Securing Your 365 Tenant

Presented by: Craig Williams
& Brad Jepsen

NETWORKS
PLUS

In the beginning…

- Passwords as the first line of defense
- App passwords for legacy authentication
- Per-user MFA (optional)
- Basic role-based access control

NETWORKS PLUS

Introduction of Security Defaults

1. Multi-Factor Authentication Enforcement

- Required for all users, including privileged roles
- Enforce MFA registration

2. Block Legacy Authentication

- Disable protocols that don’t support modern security standards
  - IMAP
  - POP
  - SMTP Auth

Microsoft eventually enforced security defaults on all existing tenants and
Enabled by default on all newly created tenants

NETWORKS
PLUS

Downsides of Security Defaults

1. Lacks customization

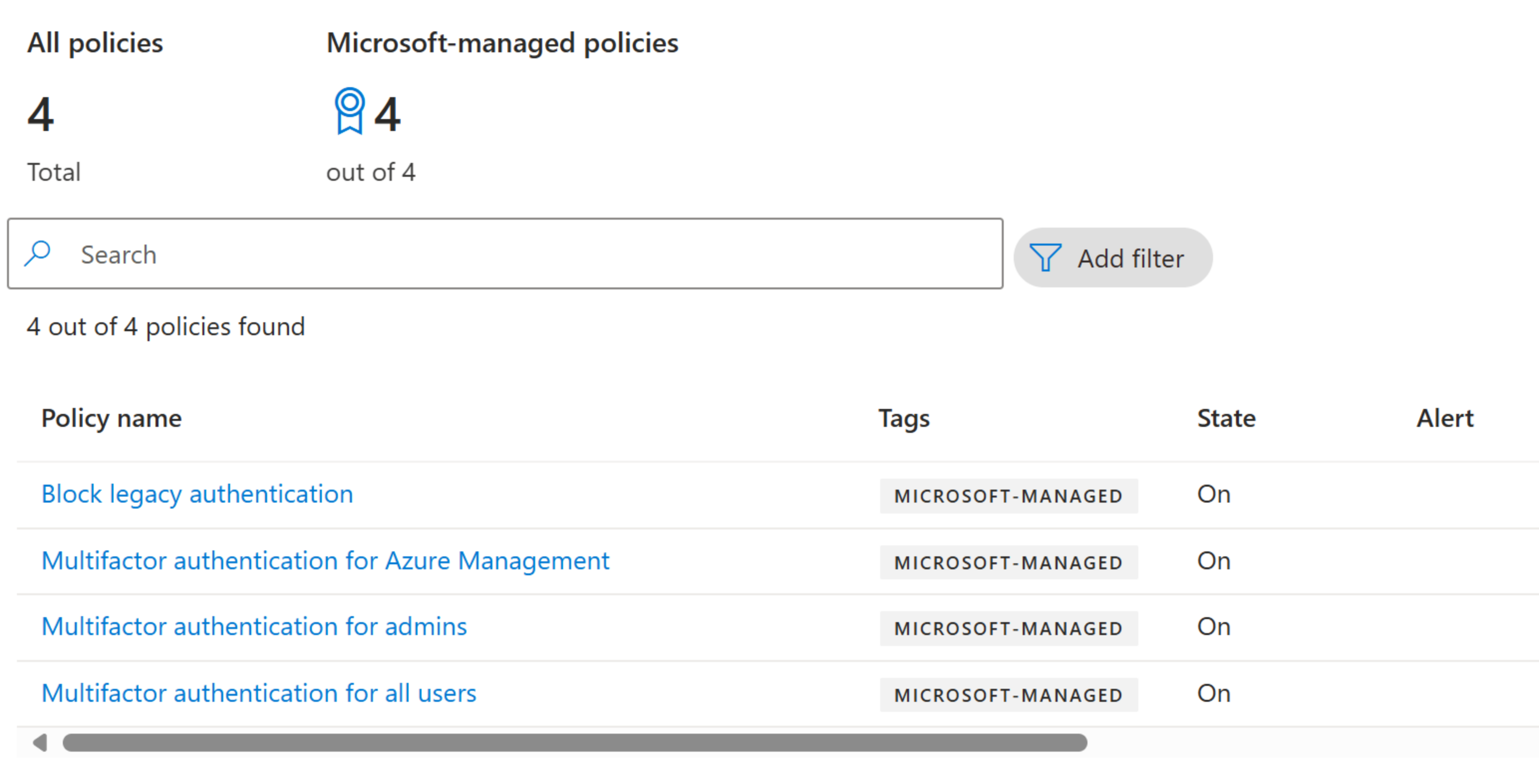
- You **can’t exclude users or groups** (e.g., service accounts, break-glass admin accounts).
- No exception for Legacy apps

NETWORKS PLUS

Shifting to Conditional access

1. Disabling security defaults

- Option to create Microsoft managed policies



All policies

4

Total

Microsoft-managed policies

4

out of 4

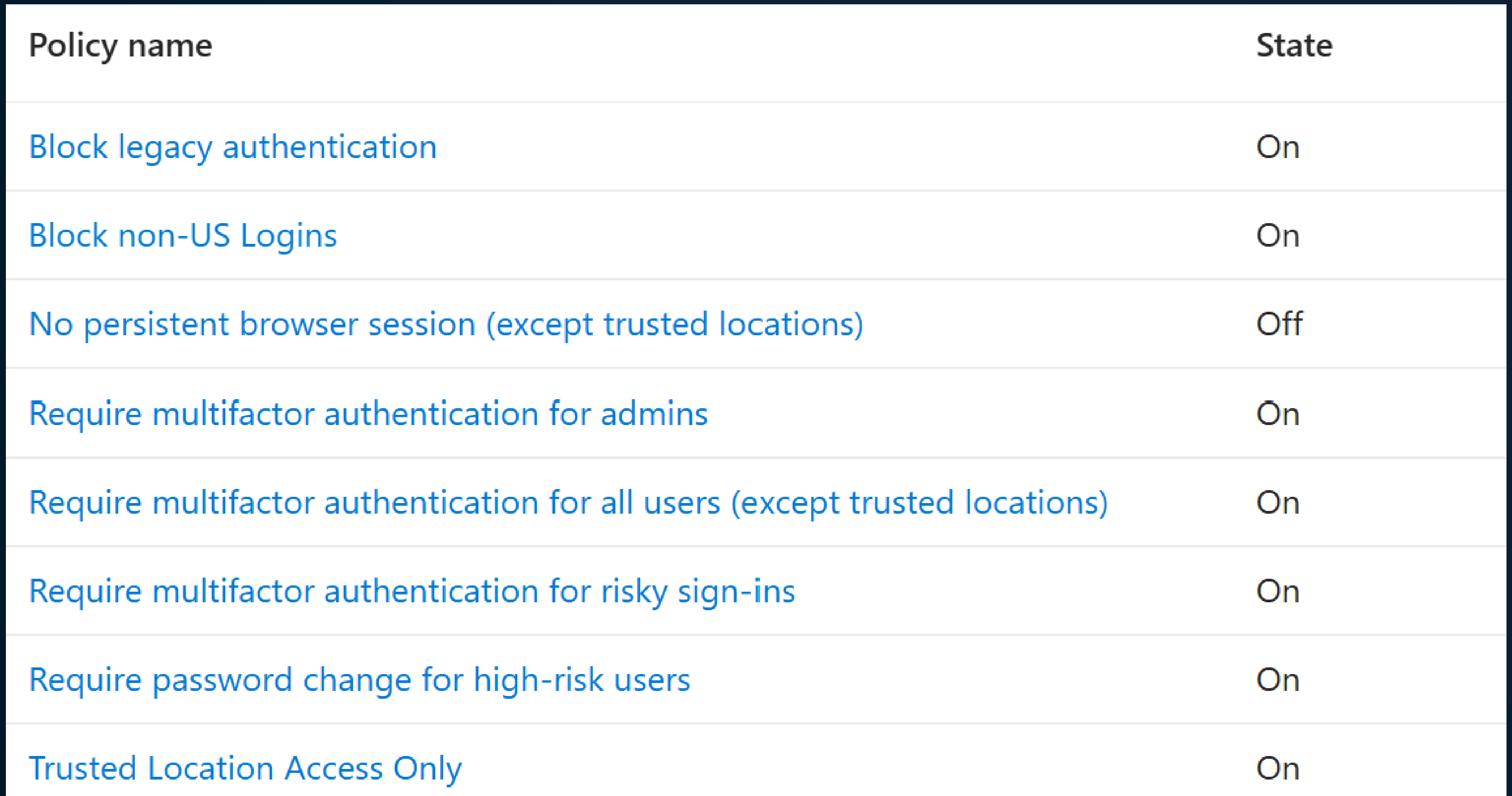
4 out of 4 policies found

Policy name	Tags	State	Alert
Block legacy authentication	MICROSOFT-MANAGED	On	
Multifactor authentication for Azure Management	MICROSOFT-MANAGED	On	
Multifactor authentication for admins	MICROSOFT-MANAGED	On	
Multifactor authentication for all users	MICROSOFT-MANAGED	On	

NETWORKS PLUS

Conditional access

- Entra ID P1 is required to use conditional access policies
- Included with Business Premium, E3 & E5
- More advanced Risk based policies wit Entra ID P2 license, included with E5 licensing or individually



Policy name	State
Block legacy authentication	On
Block non-US Logins	On
No persistent browser session (except trusted locations)	Off
Require multifactor authentication for admins	On
Require multifactor authentication for all users (except trusted locations)	On
Require multifactor authentication for risky sign-ins	On
Require password change for high-risk users	On
Trusted Location Access Only	On

NETWORKS
PLUS

Application Registration & Consent

- Often overlooked security hole
- Users can self-register apps and grant access permissions
- This poses risks if unmanaged — potential for excessive privilege
- Administrative consent flows help control and audit app access

NETWORKS
PLUS

Malicious App Consent – A Persistent Threat

OAuth-based app consent can create long-term access backdoors:

- Apps retain access using refresh tokens – even after a password reset
- No MFA challenge is triggered once access is granted
- Access continues via API without user interaction
- Password resets alone do not invalidate OAuth tokens

Protecting your session token

Prevent token replay attacks
Hello, Violet
Token
Microsoft

```
>steal_token|

...
Access is denied.
```

Reviewing Your Tenant’s Security Posture

Microsoft Secure Score

- Provides a quantified score representing your current security posture
- Recommends prioritized improvement actions across identity, apps, devices, and data

Microsoft 365 Compliance Score

- Located in the Microsoft Purview compliance portal
- Measures adherence to compliance requirements and regulatory standards

CIS Microsoft 365 Benchmark

- Industry-standard baseline developed by the Center for Internet Security (CIS)
- Provides secure configuration guidance for M365 services
- https://www.cisecurity.org/cis-benchmarks

NETWORKS
PLUS

QUESTION & CONTACT PAGE

Craig Williams
Brad Jepsen

NETWORKS PLUS

networksplus.com

website

support@networksplus.com

Email