

Advanced Identity Protection in Microsoft Entra ID

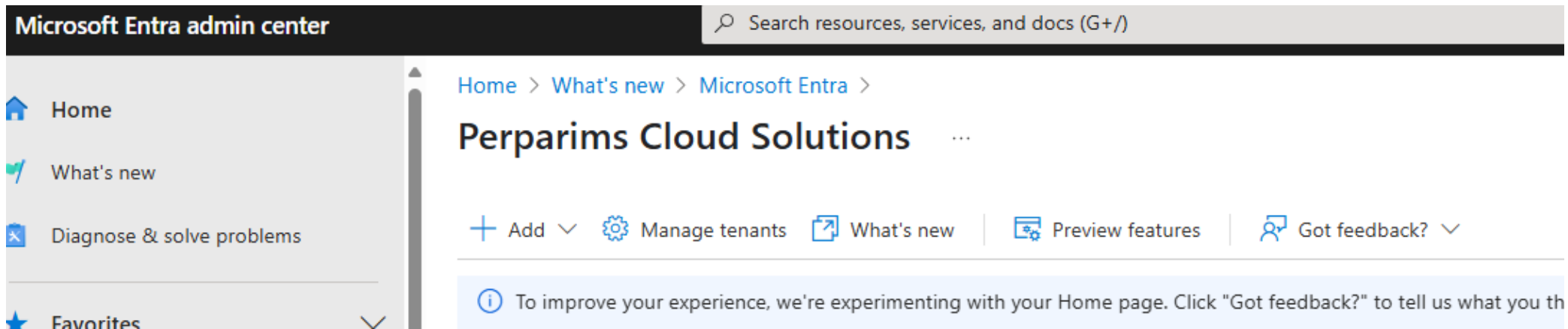
Real-World Lab: SSPR, Password Protection, Tenant Restrictions

Home > Perparims Cloud Solutions >
Perparims Cloud Solutions ...



Perparim Abdullahu | Azure Solutions Architect | SC-300 in Progress |
#PerparimLabs





Why These Identity Security Features Are Critical

- SSPR reduces helpdesk calls by allowing users to reset their passwords securely
- Password protection enforces strong credential policies in both cloud and on-prem
- Tenant restrictions prevent unauthorized access to external Microsoft tenants, reducing Shadow IT
- These tools align with **Zero Trust** and **SC-300 exam objectives**



Step 1 – Turn On SSPR

The image displays four screenshots of the Microsoft Entra admin center interface, illustrating the steps to configure Self-Service Password Reset (SSPR).

Top Left Screenshot: Shows the 'Password reset | Properties' page. The 'Self service password reset enabled' toggle is set to 'Selected'. A blue information banner states: "These settings only apply to end users in your organization. Admins are always enabled and are required to use two authentication methods to reset their password. Click here to learn more about password policies."

Top Right Screenshot: Shows the 'Password reset | Properties' page. The 'Self service password reset enabled' toggle is set to 'Selected'. A blue information banner states: "These settings only apply to end users in your organization. Admins are always enabled and are required to use two authentication methods to reset their password. Click here to learn more about password policies."

Bottom Left Screenshot: Shows the 'Password reset | Authentication methods' page. The 'Number of methods required to reset' is set to 2. A blue information banner states: "Authentication Methods for SSPR and Signin can now be managed in one converged policy. Learn more".

Bottom Right Screenshot: Shows the 'Password reset | Authentication methods' page. The 'Number of methods required to reset' is set to 2. A blue information banner states: "Authentication Methods for SSPR and Signin can now be managed in one converged policy. Learn more".

Step 1 – Turn On SSPR



Enabled SSPR for a scoped user group



Required 2 authentication methods for reset (Email + Phone)



Reviewed legacy and modern SSPR configuration methods



Microsoft is migrating SSPR & MFA to the centralized **Authentication Methods** blade

Configure Cloud-Based Password Protection

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Perparims Cloud Solutions | Security > Security | Authentication methods > Authentication methods

Authentication methods | Password protection

Perparims Cloud Solutions - Microsoft Entra ID Security

Search

Save Discard Got feedback?

Manage

- Policies
- Password protection**
- Registration campaign
- Authentication strengths
- Settings
- Monitoring

Custom smart lockout

Lockout threshold ①

Lockout duration in seconds ①

Custom banned passwords

Enforce custom list ① ☒ Yes ☐ No

Custom banned password list ①

Welcome123
Admin2025

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ① ☒ Yes ☐ No

Mode ① ☐ Enforced ☒ Audit

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Perparims Cloud Solutions | Security > Security | Authentication methods > Authentication methods

Authentication methods | Password protection

Perparims Cloud Solutions - Microsoft Entra ID Security

Search

Save Discard Got feedback?

Manage

- Policies
- Password protection**
- Registration campaign
- Authentication strengths
- Settings
- Monitoring

Custom smart lockout

Lockout threshold ①

Lockout duration in seconds ①

Custom banned passwords

Enforce custom list ① ☒ Yes ☐ No

Custom banned password list ①

Welcome123
Admin2025

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ① ☒ Yes ☐ No

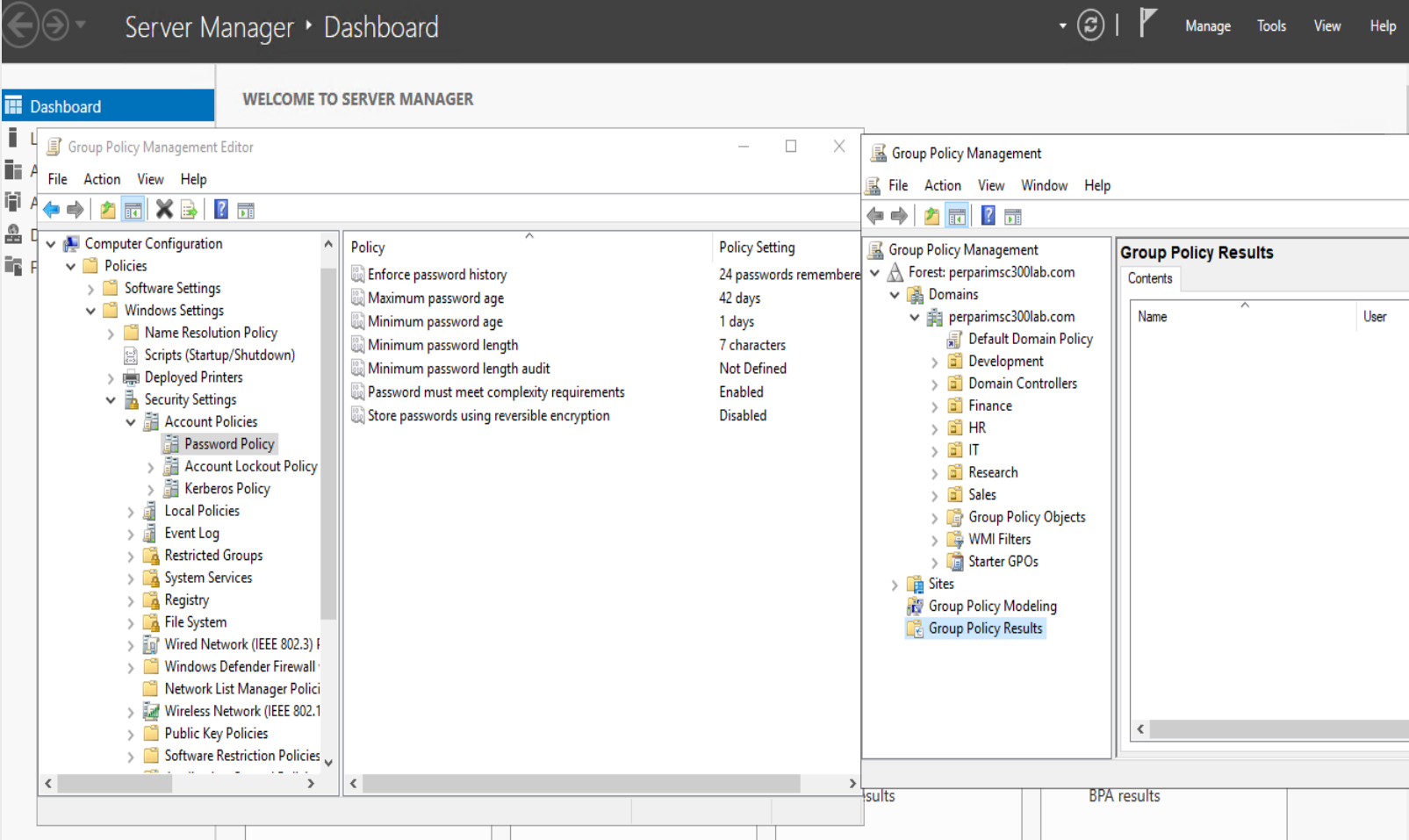
Mode ① ☐ Enforced ☒ Audit

Configure Cloud-Based Password Protection

- Configured lockout after **5 failed sign-in attempts**
- Lockout duration set to **5 minutes**
- Enabled **custom banned passwords** to block weak and common credentials
- Set **Enforce Mode** to block policy violations in real time
- Applies to **cloud-only users**, not those synced from on-prem

On-Prem Password Policy Management (AD DS)

- Configured password policy via **Default Domain Policy**
- Enforced password **complexity and length**
- Set **expiration** and **history requirements** to prevent reuse
- Applies only to **on-prem synced users**, not cloud-only users
- Synced to Microsoft Entra ID via Entra Connect



The screenshot displays the Windows Server Manager interface with the Group Policy Management console open. The console shows the configuration of the Default Domain Policy for the forest perparimsc300lab.com. The left pane shows the hierarchy: Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy. The right pane shows the following settings:

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

The Group Policy Results window is also visible, showing the results for the Default Domain Policy. The 'Contents' tab is active, displaying a list of domains and their associated policies. The 'Group Policy Results' tab is also visible, showing the results for the Default Domain Policy.



What You Learned – SSPR Essentials

- **SSPR = Self-Service Password Reset**

Lets users reset their own passwords securely without admin help

- **Not enabled by default**

Must be turned on for all users or selected groups

- **Two-step setup:**

1. Enable SSPR
2. Define authentication methods (e.g., phone, email, security questions)

- **Modern configuration** is now done via **Authentication Methods blade**
(Same place as MFA setup)

- **Reduces helpdesk load** and aligns with **Zero Trust** security principles

Every password reset that doesn't hit the helpdesk is time saved. Set up SSPR and empower users — securely

On-Prem Password Policy Management (AD DS)

- Configured using **Group Policy Management Console (GPMC)**

Path: Default Domain Policy > Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy

- Key settings include:
 - Password history, complexity, minimum/maximum age
 - Minimum password length (e.g., 7+ characters)

- **Account Lockout Policy** also managed here
 - Define lockout threshold, duration, and reset counter

- These policies **apply to all domain-synced users**
(Cloud-only users follow Entra ID password policies)

- Avoid enabling “**Store passwords using reversible encryption**” — weakens security

Strong on-prem policies +
cloud protections = hybrid
identity security done right

