Microsoft

ss the Hash and Other Credential eft and Reuse: Mitigating the Risk of Lateral ement and Privilege Escalation

ick Jungles, Trustworthy Computing
k Simos, Microsoft Consulting Services

Agenda

lem

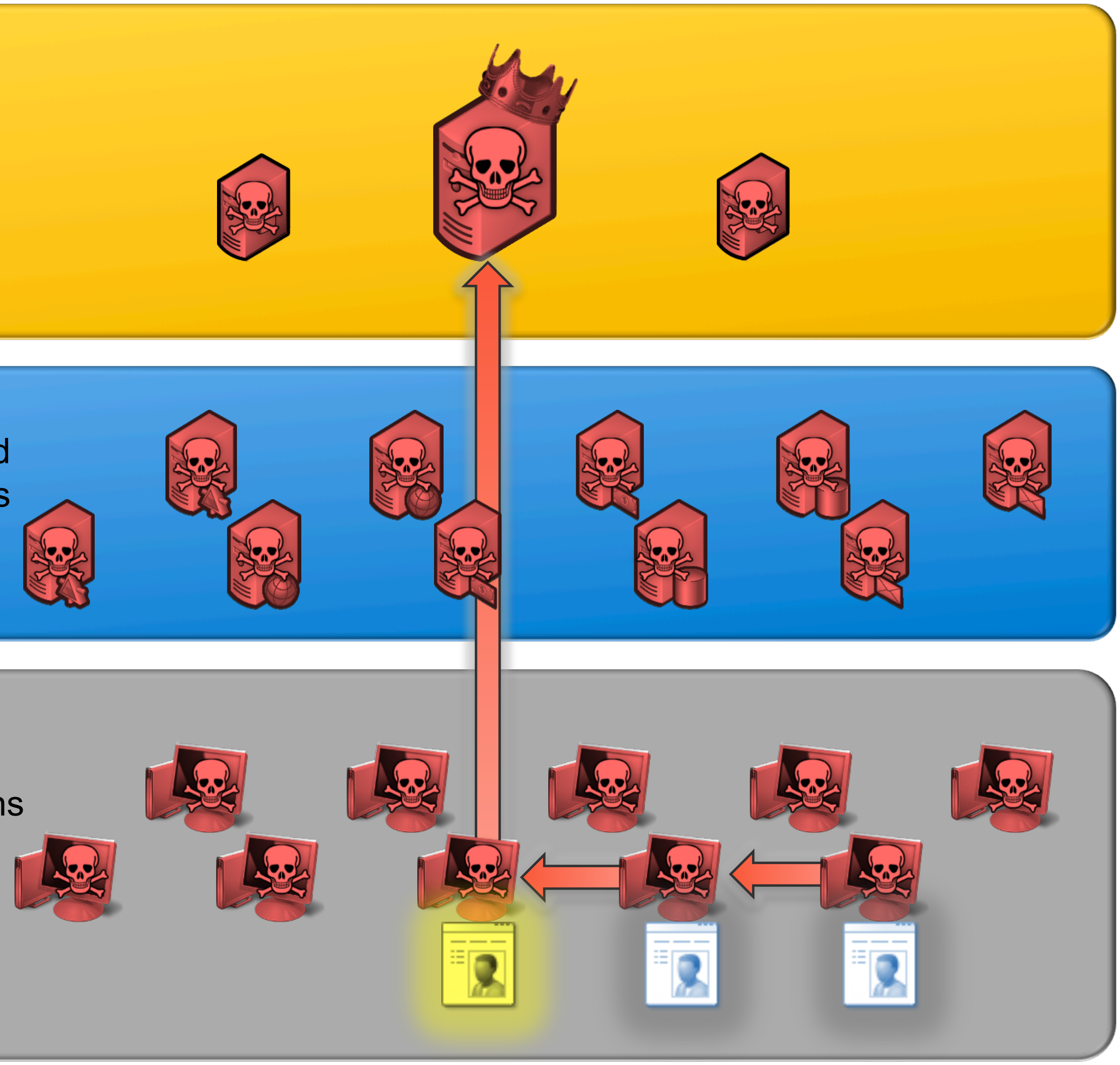
Review

Platform Updates and New Mitigations

Next S

The Problem

ss The Hash Attack



1. Attacker targets workstations en m

2. User running as local admin is com
attacker harvests credentials

3. Attacker uses credentials for latera
movement or privilege escalation

4. Attacker acquires domain admin cr

5. Attacker starts exercising this full c
data and systems in the environme

/ is this not a simple fix?

cts:

need to support single sign-on (SSO). Credentials mus
/ed or cached to allow the operating system to perform
ons on behalf of the user.

dentials can still be harvested and reused if disclosed
n attacker or a compromised computer.

Review

gation 1 - Restrict and protect high privileged nain accounts

Objective	How	Outcome
This mitigation reduces the risk of administrators from inadvertently exposing privileged credentials to higher risk computers.	• Restrict DA/EA accounts from authenticating to lower trust computers • Provide admins with accounts to perform administrative duties • Assign dedicated workstations for administrative tasks. • Mark privileged accounts as “sensitive and cannot be delegated” • Do not configure services or schedule tasks to use privileged domain accounts on lower trust computers	An attacker cannot steal credentials for an account if the credentials are never used on the compromised computer.

gation 2 - Restrict and protect local accounts w ninistrative privileges

Objective	How	Outcome
This mitigation restricts the ability of attackers to use local administrator accounts or their equivalents for lateral movement PtH attacks.	• Enforce the restrictions available in Windows Vista and later versions, preventing local accounts from being used for remote administration. • Explicitly deny network and Remote Desktop logon rights for all administrative local accounts. • Create unique passwords for local accounts with administrative privileges.	An attacker who successfully obtains local account credentials from a compromised computer will not be able to use those credentials to perform lateral movement on the organization's network.

gation 3 - Restrict inbound traffic using the ndows Firewall

Objective	How	Outcome
This mitigation restricts the ability of attackers from initiating lateral movement from a compromised workstation by blocking inbound connections.	• Restrict all inbound connections to all workstations except for those with expected traffic originating from trusted sources, such as helpdesk workstations, security compliance scanners and servers.	An attacker who successfully obtains any type of account credentials will not be able to connect to other workstations.

tigations that don’t solve PtH…

Other mitigation	Effectiveness	Effort Required
Disable NTLM	Minimal	High
Smart cards and multifactor authentication	Minimal	High
Jump servers	Minimal	High
Rebooting workstations and servers	Minimal	Low

Platform Updates nd New Mitigations

ore platform changes

Remove LM hashes from LSASS

Remove plaintext-equivalent passwords from LSA for domain credentials

Enforce credential removal after logoff

Facilitate restriction of local admin accounts

- S-1-5-113 – Local account
- S-1-5-114 – Local account and member of Administrators group

estricted Admin Mode Remote esktop

emote desktop client can connect in estrictedAdmin mode which does not provide re-able credentials to the remote host.

PO: Restrict delegation of credentials to remote rver

estricted Admin Mode Remote esktop

fect:

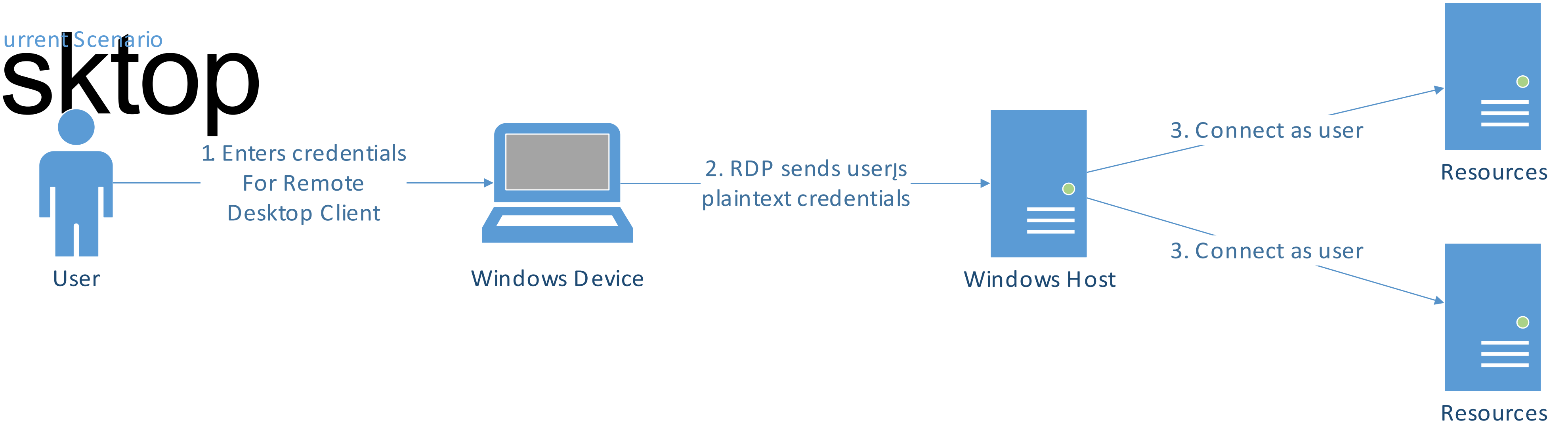
- Enable interactive administration of machines without disclosing credentials.

mitations:

- RDP connections must be initiated from a non-compromised host.

estricted Admin Mode Remote esktop

Current Scenario



User

1 Enters credentials For Remote Desktop Client

Windows Device

2. RDP sends userʅs plaintext credentials

Windows Host

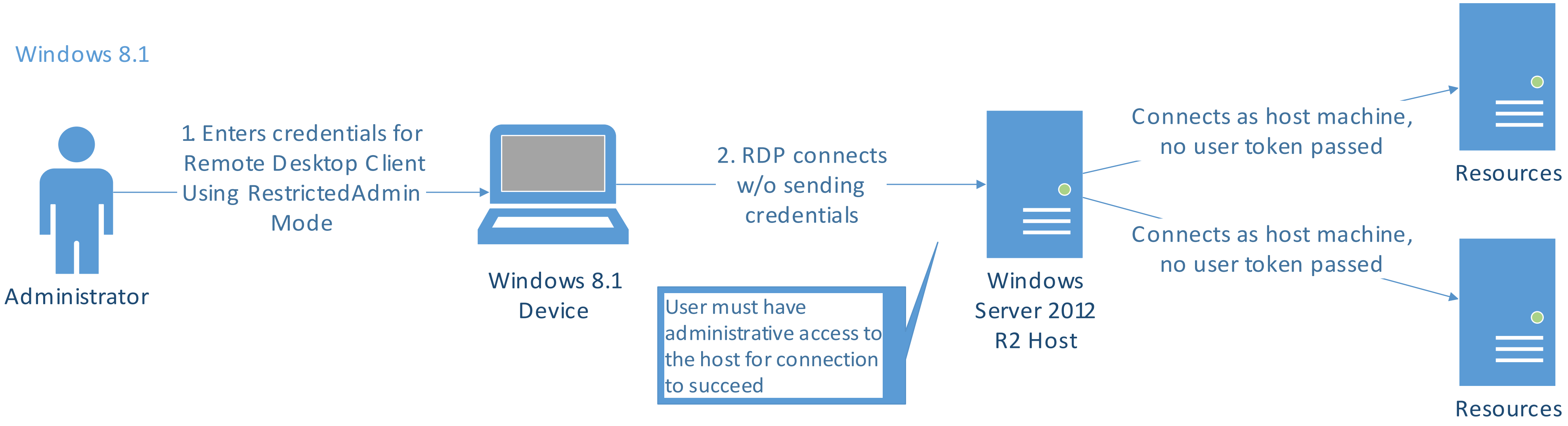
3. Connect as user

Resources

3. Connect as user

Resources

Windows 8.1



Administrator

1 Enters credentials for Remote Desktop Client Using RestrictedAdmin Mode

Windows 8.1 Device

2. RDP connects w/o sending credentials

User must have administrative access to the host for connection to succeed

Windows Server 2012 R2 Host

Connects as host machine, no user token passed

Resources

Connects as host machine, no user token passed

Resources

otected Users

Administrators and other privileged accounts can now have added protection

❖Add user to Protected Users group to enable:

- Non-configurable protections

  Only Kerberos authentication (pre-configured security settings)

  4 Hour TGT Lifetime

  Delegation forbidden

- Requires

  Windows 8.1 (or Server 2012 R2) Hosts

  Windows Server 2012 R2 Domain & DCs

otected Users

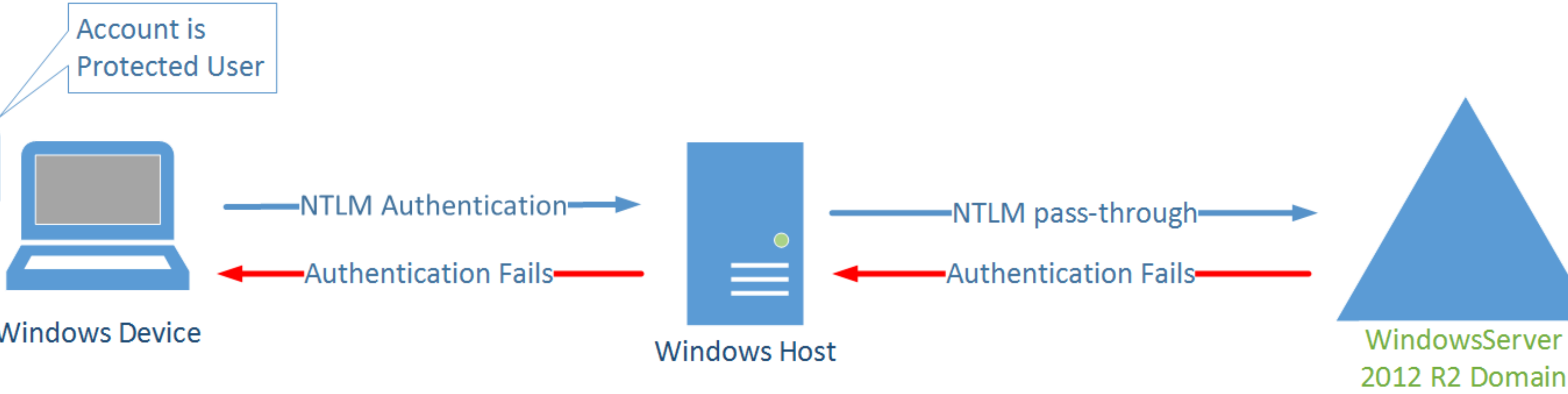
Effect:

- Restricts accounts to only using Kerberos (Required for effectiveness of Authentication Policies & Silos)

Limitations:

- Will not protect an administrator from interactively signing on to a compromised host.
- Protected Users cannot sign on if Kerberos (or dependencies) are broken

otected Users



Accounts Cannot:

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

Demos

1. Default Behavior
2. Protected User
3. RDP RestrictedAdmin

edential Storage in LSASS

	Hashes		Tspkg	Wdigest	Kerberos	LiveSSP	3rd Par SSP
	LM	NT					
	Windows 8.0						
Microsoft Account	🟥	🟥	🟥	🟥	🟩	🟥	🟥
Local Account	🟥	🟥	🟥	🟥	🟥	🟩	🟥
Domain Account	🟥	🟥	🟥	🟥	🟥	🟩	🟥
	Windows 8.1						
Microsoft Account	🟩	🟥	🟩 *	🟩 *	🟩	🟥	🟥
Local Account	🟩	🟥	🟩 *	🟩 *	🟥	🟩	🟥
Domain Account	🟩	🟥	🟩 *	🟩 *	🟩	🟩	🟥
Protected Users	🟩	🟩	🟩	🟩	🟩	🟩	🟥
estrictedAdmin RDP	🟩	🟩	🟩	🟩	🟩	🟩	🟩

* Off by default

🟩 No password data in memory

🟥 Password data in memory

e by Benjamim Delpy
entilkiwi/status/352557093640892416/photo/1)

thentication Policies & Silos

Authentication Policies – Forest-based Active Directory policies

- Apply only to accounts in Windows Server 2012 R2 domains
- Allow
  - Control of which hosts an account can sign-in to
  - Configuration of access control conditions for authentication

Authentication Policy Silos - Allows isolation of related accounts that have constrained network scope.

thentication Policies

Effect:

- Granularity on control of how accounts can be used

Limitations:

- A comprehensive network security plan must still be implemented to ensure the attack surface is reduced.
- Enforcement requires Kerberos

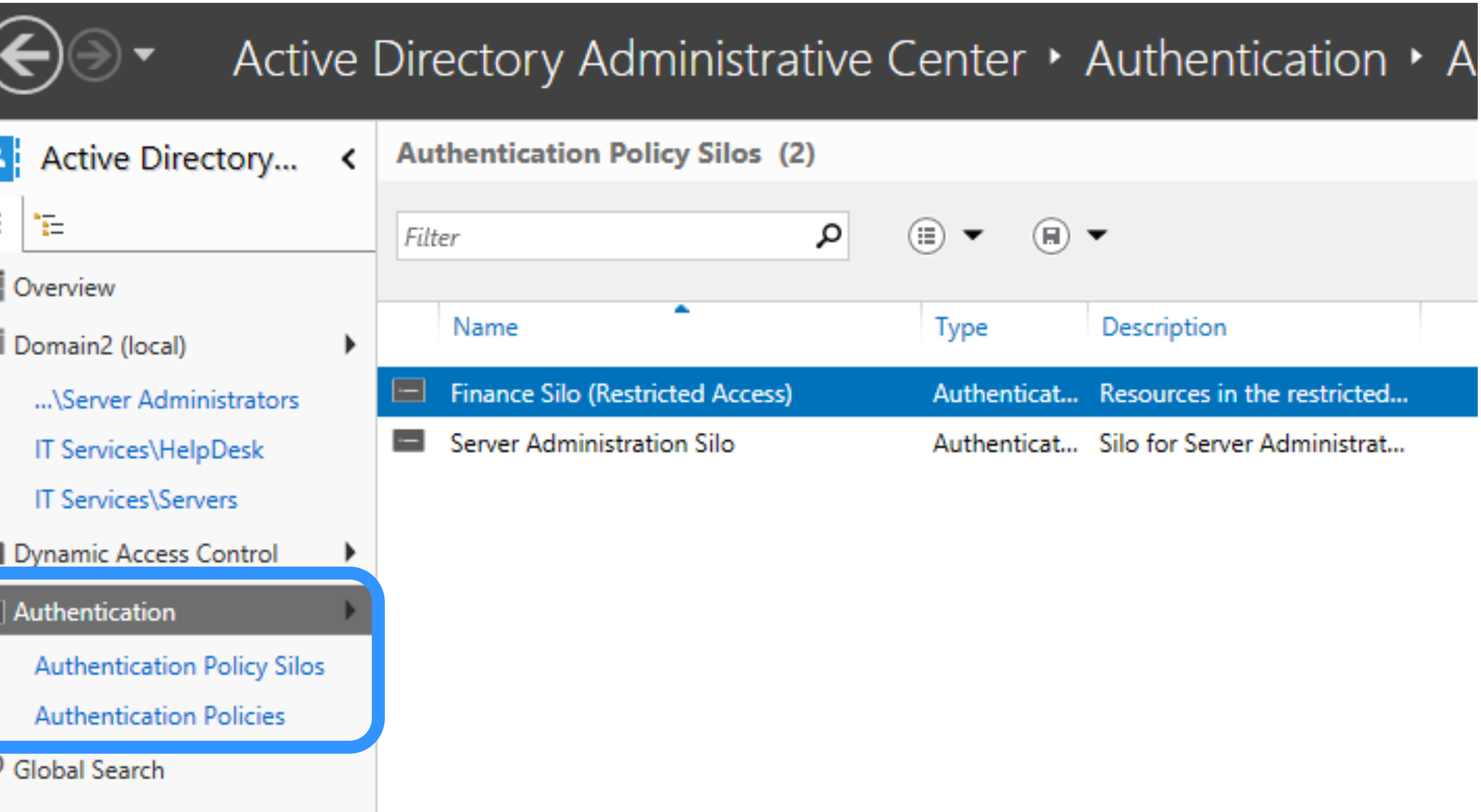
thentication Policies

New object class called Authentication Policy 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 which are referred to as Services in the UI.

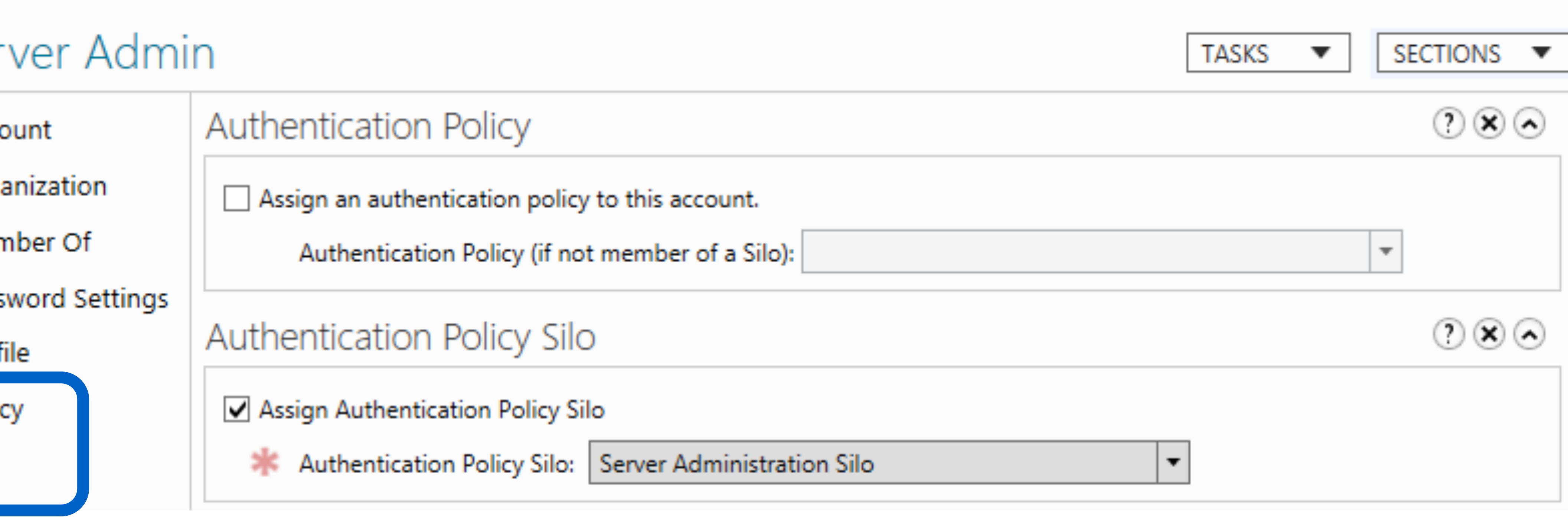
thentication Policy & Silos



Authentication Policy Silos (2)

Name	Type	Description
Finance Silo (Restricted Access)	Authenticat...	Resources in the restricted...
Server Administration Silo	Authenticat...	Silo for Server Administrat...

count Properties



Authentication Policy

□ Assign an authentication policy to this account.

Authentication Policy (if not member of a Silo):

Authentication Policy Silo

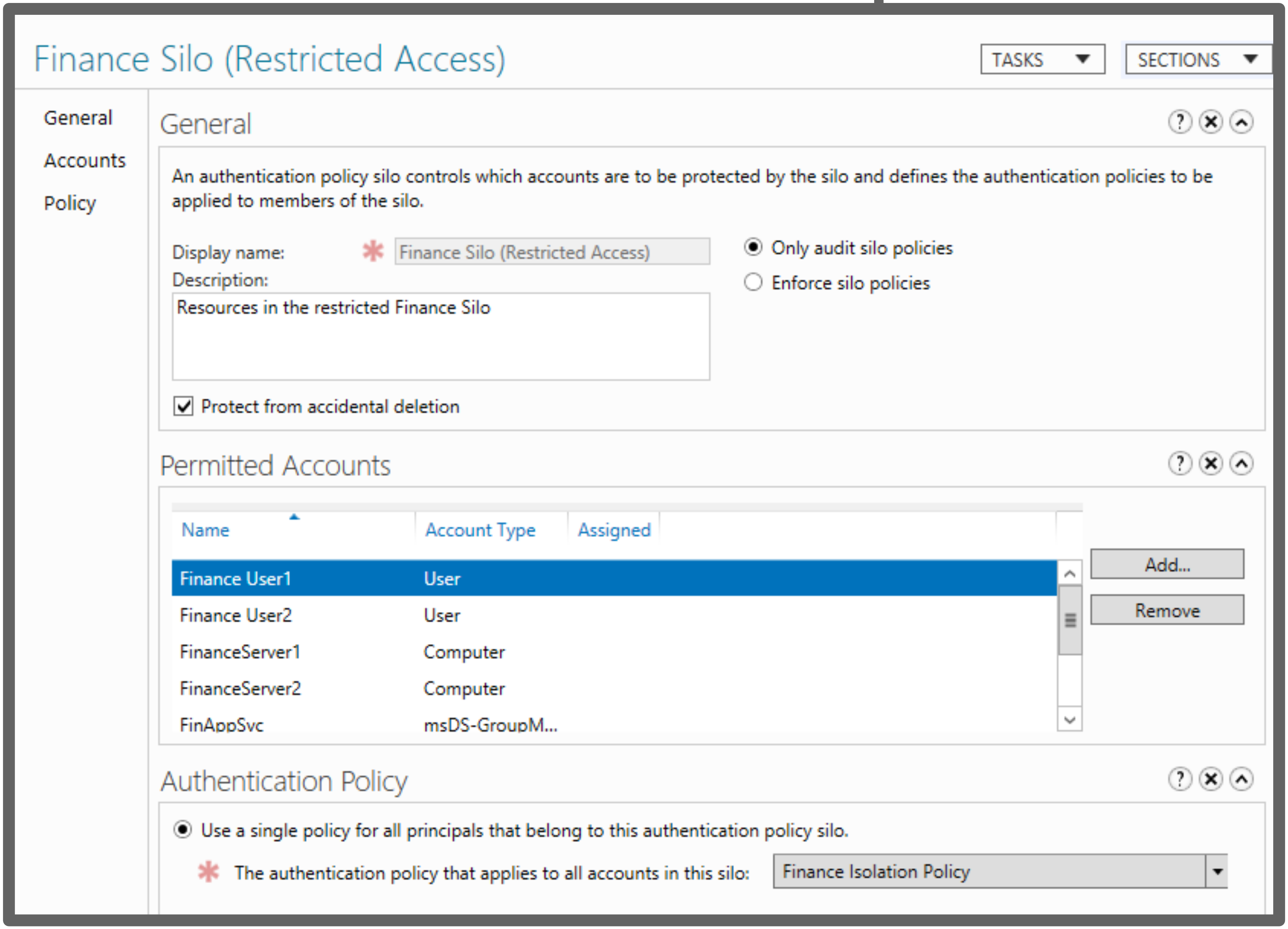
☑ Assign Authentication Policy Silo

* Authentication Policy Silo: Server Administration Silo

Account may be assigned to silo or directly to policy

- **Silo configuration takes precedence**

thentication Silo Example



Finance Silo (Restricted Access)

General

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: * Finance Silo (Restricted Access)

Description: Resources in the restricted Finance Silo

● Only audit silo policies

○ Enforce silo policies

☑ Protect from accidental deletion

Permitted Accounts

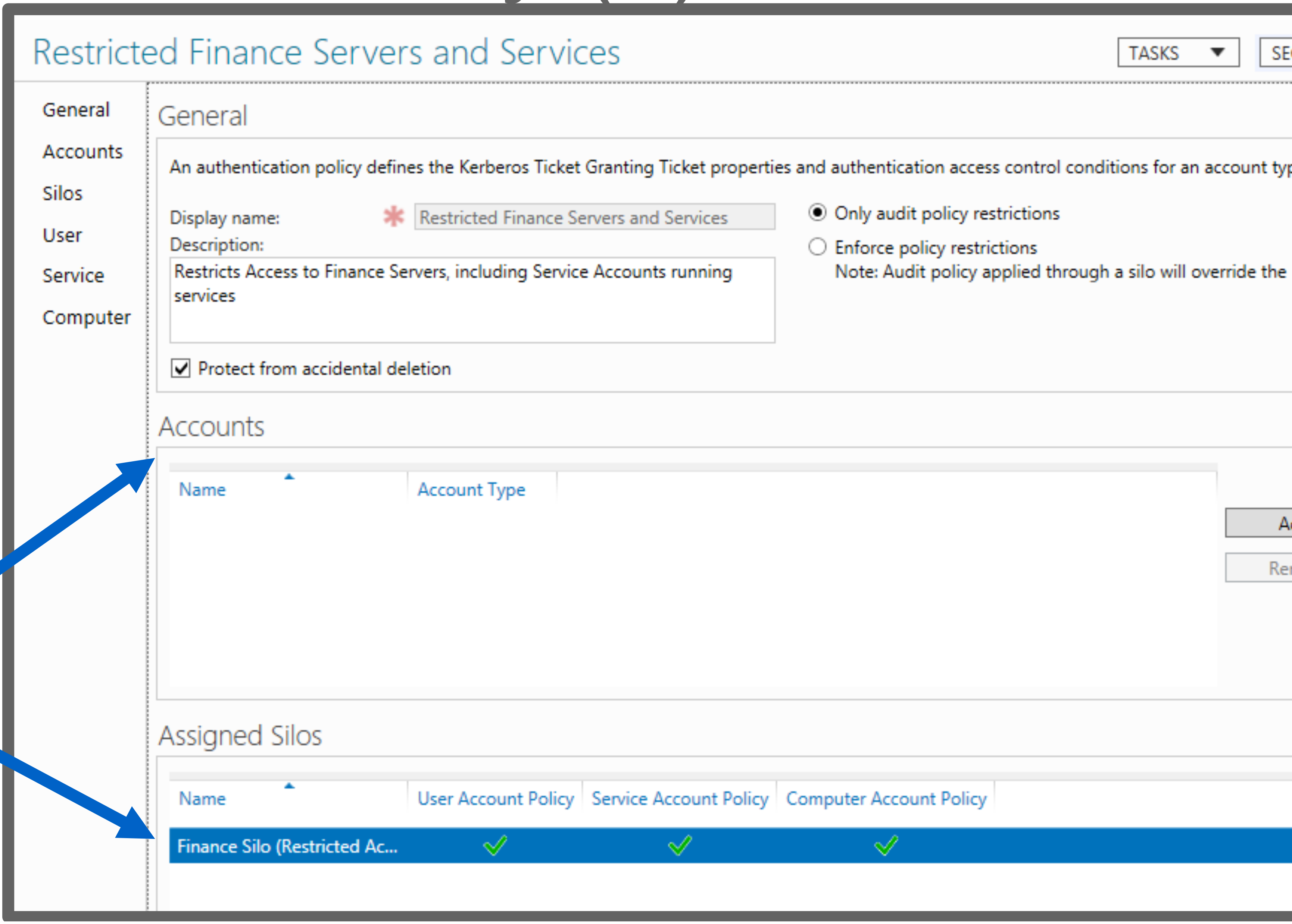
Name	Account Type	Assigned
Finance User1	User	
Finance User2	User	
FinanceServer1	Computer	
FinanceServer2	Computer	
FinAppSvc	msDS-GroupM...	

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: Finance Isolation Policy

thentication Policy (1)



Restricted Finance Servers and Services

General

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

Display name: * Restricted Finance Servers and Services

Description:

Restricts Access to Finance Servers, including Service Accounts running services

☑ Protect from accidental deletion

● Only audit policy restrictions

○ Enforce policy restrictions

Note: Audit policy applied through a silo will override the

Accounts

Name	Account Type

Assigned Silos

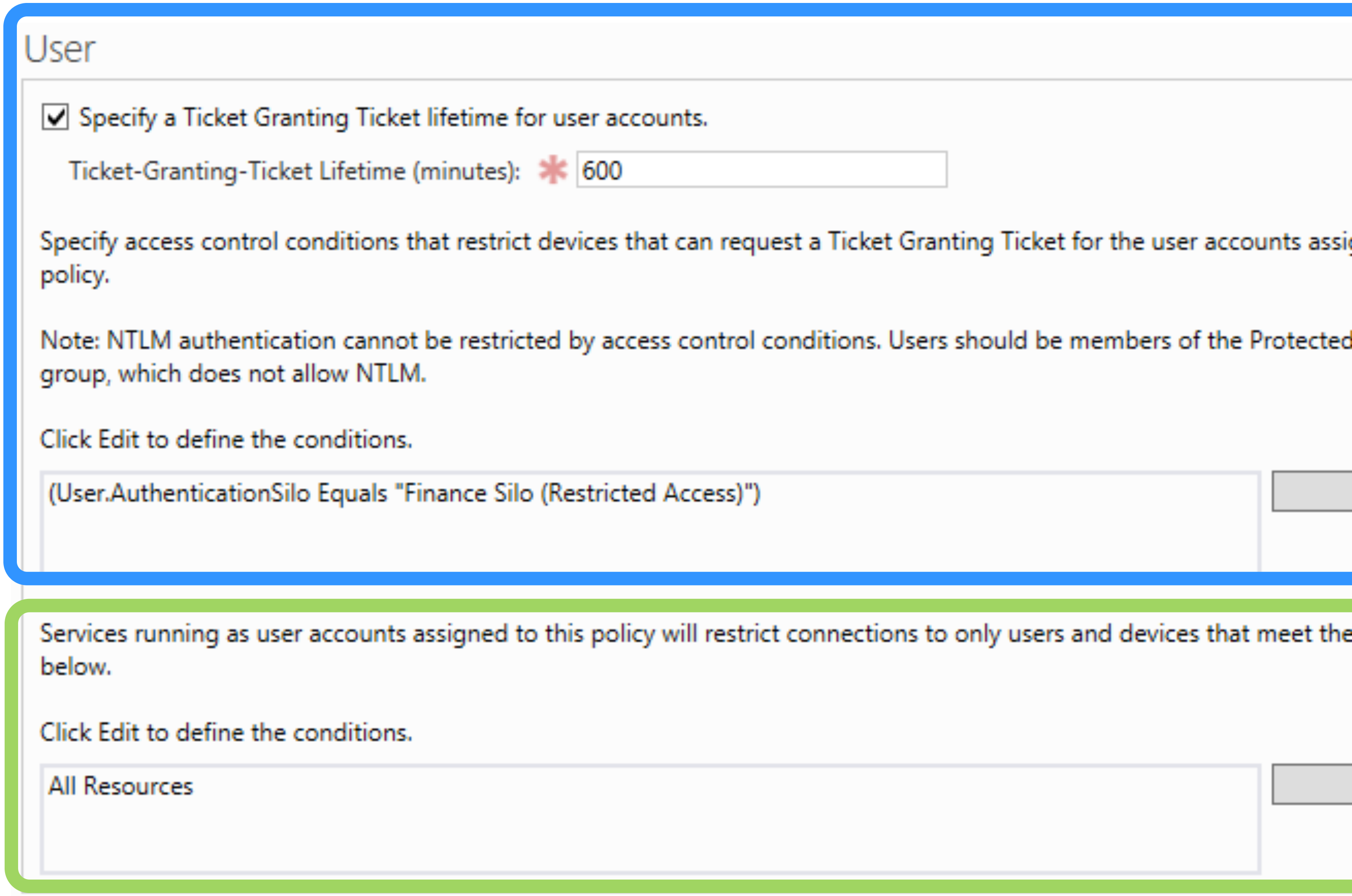
Name	User Account Policy	Service Account Policy	Computer Account Policy
Finance Silo (Restricted Ac...	✓	✓	✓

ounts or Assigned Policy

thentication Policy (2)

ere TGT
be issued
r these
counts

ounts that can
a service ticket
this account
nning service)



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 assi
policy.

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

Click Edit to define the conditions.

(User.AuthenticationSilo Equals "Finance Silo (Restricted Access)")

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

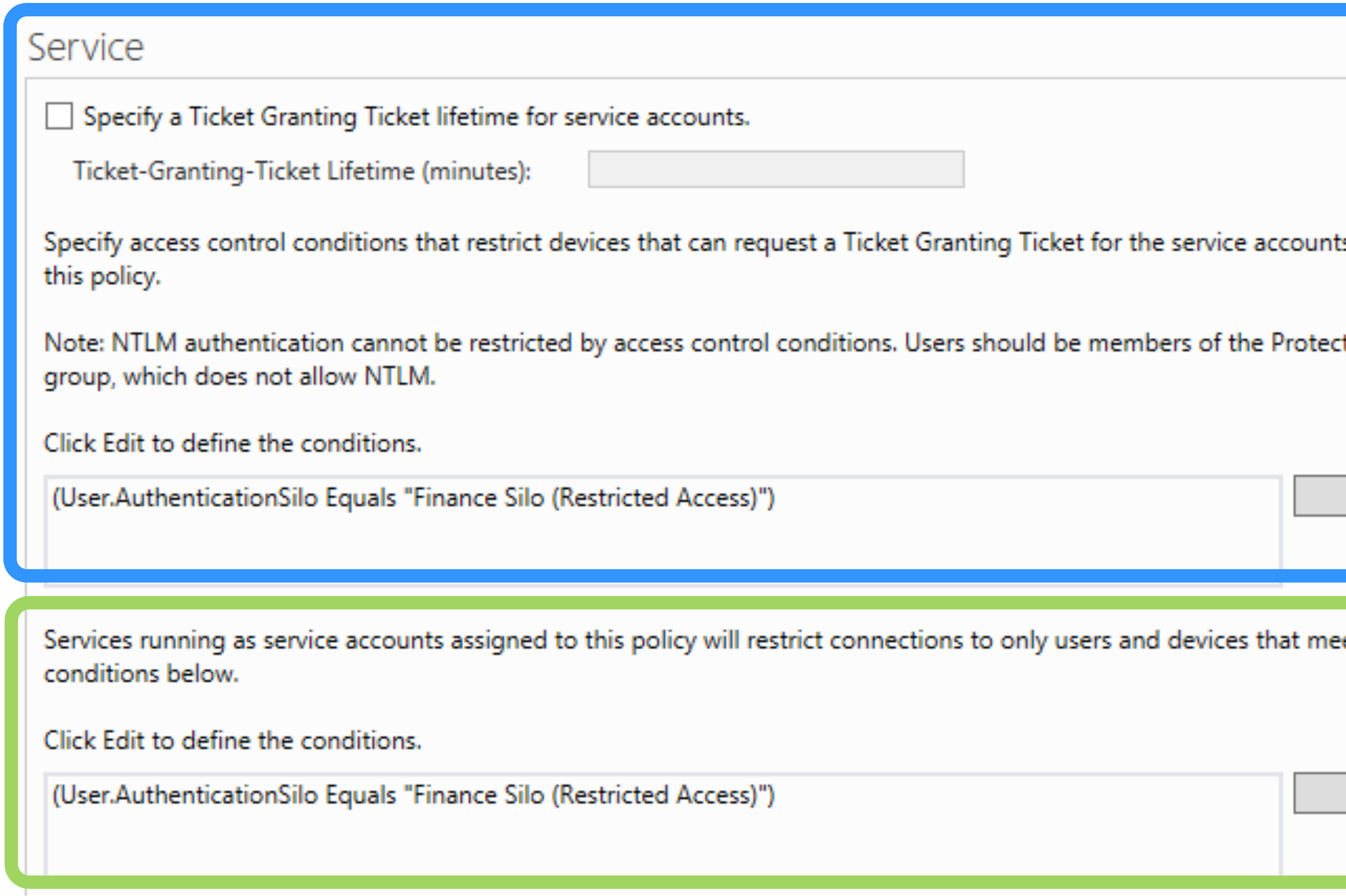
Click Edit to define the conditions.

All Resources

thentication Policy (3)

re TGT can be
ued for these
accounts

ounts that can
et a service
cket for this
count (when
ning service)



Service

□ Specify a Ticket Granting Ticket lifetime for service accounts.

Ticket-Granting-Ticket Lifetime (minutes):

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

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

Click Edit to define the conditions.

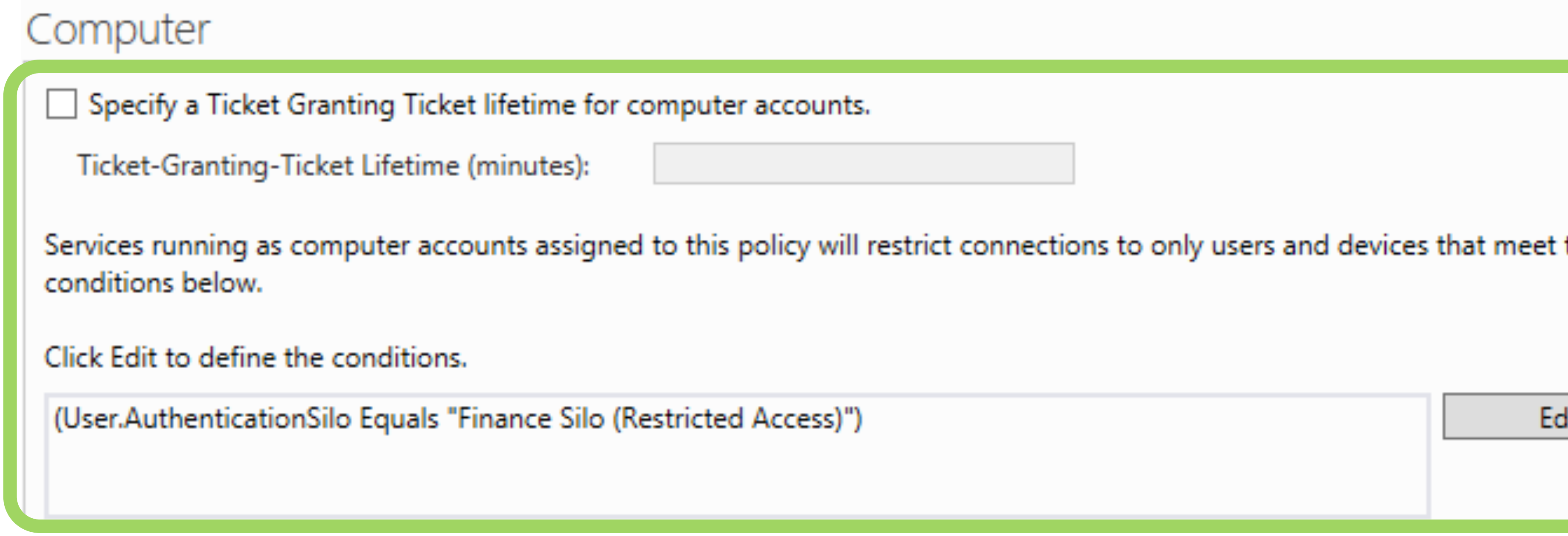
(User.AuthenticationSilo Equals "Finance Silo (Restricted Access)")

Services running as service accounts assigned to this policy will restrict connections to only users and devices that me
conditions below.

Click Edit to define the conditions.

(User.AuthenticationSilo Equals "Finance Silo (Restricted Access)")

thentication Policy (4)



Computer

☐ Specify a Ticket Granting Ticket lifetime for computer accounts.

Ticket-Granting-Ticket Lifetime (minutes):

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

Click Edit to define the conditions.

(User.AuthenticationSilo Equals "Finance Silo (Restricted Access)")

counts that can get a service ticket for this computer (and services running as system account)

SA Protection

LSA can be run as a protected process which protects the process from code injection from non protected processes.

Effect:

- Block current tools from reading LSA

Limitations:

- Not currently a security boundary
- Without Secure Boot/UEFI, it can be disabled

lore information

ndows 8.1 and Windows 8

//technet.microsoft.com/en-us/library/hh832030.aspx

ndows Server 2012 R2 and Windows Server 20

//technet.microsoft.com/en-us/library/hh801901.aspx

here are we on PtH?

Pass The Hash Workgroup formed

l steps and best practices discussed.

PtH Whitepaper released in December, 2012

Steps: Practical, effective and simple mitigations published.

Product updates proposed internally at BlueH

osed modifications reviewed by product groups.

Platform updates added to Windows 8.1, July 2013

ates available to customers.

Backport updates available to customers, TBD

ates to supported versions of Windows. Advisory will be released.

Next Steps

- **Read the Whitepaper**
  Mitigating Pass-the-Hash Attacks and other Credential Theft Techniques
  http://www.microsoft.com/en-us/download/details.aspx?id=36036

- **Questions?**
  Patrick.Jungles [at] Microsoft.com
  Mark.Simos [at] Microsoft.com

he PtH workgroup will continue to investigate mitigations for credential theft and reuse.

Want to help improve the security of our products?
We’re hiring…

Microsoft