

# Guidance about how to configure protected accounts

---

 [learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts](https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts)

## In this article

---

Through Pass-the-hash (PtH) attacks, an attacker can authenticate to a remote server or service by using the underlying NTLM hash of a user's password (or other credential derivatives). Microsoft has previously [published guidance](#) to mitigate pass-the-hash attacks. Windows Server 2012 R2 includes new features to help mitigate such attacks further. For more information about other security features that help protect against credential theft, see [Credentials Protection and Management](#). This topic explains how to configure the following new features:

- [Protected Users](#)
- [Authentication policies](#)
- [Authentication policy silos](#)

There are additional mitigations built in to Windows 8.1 and Windows Server 2012 R2 to help protect against credential theft, which are covered in the following topics:

- [Restricted Admin mode for Remote Desktop](#)
- [LSA Protection](#)

## Protected Users

---

Protected Users is a new global security group to which you can add new or existing users. Windows 8.1 devices and Windows Server 2012 R2 hosts have special behavior with members of this group to provide better protection against credential theft. For a member of the group, a Windows 8.1 device or a Windows Server 2012 R2 host does not cache credentials that are not supported for Protected Users. Members of this group have no additional protection if they are logged on to a device that runs a version of Windows earlier than Windows 8.1.

Members of the Protected Users group who are signed-on to Windows 8.1 devices and Windows Server 2012 R2 hosts can *no longer* use:

- Default credential delegation (CredSSP) - plaintext credentials are not cached even when the **Allow delegating default credentials** policy is enabled
- Windows Digest - plaintext credentials are not cached even when they are enabled
- NTLM - NTOWF is not cached

- Kerberos long term keys - Kerberos ticket-granting ticket (TGT) is acquired at logon and cannot be re-acquired automatically
- Sign-on offline - the cached logon verifier is not created

If the domain functional level is Windows Server 2012 R2 , members of the group can no longer:

- Authenticate by using NTLM authentication
- Use Data Encryption Standard (DES) or RC4 cipher suites in Kerberos pre-authentication
- Be delegated by using unconstrained or constrained delegation
- Renew user tickets (TGTs) beyond the initial 4-hour lifetime

To add users to the group, you can use UI tools such as Active Directory Administrative Center (ADAC) or Active Directory Users and Computers, or a command-line tool such as Dismod group, or the Windows PowerShell Add-ADGroupMember cmdlet. Accounts for services and computers *should not* be members of the Protected Users group. Membership for those accounts provides no local protections because the password or certificate is always available on the host.

### Warning

The authentication restrictions have no workaround, which means that members of highly privileged groups such as the Enterprise Admins group or the Domain Admins group are subject to the same restrictions as other members of the Protected Users group. If all members of such groups are added to the Protected Users group, it is possible for all of those accounts to be locked out. You should never add all highly privileged accounts to the Protected Users group until you have thoroughly tested the potential impact.

Members of the Protected Users group must be able to authenticate by using Kerberos with Advanced Encryption Standards (AES). This method requires AES keys for the account in Active Directory. The built-in Administrator does not have an AES key unless the password was changed on a domain controller that runs Windows Server 2008 or later. Additionally, any account, which has a password that was changed at a domain controller that runs an earlier version of Windows Server, is locked out. Therefore, follow these best practices:

- Do not test in domains unless **all domain controllers run Windows Server 2008 or later**.
- **Change password** for all domain accounts that were created *before* the domain was created. Otherwise, these accounts cannot be authenticated.

- **Change password** for each user before adding the account to the Protected Users group or ensure that the password was changed recently on a domain controller that runs Windows Server 2008 or later.

## Requirements for using protected accounts

---

Protected accounts have the following deployment requirements:

- To provide client-side restrictions for Protected Users, hosts must run Windows 8.1 or Windows Server 2012 R2 . A user only has to sign-on with an account that is a member of a Protected Users group. In this case, the Protected Users group can be created by transferring the primary domain controller (PDC) emulator role to a domain controller that runs Windows Server 2012 R2 . After that group object is replicated to other domain controllers, the PDC emulator role can be hosted on a domain controller that runs an earlier version of Windows Server.
- To provide domain controller-side restrictions for Protected Users, that is to restrict usage of NTLM authentication, and other restrictions, the domain functional level must be Windows Server 2012 R2 . For more information about functional levels, see Understanding Active Directory Domain Services (AD DS) Functional Levels.

### Note

The builtin domain Administrator (**S-1-5-<domain>-500**) is always exempt from Authentication Policies, even when they are assigned to an Authentication Policy Silo.

## Troubleshoot events related to Protected Users

---

This section covers new logs to help troubleshoot events that are related to Protected Users and how Protected Users can impact changes to troubleshoot either ticket-granting tickets (TGT) expiration or delegation issues.

### New logs for Protected Users

---

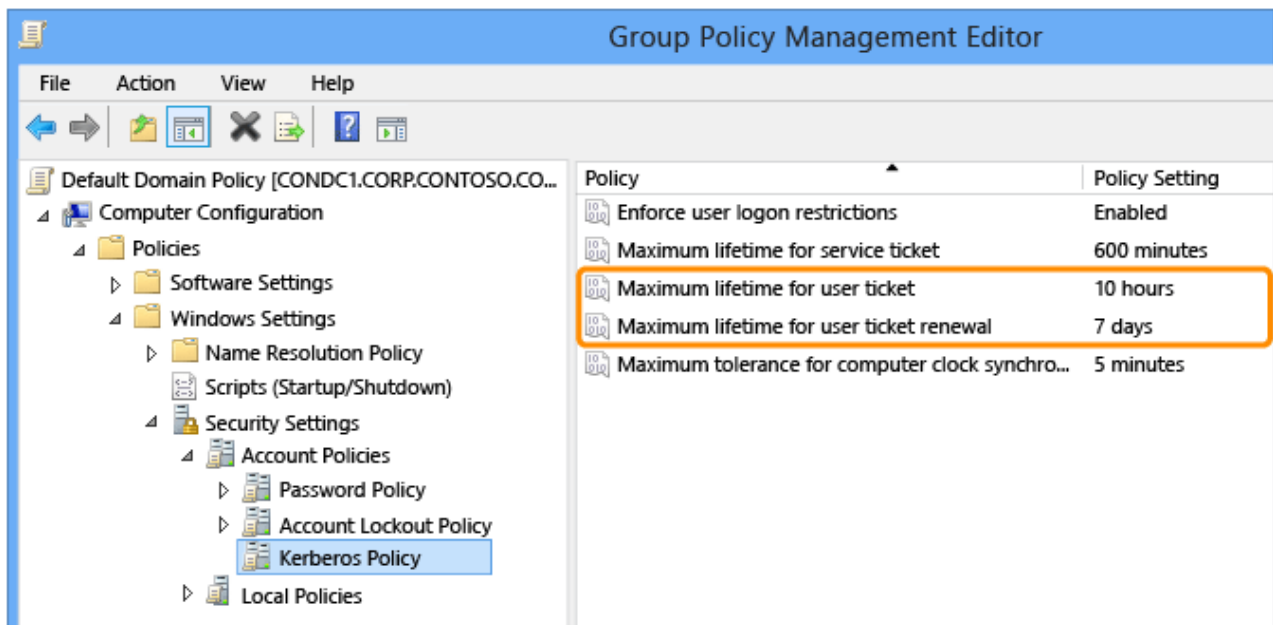
Two new operational administrative logs are available to help troubleshoot events that are related to Protected Users: Protected User - Client Log and Protected User Failures - Domain Controller Log. These new logs are located in Event Viewer and are disabled by default. To enable a log, click **Applications and Services Logs**, click **Microsoft**, click **Windows**, click **Authentication**, and then click the name of the log and click **Action** (or right-click the log) and click **Enable Log**.

For more information about events in these logs, see Authentication Policies and Authentication Policy Silos.

### Troubleshoot TGT expiration

---

Normally, the domain controller sets the TGT lifetime and renewal based on the domain policy as shown in the following Group Policy Management Editor window.

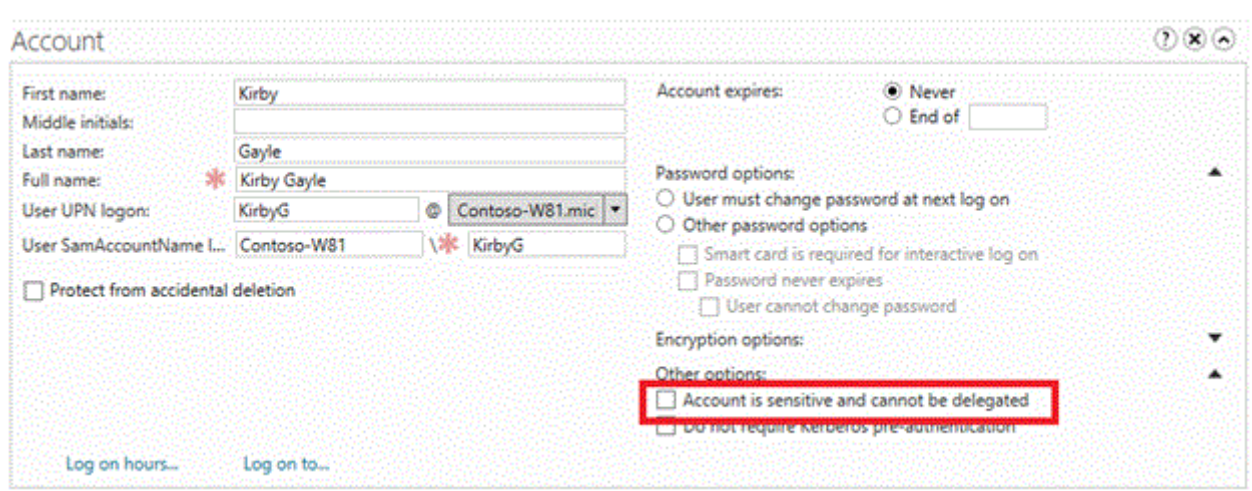


For **Protected Users**, the following settings are hard-coded:

- Maximum lifetime for user ticket: 240 minutes
- Maximum lifetime for user ticket renewal: 240 minutes

## Troubleshoot delegation issues

Previously, if a technology that uses Kerberos delegation was failing, the client account was checked to see if **Account is sensitive and cannot be delegated** was set. However, if the account is a member of **Protected Users**, it might not have this setting configured in Active Directory Administrative Center (ADAC). As a result, check the setting and group membership when you troubleshoot delegation issues.



## Audit authentication attempts

To audit authentication attempts explicitly for the members of the **Protected Users** group, you can continue to collect security log audit events or collect the data in the new operational administrative logs. For more information about these events, see [Authentication Policies and Authentication Policy Silos](#)

## Provide DC-side protections for services and computers

Accounts for services and computers cannot be members of **Protected Users**. This section explains which domain controller-based protections can be offered for these accounts:

- Reject NTLM authentication: Only configurable via [NTLM block policies](#)
- Reject Data Encryption Standard (DES) in Kerberos pre-authentication: Windows Server 2012 R2 domain controllers do not accept DES for computer accounts unless they are configured for DES only because every version of Windows released with Kerberos also supports RC4.
- Reject RC4 in Kerberos pre-authentication: not configurable.

### Note

Although it is possible to change the configuration of supported encryption types, it is not recommended to change those settings for computer accounts without testing in the target environment.

- Restrict user tickets (TGTs) to an initial 4-hour lifetime: Use Authentication Policies.
- Deny delegation with unconstrained or constrained delegation: To restrict an account, open Active Directory Administrative Center (ADAC) and select the **Account is sensitive and cannot be delegated** check box.

The screenshot shows the 'Account' settings page in ADAC. The account name is Kirby Gayle, with UPN KirbyG@Contoso-W81.mic. The 'Account expires' is set to 'Never'. Under 'Password options', 'User must change password at next log on' is selected. Under 'Encryption options', 'Do not require kerberos pre-authentication' is selected. In the 'Other options' section, the checkbox 'Account is sensitive and cannot be delegated' is highlighted with a red rectangle.

## Authentication policies

Authentication Policies is a new container in AD DS that contains authentication policy objects. Authentication policies can specify settings that help mitigate exposure to credential theft, such as restricting TGT lifetime for accounts or adding other claims-related conditions.

In Windows Server 2012 , Dynamic Access Control introduced an Active Directory forest-scope object class called Central Access Policy to provide an easy way to configure file servers across an organization. In Windows Server 2012 R2 , a new object class called Authentication Policy (objectClass msDS-AuthNPolicies) can be used to apply authentication configuration to account classes in Windows Server 2012 R2 domains. Active Directory account classes are:

- User
- Computer
- Managed Service Account and group Managed Service Account (GMSA)

## Quick Kerberos refresher

---

The Kerberos authentication protocol consists of three types of exchanges, also known as subprotocols:

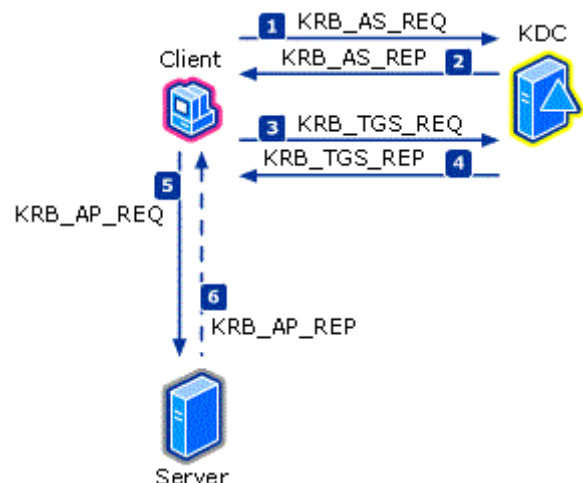
- The Authentication Service (AS) Exchange (KRB\_AS\_\*)
- The Ticket-Granting Service (TGS) Exchange (KRB\_TGS\_\*)
- The Client/Server (AP) Exchange (KRB\_AP\_\*)

The AS exchange is where the client uses the account's password or private key to create a pre-authenticator to request a ticket-granting ticket (TGT). This happens at user sign-on or the first time a service ticket is needed.

The TGS exchange is where the account's TGT is used to create an authenticator to request a service ticket. This happens when an authenticated connection is needed.

The AP exchange occurs as typically as data inside the application protocol and is not impacted by authentication policies.

For more detailed information, see [How the Kerberos Version 5 Authentication Protocol Works](#).



## Overview

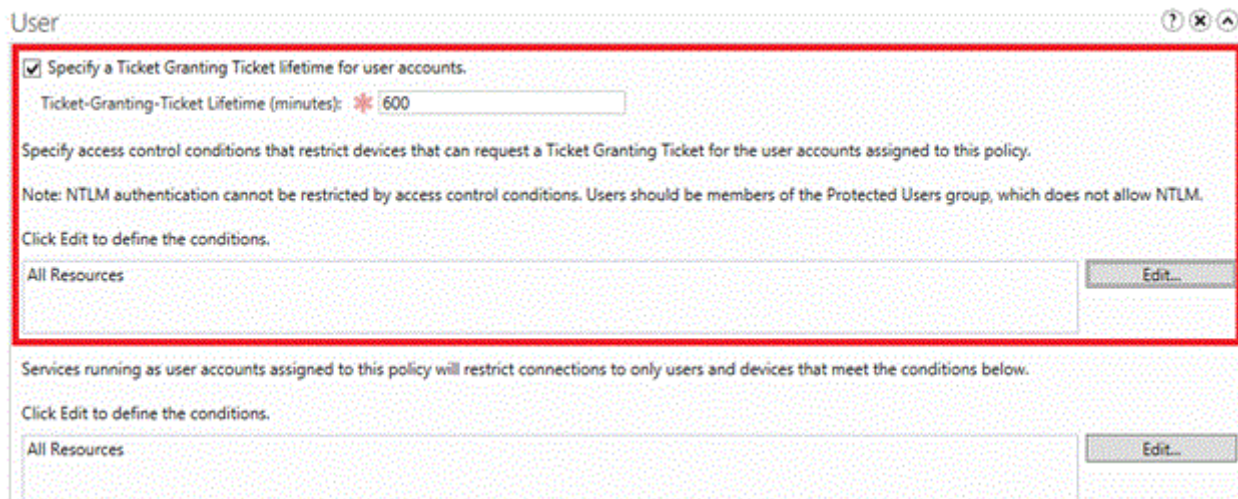
---

Authentication policies complement Protected Users by providing a way to apply configurable restrictions to accounts and by providing restrictions for accounts for services and computers. Authentication policies are enforced during either the AS exchange or the TGS exchange.



You can restrict initial authentication or the AS exchange by configuring:

- A TGT lifetime
- Access control conditions to restrict user sign-on, which must be met by devices from which the AS exchange is coming



The screenshot shows the 'User' tab in the Group Policy Management console. A red box highlights the 'Specify a Ticket Granting Ticket lifetime for user accounts' checkbox, which is checked. Below it, the 'Ticket-Granting-Ticket Lifetime (minutes)' is set to 600. The 'Access control conditions' section is also visible, showing 'All Resources' and an 'Edit...' button.

You can restrict service ticket requests through a ticket-granting service (TGS) exchange by configuring:

Access control conditions which must be met by the client (user, service, computer) or device from which the TGS exchange is coming

## Requirements for using authentication policies

Policy	Requirements
Provide custom TGT lifetimes	Windows Server 2012 R2 domain functional level account domains
Restrict user sign-on	<ul style="list-style-type: none"><li>- Windows Server 2012 R2 domain functional level account domains with Dynamic Access Control support</li><li>- Windows 8, Windows 8.1, Windows Server 2012 or Windows Server 2012 R2 devices with Dynamic Access Control support</li></ul>
Restrict service ticket issuance that is based on user account and security groups	Windows Server 2012 R2 domain functional level resource domains
Restrict service ticket issuance based on user claims or device account, security groups, or claims	Windows Server 2012 R2 domain functional level resource domains with Dynamic Access Control support

## Restrict a user account to specific devices and hosts

A high-value account with administrative privilege should be a member of the **Protected Users** group. By default, no accounts are members of the **Protected Users** group. Before you add accounts to the group, configure domain controller support and create an audit policy to ensure that there are no blocking issues.

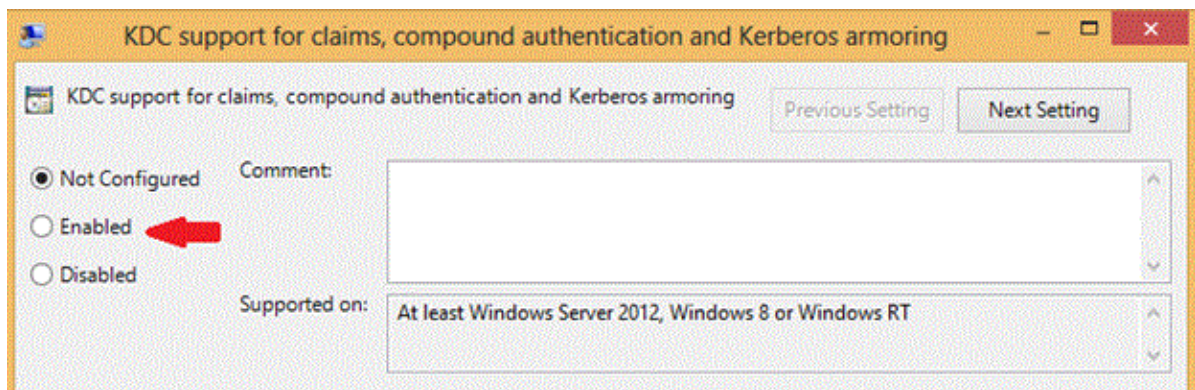
## Configure domain controller support

---

The user's account domain must be at Windows Server 2012 R2 domain functional level (DFL). Ensure all the domain controllers are Windows Server 2012 R2 , and then use Active Directory Domains and Trusts to raise the DFL to Windows Server 2012 R2 .

## To configure support for Dynamic Access Control

1. In the Default Domain Controllers Policy, click **Enabled** to enable **Key Distribution Center (KDC) client support for claims, compound authentication and Kerberos armoring** in Computer Configuration | Administrative Templates | System | KDC.

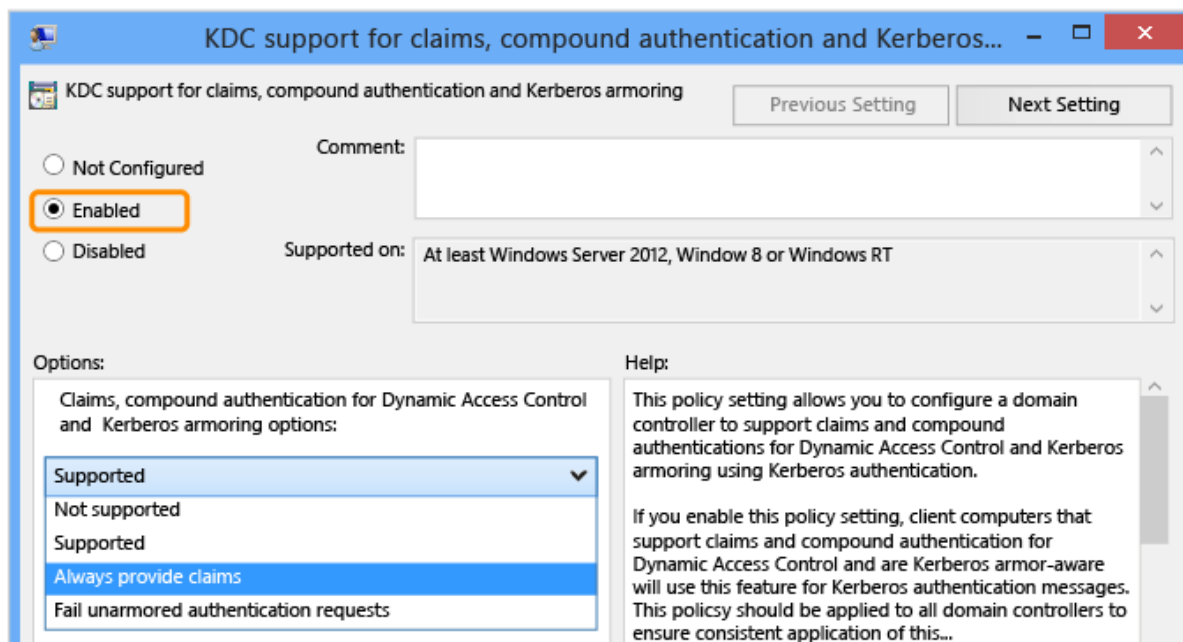




2. Under **Options**, in the drop-down list box, select **Always provide claims**.

Note

**Supported** can also be configured, but because the domain is at Windows Server 2012 R2 DFL, having the DCs always provide claims will allow user claims-based access checks to occur when using non-claims aware devices and hosts to connect to claims-aware services.



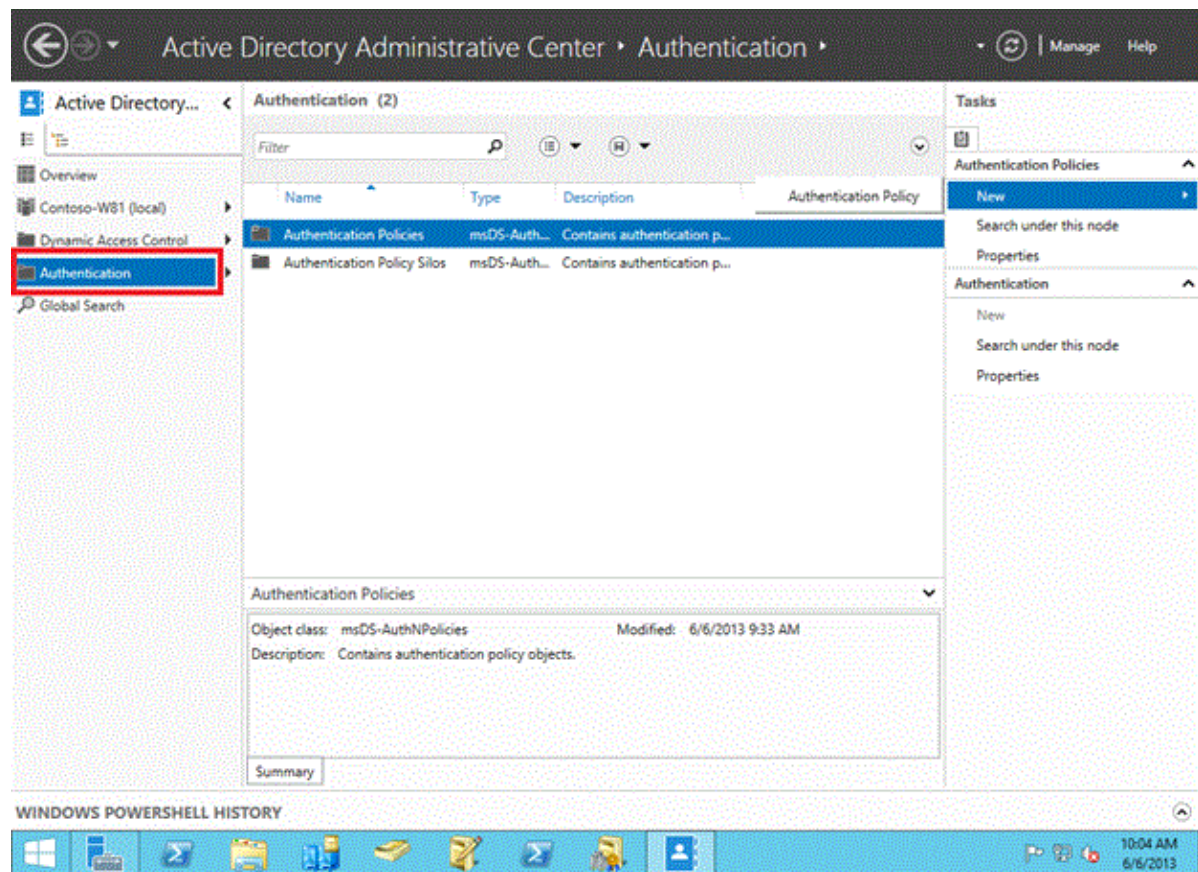
Warning

Configuring **Fail unarmored authentication requests** will result in authentication failures from any operating system which does not support Kerberos armoring, such as Windows 7 and previous operating systems, or operating systems beginning with Windows 8, which have not been explicitly configured to support it.

## Create a user account audit for authentication policy with ADAC

---

1. Open Active Directory Administrative Center (ADAC).



#### Note

The selected **Authentication** node is visible for domains which are at Windows Server 2012 R2 DFL. If the node does not appear, then try again by using a domain administrator account from a domain that is at Windows Server 2012 R2 DFL.

2. Click **Authentication Policies**, and then click **New** to create a new policy.

**Create Authentication Policy:**

**General**

An authentication policy defines the Kerberos Ticket Granting Ticket properties and authentication access control conditions for an account type.

Display name: \*

Description:

☒ Protect from accidental deletion

☐ Only audit policy restrictions

☒ Enforce policy restrictions

Note: Audit policy applied through a silo will override the policy settings of

**Accounts**

Name	Account Type
------	--------------

Add...

Remove

**Assigned Silos**

This authentication policy is not assigned to any authentication policy silos.

More Information

OK Cancel

Authentications Policies must have a display name and are enforced by default.

3. To create an audit-only policy, click **Only audit policy restrictions**.

**Create Authentication Policy: Widget Service Admins**

**General**

An authentication policy defines the Kerberos Ticket Granting Ticket properties and authentication access control conditions for an account type.

Display name: \* Widget Service Admins

Description:

☒ Only audit policy restrictions

☐ Enforce policy restrictions

Note: Audit policy applied through a silo will override the policy settings of t

☒ Protect from accidental deletion

Authentication policies are applied based on the Active Directory account type. A single policy can apply to all three account types by configuring settings for each type. Account types are:

- User
- Computer
- Managed Service Account and Group Managed Service Account

If you have extended the schema with new principals that can be used by the Key Distribution Center (KDC), then the new account type is classified from the closest derived account type.

4. To configure a TGT lifetime for user accounts, select the **Specify a Ticket-Granting Ticket lifetime for user accounts** check box and enter the time in minutes.

User

☒ Specify a Ticket-Granting Ticket lifetime for user accounts.

Ticket-Granting-Ticket Lifetime (minutes): 600

Specify access control conditions that restrict devices that can request a Ticket Granting Ticket for the user accounts assigned to this policy.

Note: NTLM authentication cannot be restricted by access control conditions. Users should be members of the Protected Users group, which does not allow NTLM.

Click Edit to define the conditions.

All Resources Edit...

Services running as user accounts assigned to this policy will restrict connections to only users and devices that meet the conditions below.

Click Edit to define the conditions.

All Resources Edit...

For example, if you want a 10-hour maximum TGT lifetime, enter **600** as shown. If no TGT lifetime is configured, then if the account is a member of the **Protected Users** group, the TGT lifetime and renewal is 4 hours. Otherwise, TGT lifetime and renewal are based on the domain policy as seen in the following Group Policy Management Editor window for a domain with default settings.

Group Policy Management Editor

File Action View Help

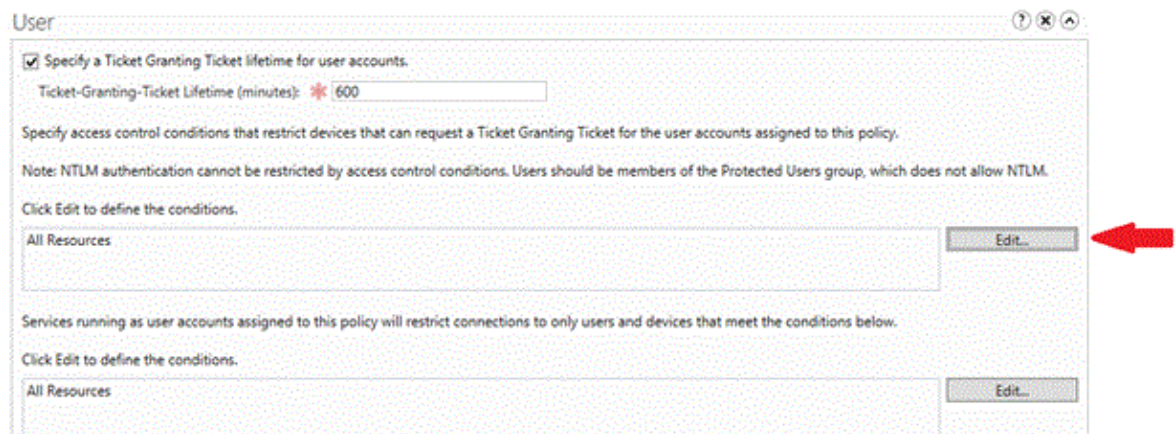
Default Domain Policy [CONDC1.CORP.CONTOSO.CO...]

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
          - Kerberos Policy
        - Local Policies

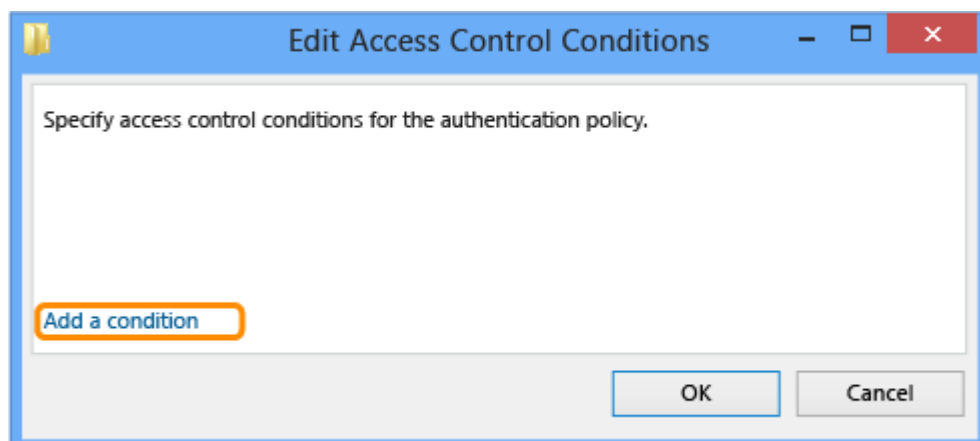
Policy	Policy Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchro...	5 minutes



5. To restrict the user account to select devices, click **Edit** to define the conditions that are required for the device.

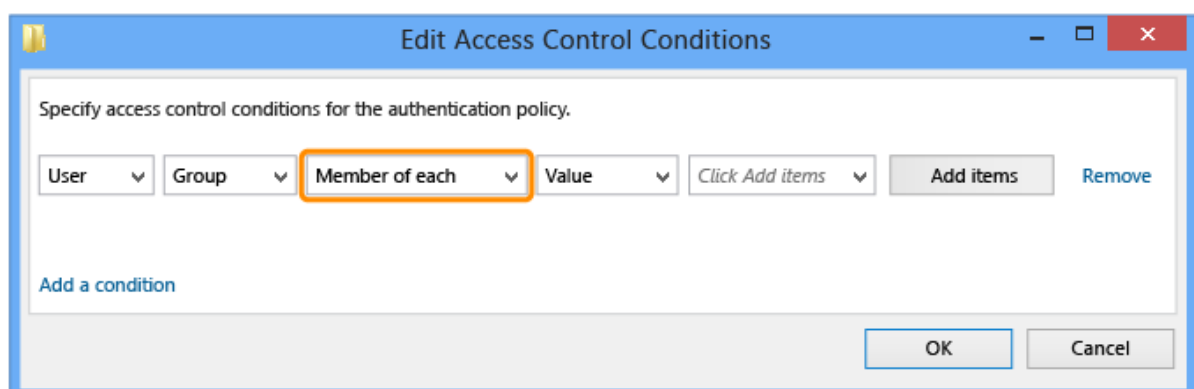


6. In the **Edit Access Control Conditions** window, click **Add a condition**.



Add computer account or group conditions

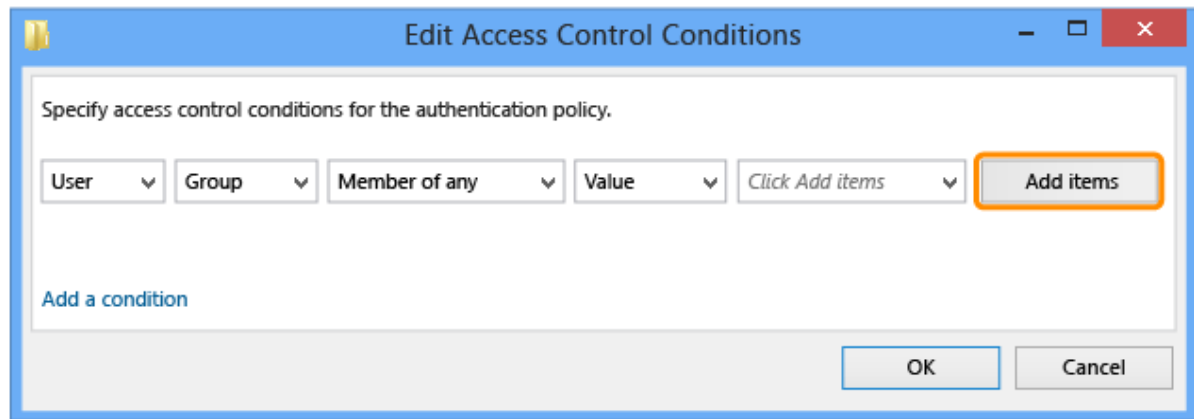
1. To configure computer accounts or groups, in the drop-down list, select the drop-down list box **Member of each** and change to **Member of any**.



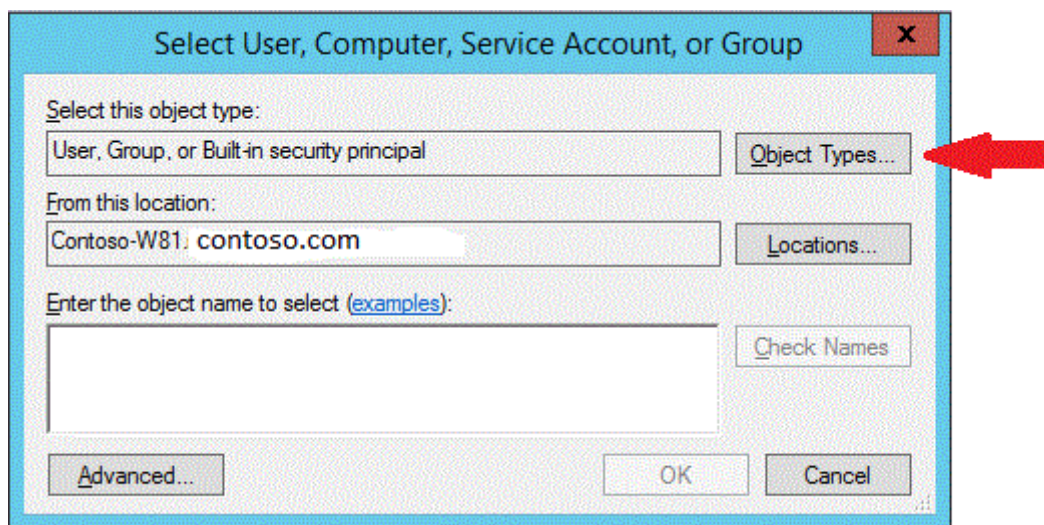
#### Note

This access control defines the conditions of the device or host from which the user signs on. In access control terminology, the computer account for the device or host is the user, which is why **User** is the only option.

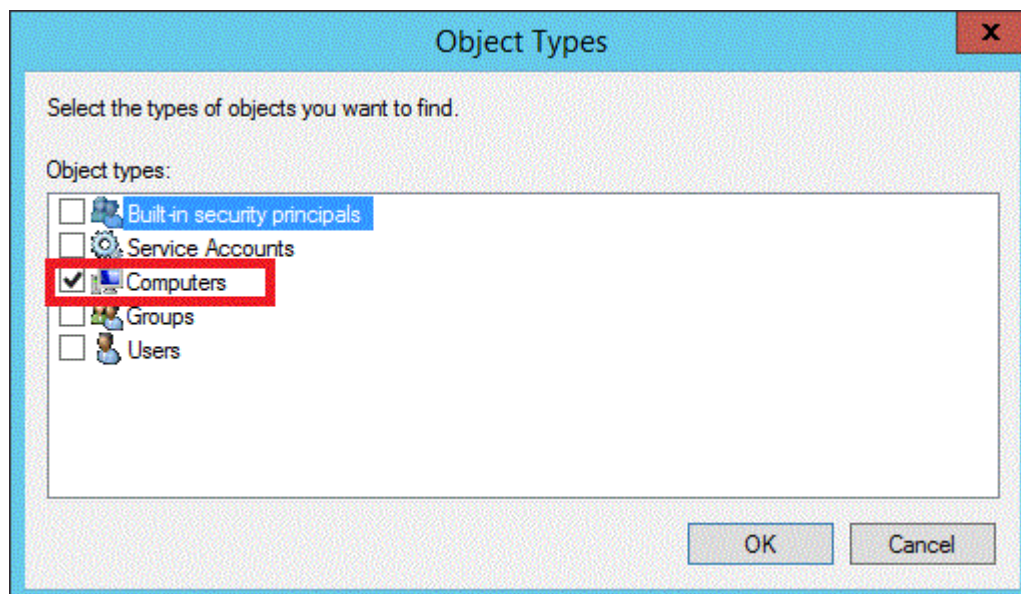
2. Click **Add items**.



3. To change object types, click **Object Types**.

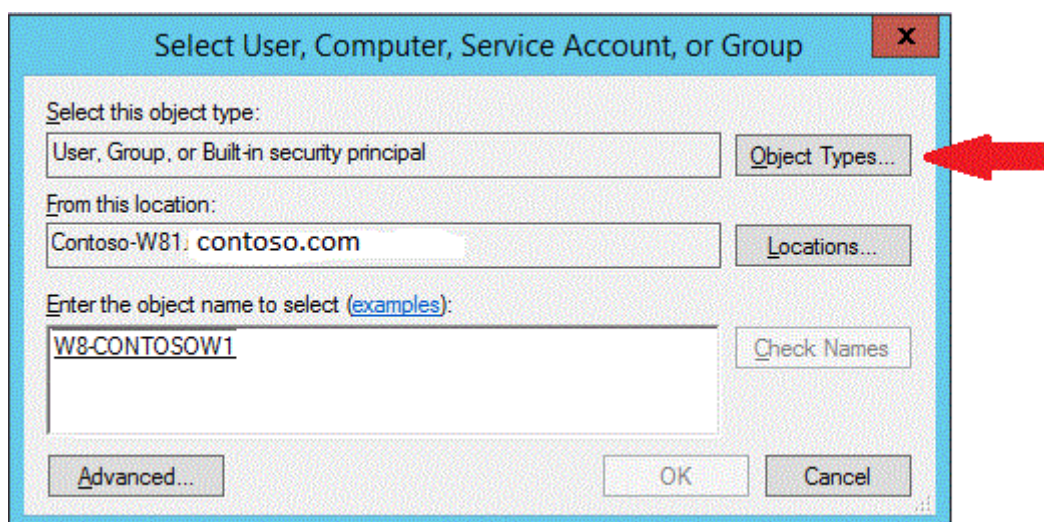


4. To select computer objects in Active Directory, click **Computers**, and then click **OK**.

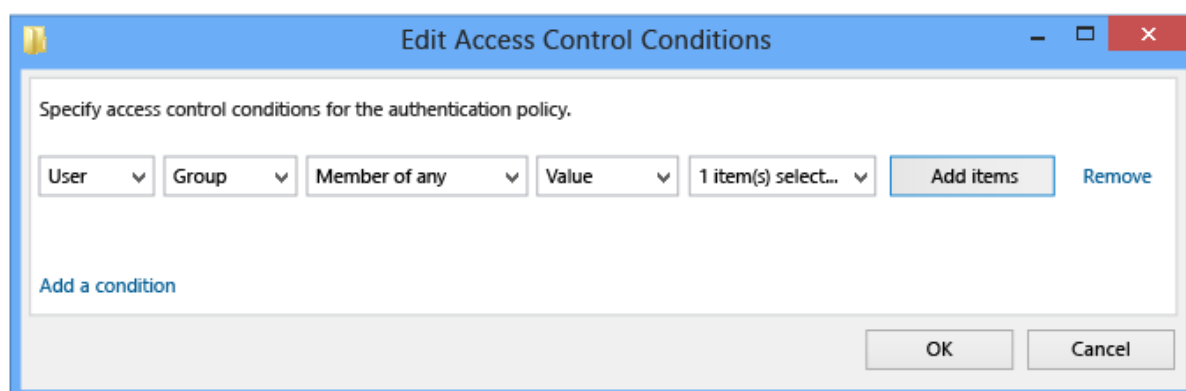




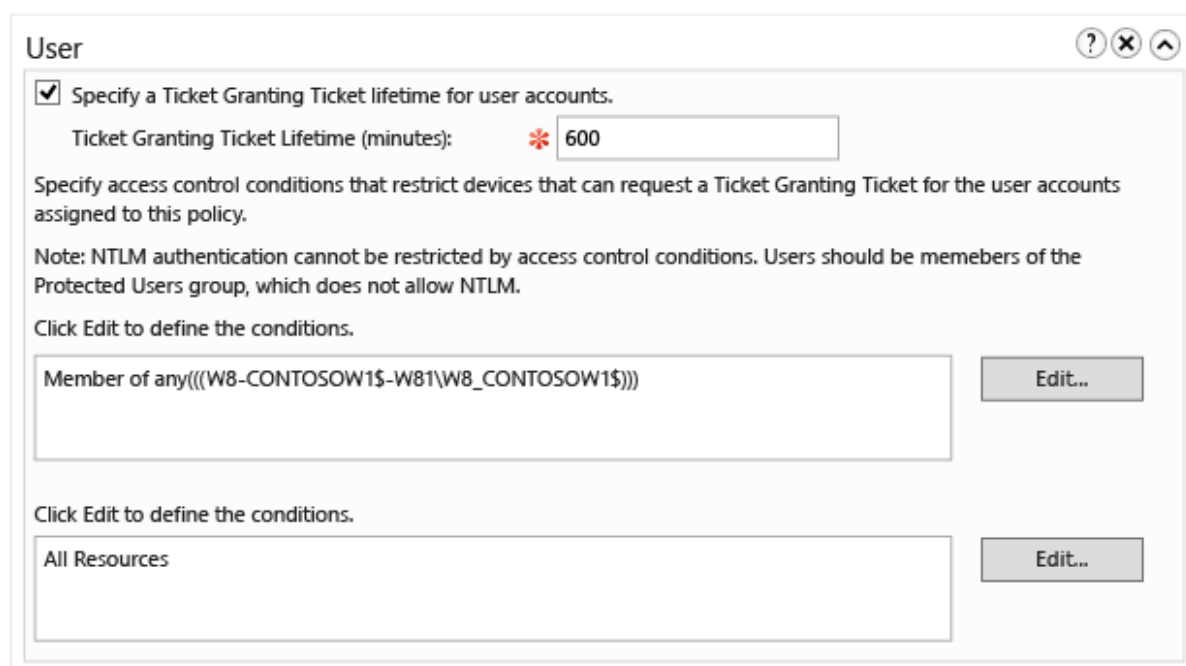
5. Type the name of the computers to restrict the user, and then click **Check Names**.



6. Click OK and create any other conditions for the computer account.

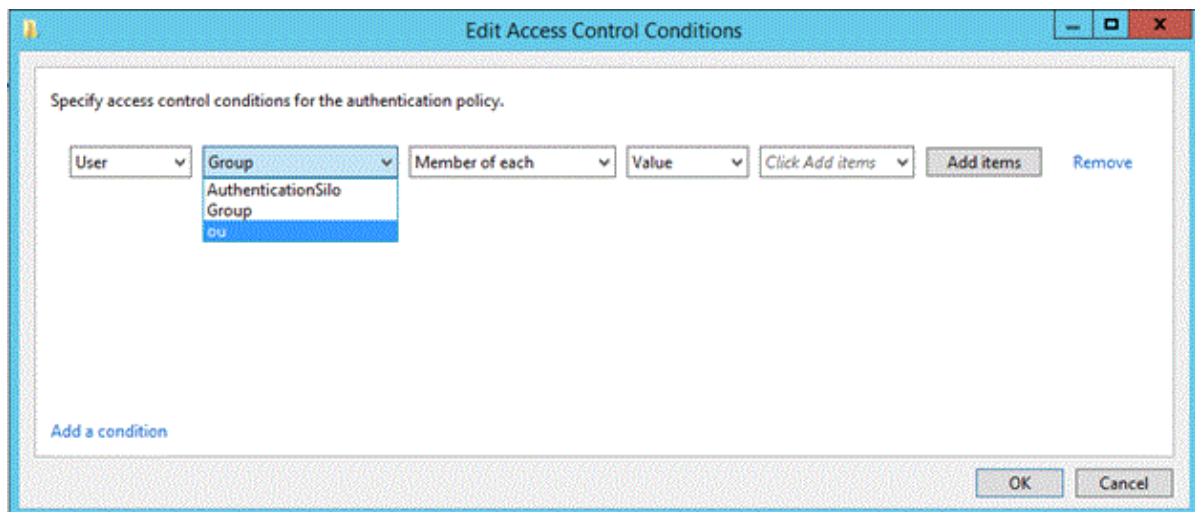


7. When done, then click **OK** and the defined conditions will appear for the computer account.



Add computer claim conditions

1. To configure computer claims, drop-down Group to select the claim.



Specify access control conditions for the authentication policy.

User Group Member of each Value Click Add items Add items Remove

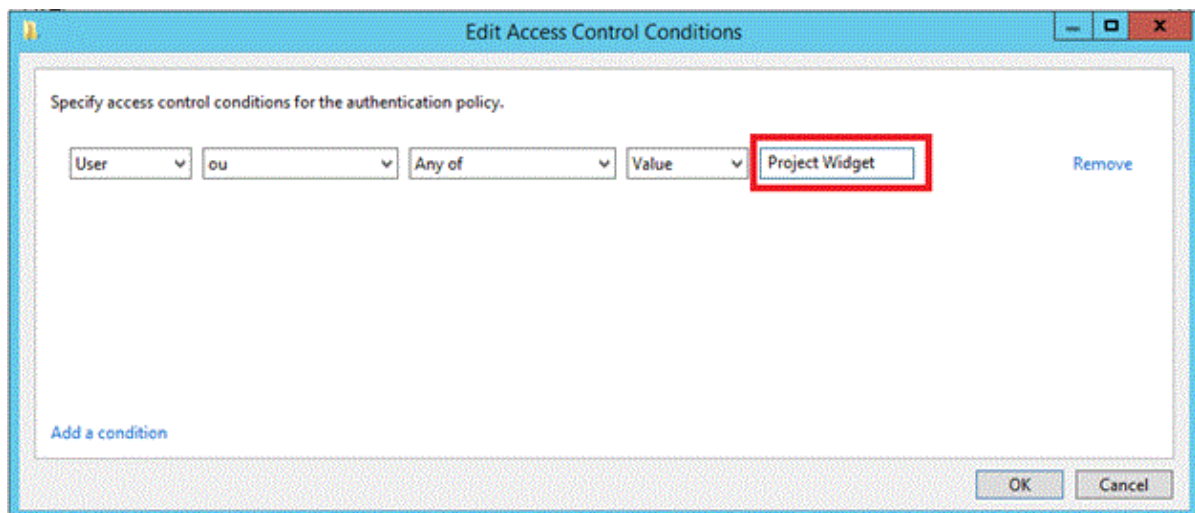
AuthenticationSilo  
Group  
ou

Add a condition

OK Cancel

Claims are only available if they are already provisioned in the forest.

2. Type the name of OU, the user account should be restricted to sign on.



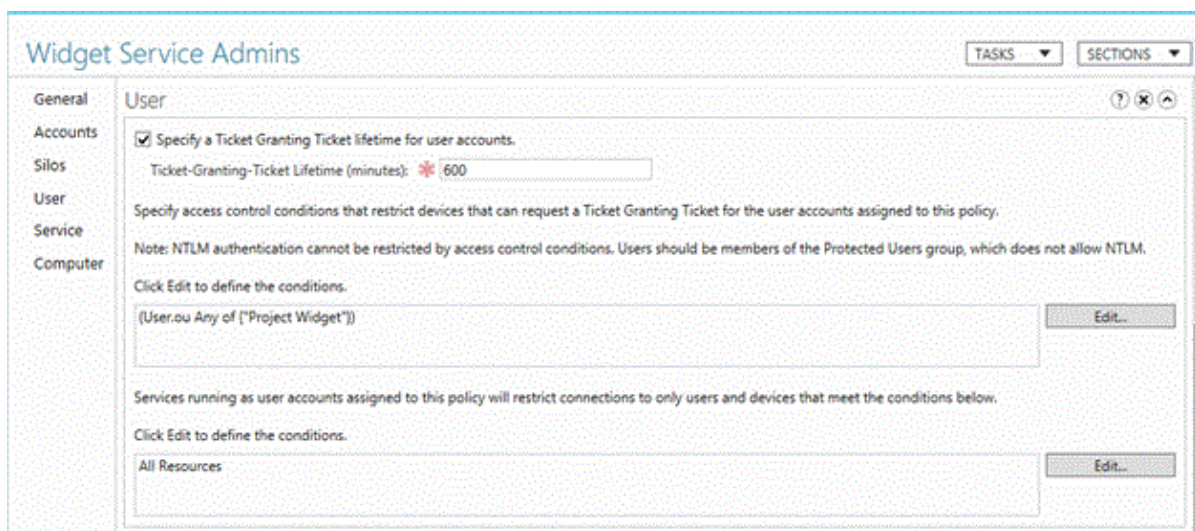
Specify access control conditions for the authentication policy.

User ou Any of Value Project Widget Remove

Add a condition

OK Cancel

3. When done, then click OK and the box will show the conditions defined.



Widget Service Admins

TASKS SECTIONS

General User

Accounts

Silos

User

Service

Computer

☒ Specify a Ticket Granting Ticket lifetime for user accounts.

Ticket-Granting-Ticket Lifetime (minutes): 600

Specify access control conditions that restrict devices that can request a Ticket Granting Ticket for the user accounts assigned to this policy.

Note: NTLM authentication cannot be restricted by access control conditions. Users should be members of the Protected Users group, which does not allow NTLM.

Click Edit to define the conditions.

(User.ou Any of ["Project Widget"])

Edit...

Services running as user accounts assigned to this policy will restrict connections to only users and devices that meet the conditions below.

Click Edit to define the conditions.

All Resources

Edit...

Troubleshoot missing computer claims



If the claim has been provisioned, but is not available, it might only be configured for **Computer** classes.

Let's say you wanted to restrict authentication based on the organizational unit (OU) of the computer, which was already configured, but only for **Computer** classes.

The screenshot shows the 'Create Claim Type' dialog for the claim type 'ou'. The 'Source Attribute' section is active, showing a list of AD attributes. The 'ou' attribute is selected. The 'Display name' is 'ou' and the 'Description' is 'Organizational-Unit-Name'. The 'Claims of this type can be issued for the following classes' section shows 'Computer' selected with a red arrow pointing to it.

Display Name	Value Type	Belongs To (CL...	ID
msTSLSP...	Multi-Valued S...	user, computer	MS-TSLSP...
msTSProperty01	Multi-Valued S...	user, computer	MS-TS-Property01
msTSProperty02	Multi-Valued S...	user, computer	MS-TS-Property02
msTSSecondar...	Multi-Valued S...	user, computer	ms-TS-Secondary...
netbootMirror...	Multi-Valued S...	computer	Netboot-Mirror-D...
netbootSIFFile	Multi-Valued S...	computer	Netboot-SIF-File
ou	Multi-Valued S...	user, computer	Organizational-Un...
o	Multi-Valued S...	user, computer	Organization-Nam...

For the claim to be available to restrict User sign-on to the device, select the **User** check box.

The screenshot shows the 'Create Claim Type' dialog for the claim type 'ou'. The 'Source Attribute' section is active, showing a list of AD attributes. The 'ou' attribute is selected. The 'Display name' is 'ou' and the 'Description' is 'Organizational-Unit-Name'. The 'Claims of this type can be issued for the following classes' section shows both 'User' and 'Computer' selected with red arrows pointing to them.

Display Name	Value Type	Belongs To (CL...	ID
operatingSyste...	String	computer	Operating-System
operatorCount	Integer	user, computer	Operator-Count
ou	Multi-Valued S...	user, computer	Organizational-Un...
o	Multi-Valued S...	user, computer	Organization-Nam...
otherLoginWor...	Multi-Valued S...	user, computer	Other-Login-Work...
otherMailbox	Multi-Valued S...	user, computer	Other-Mailbox
middleName	String	user, computer	Other-Name
personalTitle	String	user, computer	Personal-Title

## Provision a user account with an authentication policy with ADAC

1. From the **User** account, click **Policy**.

Kirby Gayle

Account

Organization

Member Of

Password Settings

Profile

**Policy**

Silo

Extensions

Account

First name: Kirby

Middle initials:

Last name: Gayle

Full name: Kirby Gayle

User UPN logon: KirbyG

User SamAccountName L... Contoso-WB1 KirbyG

Account expires: ☒ Never ☐ End of

Password options:

☐ User must change password at next log on

☐ Other password options

☐ Smart card is required for interactive log on

☐ Password never expires

☐ User cannot change password

Encryption options:

Other options:

Log on hours... Log on to...

2. Select the **Assign an authentication policy to this account** check box.

Kirby Gayle

Account

Organization

Member Of

Password Settings

Authentication Policy

☐ Assign an authentication policy to this account.

Authentication Policy (if not member of a Silo):

3. Then select the authentication policy to apply to the user.

Kirby Gayle

Account

Organization

Member Of

Password Sett...

Profile

Authentication Policy

☒ Assign an authentication policy to this account.

\* Authentication Policy (if not member of a Silo):

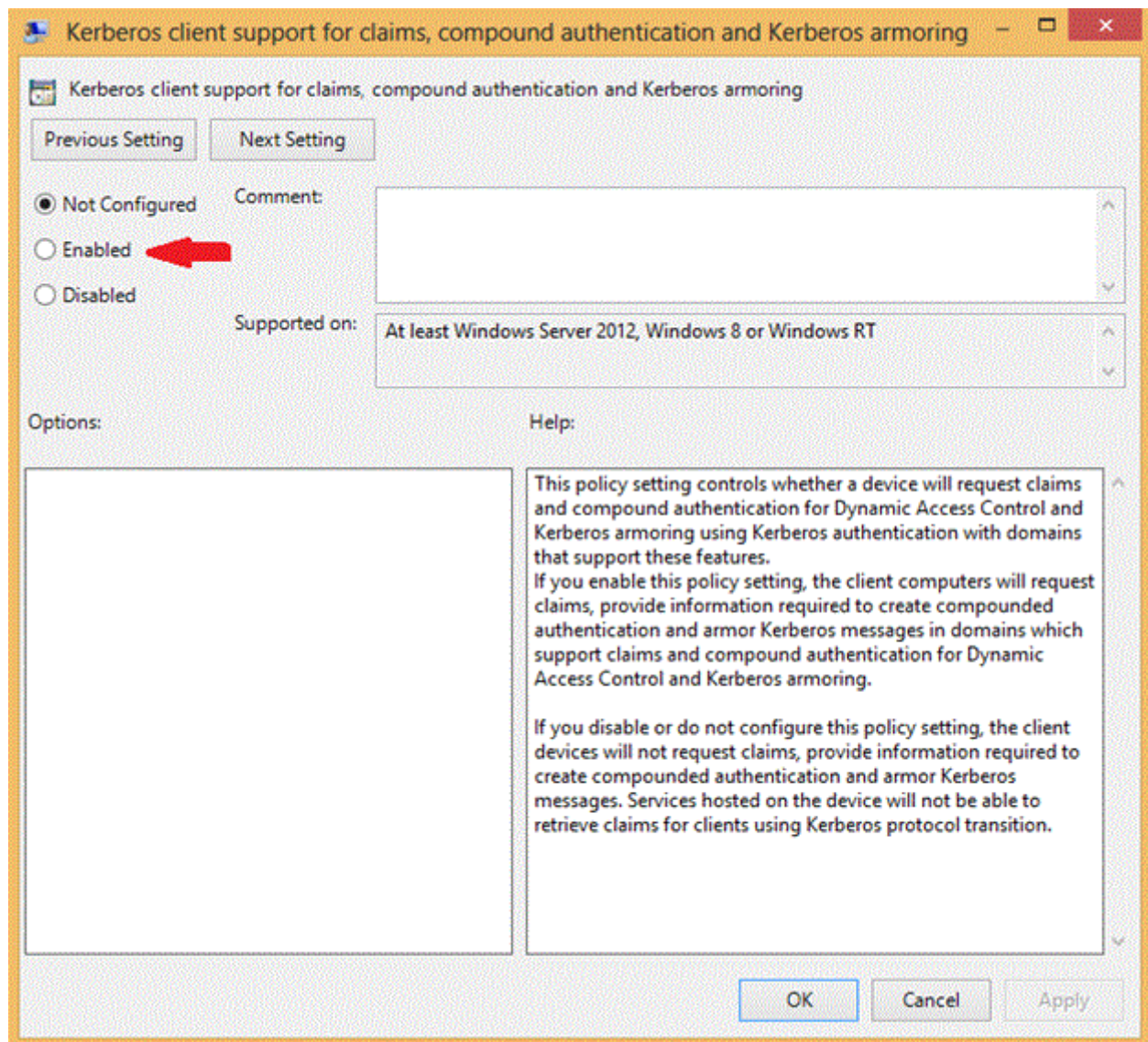
Widget Service Admins

## Configure Dynamic Access Control support on devices and hosts

You can configure TGT lifetimes without configuring Dynamic Access Control (DAC). DAC is only needed for checking `AllowedToAuthenticateFrom` and `AllowedToAuthenticateTo`.

Using either Group Policy or Local Group Policy Editor, enable **Kerberos client support for claims, compound authentication and Kerberos armoring** in Computer Configuration | Administrative Templates | System | Kerberos:

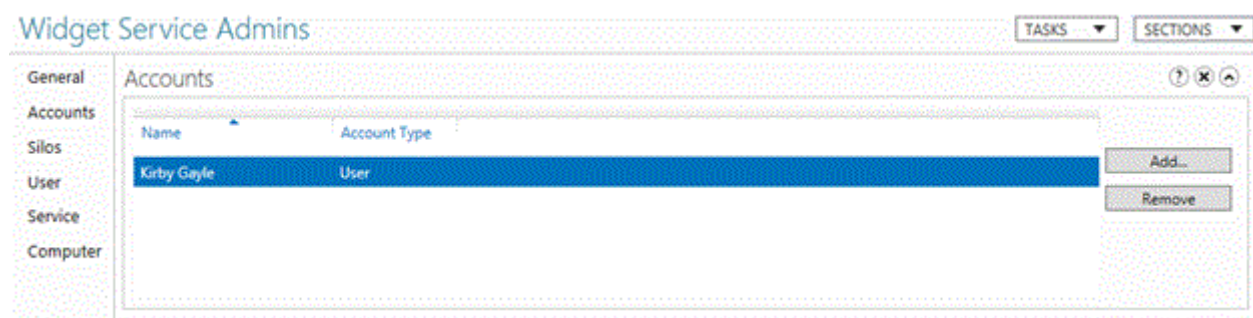




## Troubleshoot Authentication Policies

### Determine the accounts that are directly assigned an Authentication Policy

The accounts section in the Authentication Policy shows the accounts that have directly applied the policy.



### Use the Authentication Policy Failures - Domain Controller administrative log

A new **Authentication Policy Failures - Domain Controller** administrative log under **Applications and Services Logs > Microsoft > Windows > Authentication** has been created to make it easier to discover failures due to Authentication Policies. The log is

disabled by default. To enable it, right-click the log name and click **Enable Log**. The new events are very similar in content to the existing Kerberos TGT and service ticket auditing events. For more information about these events, see [Authentication Policies and Authentication Policy Silos](#).

## Manage authentication policies by using Windows PowerShell

---

This command creates an authentication policy named **TestAuthenticationPolicy**. The **UserAllowedToAuthenticateFrom** parameter specifies the devices from which users can authenticate by an SDDL string in the file named someFile.txt.

```
PS C:\> New-ADAuthenticationPolicy testAuthenticationPolicy -  
UserAllowedToAuthenticateFrom (Get-Acl .\someFile.txt).sddl
```

This command gets all authentication policies that match the filter that the **Filter** parameter specifies.

```
PS C:\> Get-ADAuthenticationPolicy -Filter "Name -like  
'testADAuthenticationPolicy*'" -Server Server02.Contoso.com
```

This command modifies the description and the **UserTGTLifetimeMins** properties of the specified authentication policy.

```
PS C:\> Set-ADAuthenticationPolicy -Identity ADAuthenticationPolicy1 -Description  
"Description" -UserTGTLifetimeMins 45
```

This command removes the authentication policy that the **Identity** parameter specifies.

```
PS C:\> Remove-ADAuthenticationPolicy -Identity ADAuthenticationPolicy1
```

This command uses the **Get-ADAuthenticationPolicy** cmdlet with the **Filter** parameter to get all authentication policies that are not enforced. The result set is piped to the **Remove-ADAuthenticationPolicy** cmdlet.

```
PS C:\> Get-ADAuthenticationPolicy -Filter 'Enforce -eq $false' | Remove-  
ADAuthenticationPolicy
```

## Authentication policy silos

---

Authentication Policy Silos is a new container (objectClass msDS-AuthNPolicySilos) in AD DS for user, computer, and service accounts. They help protect high-value accounts. While all organizations need to protect members of Enterprise Admins, Domain Admins and Schema Admins groups because those accounts could be used by an attacker to access anything in the forest, other accounts may also need protection.

Some organizations isolate workloads by creating accounts that are unique to them and by applying Group Policy settings to limit local and remote interactive logon and administrative privileges. Authentication policy silos complement this work by creating a



way to define a relationship between User, Computer and managed Service accounts. Accounts can only belong to one silo. You can configure authentication policy for each type of account in order to control:

1. Non-renewable TGT lifetime
2. Access control conditions for returning TGT (Note: cannot apply to systems because Kerberos armoring is required)
3. Access control conditions for returning service ticket

Additionally, accounts in an authentication policy silo have a silo claim, which can be used by claims-aware resources such as file servers to control access.

A new security descriptor can be configured to control issuing service ticket based on:

- User, user's security groups, and/or user's claims
- Device, device's security group, and/or device's claims

Getting this information to the resource's DCs requires Dynamic Access Control:

- User claims:
  - Windows 8 and later clients supporting Dynamic Access Control
  - Account domain supports Dynamic Access Control and claims
- Device and/or device security group:
  - Windows 8 and later clients supporting Dynamic Access Control
  - Resource configured for compound authentication
- Device claims:
  - Windows 8 and later clients supporting Dynamic Access Control
  - Device domain supports Dynamic Access Control and claims
  - Resource configured for compound authentication

Authentication policies can be applied to all members of an authentication policy silo instead of to individual accounts, or separate authentication policies can be applied to different types of accounts within a silo. For example, one authentication policy can be applied to highly privileged user accounts, and a different policy can be applied to services accounts. At least one authentication policy must be created before an authentication policy silo can be created.

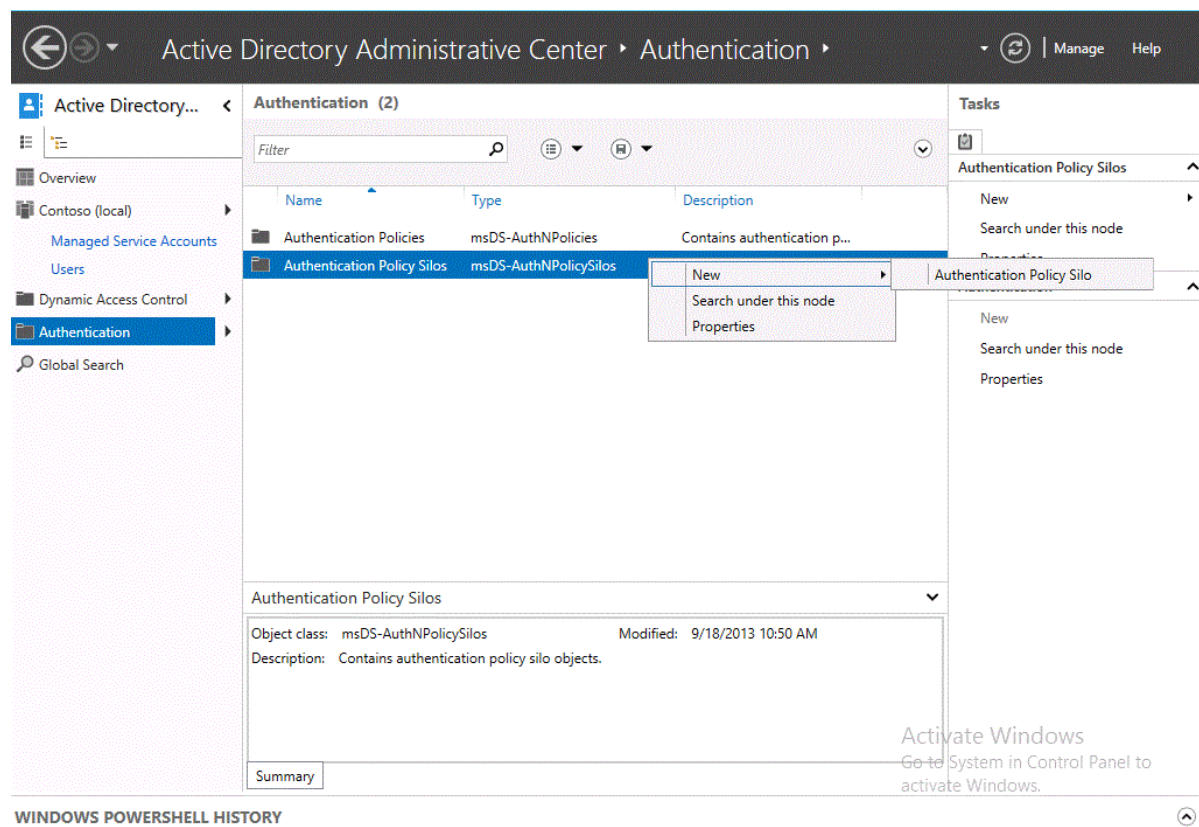
Note

An authentication policy can be applied to members of an authentication policy silo, or it can be applied independently of silos to restrict specific account scope. For example, to protect a single account or a small set of accounts, a policy can be set on those accounts without adding the accounts to a silo.

You can create an authentication policy silo by using Active Directory Administrative Center or Windows PowerShell. By default, an authentication policy silo only audits silo policies, which is equivalent to specifying the **WhatIf** parameter in Windows PowerShell cmdlets. In this case, policy silo restrictions do not apply, but audits are generated to indicate whether failures occur if the restrictions are applied.

## To create an authentication policy silo by using Active Directory Administrative Center

1. Open **Active Directory Administrative Center**, click **Authentication**, right-click **Authentication Policy Silos**, click **New**, and then click **Authentication Policy Silo**.



2. In **Display name**, type a name for the silo. In **Permitted Accounts**, click **Add**, type the names of the accounts, and then click **OK**. You can specify users, computers, or service accounts. Then specify whether to use a single policy for all principals or a separate policy for each type of principal, and the name of the policy or policies.

General

Accounts

Policy

An authentication policy silo controls which accounts are to be protected by the silo and defines the authentication policies to be applied to members of the silo.

Display name: \* ExchangeSilo

Description:

☐ Only audit silo policies

☒ Enforce silo policies

☒ Protect from accidental deletion

Permitted Accounts

Name	Account Type	Assigned
ConExchSrv1	Computer	
ExchAdmin1	User	

Authentication Policy

☒ Use a single policy for all principals that belong to this authentication policy silo.

\* The authentication policy that applies to all accounts in this silo: ExchangeAdminsAuthNPolicy

☐ Use a separate authentication policy for each type of principal.

User account policy:

Managed Service Account policy:

Activate Windows  
Go to System in Control Panel to activate Windows.

More Information

OK Cancel

## Manage authentication policy silos by using Windows PowerShell

This command creates an authentication policy silo object and enforces it.

```
PS C:\>New-ADAuthenticationPolicySilo -Name newSilo -Enforce
```

This command gets all the authentication policy silos that match the filter that is specified by the **Filter** parameter. The output is then passed to the **Format-Table** cmdlet to display the name of the policy and the value for **Enforce** on each policy.

```
PS C:\>Get-ADAuthenticationPolicySilo -Filter 'Name -like "*silo"' | Format-Table  
Name, Enforce -AutoSize
```

Name	Enforce
----	-----
silo	True
silos	False

This command uses the **Get-ADAuthenticationPolicySilo** cmdlet with the **Filter** parameter to get all authentication policy silos that are not enforced and pipe the result of the filter to the **Remove-ADAuthenticationPolicySilo** cmdlet.

```
PS C:\>Get-ADAuthenticationPolicySilo -Filter 'Enforce -eq $False' | Remove-  
ADAuthenticationPolicySilo
```

This command grants access to the authentication policy silo named *Silo* to the user account named *User01*.

```
PS C:\>Grant-ADAuthenticationPolicySiloAccess -Identity Silo -Account User01
```

This command revokes access to the authentication policy silo named *Silo* for the user account named *User01*. Because the **Confirm** parameter is set to **\$False**, no confirmation message appears.

```
PS C:\>Revoke-ADAuthenticationPolicySiloAccess -Identity Silo -Account User01 -  
Confirm:$False
```

This example first uses the **Get-ADComputer** cmdlet to get all computer accounts that match the filter that the **Filter** parameter specifies. The output of this command is passed to **Set-ADAccountAuthenticatinPolicySilo** to assign the authentication policy silo named *Silo* and the authentication policy named *AuthenticationPolicy02* to them.

```
PS C:\>Get-ADComputer -Filter 'Name -like "newComputer*"' | Set-  
ADAccountAuthenticationPolicySilo -AuthenticationPolicySilo Silo -  
AuthenticationPolicy AuthenticationPolicy02
```