



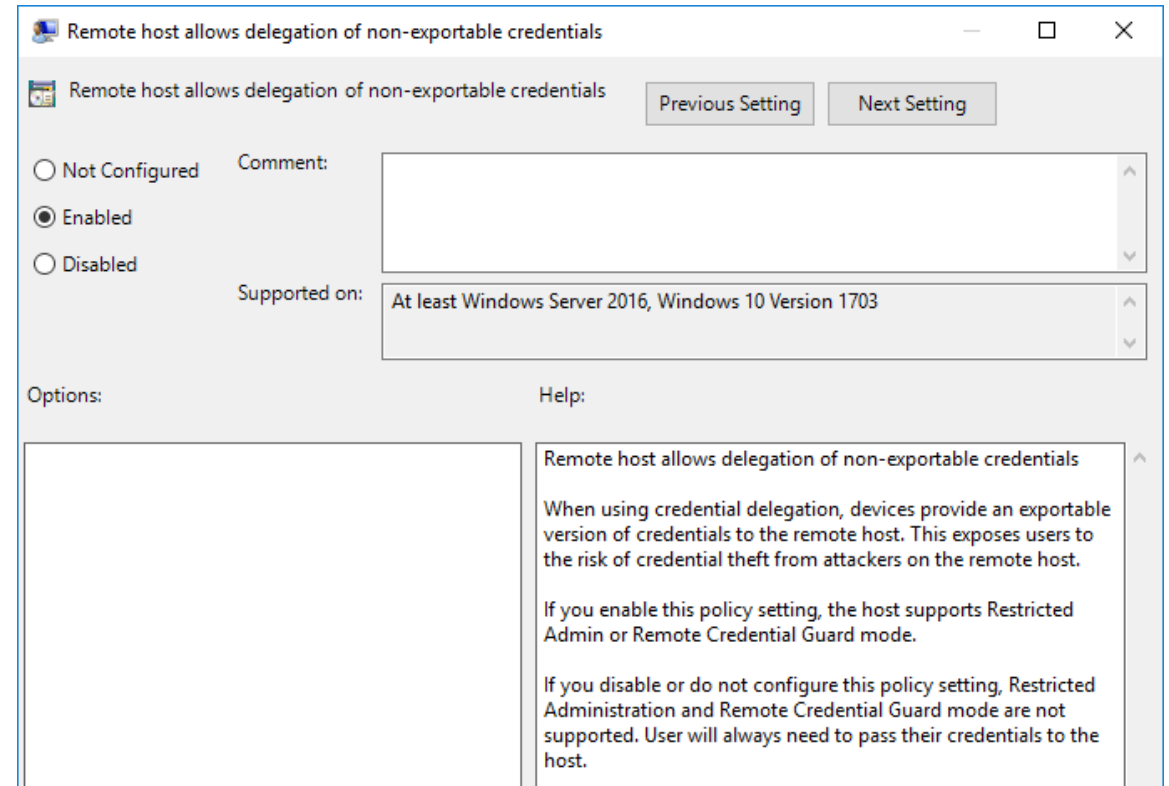
Securing Windows Active Directory

Additional Content

Securing RDP Connections

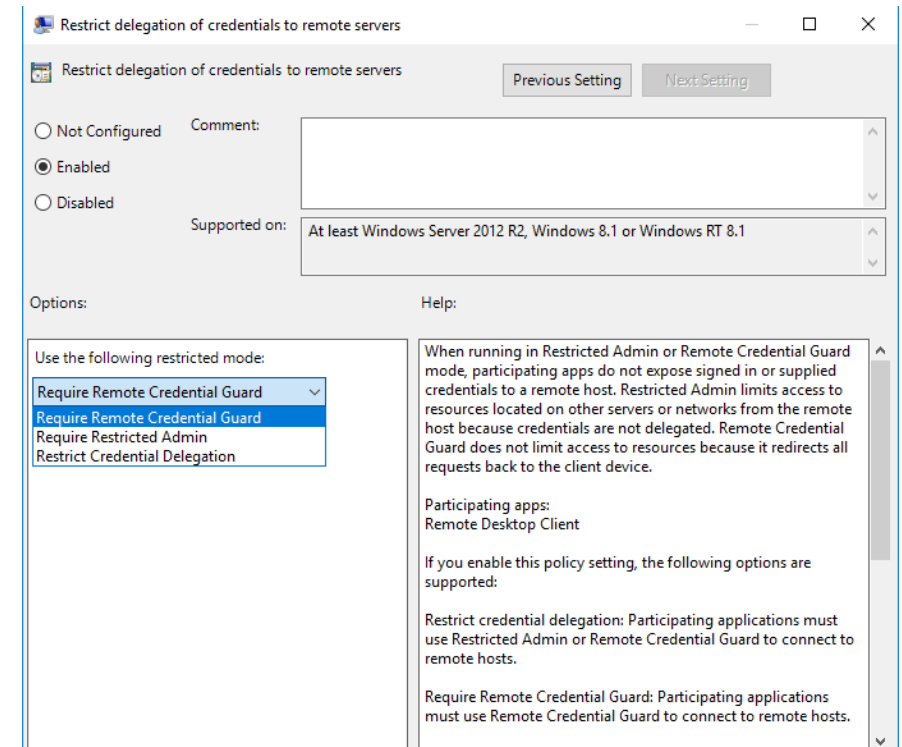
RDP Hosts

- Group Policy
 - Computer Configuration\Administrative Templates\System\Credentials Delegation - **Remote host allows delegation of nonexportable credentials**: Enabled
- Registry
 - HKLM\SYSTEM\CurrentControlSet\Control\Lsa – DisableRestrictedAdmin (DWORD): 0



RDP Clients

- Command
 - `mstsc.exe /remoteGuard`
 - `mstsc.exe /restrictedAdmin`
- Group Policy
 - Computer Configuration\Administrative Templates\System\Credentials Delegation
 - **Restrict delegation of credentials to remote servers:**
 - Require Remote Credential Guard
 - Require Restricted Admin
 - Restrict Credential Delegation (Remote Credential Guard is preferred, but it uses Restricted Admin mode (if supported) when Remote Credential Guard can't be used)
- Registry
 - HKLM\Software\Policies\Microsoft\Windows\CredentialsDelegation –
 - RestrictedRemoteAdministration (DWORD): 1
 - RestrictedRemoteAdministrationType (DWORD)
 - 1 – Require Restricted Admin
 - 2 – Require Remote Credential Guard
 - 3 - Restrict Credential Delegation



Anonymous Access of AD

Get the value of the dSHeuristics attribute.

- By default, anonymous LDAP operations to Active Directory, other than rootDSE searches and binds, are not permitted.
- If the dSHeuristics attribute is set to 0000002, anonymous clients can perform any operation against domain controllers that is permitted by the access control list (ACL).
- To get this value, run the following PowerShell command:

```
Get-ADObject -Identity "CN=Directory Service,CN=Windows  
NT,CN=Services,CN=Configuration,DC=Litware,DC=com" -Properties dSHeuristics |  
Select-Object dSHeuristics
```

Is Anonymous Logon a member of Pre-Windows 2000 Compatible Access?

- Members of the Pre-Windows 2000 Compatible Access group have Read access for all users and groups in the domain.
- This group is provided for backward compatibility for computers running Windows NT 4.0 and earlier.
- If the output of this command returns the DistinguishedName of the Pre-Windows 2000 Compatible Access group, Anonymous Logon is a member of the Pre-Windows 2000 Compatible Access security group

```
Get-ADObject -LDAPFilter '(&(objectSid=S-1-5-7)(ObjectClass=foreignSecurityPrincipal))' -  
Properties memberOf | Select-Object -  
ExpandProperty memberOf
```

DC Promo Option	Default members
Clean installation of Windows 2000	Everyone
Clean installation of Windows 2000 with “Permissions compatible with pre-Windows 2000 servers	Anonymous Logon, Everyone
Clean installation of Windows Server 2003 (and later)	Authenticated Users
Clean installation of Windows Server 2003 with “Permissions compatible with pre-Windows 2000 servers”	Anonymous Logon, Authenticated Users, Everyone

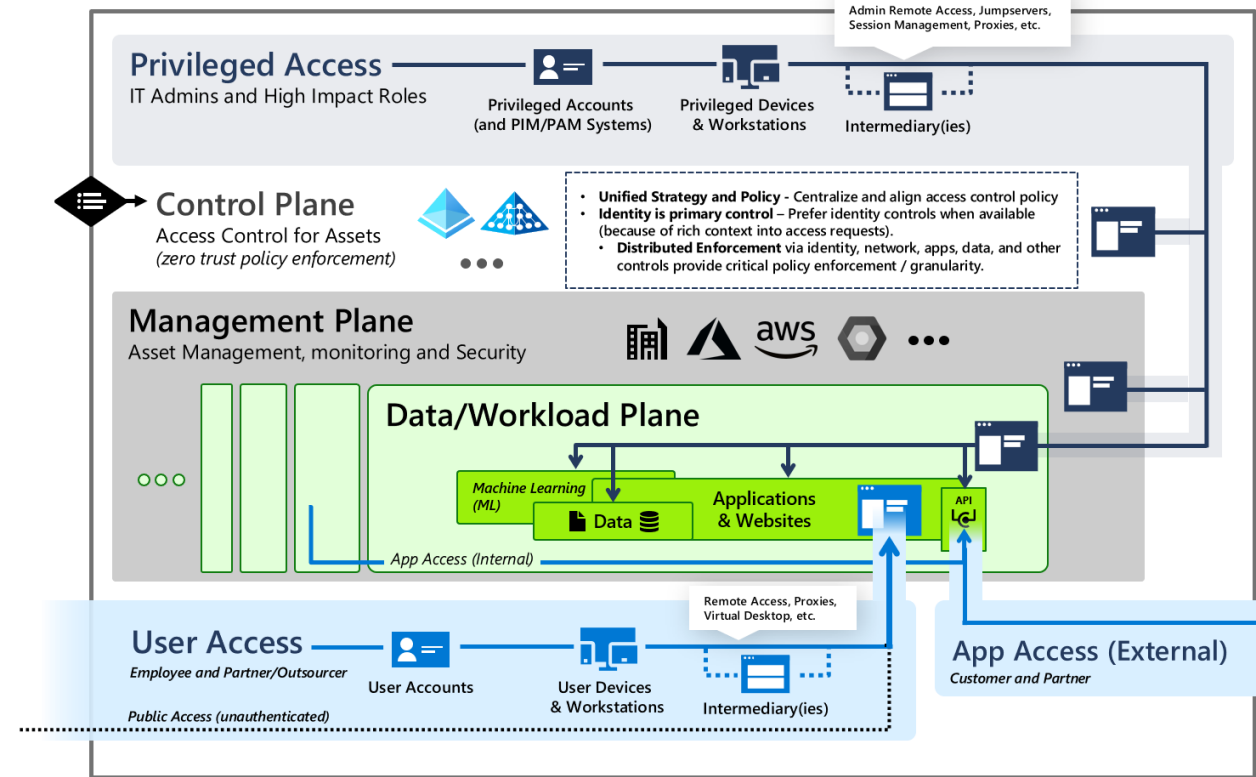
Does Everyone include Anonymous Logon?

- By Default, the Everyone SID is removed from the token created for anonymous connections.
 - Therefore, anonymous users can only access those resources for which the anonymous user has been explicitly given permission.
- If **EveryoneIncludesAnonymous** is set to “1”, anonymous users are able to access any resource for which the Everyone group has been given permissions.
- Query each DC to see if the registry value
HKLM\SYSTEM\CurrentControlSet\Control\Lsa – EveryoneIncludesAnonymous is set to “1”

Enterprise Access Model

Enterprise Access Model

- Incorporates on-premises tiering with cloud services
- Tier 0 expanded to control plane – Access Control
- Tier 1 split
 - Management plane – IT management
 - Data/Workload plane – per-workload management
- Tier 2 split
 - User access – internal users + collaboration (B2B / B2C)
 - App access – API access

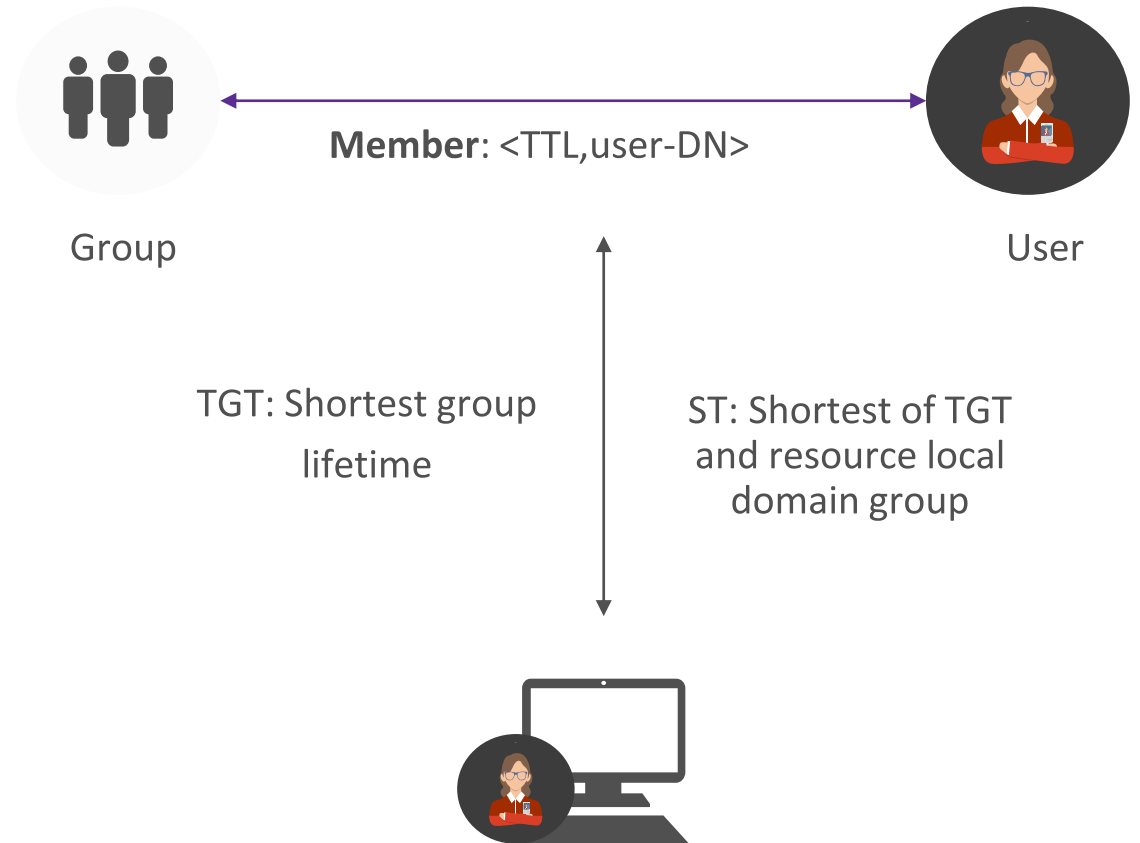


Privileged Access Management Optional Feature

Windows Server 2016 FFL

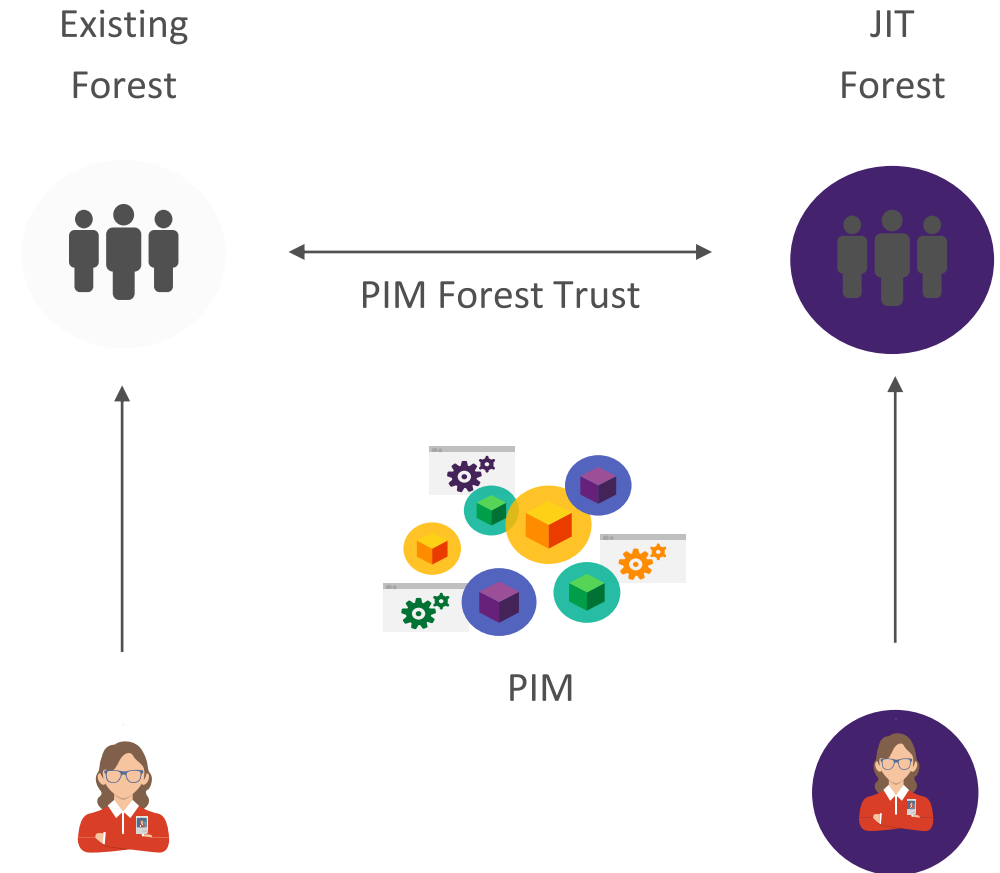
Time-limited Group Memberships

- Users can be added to a security group with time-to-live (TTL)
 - When the TTL expires, the user's membership in that group disappears
- Kerberos token lifetime will be determined by TTL of the user's memberships
 - TGT based on shortest group membership
 - Service ticket based on TGT and resource local domain group membership



Just In Time Forest

- Create new Server 2016 forest
 - No need to change existing forest
 - Create new **PIM** trust to existing forest
- Add shadow principals in new forest
 - Shadow group which is new object class created in config NC. Unlike security group, the security identifier (SID) with a domain in another forest
 - Add shadow admin user
- Remove admins from existing groups



```
PS C:\> Enable-ADOptionalFeature 'Privileged Access Management Feature' -Scope ForestOrConfigurationSet -Target Reskit.com
WARNING: Enabling 'Privileged Access Management Feature' on 'CN=Partitions,CN=Configuration,DC=Reskit,DC=com' is an irreversible action! You will not be able to
disable 'Privileged Access Management Feature' on 'CN=Partitions,CN=Configuration,DC=Reskit,DC=com' if you proceed.
```

```
Confirm
Are you sure you want to perform this action?
Performing the operation "Enable" on target "Privileged Access Management Feature".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A
PS C:\> _
```

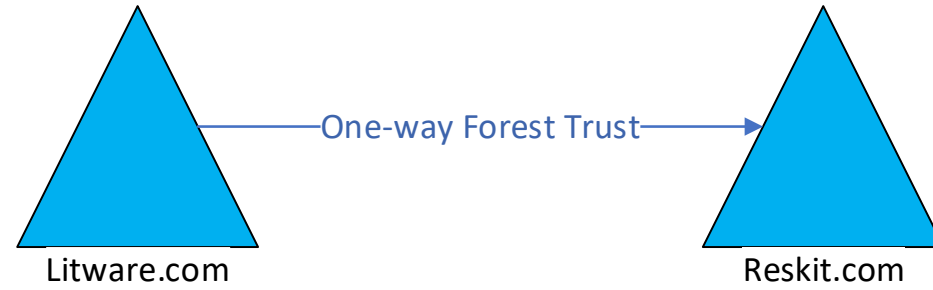
```
PS C:\> Get-ADOptionalFeature -Identity "Privileged Access Management Feature"
```

```
DistinguishedName : CN=Privileged Access Management Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=Reskit,DC=com
EnabledScopes      : {CN=Partitions,CN=Configuration,DC=Reskit,DC=com, CN=NTDS
                     Settings,CN=R00TDC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=Reskit,DC=com}
FeatureGUID        : ec43e873-cce8-4640-b4ab-07ffe4ab5bcd
FeatureScope       : {ForestOrConfigurationSet}
IsDisableable      : False
Name               : Privileged Access Management Feature
ObjectClass         : msDS-OptionalFeature
ObjectGUID         : 08ed1add-6b50-4445-80dd-465ee7687c8d
RequiredDomainMode : 
RequiredForestMode : Windows2016Forest
```

```
PS C:\> Add-ADGroupMember -Identity 'Domain Admins' -Members 'Temp_DA' -MemberTimeToLive (New-TimeSpan -Hours 8)
PS C:\>
```

```
PS C:\> Get-ADGroup -Identity "Domain Admins" -Properties member -ShowMemberTimeToLive
```

```
DistinguishedName : CN=Domain Admins,CN=Users,DC=Reskit,DC=com
GroupCategory      : Security
GroupScope         : Global
member             : {<TTL=28694>,CN=Temp_DA,OU=Reskit_Users,DC=Reskit,DC=com, CN=PParker,CN=Users,DC=Reskit,DC=com}
Name               : Domain Admins
ObjectClass         : group
ObjectGUID         : e07e3813-5dc2-4495-a519-bf6080cafea4
SamAccountName     : Domain Admins
SID                : S-1-5-21-2632454862-2292402223-684154031-512
```



```
C:\>netdom trust Litware.com /domain:Reskit.com /EnableSIDHistory:Yes
Enabling SID history for this trust.

The command completed successfully.

C:\>netdom trust Litware.com /domain:Reskit.com /EnablePIMTrust:Yes
Enabling PIM Trust.

The command completed successfully.

C:\>netdom trust Litware.com /domain:Reskit.com /Quarantine:No
SID filtering is not enabled for this trust.

The command completed successfully.
```

```
$LitwareDomainAdminsSID = (Get-ADGroup -Identity "Domain Admins" -Properties ObjectSID -Server RootDC02.Litware.com).ObjectSID.Value
```

```
New-ADObject -Type "msDS-ShadowPrincipal" `
    -Name "Litware-Domain_Admins" `
    -Path "CN=Shadow Principal Configuration,CN=Services,CN=Configuration,DC=Reskit,DC=com" `
    -OtherAttributes @{ 'msDS-ShadowPrincipalSid' = $LitwareDomainAdminsSID }
```

The screenshot shows the ADSI Edit console on the left and the 'CN=Litware-Domain_Admins Properties' dialog box on the right.

ADSI Edit Console:

- Schema [RootDC01.Reskit.com]
- Configuration [RootDC01.Reskit.com]
- CN=Configuration,DC=Reskit,DC=com
 - CN=DisplaySpecifiers
 - CN=Extended-Rights
 - CN=ForestUpdates
 - CN=LostAndFoundConfig
 - CN=NTDS Quotas
 - CN=Partitions
 - CN=Physical Locations
- CN=Services
 - CN=AuthN Policy Configuration
 - CN=Claims Configuration
 - CN=Group Key Distribution Service
 - CN=Microsoft SPP
 - CN=MsmqServices
 - CN=NetServices
 - CN=Public Key Services
 - CN=RRAS
 - CN=Shadow Principal Configuration
 - CN=Windows NT
- CN=Sites
- CN=WellKnown Security Principals

Domain_Reskit.com [RootDC01.Reskit.com]

CN=Litware-Domain_Admins Properties Dialog:

Name	Class	Distinguished Name
CN=Litware-Domain_Admins	msDS-Shado...	CN=Litware-Domain_Admins,CN=Shadow Principal Configuration,CN=Services,...

Attribute	Value
cn	Litware-Domain_Admins
distinguishedName	CN=Litware-Domain_Admins,CN=Shadow Principal Configuration,CN=Services,...
dSCorePropagationData	0x0 = ()
instanceType	0x4 = (WRITE)
msDS-ShadowPrincipalSid	S-1-5-21-1624139221-625062452-422627...
name	Litware-Domain_Admins
objectCategory	CN=ms-DS-Shadow-Principal,CN=Schema,...
objectClass	top; msDS-ShadowPrincipal
objectGUID	ee720de4-5c7e-4957-ac58-87caf2bed3a...
replPropertyMetaData	AttID Ver Loc:USN Org:DSA
uSNChanged	20613
uSNCreated	20613
whenChanged	3/9/2023 3:18:39 AM Coordinated Univer...
whenCreated	3/9/2023 3:18:39 AM Coordinated Univer...

Buttons: Edit, Filter, OK, Cancel, Apply, Help


```
Set-ADObject -Identity "CN=Litware-Domain_Admins,CN=Shadow Principal  
Configuration,CN=Services,CN=Configuration,DC=Reskit,DC=com"
```

```
-Add @{ 'member' = "<TTL=3600,CN=Litware_Admin_1,OU=Reskit-Admins,DC=Reskit,DC=com>" }
```

```
C:\>whoami /user
```

```
USER INFORMATION
```

User Name	SID
reskit\litware_admin_1	S-1-5-21-2632454862-2292402223-684154031-2103

```
C:\>whoami /groups
```

```
GROUP INFORMATION
```

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default, Enabled group
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators	Alias	S-1-5-32-544	Group used for deny only
NT AUTHORITY\INTERACTIVE	Well-known group	S-1-5-4	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory group, Enabled by default, Enabled group
LOCAL	Well-known group	S-1-2-0	Mandatory group, Enabled by default, Enabled group
LITWARE\Domain Admins	Group	S-1-5-21-1624139221-625062452-4226278533-512	Group used for deny only
Authentication authority asserted identity	Well-known group	S-1-18-1	Mandatory group, Enabled by default, Enabled group
LITWARE\Denied RODC Password Replication Group	Alias	S-1-5-21-1624139221-625062452-4226278533-572	Mandatory group, Enabled by default, Enabled group, Local Group
Mandatory Label\Medium Mandatory Level	Label	S-1-16-8192	

```

C:\>dir \\RootDC01.Litware.com\c$
Volume in drive \\RootDC01.Litware.com\c$ is Windows
Volume Serial Number is 76F7-2DA4

Directory of \\RootDC01.Litware.com\c$

02/20/2023  04:23 PM    <DIR>          Packages
02/07/2023  10:27 AM    <DIR>          PerfLogs
03/07/2023  01:05 PM    <DIR>          Program Files
02/07/2023  11:07 AM    <DIR>          Program Files (x86)
03/08/2023  02:00 PM    <DIR>          Temp
02/20/2023  04:46 PM    <DIR>          Users
02/20/2023  04:59 PM    <DIR>          Windows
02/20/2023  07:48 PM    <DIR>          WindowsAzure
               0 File(s)              0 bytes
               8 Dir(s) 122,447,331,328 bytes free

```

```

C:\>klist tickets
Current LogonId is 0:0xb2badc
Cached Tickets: (4)
#0> Client: Litware_Admin_1 @ RESKIT.COM
    Server: krbtgt/LITWARE.COM @ RESKIT.COM
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
    Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
    Start Time: 3/9/2023 3:37:36 (local)
    End Time: 3/9/2023 4:27:03 (local)
    Renew Time: 3/9/2023 4:27:03 (local)
    Session Key Type: AES-256-CTS-HMAC-SHA1-96
    Cache Flags: 0x200 -> DISABLE-TGT-DELEGATION
    Kdc Called: RootDC01.Reskit.com
#1> Client: Litware_Admin_1 @ RESKIT.COM
    Server: krbtgt/RESKIT.COM @ RESKIT.COM
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
    Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
    Start Time: 3/9/2023 3:34:25 (local)
    End Time: 3/9/2023 4:27:03 (local)
    Renew Time: 3/9/2023 4:27:03 (local)
    Session Key Type: AES-256-CTS-HMAC-SHA1-96
    Cache Flags: 0x1 -> PRIMARY
    Kdc Called: RootDC01.Reskit.com
#2> Client: Litware_Admin_1 @ RESKIT.COM
    Server: cifs/RootDC01.Litware.com @ LITWARE.COM
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
    Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
    Start Time: 3/9/2023 3:37:36 (local)
    End Time: 3/9/2023 4:27:03 (local)
    Renew Time: 3/9/2023 4:27:03 (local)
    Session Key Type: AES-256-CTS-HMAC-SHA1-96
    Cache Flags: 0x200 -> DISABLE-TGT-DELEGATION
    Kdc Called: RootDC01.Litware.com
#3> Client: Litware_Admin_1 @ RESKIT.COM
    Server: cifs/RootDC01.Litware.com @ LITWARE.COM
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
    Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
    Start Time: 3/9/2023 3:37:36 (local)
    End Time: 3/9/2023 4:27:03 (local)
    Renew Time: 3/9/2023 4:27:03 (local)
    Session Key Type: AES-256-CTS-HMAC-SHA1-96
    Cache Flags: 0x200 -> DISABLE-TGT-DELEGATION
    Kdc Called: RootDC01.Litware.com

```

Windows Hello for Business

Windows Hello for Business

- User Friendly
 - Passwordless biometrics or PIN
 - SSO for on-premises and the cloud
- Enterprise Grade
 - Asymmetric key pair authentication model
 - Strong two-factor authentication
 - Multiple accounts per device
 - Deploy in the cloud, hybrid, or on-prem



Windows Hello for Business

- Replace Passwords with Keys
 - Unlocked through a user gesture of biometrics or PIN
 - FIDO2 Certified
 - Can leverage enterprise PKI for certificates
- Private Key is Never Shared
 - Keys are always generated in hardware by Trusted Platform Module [TPM]
 - Hardware bound keys are attested by Trusted Computing Group Protocols



Windows Hello for Business Adoption

10 Million

Monthly active Windows Hello for Business users

50K+

Enterprises have deployed Windows Hello for Business

>450K

Largest single enterprise deployment

Statistics, June 2022



Windows Hello for Business Deployment

Cloud



Hybrid



Cert Trust

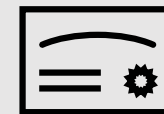
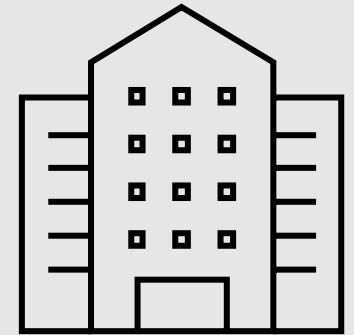


Key Trust



Cloud Trust
(Preview)

On-Premises

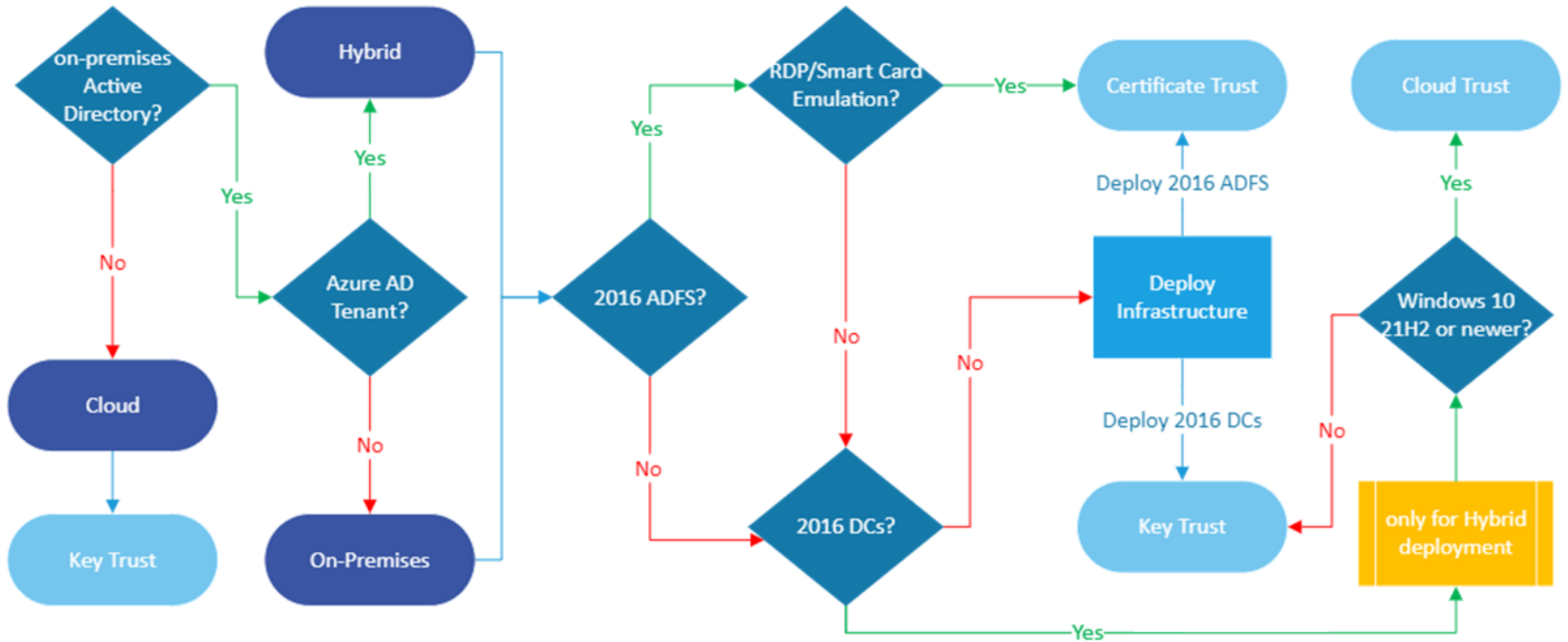


Cert Trust



Key Trust

WH4B - Choosing a Deployment Model



Key, Certificate and Cloud Trust: Security



Key Trust

- Authenticates using raw key to Azure AD
- Authenticates using raw key to Active Directory
- Does not require issuance of end user certificate from PKI
- Requires 2016 or later Domain Controllers

- Authenticates using raw key to Azure AD
- Authenticates using PKI user cert to Active Directory
- Requires issuance of end user certificate from PKI
- Requires 2012 or later Domain Controllers



Cert Trust



Cloud Trust

- Authenticates using raw key to Azure AD
- Authenticates using TGT issued from Azure AD Kerberos to Active Directory
- Does not require issuance of any certificate
- Requires 2016 or later Domain Controllers

- All trusts use asymmetric key pairs
- All trusts use the same TPM hardware
- All trusts require the same strong proof-up [MFA] for enrollment

Hybrid Cloud Trust Components (Preview)

CLIENT

Windows 10
Windows 11



Windows 10
21H2 or later
Windows 11

DIRECTORY

Active
Directory
Domain
Services



Server 2016 or later
2008 R2 DFL/FFL
or later

Azure Active
Directory



Azure AD Kerberos
PowerShell module
Device Registration

Azure Active
Directory
Connect



Optional

INFRASTRUCTURE



Active
Directory
Federation
Services



Optional:
AD FS 2016 or later
Needed for 3rd party
MFA provider

Multi-factor
Auth



Azure MFA
or
3rd party MFA
provider

MANAGEMENT

Group Policy



WHFB Config

MDM



Optional:
WHFB Config

Hybrid Key Trust Components

CLIENT

Windows 10



DIRECTORY

Active Directory Domain Services



Server 2016 or later
2008 R2 DFL/FFL or later

Azure Active Directory



Device Registration
Key Registration

Azure Active Directory Connect



Directory Synchronization with write-back (ADP)

INFRASTRUCTURE

Active Directory Certificate Services



AD CS 2012 or later
KDC Certificate

Active Directory Federation Services



Optional:
AD FS 2016 or later
Needed for 3rd party MFA provider

Multi-factor Auth



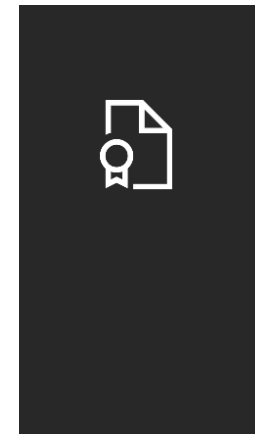
Azure MFA
or
3rd party MFA provider

MANAGEMENT

Group Policy



Autoenrollment
Intranet Zone
WHFB Config



MDM



Optional:
WHFB Config

Hybrid Certificate Trust Components

CLIENT

Windows 10



DIRECTORY

Active Directory Domain Services



Server 2012 or later
2008 R2 DFL/FFL or later

Azure Active Directory



Device Registration
Key Registration

Azure Active Directory Connect



Directory Synchronization with write-back (ADP)

INFRASTRUCTURE

Active Directory Certificate Services



AD CS 2012 or later
KDC, Enrollment, and User Certificate

Active Directory Federation Services



AD FS 2016 or later
Registration Authority
MFA

Multi-factor Auth



Azure MFA
or
3rd party MFA provider

MANAGEMENT

Group Policy



Autoenrollment
Intranet Zone
WHFB Config

NDES Role



Optional:
MDM Certificate
Registration
Authority

MDM



Optional:
WHFB Config

WH4B – Trust Types (Hybrid)

	Cloud Trust	Key Trust	Certificate Trust
AuthN factor to Azure AD	Keys	Keys	Keys
AuthN factor to AD DS	Kerberos	Keys	Certificate
Domain controller min version	Win Svr 2016 + KB3534307 Win Svr 2019 + KB4534321	Server 2016	Server 2012 R2
Client min version	Win 10 21H2 + KB5010415 Win 11 21H2 + KB5010414		
DFL/FFL min version	Server 2008 R2	Server 2008 R2	Server 2008 R2
DC cert requirement	No	Yes*	Yes*
Client cert requirement	No	No	Yes
AD DS Schema min version	Server 2016	Server 2016	Server 2016
Authentication Type Support	Federated and Managed (PHS / PTA)	Federated and Managed (PHS / PTA)	Federated only
AD FS Required	No	No	Yes (Server 2016+)
Device Writeback Required	No	No	Yes