# Overview

Windows Server has several features that ease the configuration of security for user and computers. In this guided practice, you will explore the use of security templates and group policy in configuring workstation and user security.

# Objectives

* Explain the use of security templates to implement computer and user security
* Explain the security features available in Windows Server to secure information at rest and in transit.
* Be able to use security templates and group policy to implement a security plan

# Prerequisites

Guided practice – **Creating Active Directory Objects** is complete.

# Scenario

ABS Corporation is interested in leveraging Active Directory to enhance the security of their organization. They would like to use security templates and group policy to configure

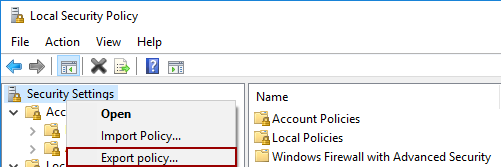
# Tasks

Security templates are text files that contain preconfigured settings used to secure a Windows workstation. The templates can be used to apply the settings to computers individually or to groups of computers using group policy.

## Exporting a Security Template

In most instances, you will not want to start from scratch when configuring security. You will want to take your existing security configuration and modify it to suit your needs. To do this you must first export your security configuration from an existing system so that you can later import it into a template.

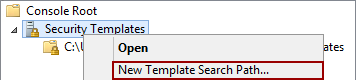
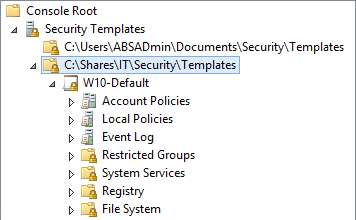
To export the security settings from an existing system, perform the following:

1. Login to the **CIS256-Client1** virtual machine as **Anna** **Duncan (**anduncan**).**
2. Open **File Explorer** andbrowse to the **IT** share on **ABSDC1.**
3. Create a folder called **Security.**
4. Create a folder called **Templates** in the folder you created above. This will be the location that you will used to hold the security templates for your organization
5. Open the **Local Security Policy** management console. You will need to **run as an administrator**.
6. Select the **Security Settings** node and **choose** the **Export Policy…** option from the context menu as shown in the figure.
7. Save the **template** as **W10-Default.inf** in the **Templates** folder you created above. **Note:** it will open in a templates folder on your local machine, this is not the right location. You need to save it to the folder that you created in the **IT** share on **ABSDC1**.
8. Close the **Local Security Policy** console.

## Creating and Saving a Security template

To create a group policy, you must first open an MMC console and add the security templates snap-in. Once this is done, you can configure security settings and save them for later use.

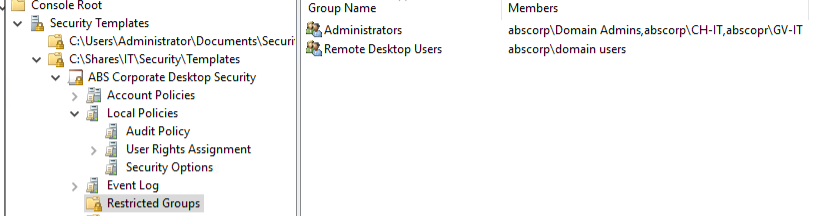
Create a security policy for **ABSCorp**

1. Login to the **CIS256-DC1** virtual machine with an administrative account
2. Open an **MMC** console and **add** the **Security Templates** snap-in.
3. Right-click the **Security Templates** node and select **New Template Search Path…** from the context menu as shown in the figure.
4. In the **Browse for Folder** dialog box, **browse** to the **C:\Shares\IT\Security\Templates** folder and click the **OK** button.
5. You should see the **W10-Default** template you created in the previous section as shown in the figure.
6. Right-click the **W10-Default** template and select **Save** **As…** from the context menu and **save** the policy **ABS Corporate Desktop Security**.

## Modifying a Security Template

Once you have the default security template for a workstation you can customize it for use in your organization.

To modify the template, perform the following:

1. In the **Security Templates** snap-in, in the **ABS Corporate Desktop Security** policy and configure the following:
   1. **Local Policies à Audit Policy à Audit object access,** configure this to audit success and failure events.
   2. **Security Options à Interactive Logon:** **Do not display last user name at sign-in** à **Enabled**
   3. **Security Options à Interactive Logon: Message text for users attempting to log onà** Access to this computer is only authorized for employees of ABS Corporation. By logging in to this computer you give ABS Corporation consent to monitor all actions that you perform.
   4. **Security Options à Interactive Logon: Message title for users attempting to log onà** Warning
   5. **Security Options à User Account Control: Admin Approval Mode for Built-in Administrator accountà** Enabled
   6. **Restricted Groups:**
      1. **Administrators**
         1. **Members:** abscorp\CH-IT,abscorp\GV-IT,abscorp\Domain Admins
      2. **Remote Desktop Users**
         1. **Members:** abscorp\domain users
   7. **System Services à Themes** à Disabled
2. Save the **policy**.

## Importing a Security template into a group policy

To apply these settings to a group of computers, you will need to import the security template into a Group Policy and link the policy to an OU that contains computer accounts.

**Note!!!**

**Follow these steps carefully. Failure to do so may render all your domain controllers inoperative**

**Hint**: Now is a good time to make checkpoints of all VMs used in the GPs.

To import the security template into a group policy, perform the following:

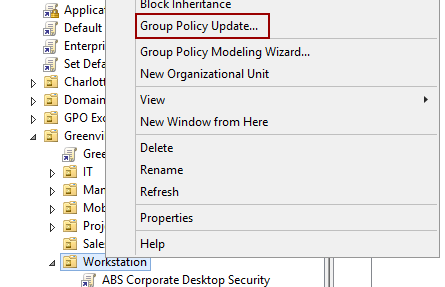
1. Login to the **CIS256-DC1** virtual machine with an administrative account
2. Open the **GPMC** and **create** a **new group policy object** named **ABS Corporate Desktop Security** in the **Group Policy Objects** node
3. Open the **policy** for editing.
4. Browse to the **Computer Configuration à Policies à Windows Settings.**
5. Right-Click the **Security Settings** node and select **Import Policy…** from the context menu.
6. Browse to the **ABS Corporate Desktop Security Policy** you just created and select **Open.**
7. Verify that the settings were imported.
8. Close the **Group Policy Management Editor**

## Verifying the Security settings

To make this policy work, you must now link it to an OU that contains computer accounts. Refresh the policy for that computer and verify the settings. To do this, perform the following:

1. Login to the **CIS256-DC1** virtual machine
2. Open the **GPMC.**
3. Link the **ABS** **Corporate Desktop Security** policy the **Greenville** **Workstation** OU.

**!!!WARNINGà Do not link this to the domain ßWarning!!!!**

1. Open **Active Directory Users and Computers**
2. Move the **DT1** computer account **to** the **Greenville Workstation** OU.
3. In the **GPMC**, select **Group Policy Update…** from the context menu of the **Greenville Workstation** OUto force the group policy to be updated on the computers in that OU. The firewall on **DT1** may block this. You can update the group policy locally when you login to the **CIS256-Client1**.
4. Restart **CIS256-Client1** VM and log in to verify the settings were applied.
   1. Verify the **Warning** message at logon
   2. Verify the **Themes** service is disabled
   3. Attempt to open **PowerShell** as Administrator and verify you receive the User Account Control prompt.
   4. Verify that **ABSCorp\CH-IT**, **ABSCorp\GV-IT**, and **ABSCorp\Domain Admins** are in the local administrators group.
   5. Verify that the Domain Users group is a member of the local **Remote Desktop Users** group.

## Submission requirements

1. **Download** the **grading** **script** from the assignment page to the **C:\Scripts** folder.
2. Check your lab by running the following command:

Invoke-Pester -Path C:\Scripts\GP17-Configuring\_Security\_ with\_Group\_Policy.test.ps1

**Note**: You will see a security warning when running the script. Enter **R** to run the script.

If you want to see more detail, add **-Output Detailed** to the command. This may assist you with troubleshooting

Invoke-Pester -Path C:\Scripts\GP17-Configuring\_Security\_ with\_Group\_Policy.test.ps1 -Output Detailed

1. You should not see any red in the output. Red in the PowerShell way of telling you that an error condition exists. Most of the time, the output will tell you what is wrong. If it is not obvious, contact your teacher and ask for assistance. You will be learning PowerShell during this term. **Correct** any **errors** you may have and run the script until all the output has no red. You should see the output like the images below. Text

   Description automatically generated
2. Capture a snippet that shows the PowerShell Command and all its output. If you must use more than one snippet to capture the output, you must have at least **one line of overlap** in the snippets. The text in the snippets **must be legible** when pasted into the Word document. Paste the snippet(s) into a **new** **Word** **document.** Save the file as **Security\_*Firstname*\_*LastName*** (where ***Firstname*** is your first name and ***Lastname*** is your last name).
3. **Upload** the **document** in the submission area of this assignment.