برای کارمندان و فروشندگان.
- **Devices**: افزودن دستگاه‌های سخت افزاری و فعال/غیرفعال نمودن دستگاه‌های موجود.
- **Folder options**: پیکربندی تنظیمات فایل‌ها برروی Windows Explorer و Desktop توسط مدیران و کاربران.
- **Internet settings**: پیکربندی تنظیمات مرتبط با اینترنت و برنامه Internet Explorer.
- **Local users and groups**: مدیریت کاربران و گروه‌ها برروی سرور و کامپیوترها
- **Power options**: کنترل و مدیریت تنظیمات مرتبط با منبع برق کامپیوترها (مانند حالت Standby و ...).
- **Printers**: انجام تنظیمات مرتبط با افزودن و یا مدیریت پرینترها (Local و تحت شبکه).
- **Scheduled tasks**: ایجاد برنامه‌های زمانبندی شده به منظور انجام اقداماتی مشخص (مانند اجرای

برنامه‌ها و ...).

- **Services**: پیکربندی و مدیریت سرویس‌ها به منظور افزایش امنیت و ... .
- **Start Menu**: مدیریت منوی Start و افزودن/حذف کردن آیتم‌های موجود در آن.

در شکل ۸-۳۹ نحوه استفاده از آپشن Devices (پس از کلیک‌راست برروی Devices و انتخاب New » Device) نشان داده شده است.



شکل ۸-۳۸