Lesson 20: Configuring Group Policy Settings

MOAC 70-411: Administering Windows Server 2012

Microsoft®
Official Academic Course

WILEY

Overview

- Exam Objective 6.2: Configure Group Policy Settings
- Configuring Group Policy Settings

Configuring Group Policy Settings

Lesson 20: Configuring Group Policy Settings

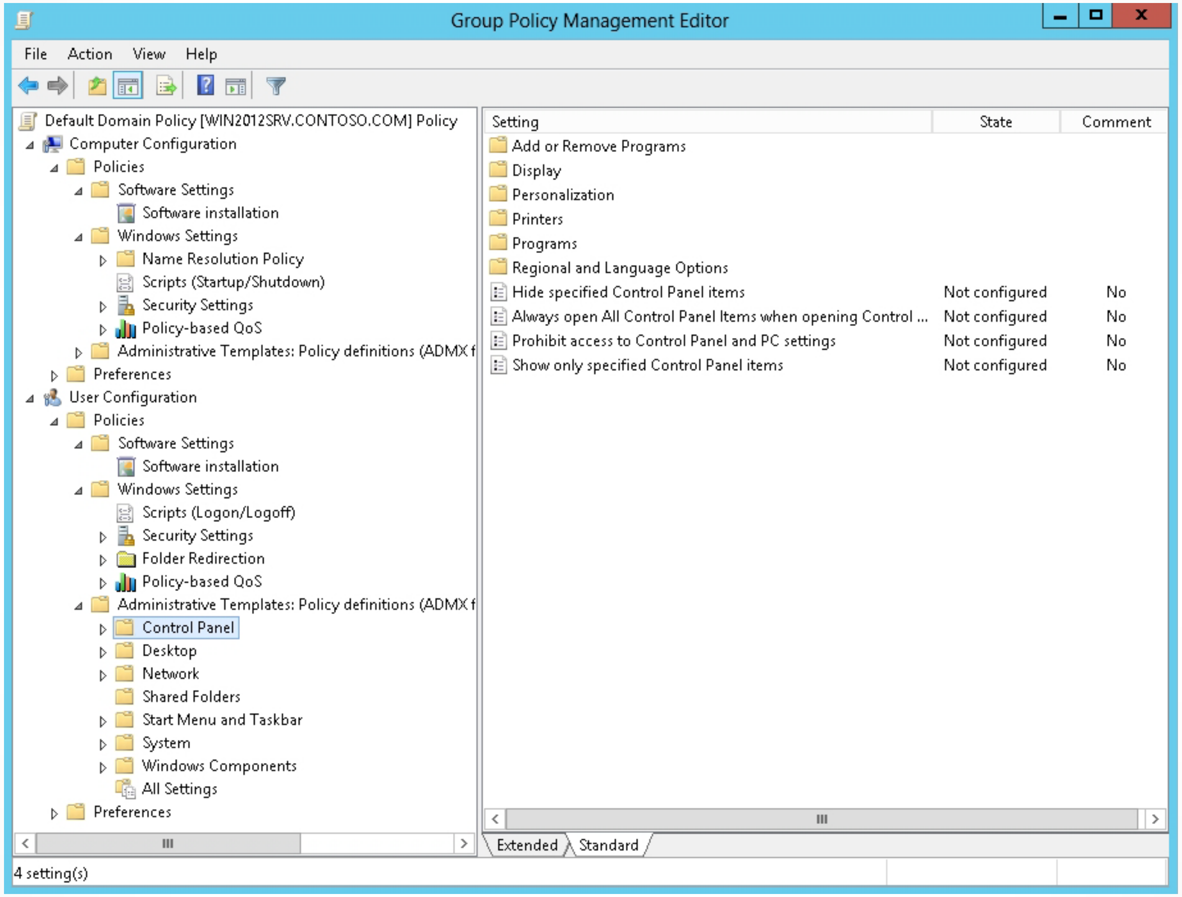
Group Policy Settings

- The ***Computer Configuration*** node contains settings that are applied to the computer regardless of who logs on to the computer. By default, computer settings are applied when the computer is started.
- The ***User Configuration*** node contains settings that are applied when the user logs on.

Group Policy Settings

- Group policy settings are refreshed every 90 minutes with a random delay of 30 minutes (giving a random range between 90 minutes and 120 minutes).
- On domain controllers, group policies get refreshed every 5 minutes.

GPO Node Structure



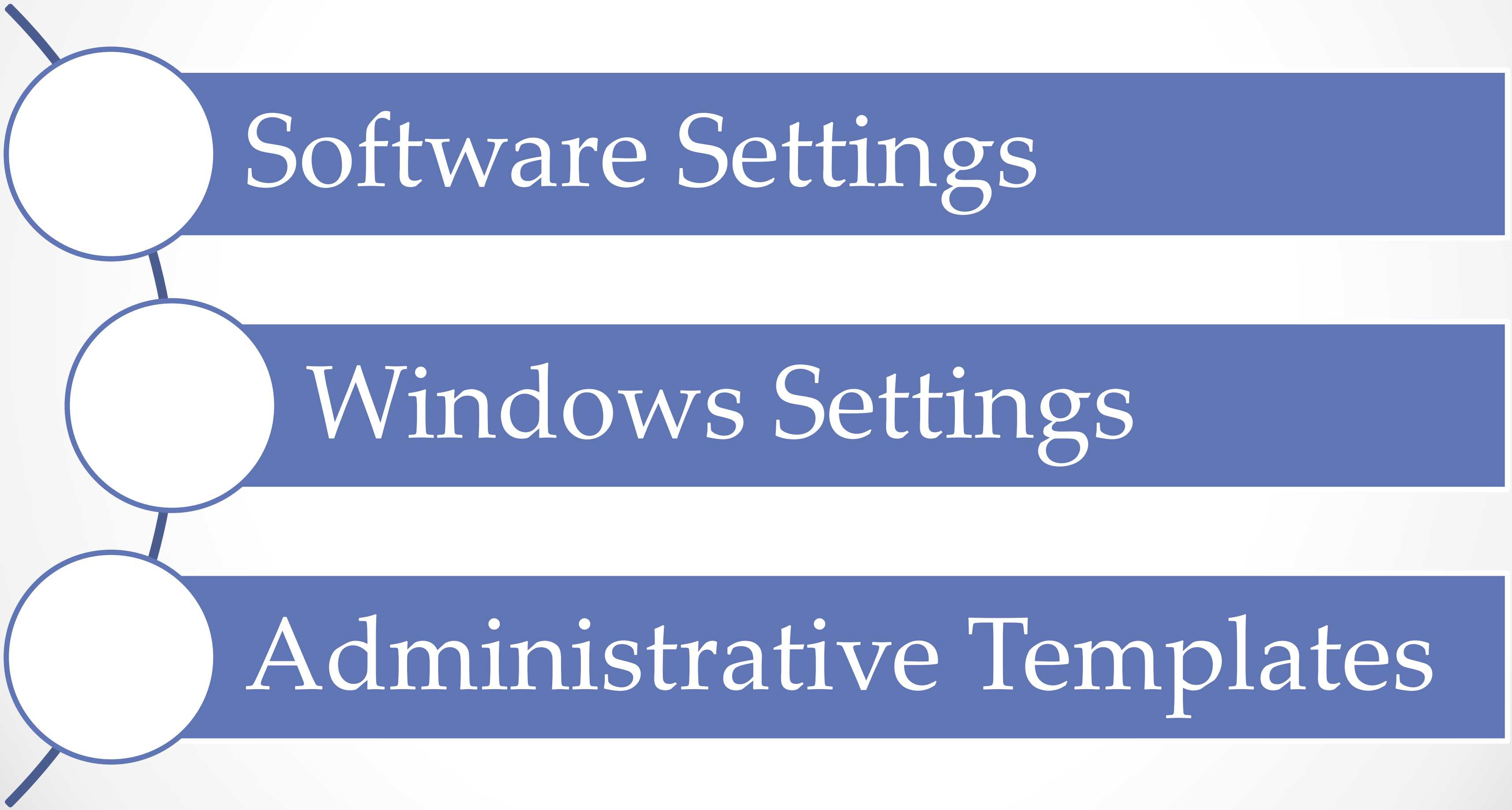
- Default Domain Policy [WIN2012SRV.CONTOSO.COM] Policy
  - Computer Configuration
    - Policies
      - Software Settings
        - Software installation
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
        - Policy-based QoS
      - Administrative Templates: Policy definitions (ADMX f
    - Preferences
  - User Configuration
    - Policies
      - Software Settings
        - Software installation
      - Windows Settings
        - Scripts (Logon/Logoff)
        - Security Settings
        - Folder Redirection
        - Policy-based QoS
      - Administrative Templates: Policy definitions (ADMX f
        - Control Panel
        - Desktop
        - Network
        - Shared Folders
        - Start Menu and Taskbar
        - System
        - Windows Components
        - All Settings
    - Preferences

Setting	State	Comment
Add or Remove Programs		
Display		
Personalization		
Printers		
Programs		
Regional and Language Options		
Hide specified Control Panel items	Not configured	No
Always open All Control Panel Items when opening Control ...	Not configured	No
Prohibit access to Control Panel and PC settings	Not configured	No
Show only specified Control Panel items	Not configured	No

4 setting(s)

Viewing the Group Policy Object (GPO) node structure

Computer Configuration \ Policies Nodes

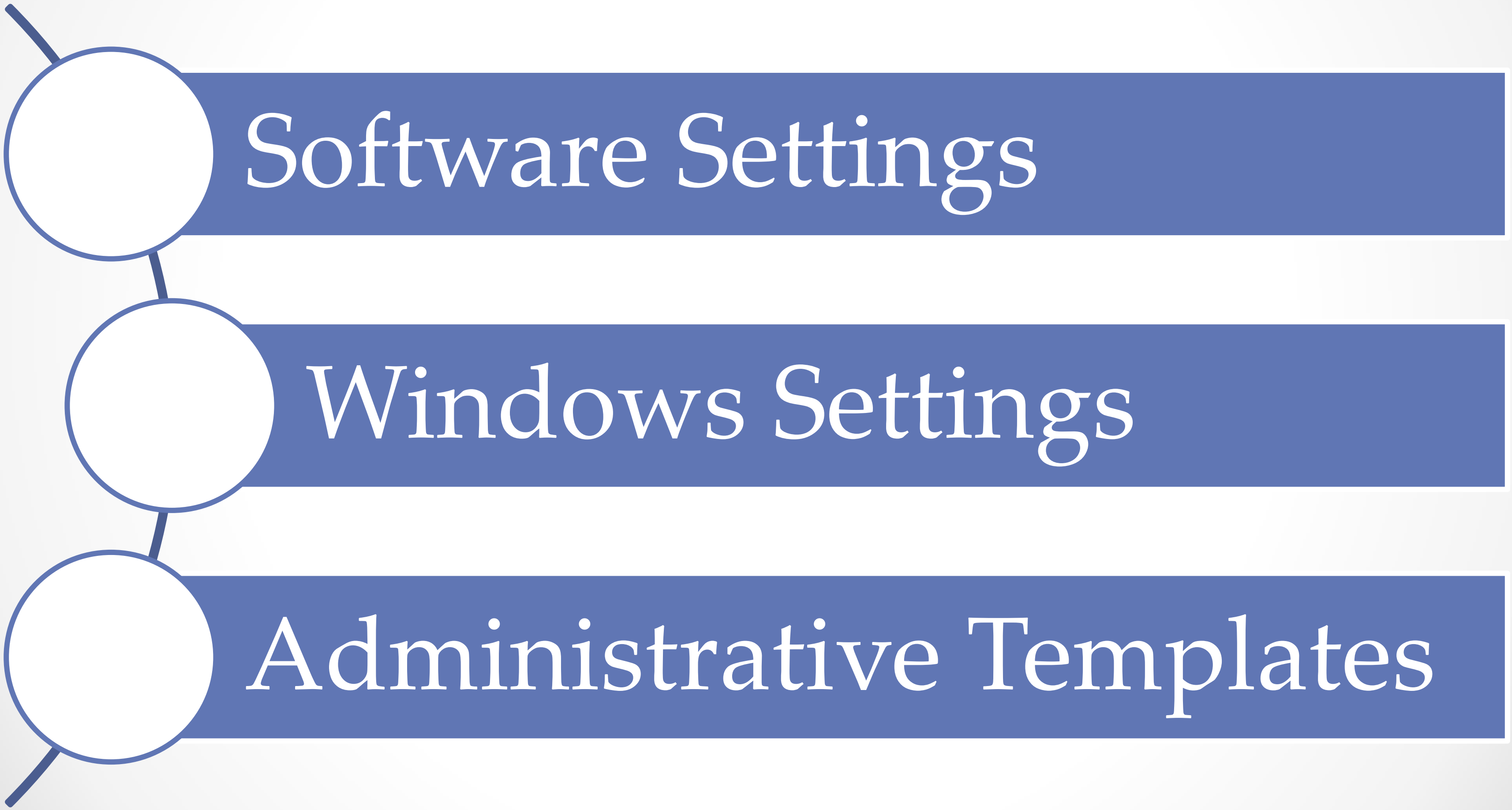


Software Settings

Windows Settings

Administrative Templates

Software Configuration \ Policies Nodes



- Software Settings
- Windows Settings
- Administrative Templates

Software Installation Using Group Policies

- **Windows Installer**: A software component used for the installation, maintenance, and removal of software on Windows.
- **Microsoft Software Installation (MSI) file**: Contains installation information for software.
- **MSI Transform files**: Used to deploy customized MSI files.
- **MSI Patch files**: Used to apply service packs and hot fixes to installed software.

Assigning or Publishing a Package

To deploy software with group policies, take the following steps:

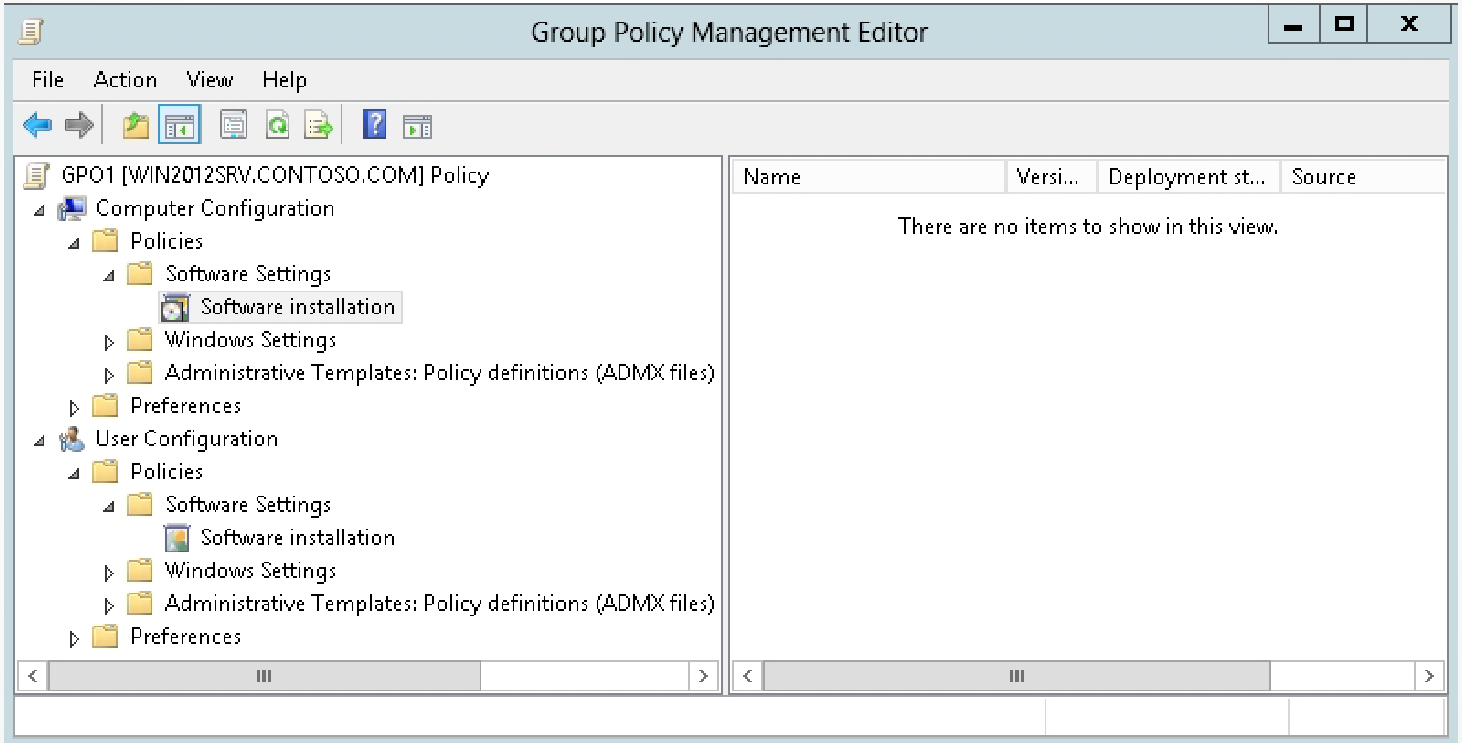
1. Create a distribution point on the publishing server.
2. Create a GPO to use to distribute the software package.
3. Assign or publish a package to a user or computer.

Assigning or Publishing a Package

When you install to a user or computer, you have the option to assign software or publish software with these options:

- Assign software to a user
- Assign software to a computer
- Publish software to a user

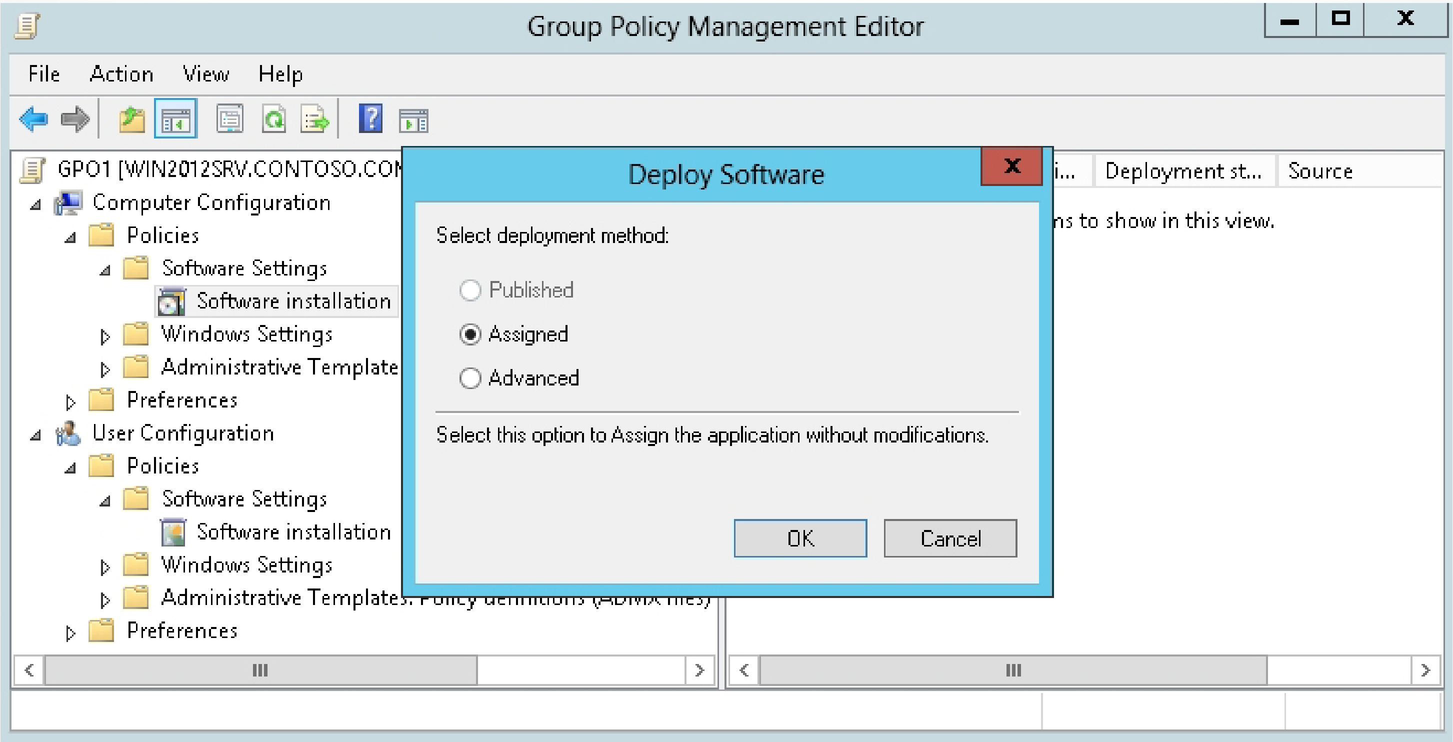
Create a New Software Installation Package



There are no items to show in this view.

Opening the Software Installation node

Create a New Software Installation Package



Deploy Software

Select deployment method:

○ Published

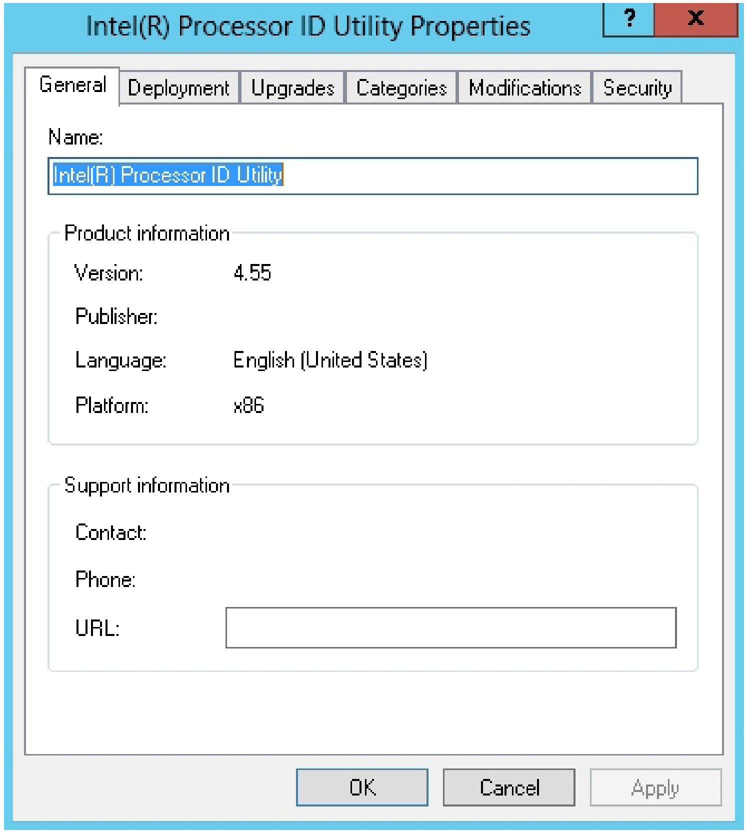
● Assigned

○ Advanced

Select this option to Assign the application without modifications.

Selecting the deployment method

Create a New Software Installation Package



Intel(R) Processor ID Utility Properties

Name: Intel(R) Processor ID Utility

Product information

Version: 4.55

Publisher:

Language: English (United States)

Platform: x86

Support information

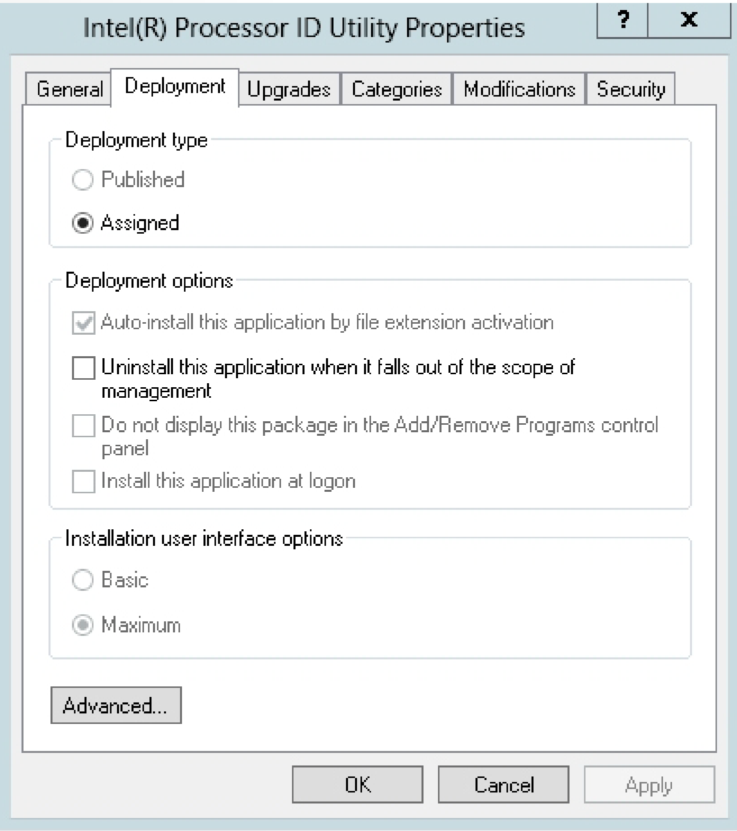
Contact:

Phone:

URL:

Opening the Properties dialog box for a software package

Create a New Software Installation Package



Intel(R) Processor ID Utility Properties

Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

□ Uninstall this application when it falls out of the scope of management

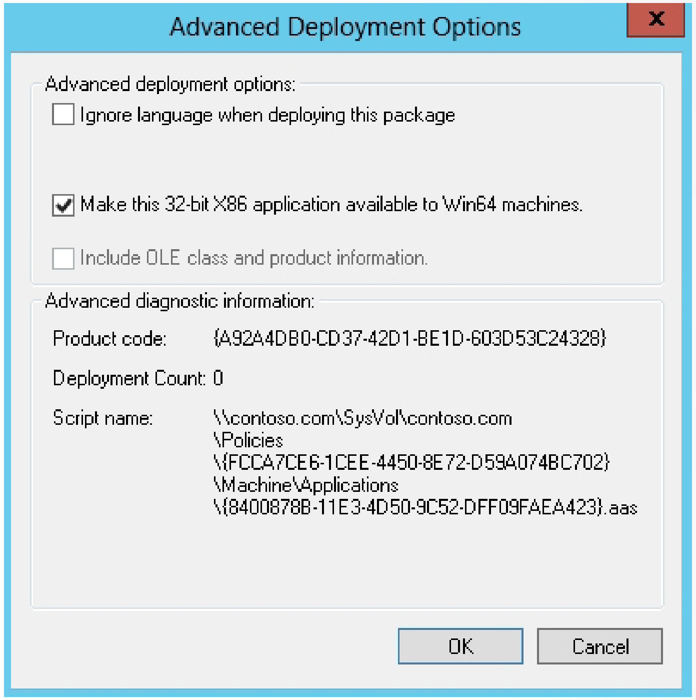
□ Do not display this package in the Add/Remove Programs control panel

□ Install this application at logon

Installation user interface options

○ Basic

● Maximum



Advanced Deployment Options

Advanced deployment options:

□ Ignore language when deploying this package

☑ Make this 32-bit X86 application available to Win64 machines.

□ Include OLE class and product information.

Advanced diagnostic information:

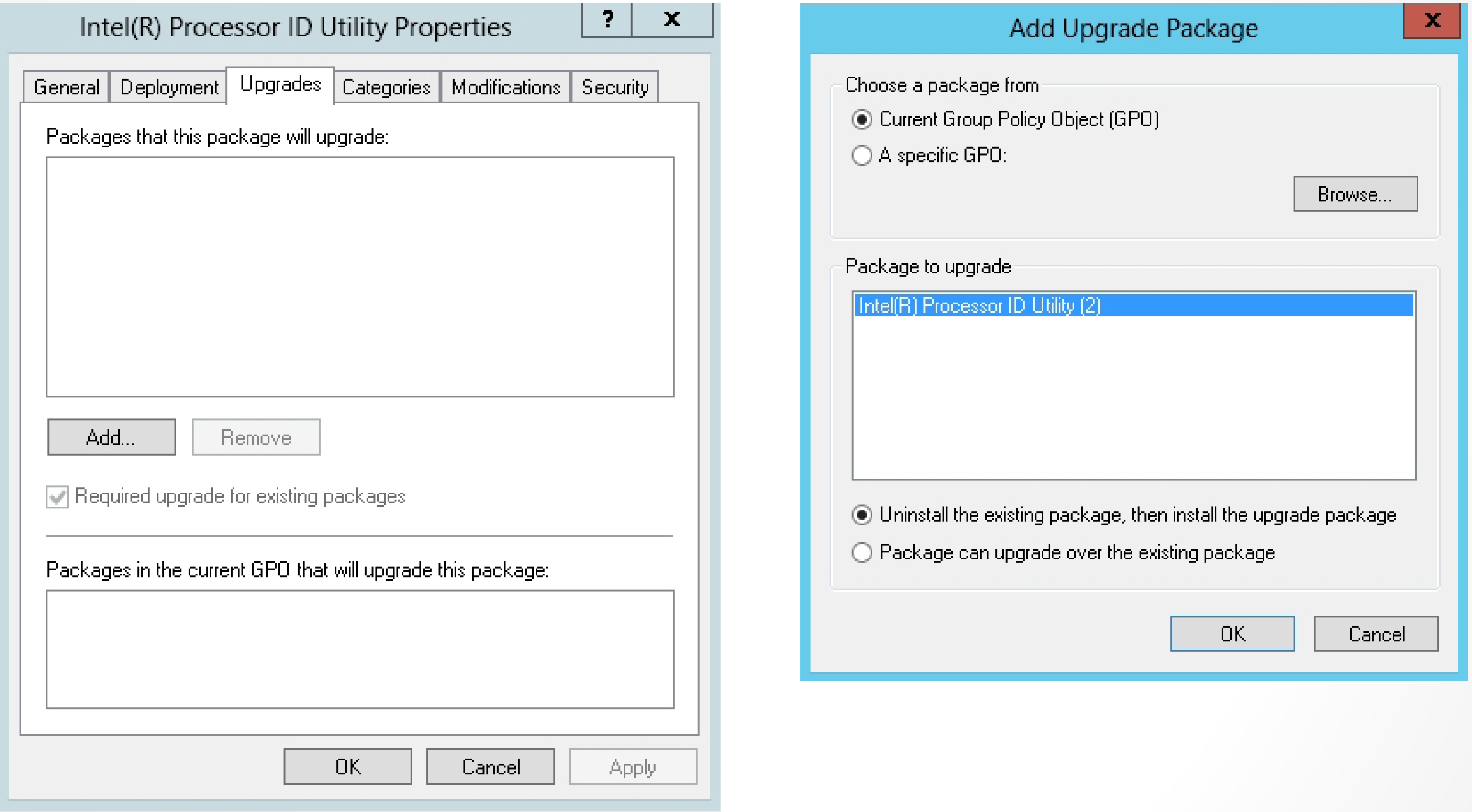
Product code: {A92A4DB0-CD37-42D1-BE1D-603D53C24328}

Deployment Count: 0

Script name: \\contoso.com\SysVol\contoso.com
\Policies
\{FCCA7CE6-1CEE-4450-8E72-D59A074BC702}
\Machine\Applications
\{8400878B-11E3-4D50-9C52-DFF09FAEA423}.aas

Changing the deployment type and deployment options

Create a New Software Installation Package



Packages that this package will upgrade:

☑ Required upgrade for existing packages

Packages in the current GPO that will upgrade this package:

Choose a package from

● Current Group Policy Object (GPO)

○ A specific GPO:

Package to upgrade

Intel(R) Processor ID Utility (2)

● Uninstall the existing package, then install the upgrade package

○ Package can upgrade over the existing package

Upgrading a software package

Uninstalling a Package

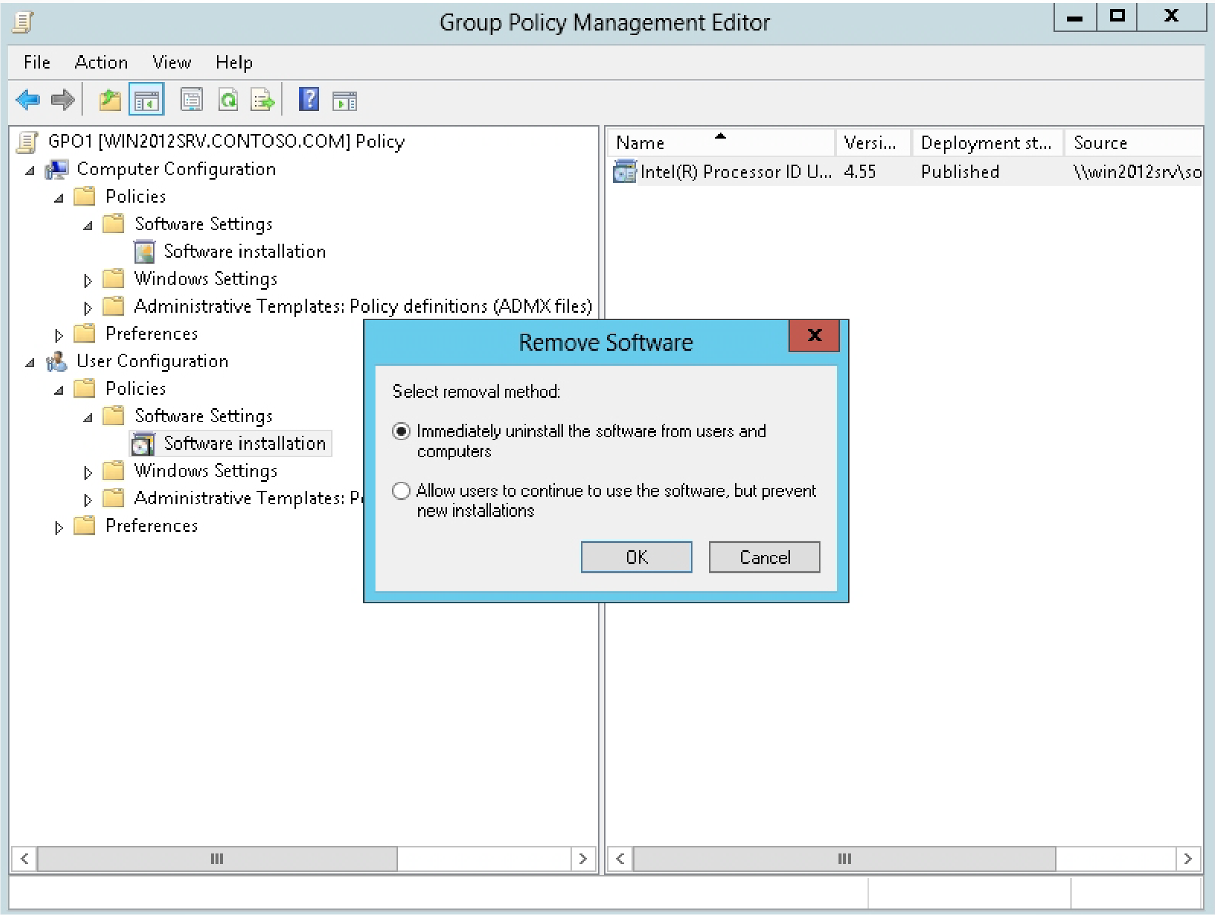
To remove an application:

1. Right-click the package.
2. Click *All Tasks*.
3. Click *Remove*.

When the Remove Software dialog box opens, choose one of these options:

- Immediately uninstall the software from users and computers
- Allow users to continue to use the software, but prevent new installations

Uninstalling a Package



Name	Versi...	Deployment st...	Source
Intel(R) Processor ID U...	4.55	Published	\\win2012srv\so

Remove Software

Select removal method:

● Immediately uninstall the software from users and computers

○ Allow users to continue to use the software, but prevent new installations

Removing software

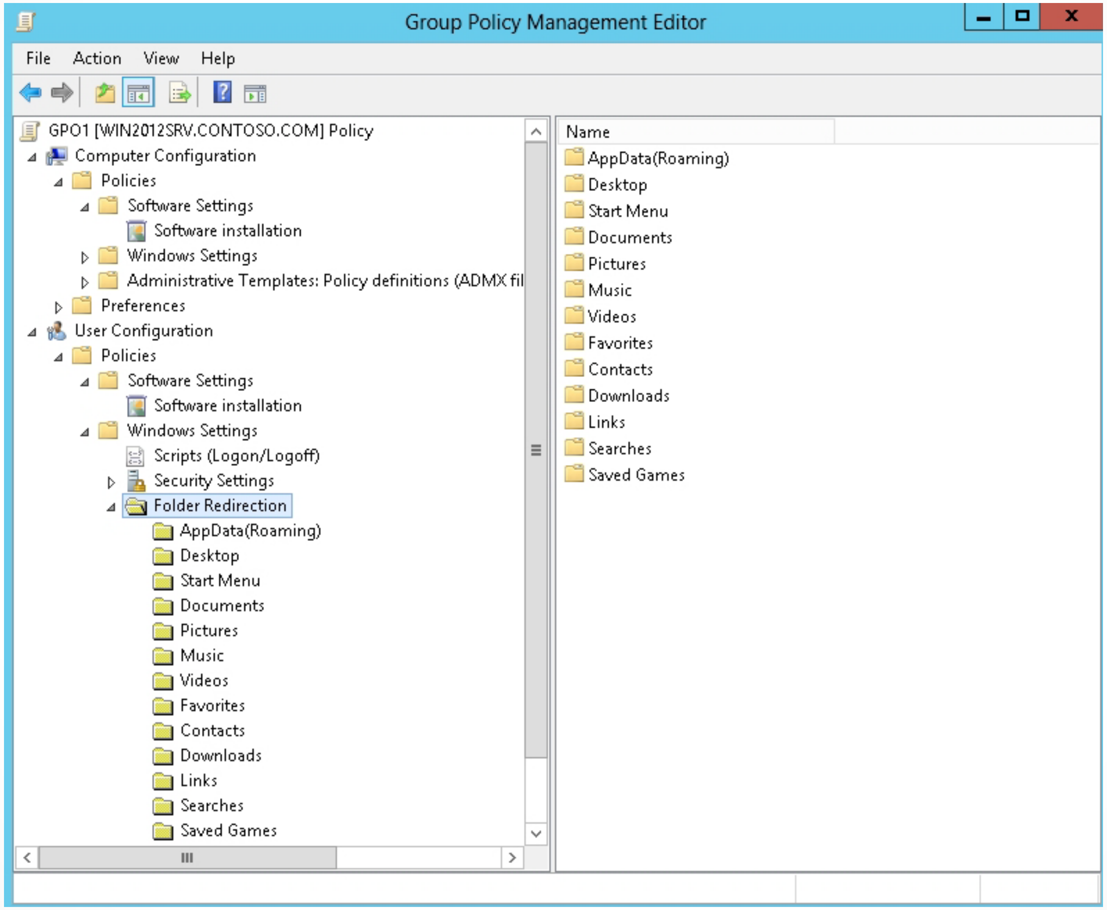
Using Folder Redirection

Use ***Folder Redirection*** to:

- Redirect the content of a certain folder to a network location or to another location on the user's local computer.
- Redirect the Desktop, Start Menu, Documents, Picture, Music, Videos, Favorites, Downloads, and other related folders.

It is found under \User Configuration\Policies\Windows Settings.

Using Folder Redirection

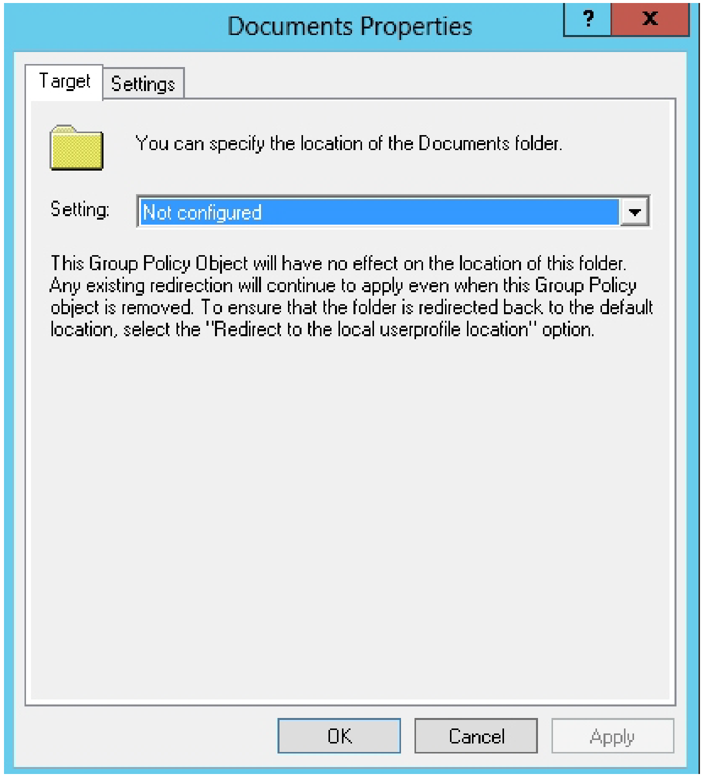


- GPO1 [WIN2012SRV.CONTOSO.COM] Policy
  - Computer Configuration
    - Policies
      - Software Settings
        - Software installation
      - Windows Settings
      - Administrative Templates: Policy definitions (ADMX fil
    - Preferences
  - User Configuration
    - Policies
      - Software Settings
        - Software installation
      - Windows Settings
        - Scripts (Logon/Logoff)
        - Security Settings
        - Folder Redirection
          - AppData(Roaming)
          - Desktop
          - Start Menu
          - Documents
          - Pictures
          - Music
          - Videos
          - Favorites
          - Contacts
          - Downloads
          - Links
          - Searches
          - Saved Games

Name
AppData(Roaming)
Desktop
Start Menu
Documents
Pictures
Music
Videos
Favorites
Contacts
Downloads
Links
Searches
Saved Games

Viewing the Folder Redirection folders

Configure Folder Redirection



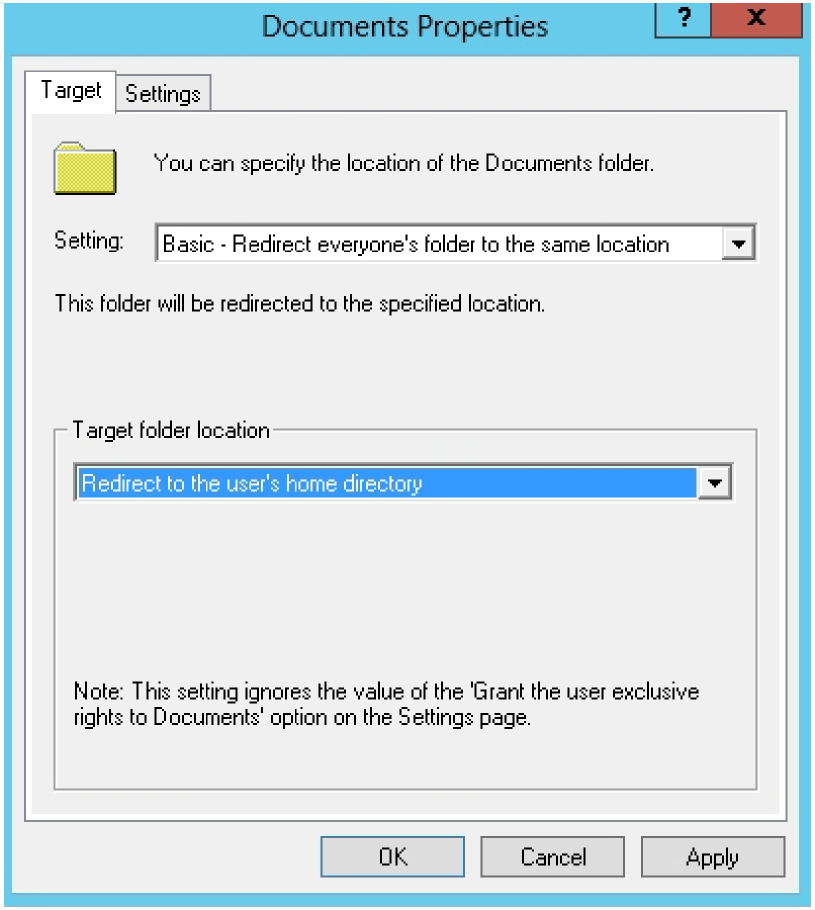
You can specify the location of the Documents folder.

Setting: Not configured

This Group Policy Object will have no effect on the location of this folder. Any existing redirection will continue to apply even when this Group Policy object is removed. To ensure that the folder is redirected back to the default location, select the "Redirect to the local userprofile location" option.

Configuring the Documents Properties

Configure Folder Redirection



You can specify the location of the Documents folder.

Setting: Basic - Redirect everyone's folder to the same location

This folder will be redirected to the specified location.

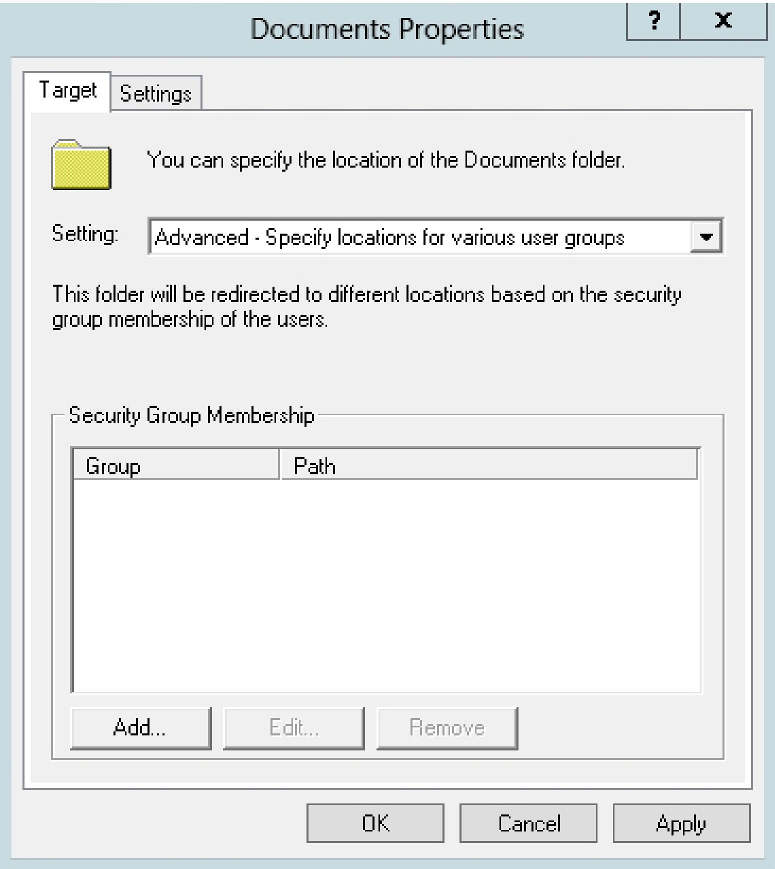
Target folder location

Redirect to the user's home directory

Note: This setting ignores the value of the 'Grant the user exclusive rights to Documents' option on the Settings page.

Redirecting to the user's home directory

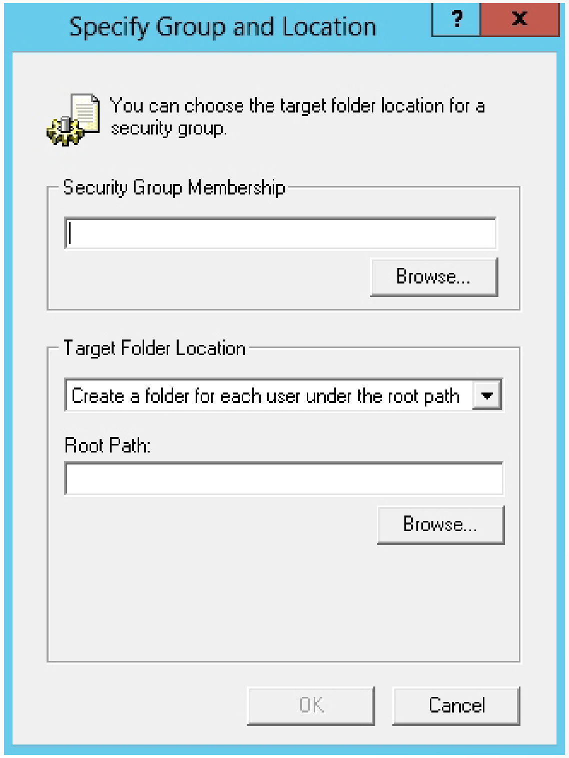
Configure Folder Redirection


Documents Properties

You can specify the location of the Documents folder.

Setting: Advanced - Specify locations for various user groups

This folder will be redirected to different locations based on the security group membership of the users.

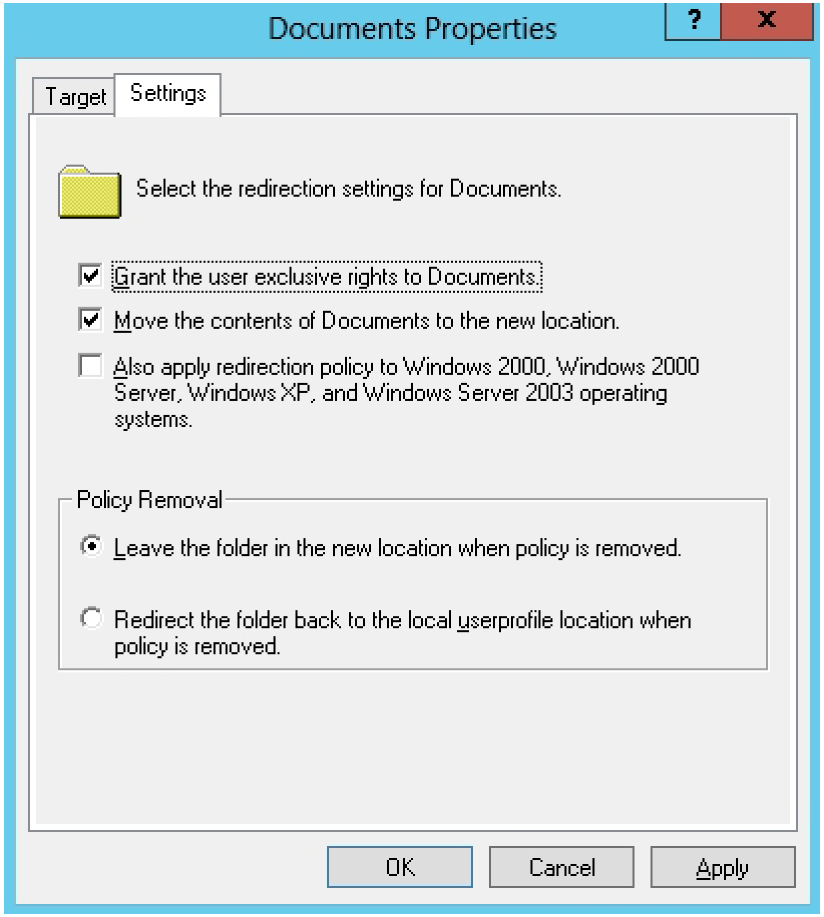

Specify Group and Location

You can choose the target folder location for a security group.

Target Folder Location: Create a folder for each user under the root path

Specifying the Security Group Membership
when using Advanced mode

Configure Folder Redirection



Documents Properties

Select the redirection settings for Documents.

☑ Grant the user exclusive rights to Documents.

☑ Move the contents of Documents to the new location.

□ Also apply redirection policy to Windows 2000, Windows 2000 Server, Windows XP, and Windows Server 2003 operating systems.

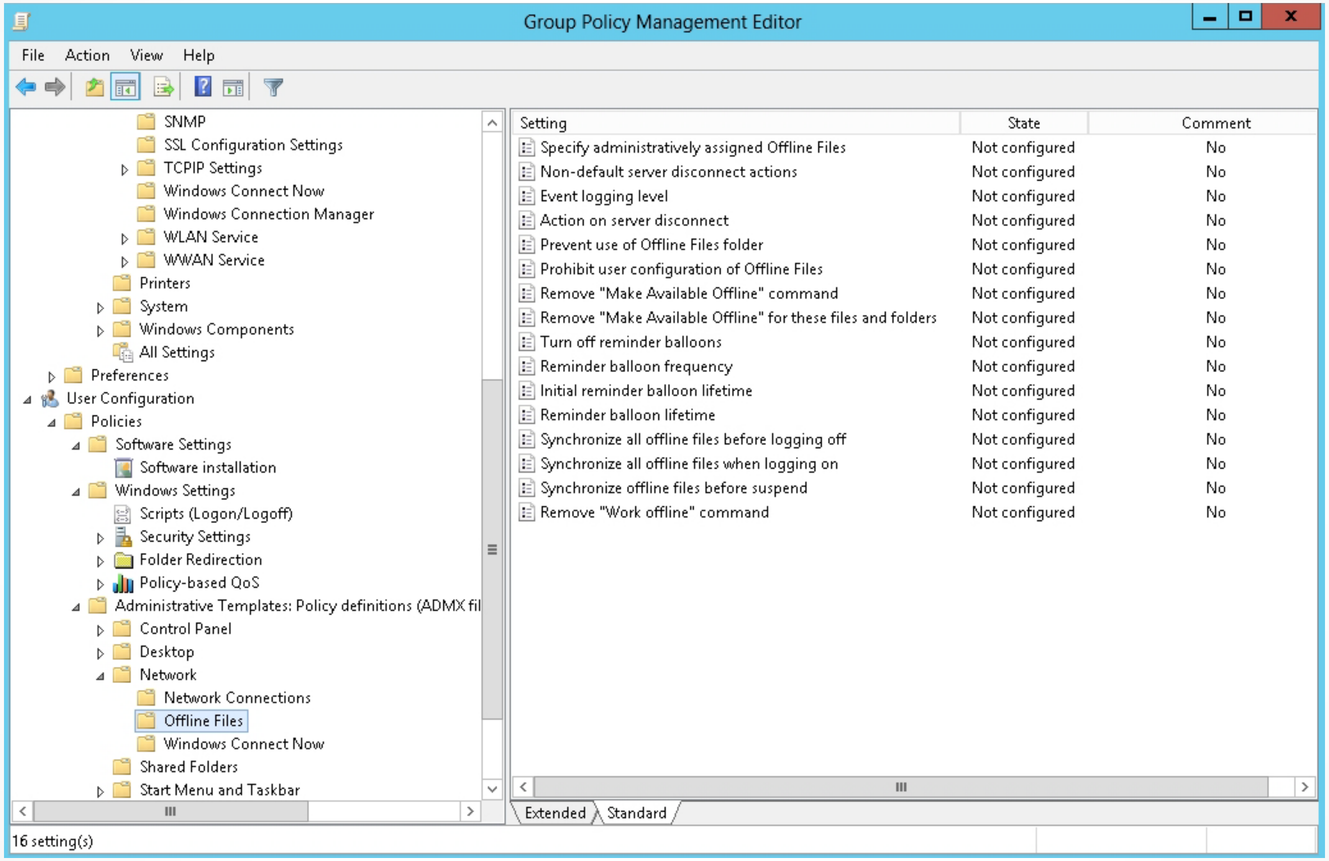
Policy Removal

● Leave the folder in the new location when policy is removed.

○ Redirect the folder back to the local userprofile location when policy is removed.

Configuring settings when using Advanced mode

Configure Folder Redirection



Setting	State	Comment
Specify administratively assigned Offline Files	Not configured	No
Non-default server disconnect actions	Not configured	No
Event logging level	Not configured	No
Action on server disconnect	Not configured	No
Prevent use of Offline Files folder	Not configured	No
Prohibit user configuration of Offline Files	Not configured	No
Remove "Make Available Offline" command	Not configured	No
Remove "Make Available Offline" for these files and folders	Not configured	No
Turn off reminder balloons	Not configured	No
Reminder balloon frequency	Not configured	No
Initial reminder balloon lifetime	Not configured	No
Reminder balloon lifetime	Not configured	No
Synchronize all offline files before logging off	Not configured	No
Synchronize all offline files when logging on	Not configured	No
Synchronize offline files before suspend	Not configured	No
Remove "Work offline" command	Not configured	No

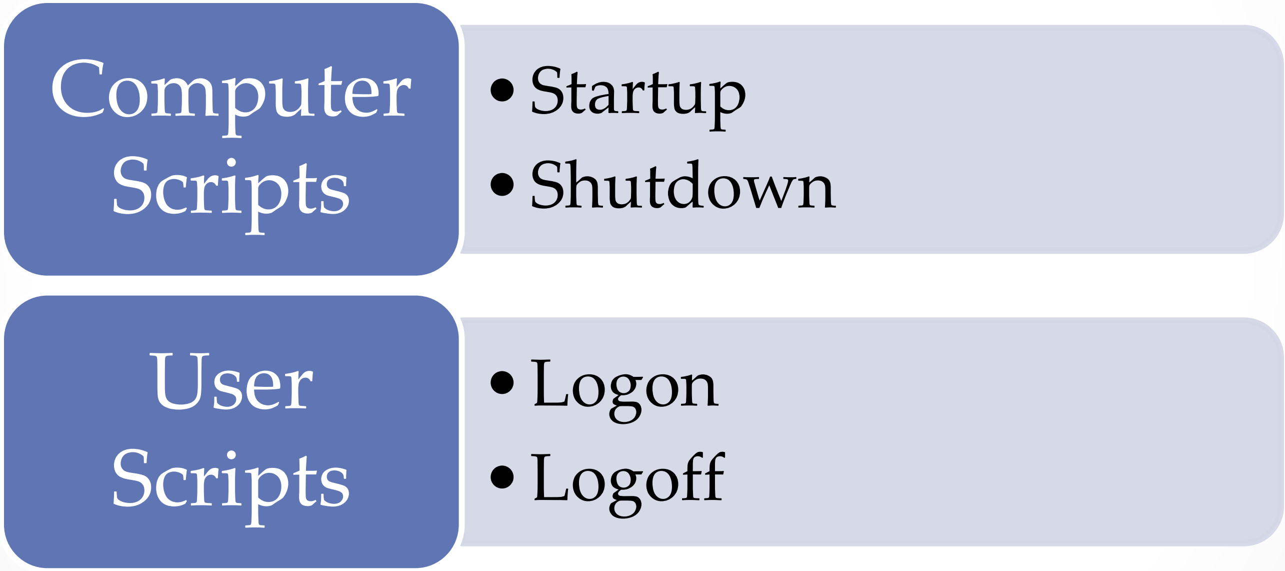
16 setting(s)

Using group policies to configure offline files

Using Scripts with Group Policies

- A ***script*** is a list of commands that can be executed within a single file, which can perform repetitive tasks.
- The ***Microsoft Windows Script Hosts (WSH)*** is the component that provides scripting capabilities to Windows.

Types of Scripts



Computer Scripts

- Startup
- Shutdown

User Scripts

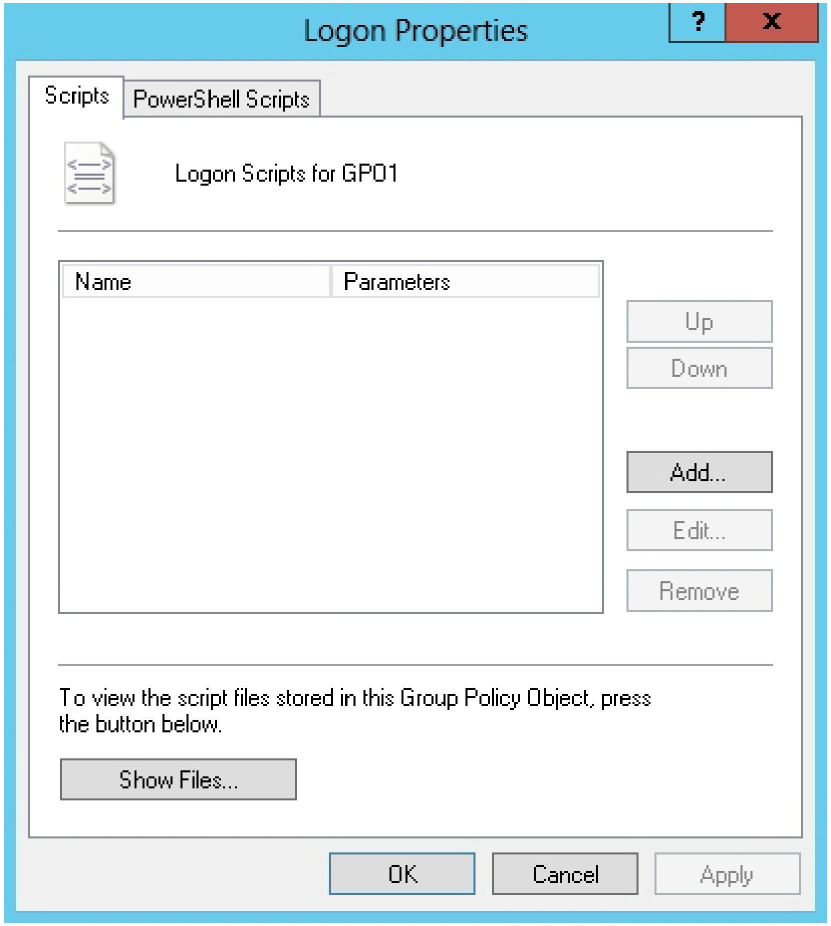
- Logon
- Logoff

Using Scripts with Group Policies

To use scripts:

1. Create the login script.
2. Execute the script manually to make sure that the script runs and performs as planned.
3. Copy the script to the c:\Windows\Sysvol\Sysvol\Domain Name\Scripts folder on a domain controller. The content of SYSVOL volume is automatically replicated to the other domain controllers within the domain.
4. Configure a GPO to execute the script during startup, shutdown, logon, or logoff.

Implement a Login Script Using Group Policies



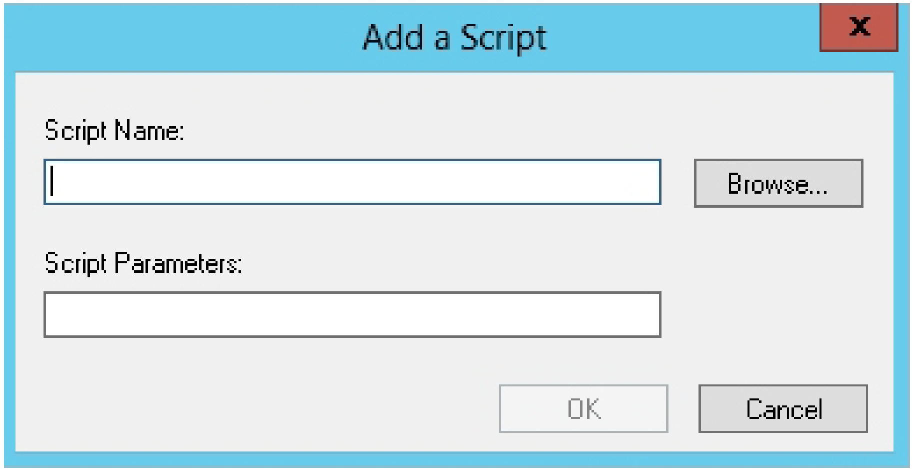
Logon Scripts for GPO1

Name	Parameters

To view the script files stored in this Group Policy Object, press the button below.

Opening the Logon Properties dialog box

Implement a Login Script Using Group Policies



Adding a script to a GPO

Using Administrative Templates

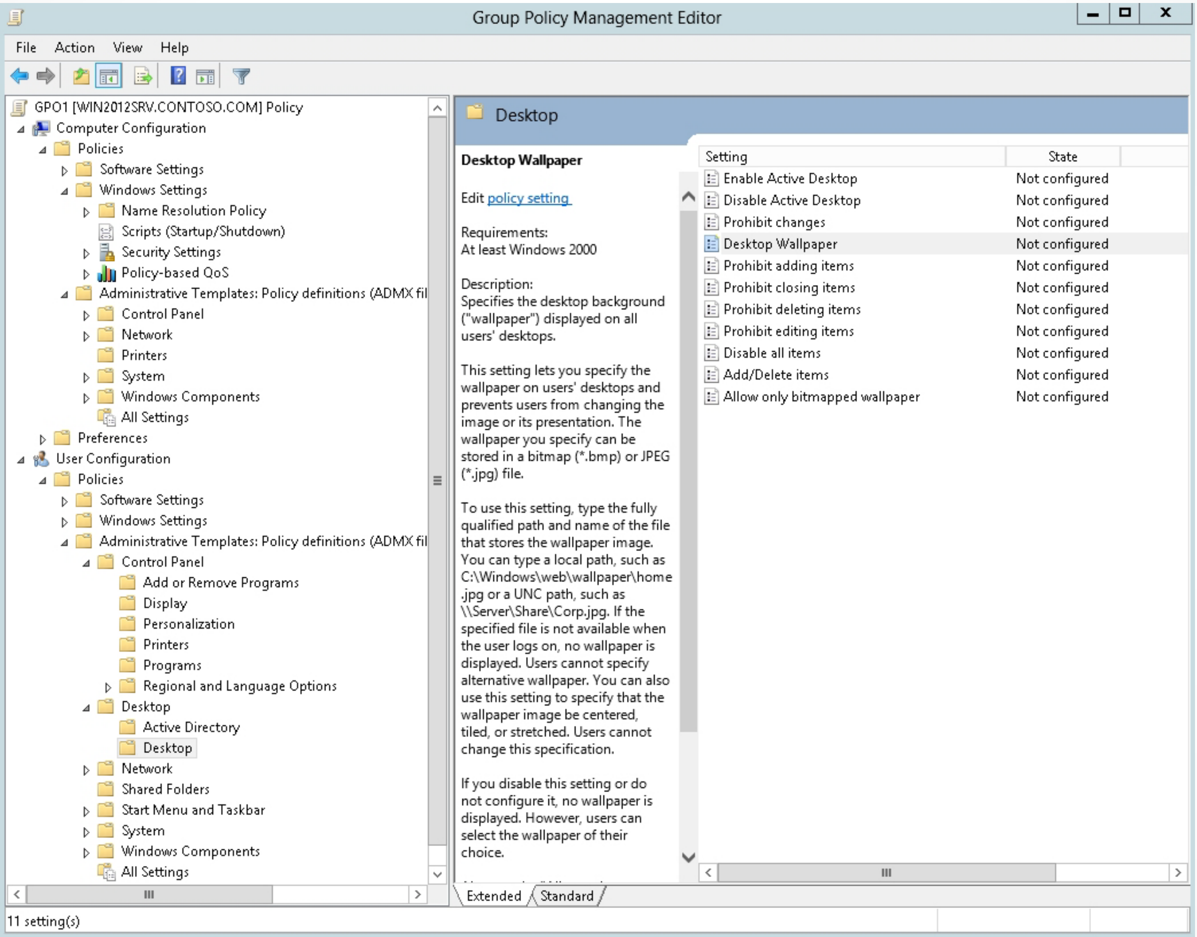
- ***ADM files***: Used to define the settings that an administrator can configure through Group Policy.
- ***ADMX files***: Like ADM files but based on eXtensible Markup Language (XML). Can be stored in a single location called the *Central Store* in the SYSVOL directory.
- ***ADML files***: Language-specific files used to store descriptions of settings.

Managing Administrative Templates

Requirements for an Administrative Template setting are displayed:

- On the Extended tab, when you click to select an Administrative Template setting
- When you double-click an Administrative Template setting

Managing Administrative Templates



- GPO1 [WIN2012SRV.CONTOSO.COM] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
        - Policy-based QoS
      - Administrative Templates: Policy definitions (ADMX fil
        - Control Panel
        - Network
        - Printers
        - System
        - Windows Components
        - All Settings
    - Preferences
  - User Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy definitions (ADMX fil
        - Control Panel
          - Add or Remove Programs
          - Display
          - Personalization
          - Printers
          - Programs
          - Regional and Language Options
        - Desktop
          - Active Directory
          - Desktop
        - Network
        - Shared Folders
        - Start Menu and Taskbar
        - System
        - Windows Components
        - All Settings

Desktop

Desktop Wallpaper

Edit policy setting

Requirements:
At least Windows 2000

Description:
Specifies the desktop background ("wallpaper") displayed on all users' desktops.

This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp) or JPEG (*.jpg) file.

To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home.jpg or a UNC path, such as \\Server\Share\Corp.jpg. If the specified file is not available when the user logs on, no wallpaper is displayed. Users cannot specify alternative wallpaper. You can also use this setting to specify that the wallpaper image be centered, tiled, or stretched. Users cannot change this specification.

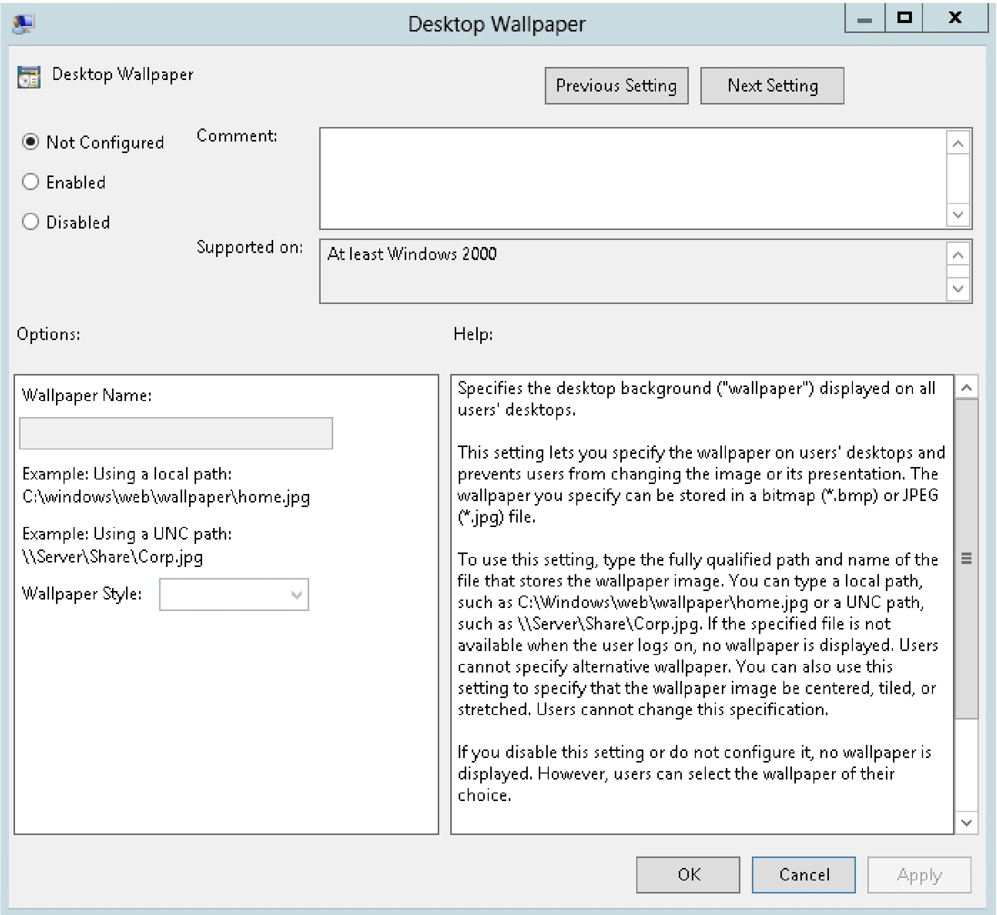
If you disable this setting or do not configure it, no wallpaper is displayed. However, users can select the wallpaper of their choice.

Setting	State
Enable Active Desktop	Not configured
Disable Active Desktop	Not configured
Prohibit changes	Not configured
Desktop Wallpaper	Not configured
Prohibit adding items	Not configured
Prohibit closing items	Not configured
Prohibit deleting items	Not configured
Prohibit editing items	Not configured
Disable all items	Not configured
Add/Delete items	Not configured
Allow only bitmapped wallpaper	Not configured

11 setting(s)

Selecting an Administrative Template

Managing Administrative Templates



● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Wallpaper Name:

Example: Using a local path:
C:\windows\web\wallpaper\home.jpg

Example: Using a UNC path:
\\Server\Share\Corp.jpg

Wallpaper Style:

Help:

Specifies the desktop background ("wallpaper") displayed on all users' desktops.

This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp) or JPEG (*.jpg) file.

To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home.jpg or a UNC path, such as \\Server\Share\Corp.jpg. If the specified file is not available when the user logs on, no wallpaper is displayed. Users cannot specify alternative wallpaper. You can also use this setting to specify that the wallpaper image be centered, tiled, or stretched. Users cannot change this specification.

If you disable this setting or do not configure it, no wallpaper is displayed. However, users can select the wallpaper of their choice.

Viewing the Settings dialog box

Managing Administrative Templates

When configuring Administrative Templates, there are three states:

- **Not Configured**: The registry key is not modified or overwritten.
- **Enabled**: The registry key is modified by this setting.
- **Disabled**: The Disabled settings undo a change made by a prior Enabled setting.

The Central Store

The ***Central Store***:

- Is a folder structure created in the SYSVOL directory on the domain controllers in each domain in your organization.
- Is created only on a single domain controller for each domain.

The content of the SYSVOL will be replicated to the other domain controllers.

Creating a Central Store

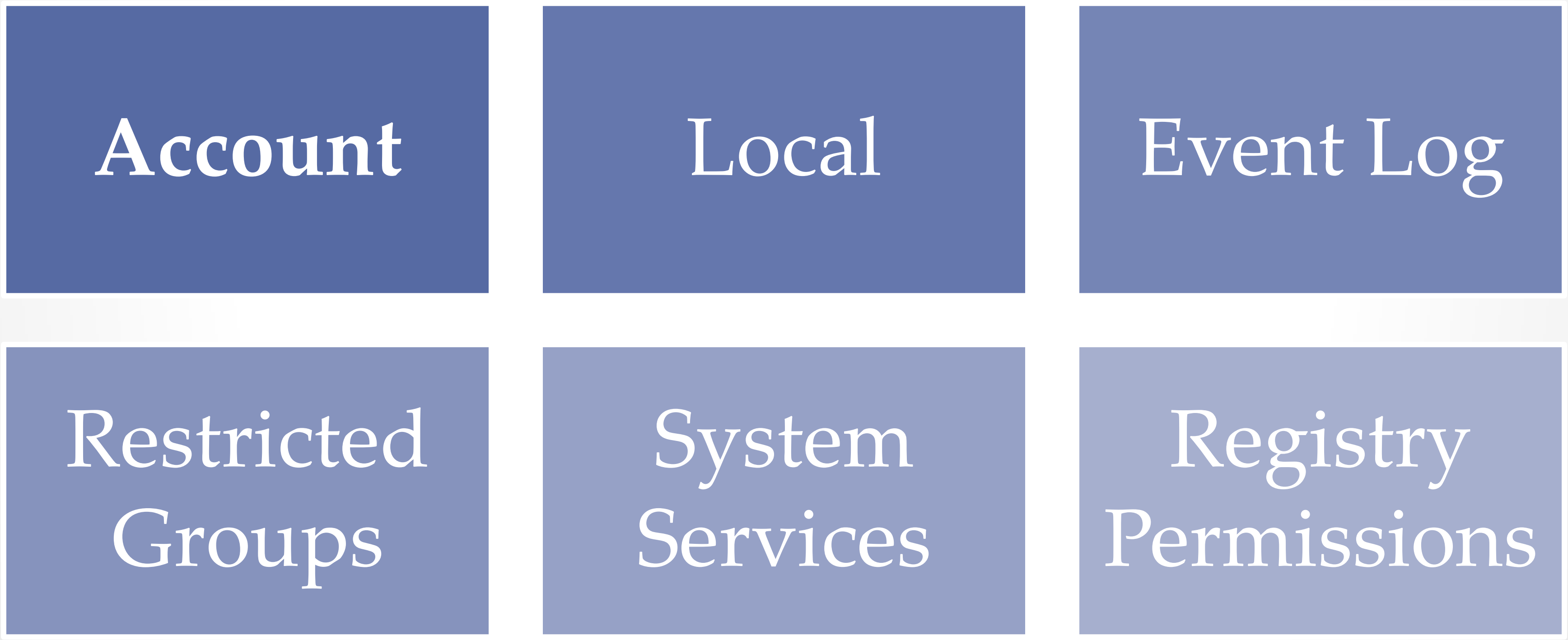
1. Create a PolicyDefinitions folder in the %systemroot%\sysvol\domain\policies\ folder.
2. The PolicyDefinitions folder stores all language-neutral ADMX files. Therefore, copy all files from the %systemroot%\PolicyDefinitions\* folder to the %systemroot%\sysvol\domain\policies\ folder.
3. Copy all the language folders and files to %systemroot%\sysvol\domain\policies\ PolicyDefinitions.

Security Templates

A ***security template*** is a collection of configuration settings stored in a text file with the .inf extension. They can be used to:

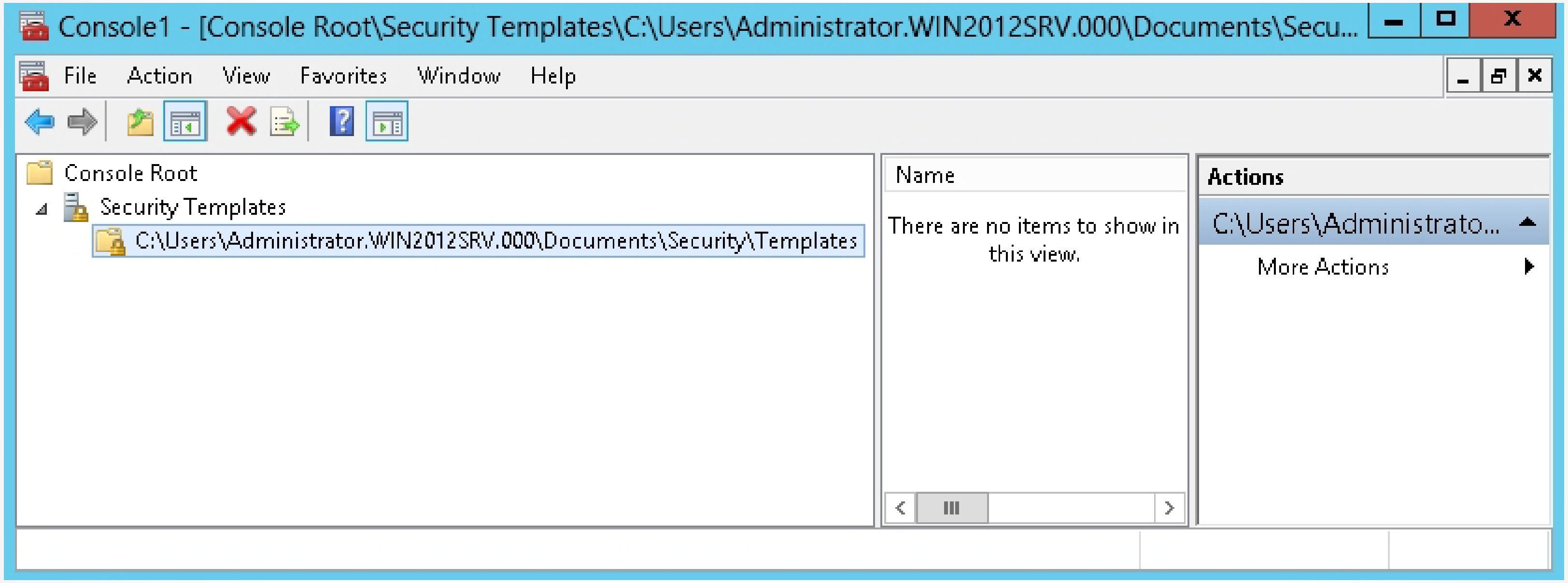
- Save the security configuration to a file.
- Deploy the security settings to a computer or group policy.
- Analyze compliance of a computer’s current configuration against the desired configuration.

Policies Configured with Security Templates



- **Account**
- Local
- Event Log
- Restricted Groups
- System Services
- Registry Permissions

The Security Templates Snap-In

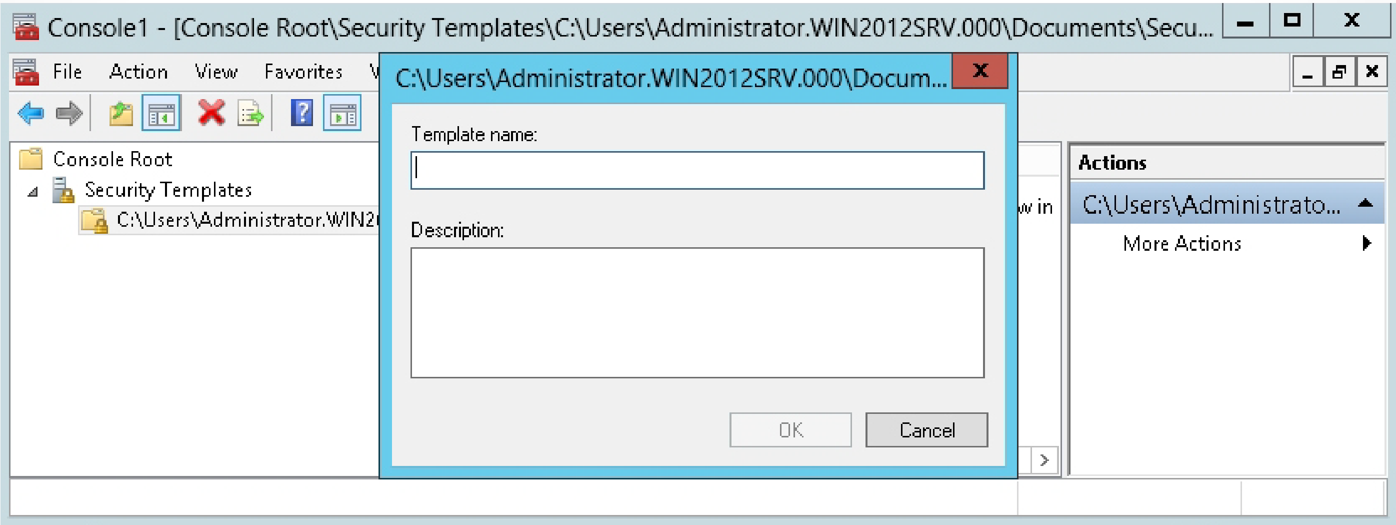


Console1 - [Console Root\Security Templates\C:\Users\Administrator.WIN2012SRV.000\Documents\Secu...
File Action View Favorites Window Help
Console Root
Security Templates
C:\Users\Administrator.WIN2012SRV.000\Documents\Security\Templates
Name
Actions
C:\Users\Administrato...
More Actions

There are no items to show in this view.

To create a new security template, right-click the node where you want to store the security template, and click New Template

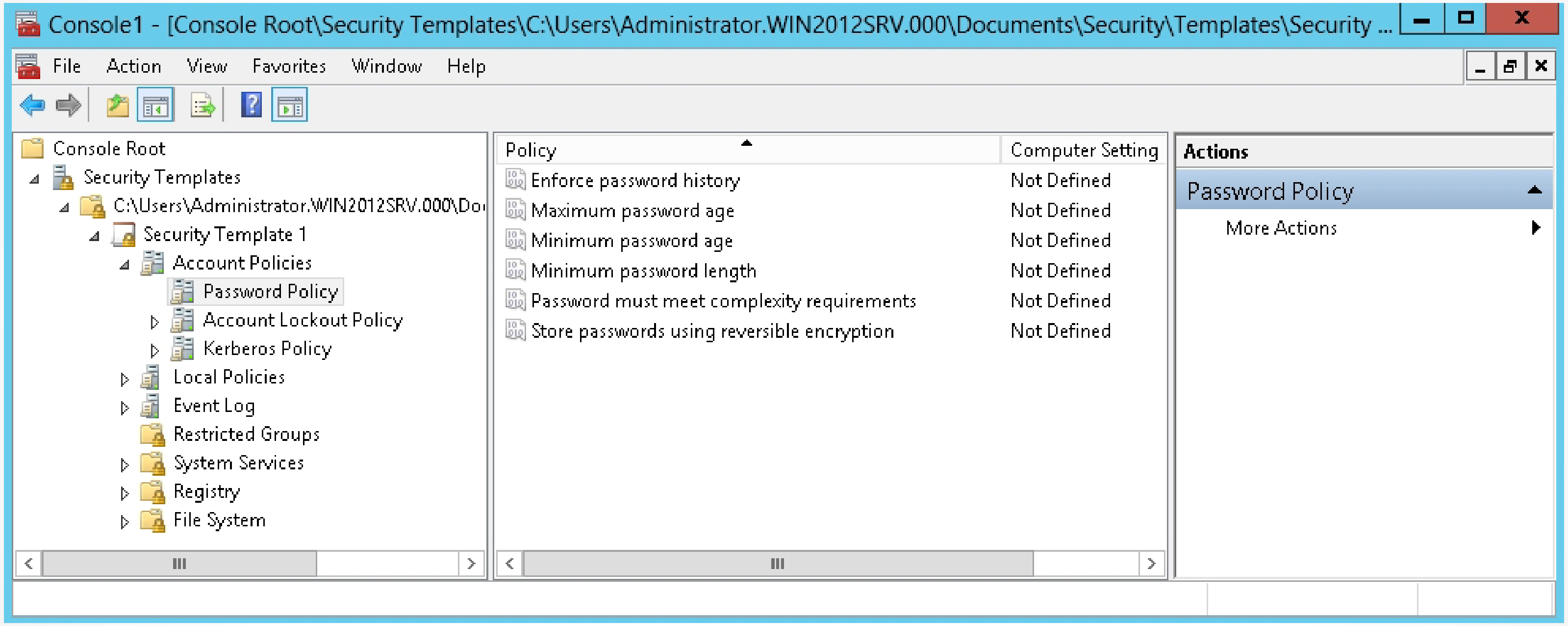
Open the Security Templates Snap-In



Console1 - [Console Root\Security Templates\C:\Users\Administrator.WIN2012SRV.000\Documents\Secu...
File
Action
View
Favorites
Console Root
Security Templates
C:\Users\Administrator.WIN2
C:\Users\Administrator.WIN2012SRV.000\Docum...
Template name:
Description:
OK
Cancel
Actions
C:\Users\Administrato...
More Actions

Naming the security template

Open the Security Templates Snap-In

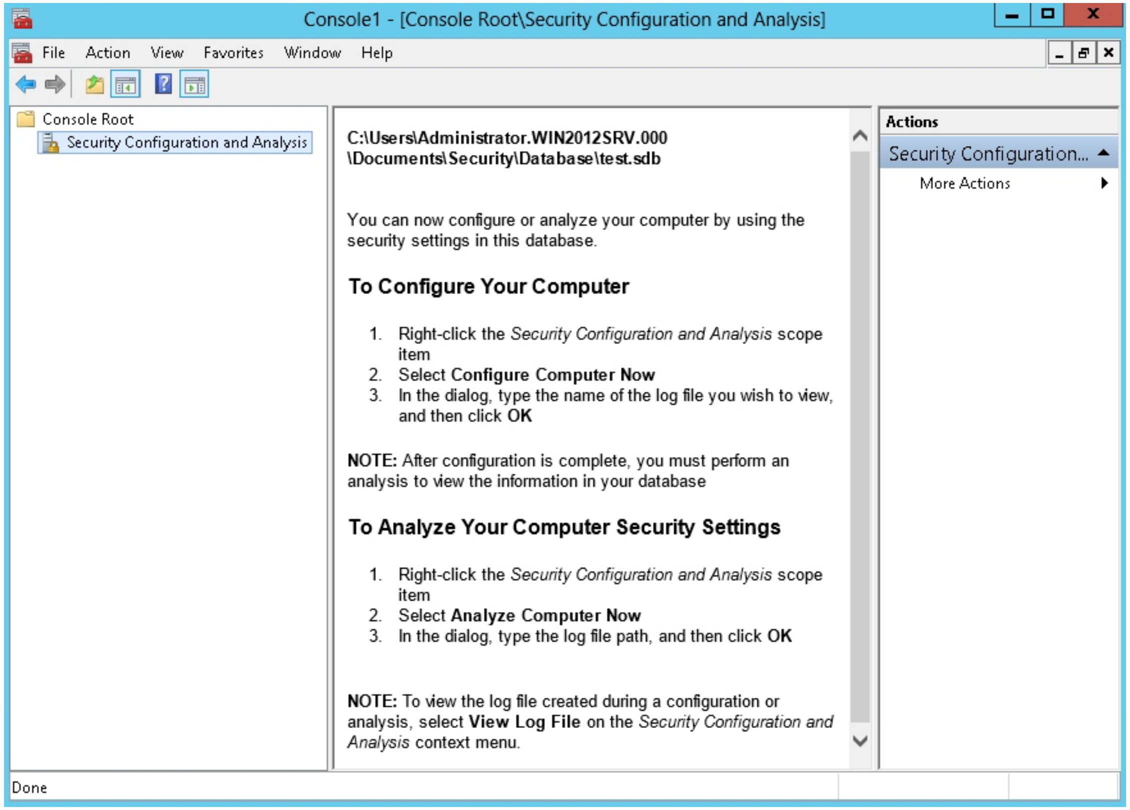

Console1 - [Console Root\Security Templates\C:\Users\Administrator.WIN2012SRV.000\Documents\Security\Templates\Security ...
File
Action
View
Favorites
Window
Help
Actions
Password Policy
More Actions

- Console Root
  - Security Templates
    - C:\Users\Administrator.WIN2012SRV.000\Do
      - Security Template 1
        - Account Policies
          - Password Policy
          - Account Lockout Policy
          - Kerberos Policy
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System

Policy	Computer Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	Not Defined
Password must meet complexity requirements	Not Defined
Store passwords using reversible encryption	Not Defined

Viewing a security template

Compare Settings with a Security Template



Console1 - [Console Root\Security Configuration and Analysis]
File
Action
View
Favorites
Window
Help
Console Root
Security Configuration and Analysis
Actions
Security Configuration...
More Actions
Done

C:\Users\Administrator.WIN2012SRV.000 \Documents\Security\Database\test.sdb

You can now configure or analyze your computer by using the security settings in this database.

To Configure Your Computer

1. Right-click the *Security Configuration and Analysis* scope item
2. Select **Configure Computer Now**
3. In the dialog, type the name of the log file you wish to view, and then click **OK**

NOTE: After configuration is complete, you must perform an analysis to view the information in your database

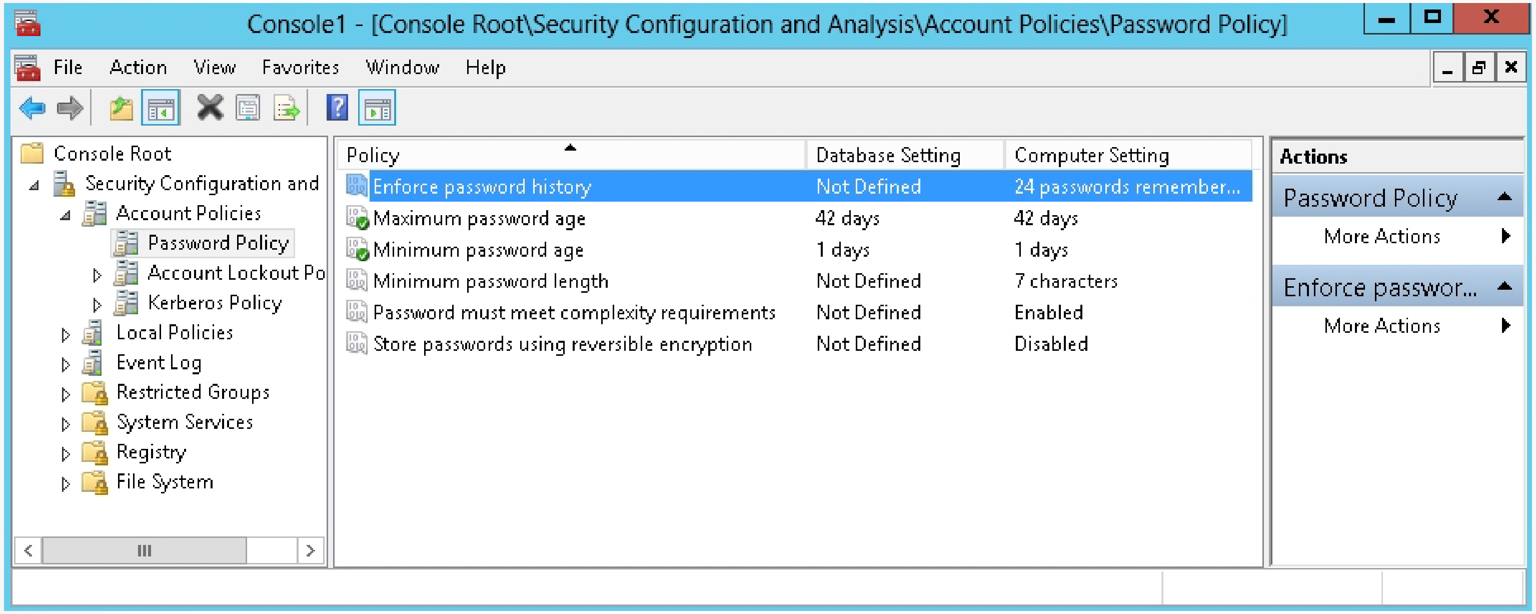
To Analyze Your Computer Security Settings

1. Right-click the *Security Configuration and Analysis* scope item
2. Select **Analyze Computer Now**
3. In the dialog, type the log file path, and then click **OK**

NOTE: To view the log file created during a configuration or analysis, select **View Log File** on the *Security Configuration and Analysis* context menu.

Viewing the Security Configuration and Analysis console

Compare Settings with a Security Template



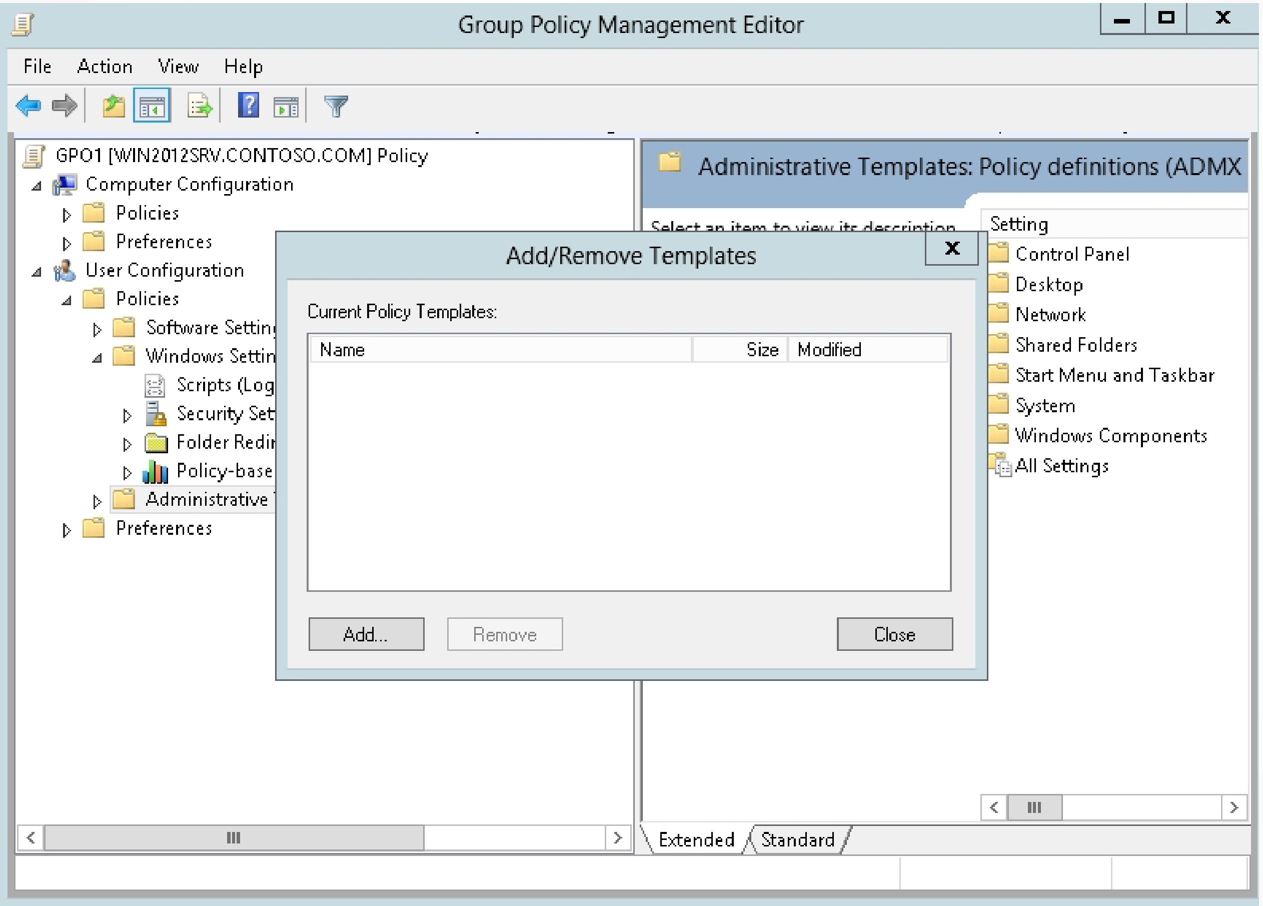
Policy	Database Setting	Computer Setting
Enforce password history	Not Defined	24 passwords remember...
Maximum password age	42 days	42 days
Minimum password age	1 days	1 days
Minimum password length	Not Defined	7 characters
Password must meet complexity requirements	Not Defined	Enabled
Store passwords using reversible encryption	Not Defined	Disabled

Comparing a security template with actual settings

Custom Administrative Template Files

- To make settings in ADMX files available to a GPO, add the Administrative Templates file to the GPO.
- If you have older ADM files, either add them to the GPO or convert the ADM file to an ADMX file.

Add Custom ADM Administrative Template Files



Group Policy Management Editor

GPO1 [WIN2012SRV.CONTOSO.COM] Policy
- Computer Configuration
  - Policies
  - Preferences
- User Configuration
  - Policies
    - Software Settin
    - Windows Settin
      - Scripts (Log
      - Security Set
      - Folder Redir
      - Policy-base
    - Administrative
  - Preferences

Administrative Templates: Policy definitions (ADMX

Select an item to view its description

Setting
Control Panel
Desktop
Network
Shared Folders
Start Menu and Taskbar
System
Windows Components
All Settings

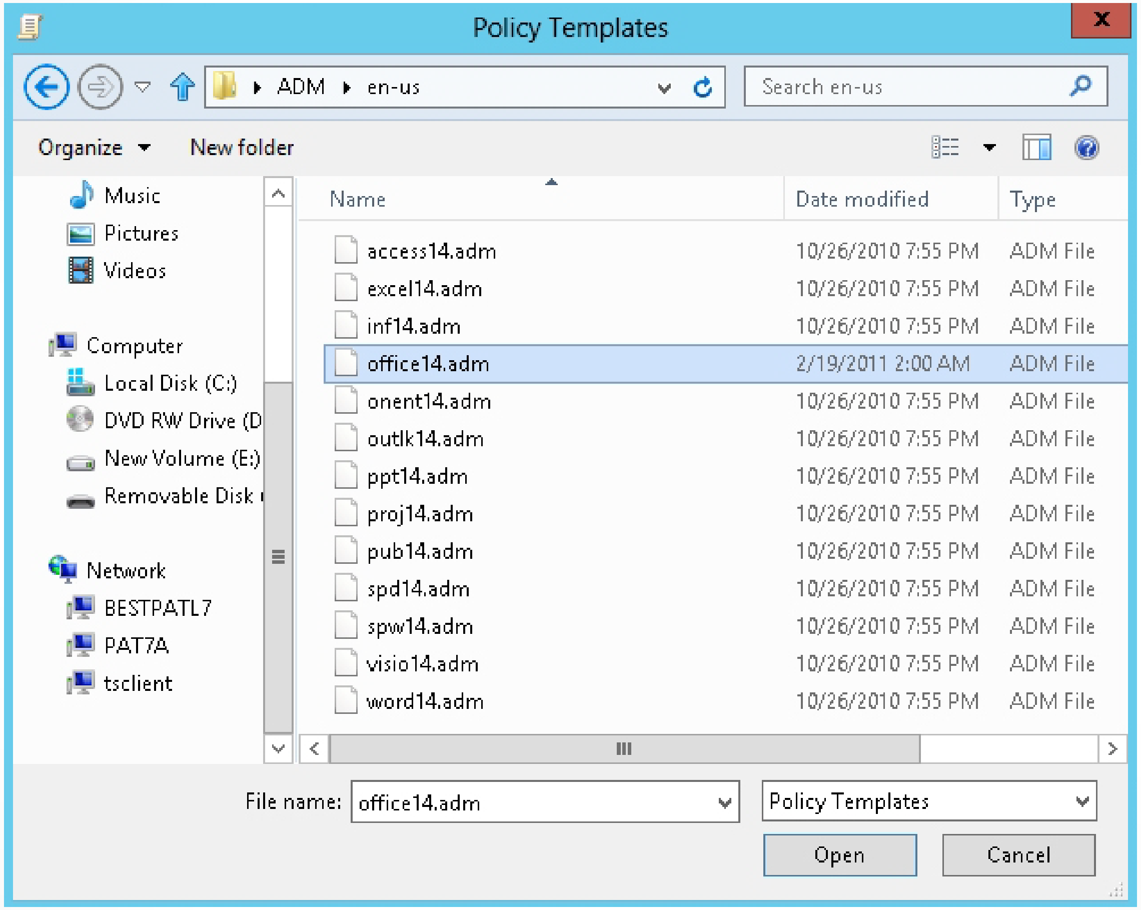
Add/Remove Templates

Current Policy Templates:

Name	Size	Modified

Opening the Add/Remove Templates dialog box

Add Custom ADM Administrative Template Files



Name	Date modified	Type
access14.adm	10/26/2010 7:55 PM	ADM File
excel14.adm	10/26/2010 7:55 PM	ADM File
inf14.adm	10/26/2010 7:55 PM	ADM File
office14.adm	2/19/2011 2:00 AM	ADM File
onent14.adm	10/26/2010 7:55 PM	ADM File
outlk14.adm	10/26/2010 7:55 PM	ADM File
ppt14.adm	10/26/2010 7:55 PM	ADM File
proj14.adm	10/26/2010 7:55 PM	ADM File
pub14.adm	10/26/2010 7:55 PM	ADM File
spd14.adm	10/26/2010 7:55 PM	ADM File
spw14.adm	10/26/2010 7:55 PM	ADM File
visio14.adm	10/26/2010 7:55 PM	ADM File
word14.adm	10/26/2010 7:55 PM	ADM File

File name: office14.adm

Policy Templates

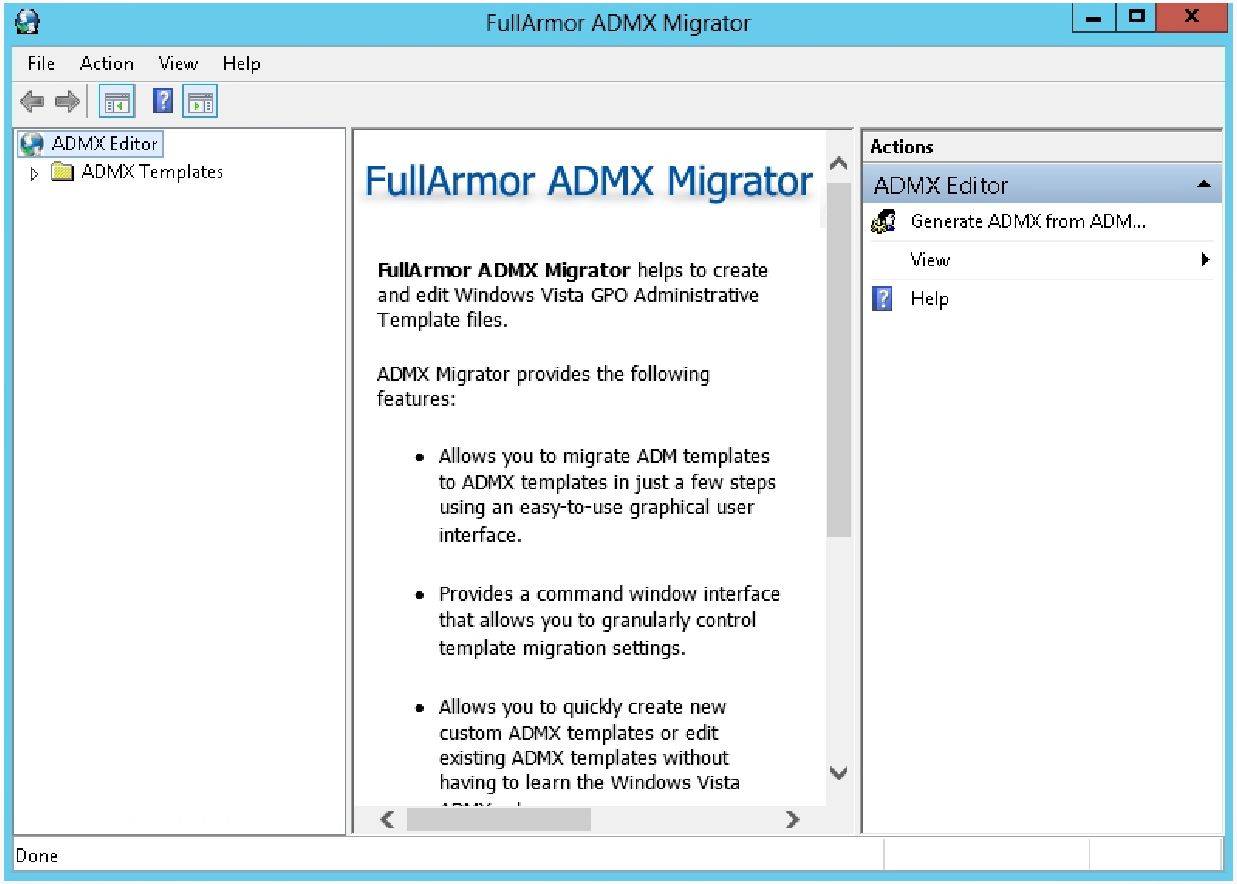
Navigating to and opening an ADM file

Using ADMX Migrator

ADMX Migrator:

- Is a snap-in for the MMC that simplifies the process of converting existing Group Policy ADM templates to the new ADMX format.
- Provides a graphical user interface for creating and editing Administrative Templates.

Use ADMX Editor to Migrate ADM Templates



FullArmor ADMX Migrator

FullArmor ADMX Migrator helps to create and edit Windows Vista GPO Administrative Template files.

ADMX Migrator provides the following features:

- Allows you to migrate ADM templates to ADMX templates in just a few steps using an easy-to-use graphical user interface.
- Provides a command window interface that allows you to granularly control template migration settings.
- Allows you to quickly create new custom ADMX templates or edit existing ADMX templates without having to learn the Windows Vista

Opening the ADMX Migrator

Property Filters for Administrative Templates

- By default, all policy settings are displayed.
- To narrow down the displayed list of settings, use ***Administrative Templates Property Filters***.

Property Filters for Administrative Templates

- To filter the settings displayed, select or deselect the following filter options:
  - Managed or Unmanaged
  - Configured or Not Configured
  - Keyword Filters
  - Requirements Filters

Lesson Summary

- Group Policies provides centralized management and configuration of operating systems, applications, and user settings.
- Windows Installer installs, maintains, and removes software on Windows.
- Installation information for software is stored in a Microsoft Software Installation (MSI) file.
- To deploy software with group policies, create a distribution point on the publishing server, create a GPO to use to distribute the software package, and assign or publish a package to a user or computer.
- Folder redirection allows you to redirect the content of a certain folder to a network location or to another location on the user's local computer.

Lesson Summary

- Starting with Windows Vista and Windows Server 2008, ADMX files define the settings that an administrator can configure through Group Policy.
- The Central Store is a folder structure created in the SYSVOL directory on the domain controllers in each domain in your organization.
- Security templates help you implement security settings quickly and efficiently.
- ADMX Migrator is a snap-in for the Microsoft Management Console (MMC) that simplifies the process of converting your existing Group Policy ADM templates to the new ADMX format and provides a graphical user interface for creating and editing Administrative Templates.