Implementing Endpoint Protection

(CompTIA Security + SY – 601)

Objectives:

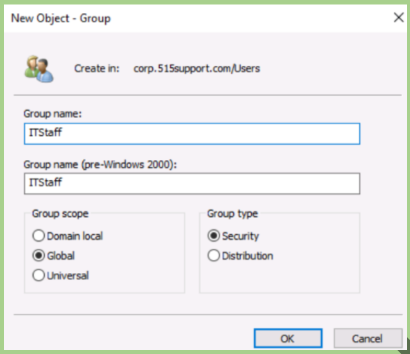
- To implement host or application security solutions

Resources:

- Windows Virtual Machine (DC1)

Instructions:

- Sign-in on the **DC1**VM
- From Server Manager, select **Tools > Active Directory Users and Computers**
- Right-click the **Users** container and select **New > Group**. In the Group name box, type **ITStaff** them select **OK**



New Object - Group

Create in: corp.515support.com/Users

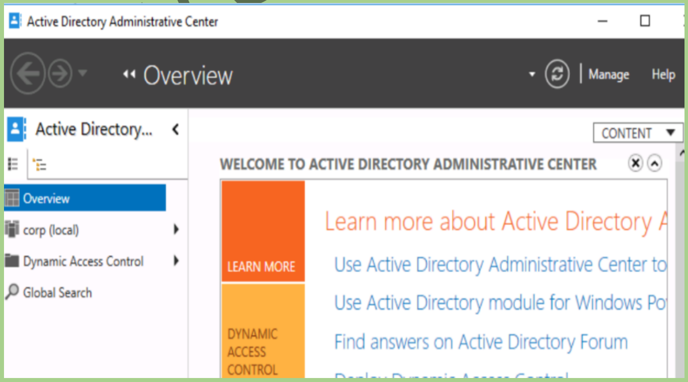
Group name: ITStaff

Group name (pre-Windows 2000): ITStaff

Group scope: ○ Domain local ● Global ○ Universal

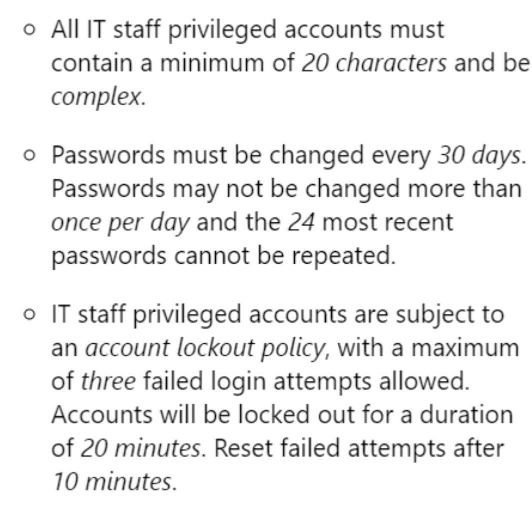
Group type: ● Security ○ Distribution

- Select the **Users** node **CTRL**+ click to select the **Domain Admins** and **LocalAdmin** objects, then right-click and select Add to a group. Type ITStaff group then select **OK**. Select **OK**
- Leave the Active Directory Users and Computers console open. From Server Manager, select **Tools > Active Directory Administrative Center**



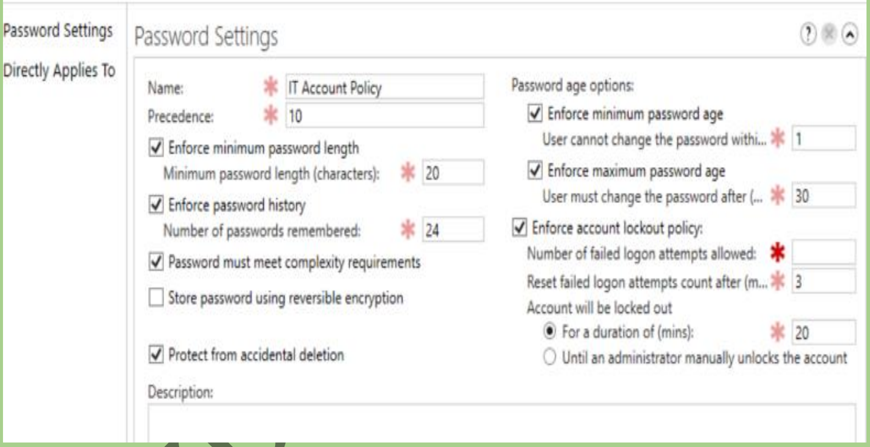
Active Directory Administrative Center
Overview
Manage
Help
Active Directory...
Overview
corp (local)
Dynamic Access Control
Global Search
CONTENT
WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER
LEARN MORE
Learn more about Active Directory A
Use Active Directory Administrative Center to
Use Active Directory module for Windows Po
Find answers on Active Directory Forum
DYNAMIC ACCESS CONTROL

- In the left-hand pane, select **corp (local)** in the main pane. **Select System > Password Settings Container**
- Review the following security policy summary for IT Staff user account password management



- All IT staff privileged accounts must contain a minimum of *20 characters* and be *complex*.
- Passwords must be changed every *30 days*. Passwords may not be changed more than *once per day* and the *24* most recent passwords cannot be repeated.
- IT staff privileged accounts are subject to an *account lockout policy*, with a maximum of *three* failed login attempts allowed. Accounts will be locked out for a duration of *20 minutes*. Reset failed attempts after *10 minutes*.

- Right-click some empty space and select **New > Password Settings**. Enter the name **IT Account Policy** and set a precedence level of 10 on the policy



Password Settings

Name: * IT Account Policy

Precedence: * 10

☑ Enforce minimum password length

Minimum password length (characters): * 20

☑ Enforce password history

Number of passwords remembered: * 24

☑ Password must meet complexity requirements

☐ Store password using reversible encryption

☑ Protect from accidental deletion

Description:

Password age options:

☑ Enforce minimum password age

User cannot change the password withi... * 1

☑ Enforce maximum password age

User must change the password after (... * 30

☑ Enforce account lockout policy:

Number of failed logon attempts allowed: *

Reset failed logon attempts count after (m... * 3

Account will be locked out

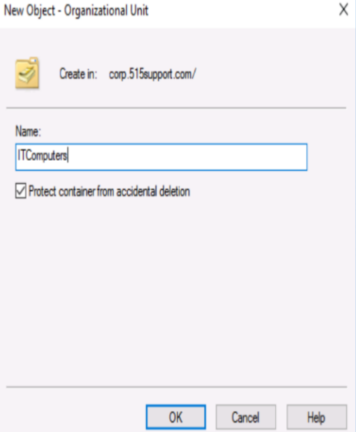
● For a duration of (mins): * 20

○ Until an administrator manually unlocks the account

- Configure settings that meet the requirements listed in the organization's security policy:
- Under Directly Applies, select the **Add** button.
- Type **ITStaff** then select **OK**
- Select **OK**
- Close the Active Directory Administrative Center

Implement GPO settings

- In the Active Directory Users and Computers console; right-click the **corp.515support.com** domain object. Select **New** and then create an OU for ITComputers

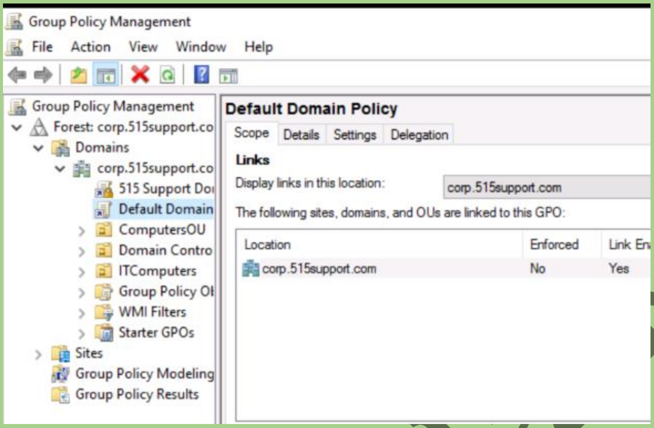

New Object - Organizational Unit

Create in: corp.515support.com/

Name: ITComputers

☑ Protect container from accidental deletion

- ➢ Close Active Directory Users and Computers
- ➢ From Server Manager, select **Tools > Group Policy Management**


Group Policy Management

Default Domain Policy

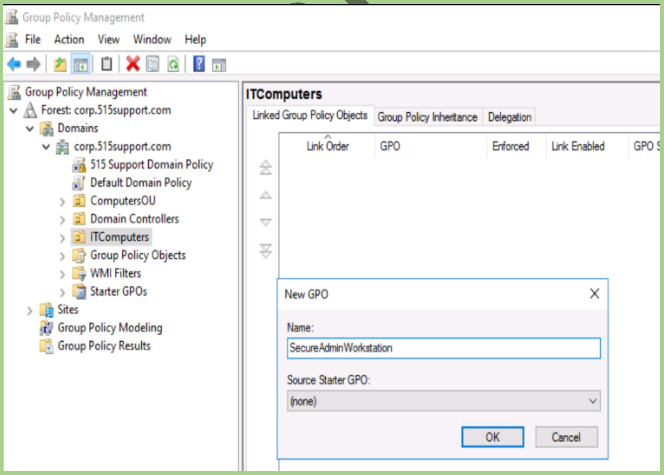
Links

Display links in this location: corp.515support.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link En
corp.515support.com	No	Yes

- ➢ Browse to the **corp.515support.com** object, right-click the **ITComputers** OU and select **Create a GPO in this domain and Link it here**. Name the new **GPO SecureAdminWorkstation**


Group Policy Management

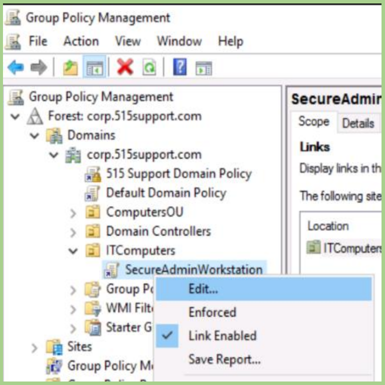
ITComputers

New GPO

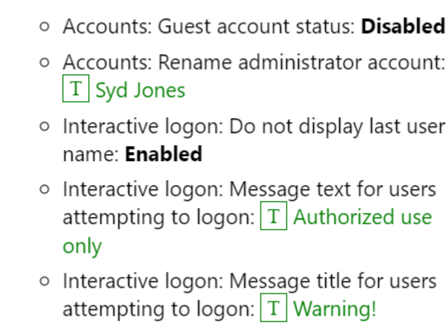
Name: SecureAdminWorkstation

Source Starter GPO: (none)

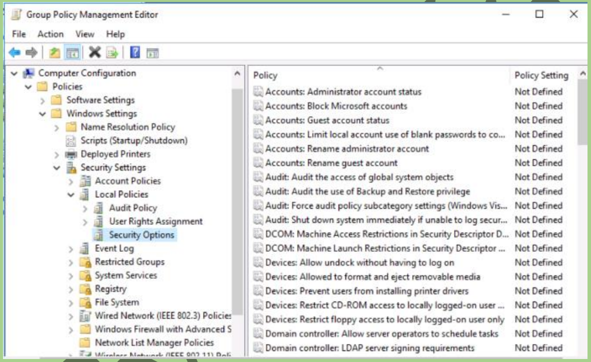
- Expand **ITComputers** OU, right-click the **SecureAdminWorkstation** OU, and then select **Edit**



- Browse to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options. Configure the following settings:

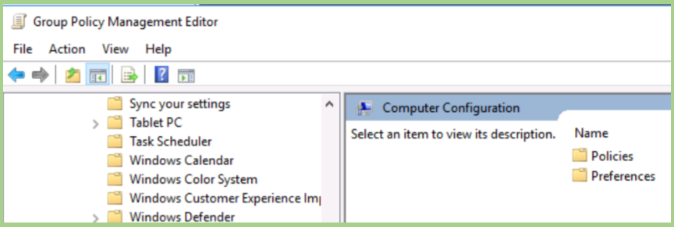


- Accounts: Guest account status: **Disabled**
- Accounts: Rename administrator account: T Syd Jones
- Interactive logon: Do not display last user name: **Enabled**
- Interactive logon: Message text for users attempting to logon: T Authorized use only
- Interactive logon: Message title for users attempting to logon: T Warning!

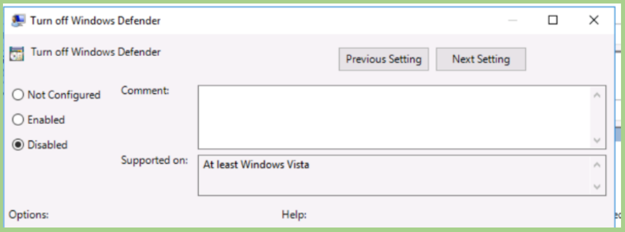


Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined

- In the navigation pane of the Group Policy Management Editor window, expand **Computer Configuration > Policies > Administrative Templates > Window Components > Windows Defender**



- ➢ In the detail pane, open Turn off windows Defender, read the help text in the **Turn off Windows Defender**, read the help text in the Turn off Windows Defender window, then select Disable and select **OK**



Turn off Windows Defender

Turn off Windows Defender

○ Not Configured
○ Enabled
● Disabled

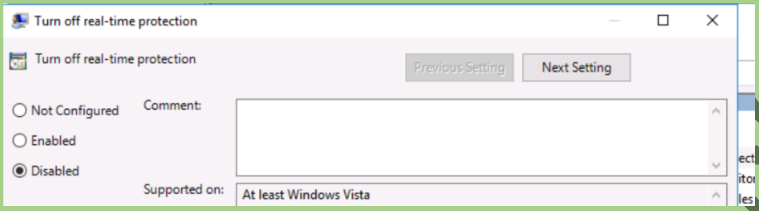
Comment:

Supported on: At least Windows Vista

Options:

Help:

- ➢ Within the same group of settings, set **Turn off routine remediation** to **Disable**
- ➢ Expand the Real-time Protection node within Windows Defender. Set **Turn off real-time protection** to **Disable**



Turn off real-time protection

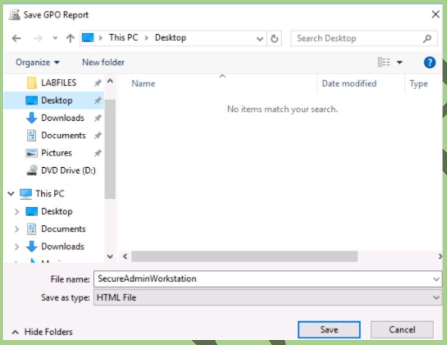
Turn off real-time protection

○ Not Configured
○ Enabled
● Disabled

Comment:

Supported on: At least Windows Vista

- ➢ Close the Group Policy Management
- ➢ In the Group Policy Management console, right-click the SecureAdminWorkstation GPO and select **Save Report**. Save the report to the desktop



Save GPO Report

No items match your search.

File name: SecureAdminWorkstation

Save as type: HTML File

- ➢ Close the Group Policy Management Editor

Observations:

- ➢ **Active Directory Configuration**: The ITStaff group was successfully created and populated with necessary administrative users.
- ➢ **Password Policy Implementation**: A new password policy, IT Account Policy, was created and applied to the ITStaff group to enforce security requirements.
- ➢ **Group Policy Management**: A new Organizational Unit (OU) named ITComputers was created, and a Group Policy Object (GPO) named SecureAdminWorkstation was linked to this OU.

- **Windows Defender Settings**: Specific settings within Windows Defender were configured to enhance endpoint protection, including disabling the option to turn off Windows Defender and ensuring real-time protection is enabled.
- **GPO Report**: A report of the SecureAdminWorkstation GPO was generated and saved, documenting the applied security settings.

Results:

- **Enhanced Security for Admin Accounts**: The application of the IT Account Policy improved the password management and security posture for IT administrative accounts.
- **Streamlined Group Policy Application**: The SecureAdminWorkstation GPO ensured consistent security settings across all computers within the ITComputers OU.
- **Active Directory Structure**: The creation of the ITComputers OU provided a dedicated space for managing IT-related computers and applying specific security policies.
- **Improved Endpoint Protection**: The adjustments to Windows Defender settings fortified the endpoint protection on all devices within the scope of the GPO.
- **Documented Security Configurations**: The GPO report provided a clear record of the security settings, aiding in future audits and compliance checks.

Conclusion:

The implementation of endpoint protection measures, including the configuration of password policies and Group Policy Objects, significantly enhanced the security of the IT infrastructure. These steps ensured a higher level of protection for administrative accounts and endpoints, creating a more secure environment. Ongoing reviews and updates, coupled with user training and advanced threat detection, will further bolster the organization's cybersecurity posture.

Future Work:

- **Regular Policy Reviews**: Periodically review and update the password and GPO settings to ensure they align with evolving security standards and organizational requirements.
- **Expand Endpoint Protection**: Investigate additional endpoint protection solutions and integrate them into the current security framework.
- **User Training Programs**: Develop and implement training programs for IT staff to ensure they are aware of and adhere to security policies and best practices.
- **Advanced Threat Detection**: Incorporate advanced threat detection and response tools to enhance the ability to detect and mitigate sophisticated cyber threats.
- **Compliance and Auditing**: Schedule regular compliance checks and security audits to ensure adherence to security policies and identify areas for improvement.