Microsoft 365 Business Premium

Learning Lab

Complete Hybrid Infrastructure, Domain, Entra & Intune Deployment

Public Portfolio Edition - Corrected, Expanded & Illustrated

Source boundary: initial VMware server build through final Windows security configuration, managed-device synchronization, and Intune validation

August 22, 2026

Prepared and documented by Jeremy Bernsdorff
jeremybernsdorff.com

Copyright © 2026 Jeremy Bernsdorff. All rights reserved.

Evidence labels: [RECORDED] [RECONSTRUCTED] [NOT RECOVERED]

Publication & Copyright Notice

Authorship

This learning reference was prepared and documented by Jeremy Bernsdorff from his hands-on Microsoft 365 Business Premium learning lab, retained screenshots, command output, administrative state, and reconstruction notes.

Copyright

Copyright © 2026 Jeremy Bernsdorff. All rights reserved. No part of this publication may be reproduced, republished, sold, or redistributed as a substantially complete work without written permission from the copyright holder. Brief quotations and links to the publicly hosted copy are permitted with attribution.

Portfolio purpose

This document is published as a professional portfolio artifact and learning reference. It demonstrates lab work, troubleshooting methodology, documentation practice, and technical learning; it is not a claim of production administration for any employer or client unless explicitly stated.

Independent publication and trademarks

This is an independent learning-lab publication. It is not an official Microsoft, VMware, or Broadcom publication and is not sponsored by or affiliated with those companies. Microsoft, Microsoft 365, Windows, Windows Server, Microsoft Entra, Intune, and related names and interface elements are trademarks or product identifiers of Microsoft Corporation. VMware and related marks are trademarks or product identifiers of Broadcom Inc. or its affiliates. Other product names and marks belong to their respective owners.

Screenshots

Administrative-console and operating-system screenshots are included as documentary evidence of the lab environment and for educational, commentary, and portfolio purposes. They remain subject to the rights of their respective software publishers.

Accuracy and evidence labels

The document distinguishes recorded evidence from reconstruction. [RECORDED] identifies material directly supported by surviving evidence; [RECONSTRUCTED] identifies actions established by the discussion where exact details were not retained; [NOT RECOVERED] identifies details intentionally left unspecified rather than invented.

Public copy

Author: Jeremy Bernsdorff
Portfolio: jeremybernsdorff.com
Edition date: August 22, 2026

How to Read This Reconstruction

Documentation and reconstruction by Jeremy Bernsdorff

This edition preserves the original infrastructure and endpoint-management reconstruction, including its recorded screenshots, and extends the learning sequence through Intune Windows security configuration, PowerShell execution policy, SmartScreen, device synchronization, automatic background check-in, and final profile-level validation.

[RECORDED] - directly supported by surviving discussion, screenshots, logs, command output, or administrative state.
[RECONSTRUCTED] - the action occurred, but the exact click path, command, or value was not retained.
[NOT RECOVERED] - the exact value or action is not recoverable and is not invented.

Contents

1. Final Lab Architecture and Control Planes

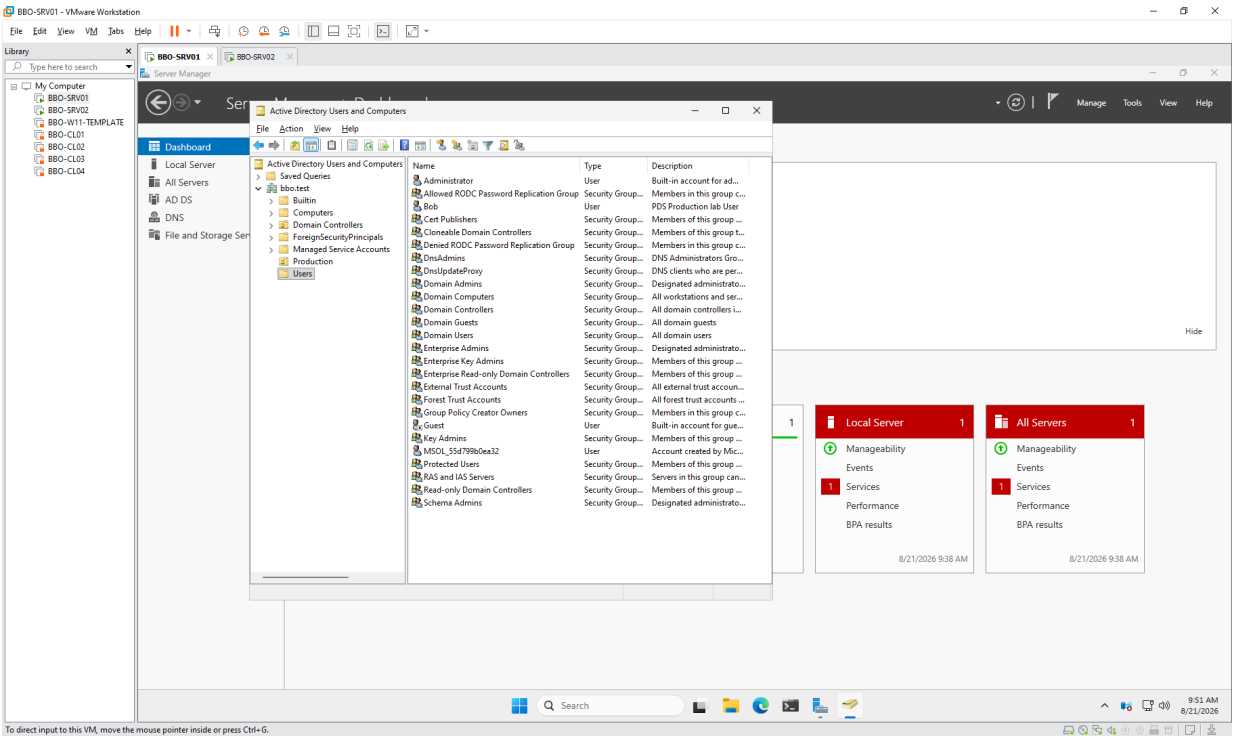

Figure 1 - VMware fleet, BBO-SRV01 Server Manager, and Active Directory Users and Computers.

What this demonstrates: The lab is a coordinated environment: multiple VMware VMs, Windows Server roles, and the bbo.test directory are visible together.

The lab became a small hybrid enterprise environment rather than merely a set of domain-joined VMs. VMware supplied the virtual infrastructure; Windows Server supplied AD DS/DNS; BBO-SRV02 bridged on-premises identity to Microsoft Entra ID; Windows 11 clients were generalized and cloned; Microsoft Intune managed the endpoints and evaluated compliance.

```
Windows 10 Pro host (PocketBookWin10)
  VMware Workstation 26.0.0 build 25388281
  VMnet8 NAT: 192.168.219.0/24
    |
    +-- BBO-SRV01  -> AD DS + DNS -> bbo.test
    +-- BBO-SRV02  -> Microsoft Entra Connect / directory synchronization
    +-- BBO-W11-TEMPLATE
        +-- BBO-CL01
        +-- BBO-CL02
        +-- BBO-CL03
        +-- BBO-CL04
    |
    +-- Microsoft Entra ID / Microsoft Intune / Microsoft 365 tenant
```

A useful mental model is that the lab spans four related but distinct control planes:

Control plane	Primary purpose
VMware	Virtual hardware, snapshots, cloning, NAT networking
Active Directory / DNS	On-premises identity, computer membership, authentication, domain discovery
Microsoft Entra ID	Cloud identity and hybrid device identity
Microsoft Intune	Endpoint enrollment, management, policy, sync, and compliance evaluation

2. VMware Host and First Windows Server VM

[RECORDED] The original first server VM was created as PDS-SRV01. VMware retained the library path even after the Windows guest was renamed:

```
C:\Users\PocketBook10\Documents\Virtual Machines\PDS-SRV01\PDS-SRV01.vmx
```

[RECORDED] Windows Server 2025 Standard Evaluation media was used. VMware NAT networking provided Internet access while keeping the lab on a private subnet.

[NOT RECOVERED] Exact first-day server vCPU, RAM, virtual disk capacity, were not preserved; the later recorded static IPv4 address was 192.168.219.10.

Troubleshooting and Resolution

What went wrong: VMware temporarily reported that BBO-SRV01 was being edited after virtual-hardware work.

Symptoms / evidence: The edit operation was still progressing; Windows Server itself had not failed.

What was done: No additional edits were made while VMware committed the configuration.

What resolved it: The VMware operation completed on its own.

Operational lesson: Distinguish a hypervisor management-state message from a guest operating-system failure before taking destructive action.

3. PDS-to-BroadbandOps Naming Reframe

[RECORDED] The environment was renamed from the earlier PDS-oriented lab to BroadbandOps conventions. The server guest became BBO-SRV01, client names became BBO-CLxx, and the new AD forest/domain became bbo.test.

Renaming before domain-controller promotion reduced later DNS/SPN/replication complexity. A VMware folder can retain an old name even when the Windows hostname has changed; the two naming layers should not be confused.

4. Server Networking Before AD DS

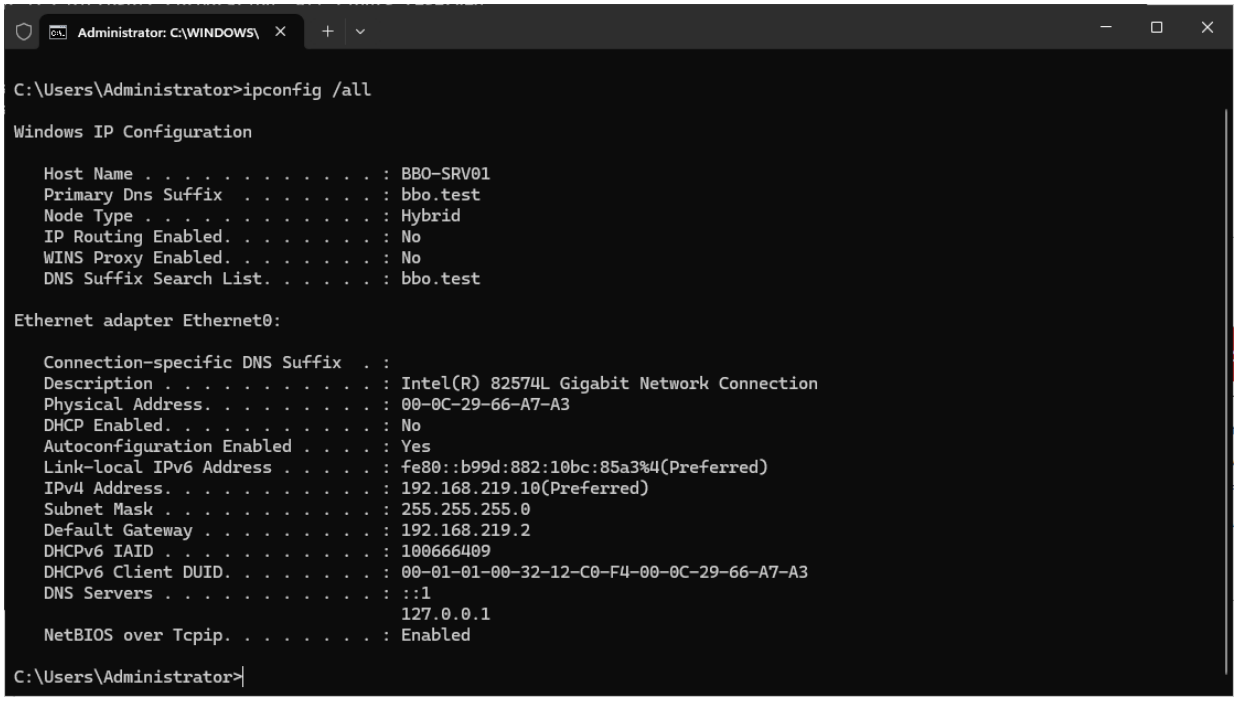

Figure 2 - Recorded BBO-SRV01 TCP/IP configuration.

What this demonstrates: BBO-SRV01 is using 192.168.219.10/24 with VMware NAT gateway 192.168.219.2; DHCP is disabled and local DNS is in use.

Item	Recorded value
VMware network	VMnet8 / NAT
NAT subnet	192.168.219.0/24
Dynamic server address observed	192.168.219.128
Default gateway observed	192.168.219.2
Pre-AD DNS observed	192.168.219.2

[RECORDED] BBO-SRV01 later showed static IPv4 address 192.168.219.10/24, gateway 192.168.219.2, DHCP disabled, and local DNS on ::1 / 127.0.0.1. After DNS installation, domain clients needed to use the AD DNS service rather than only VMware's NAT resolver.

```
Get-NetIPConfiguration

New-NetIPAddress -InterfaceAlias "Ethernet" `
 -IPAddress <BBO-SRV01-STATIC-IP> `
 -PrefixLength 24 `
 -DefaultGateway 192.168.219.2

Set-DnsClientServerAddress -InterfaceAlias "Ethernet" `
 -ServerAddresses <BBO-SRV01-STATIC-IP>
```

Troubleshooting and Resolution

What went wrong: The initial DHCP/NAT-provided configuration was not appropriate as the permanent identity of the first DC/DNS server.

Symptoms / evidence: The server initially depended on VMware's NAT DNS, which cannot host the private AD-integrated bbo.test zone.

What was done: A stable server address and AD DNS configuration were established.

What resolved it: The domain controller became the DNS authority used for AD discovery.

Operational lesson: For AD join failures, DNS is one of the highest-value first checks.

5. Install AD DS/DNS and Create bbo.test

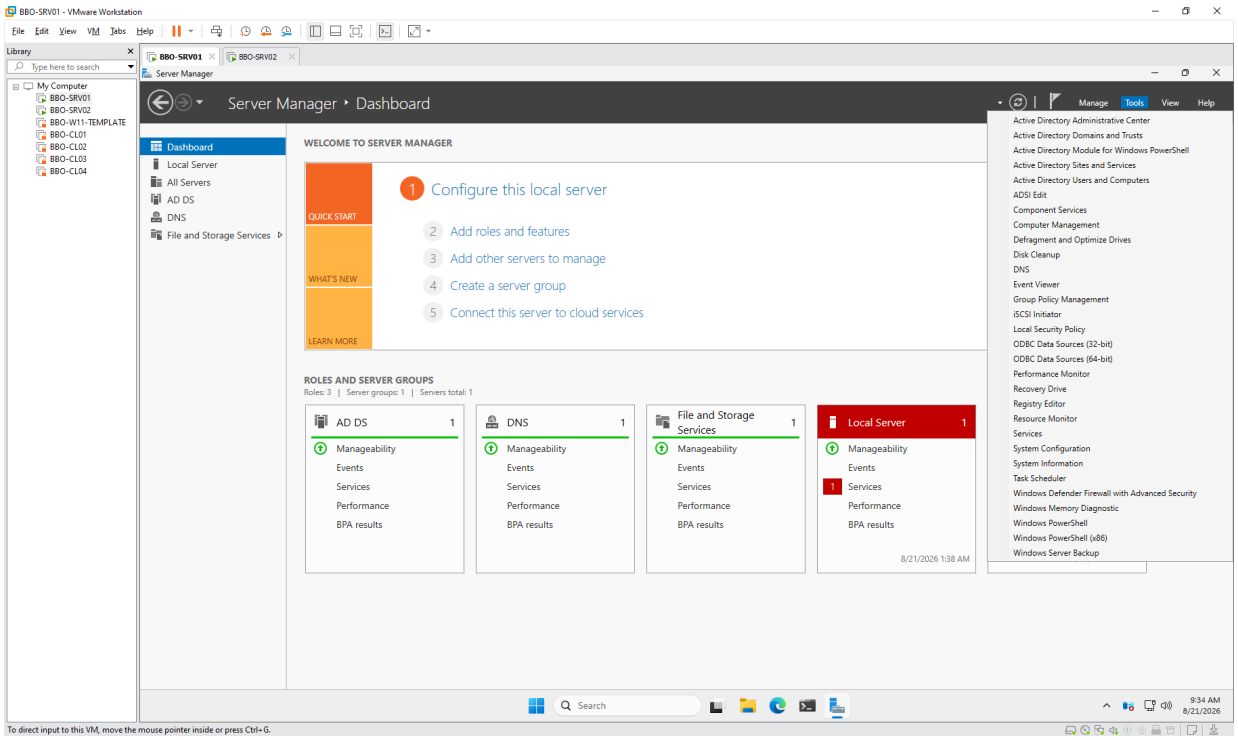

Figure 3 - BBO-SRV01 Server Manager showing AD DS and DNS roles.

What this demonstrates: The first server is operating as the AD DS/DNS platform and exposes the expected Active Directory administrative tools.

1. Open Server Manager > Manage > Add Roles and Features.
2. Choose Role-based or feature-based installation and select BBO-SRV01.
3. Add Active Directory Domain Services and its management tools; include DNS for the first domain controller.
4. After installation, choose Promote this server to a domain controller.
5. Choose Add a new forest and enter bbo.test.
6. Set the Directory Services Restore Mode password, complete prerequisite checks, promote, and restart.

Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
Install-ADDSForest -DomainName "bbo.test" -InstallDNS

Get-ADDomain
Get-ADForest
Get-Service ADWS,DNS,Netlogon,KDC

6. Active Directory Administration

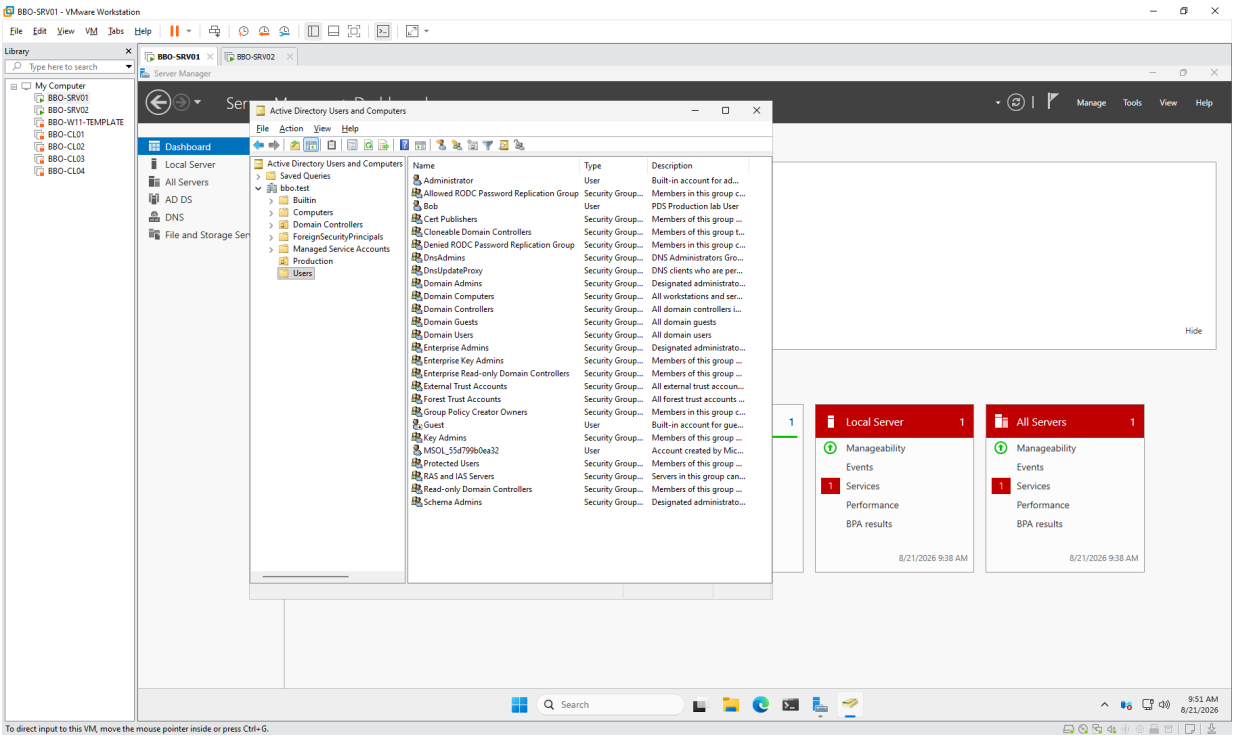

Figure 4 - Active Directory Users and Computers for bbo.test.

What this demonstrates: The directory tree and built-in Users container are visible, reinforcing the CN=Users versus OU=Users distinguished-name lesson.

Get-ADUser -Filter *
Get-ADGroup -Filter *
Get-ADComputer -Filter *
Get-ADGroupMember -Identity "Production-Users"
Get-ADPrincipalGroupMembership -Identity "alice"

The two membership commands answer opposite questions: Get-ADGroupMember asks who is in a group; Get-ADPrincipalGroupMembership asks which groups a principal belongs to.

6.1 The Users container syntax mistake

The default Users location is a container (CN), not an Organizational Unit (OU).

Incorrect:
OU=Users,DC=bbo,DC=test

```
Correct:
CN=Users,DC=bbo,DC=test
$password = Read-Host "Temporary password" -AsSecureString
New-ADUser `
  -Name "Alice Example" `
  -GivenName "Alice" `
  -Surname "Example" `
  -SamAccountName "alice" `
  -UserPrincipalName "alice@bbo.test" `
  -AccountPassword $password `
  -Enabled $true `
  -ChangePasswordAtLogon $true `
  -Path "CN=Users,DC=bbo,DC=test"
```

Troubleshooting and Resolution

What went wrong: A New-ADUser path treated the built-in Users container as OU=Users.

Symptoms / evidence: User creation failed even though the rest of the command was essentially valid.

What was done: The distinguished name was corrected to CN=Users,DC=bbo,DC=test.

What resolved it: The object was targeted at the actual AD container type/path.

Operational lesson: CN= and OU= are not interchangeable labels in a distinguished name.

7. BBO-SRV02 and Microsoft Entra Connect

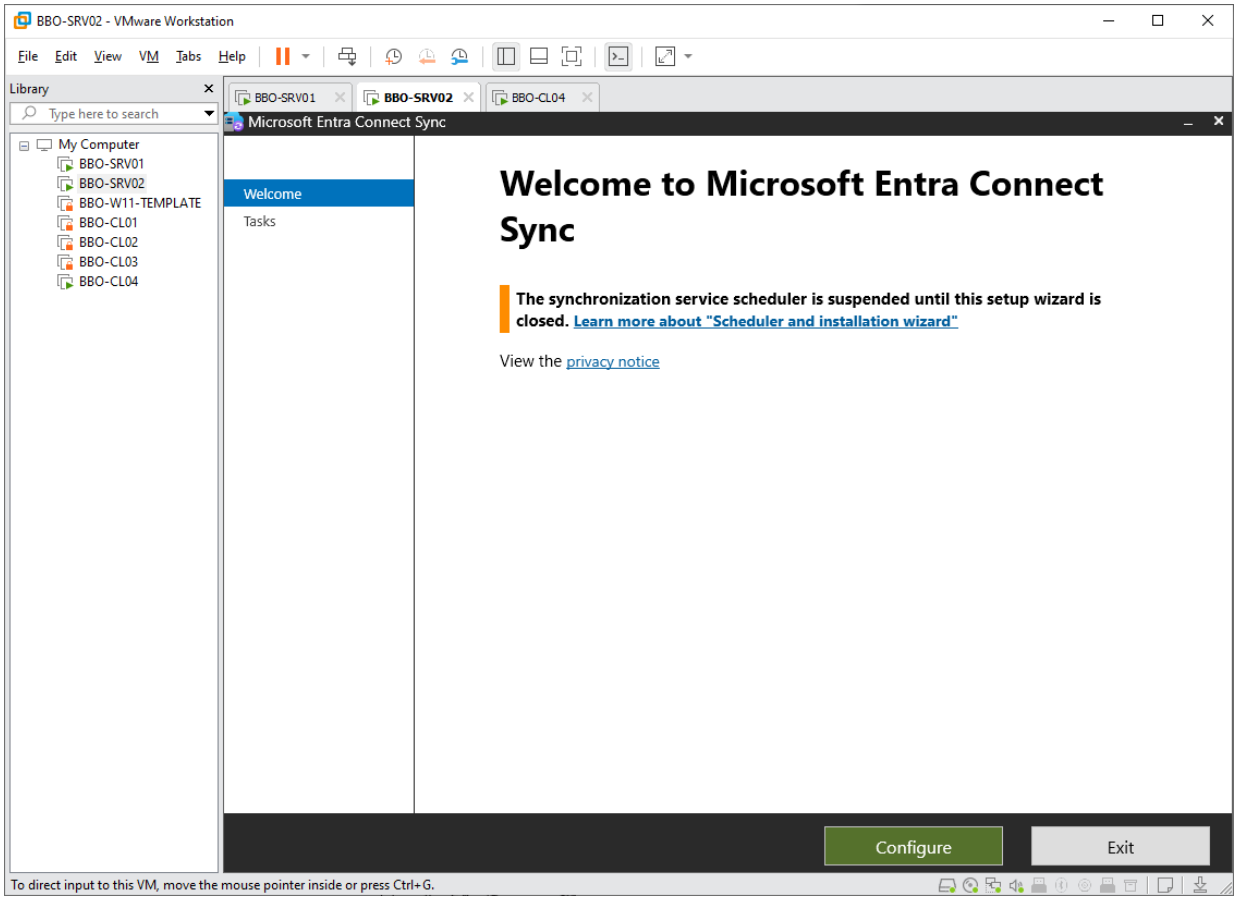

Figure 5 - Microsoft Entra Connect Sync on BBO-SRV02.

What this demonstrates: Directory synchronization is intentionally separated from the domain controller and hosted on the second server.

[RECORDED] BBO-SRV02 became the directory-synchronization bridge. Entra audit evidence identified a synchronization service associated with BBO-SRV02. Keeping Entra Connect off the domain controller separated AD DS/DNS from cloud synchronization.

7.1 Public UPN suffix

The internal forest remained bbo.test while cloud sign-in identities used the verified broadbandops.com domain.

```
Set-ADForest -Identity "bbo.test" -UPNSuffixes @{Add="broadbandops.com"}
```

- jordan.blake@broadbandops.com
- nina.patel@broadbandops.com
- marcus.reed@broadbandops.com
- avery.collins@broadbandops.com

7.2 Admin-center verification

7. Microsoft Entra admin center > Identity > Users > All users: verify synchronized users and intended UPNs.

8. Use Entra audit logs to confirm DirectorySync activity and the synchronization service.
9. Microsoft Entra admin center > Identity > Devices > All devices: later verify Windows device identities as the endpoint phase progresses.

8. Entra Connect Authentication Hang

```
Test-NetConnection login.microsoftonline.com -Port 443
Invoke-WebRequest <Microsoft-login-URL> -UseBasicParsing
AzureADConnect.exe /InteractiveAuth
```

Troubleshooting and Resolution

What went wrong: The Entra Connect wizard hung during cloud authentication even though the server had Internet connectivity.

Symptoms / evidence: TCP 443 and HTTPS tests could succeed while the authentication UI still failed to advance.

What was done: Network reachability was tested separately from authentication; Entra Connect was relaunched with interactive authentication.

What resolved it: Interactive authentication completed and later directory synchronization succeeded.

Operational lesson: A successful TCP/TLS test does not prove an embedded authentication/token flow is healthy.

9. Windows 11 Golden Template

[RECORDED] The fleet was standardized around BBO-W11-TEMPLATE using Windows 11 Enterprise Evaluation.

Setting	Recorded value
Guest OS type	windows11-64
vCPU	2
Cores per socket	2
Memory	4096 MB
Firmware	UEFI
Primary disk controller	NVMe
Network	NAT / VMnet8
Virtual NIC	e1000e
CD/DVD	SATA virtual CD/DVD; later disconnected/disabled

- Windows 11 installed and patched.
- VMware Tools installed.
- No production-user Entra/Intune enrollment before cloning.
- Generalize before cloning.

At OOBE, Audit Mode was entered with:

Ctrl + Shift + F3

Sysprep target state: OOBE + Generalize + Shutdown.

10. Sysprep Failure Caused by BitLocker

manage-bde -status C:

manage-bde -off C:

Troubleshooting and Resolution

What went wrong: Sysprep refused to generalize the Windows 11 template because C: was encrypted/protected by BitLocker/device encryption.

Symptoms / evidence: Sysprep failed; setuperr.log and manage-bde status exposed the encryption state.

What was done: Encryption was disabled and the machine was left until decryption reached 0.0%, then Sysprep was retried.

What resolved it: Sysprep completed after full decryption.

Operational lesson: Check BitLocker/device-encryption state before final golden-image generalization.

11. Snapshot and Full-Clone Fleet Creation

[RECORDED] After successful Sysprep shutdown, the clean snapshot was named "Clean Generalized Template".

10. Keep the generalized template powered off.
11. Open Snapshot Manager and select Clean Generalized Template.
12. Choose Clone.
13. Create a full clone, not a linked clone.
14. Create BBO-CL01 through BBO-CL04.
15. Before first boot, verify NAT, TPM, storage, and removable-media settings.
16. Disconnect the installation ISO and disable Connect at power on when no longer needed.

Troubleshooting and Resolution

What went wrong: Installation media could remain attached to clones and reconnect at startup.

Symptoms / evidence: That can produce confusing startup/OOBE behavior and makes a clone less representative of a deployed workstation.

What was done: The ISO was removed/disconnected and CD/DVD startup connection was disabled.

What resolved it: Clients booted into the intended OOBE/deployment path.

Operational lesson: Always inspect virtual hardware and removable media before first boot of a clone.

12. OOBE and Client Baseline

[RECORDED] Local administration used BBO-LocalAdmin in the captured client state. BBO-CL04 was captured before final domain join as a standalone workstation.

```
CsCaption      : BBO-CL04
CsDNSHostName  : BBO-CL04
CsDomain       : WORKGROUP
CsDomainRole   : StandaloneWorkstation
CsPartOfDomain : False
CsUserName     : BBO-CL04\BBO-LocalAdmin
OsName         : Microsoft Windows 11 Enterprise Evaluation
OsVersion      : 10.0.26200
OsBuildNumber  : 26200
```

13. Join Clients to bbo.test

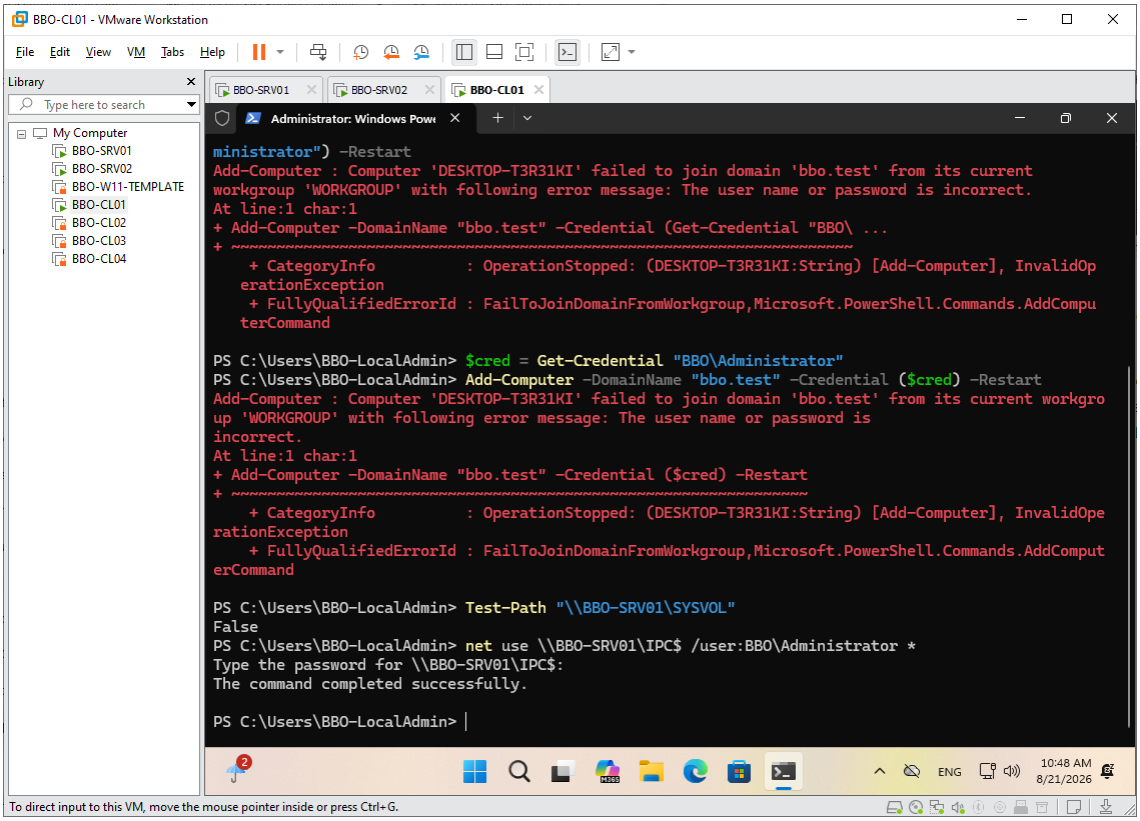

Figure 6 - BBO-CL01 domain-join troubleshooting after invalid credentials.

What this demonstrates: The captured Add-Computer error explicitly reports an incorrect user name or password; the later IPC$ test succeeds after corrected authentication.

The workstation must discover AD services through the AD DNS server before domain join. Once DNS and reachability are proven, read the actual Add-Computer error: the retained BBO-CL01 failure was credential-related.

```
Get-DnsClientServerAddress
Resolve-DnsName bbo.test
Resolve-DnsName -Type SRV _ldap._tcp.dc._msdcs.bbo.test
Test-NetConnection BBO-SRV01 -Port 53

Add-Computer -DomainName "bbo.test" -Credential (Get-Credential) -Restart
Get-ComputerInfo
```

Successful post-restart state should include CsDomain = bbo.test, CsDomainRole = MemberWorkstation, and CsPartOfDomain = True.

Troubleshooting and Resolution

What went wrong: Domain joining exposed multiple possible failure domains. In the retained BBO-CL01 screenshot, Add-Computer specifically failed because the supplied user name or password was incorrect; other lab checks also emphasized DNS and state/timing.

Symptoms / evidence: A GUI success message alone was not treated as sufficient proof.

What was done: DNS/domain discovery was corrected, the join was performed, the client restarted, and Get-ComputerInfo was used for verification.

What resolved it: Clients became members of bbo.test.

Operational lesson: Validate the resulting state, not merely whether the join command/dialog reported success.

14. Hybrid Microsoft Entra Device Identity

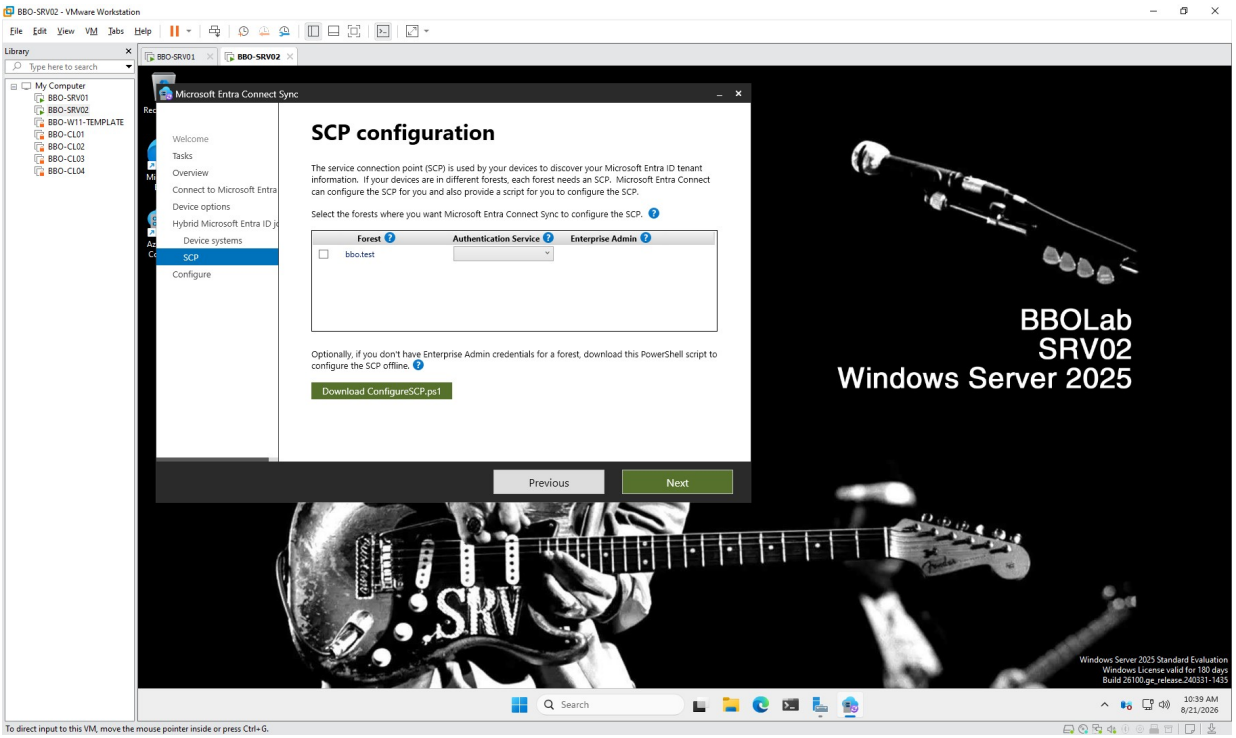

Figure 7 - Entra Connect hybrid-join SCP configuration for bbo.test.

> **What this demonstrates:** The Service Connection Point is configured so domain clients can discover the Microsoft Entra tenant for hybrid registration.

After local domain membership and Entra Connect were functioning, the lab extended the Windows clients into Microsoft Entra device identity. This is a separate state from ordinary AD domain membership.

```
gpupdate /force
dsregcmd /status
```

- AzureAdJoined
- DomainJoined
- DomainName
- DeviceId
- TenantId
- AzureAdPrt

[RECORDED/RECONSTRUCTED] Group Policy refresh and restart/registration cycles were used during hybrid-join troubleshooting. The precise final dsregcmd transcript is not retained, so this document does not invent one.

Troubleshooting and Resolution

What went wrong: A client could be correctly joined to bbo.test without immediately showing the expected Entra hybrid-device state.

Symptoms / evidence: Local AD membership and cloud device registration did not necessarily converge at the same moment.

What was done: Policy was refreshed, the registration/restart cycle was allowed to run, and dsregcmd /status was used to inspect state.

What resolved it: The cloud device-registration path subsequently functioned and Entra device activity was observable.

Operational lesson: AD DS membership and Entra device identity are related but separate control planes.

15. Intune / MDM Enrollment

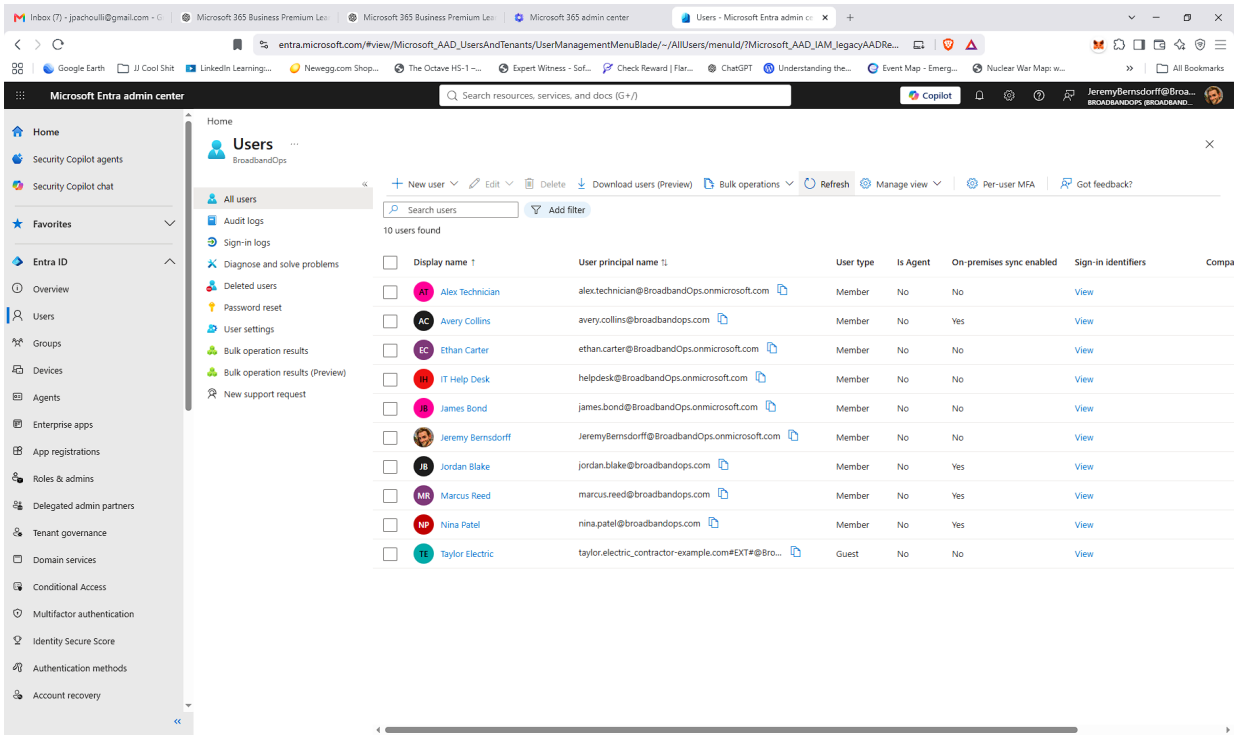

Figure 8 - Microsoft Entra users showing synchronized BroadbandOps identities.

What this demonstrates: Avery Collins, Jordan Blake, Marcus Reed, and Nina Patel show on-premises synchronization enabled and use the broadbandops.com namespace.

[RECORDED] The lab used the BBOLAB-Intune-Enrollment group as part of the Windows enrollment work. Jordan Blake and Nina Patel were explicitly used during the client enrollment/testing sequence.

Client	Recorded test user
BBO-CL03	Jordan Blake
BBO-CL04	Nina Patel

15.1 Administrative verification

17. Microsoft Entra admin center > Groups: verify the intended enrollment-targeting group membership.
18. Microsoft Entra admin center > Devices > All devices: verify the Windows device identity.
19. Microsoft Intune admin center > Devices > Windows > Windows devices / All devices: verify that the endpoint appears as managed.
20. Open the device record and verify the primary user, last check-in, management state, and compliance state.
21. On the Windows client, inspect EnterpriseMgmt enrollment tasks when enrollment status is uncertain.

```
Get-ScheduledTask | Where-Object {
 $_.TaskPath -like "*EnterpriseMgmt*" -or
 $_.TaskName -like "*enrollment*"
} | Select-Object TaskPath,TaskName,State
```

The EnterpriseMgmt task tree is strong evidence that Windows MDM enrollment machinery has been provisioned. It does not, by itself, prove that every later compliance policy has finished evaluating.

16. Windows Baseline Compliance Policy

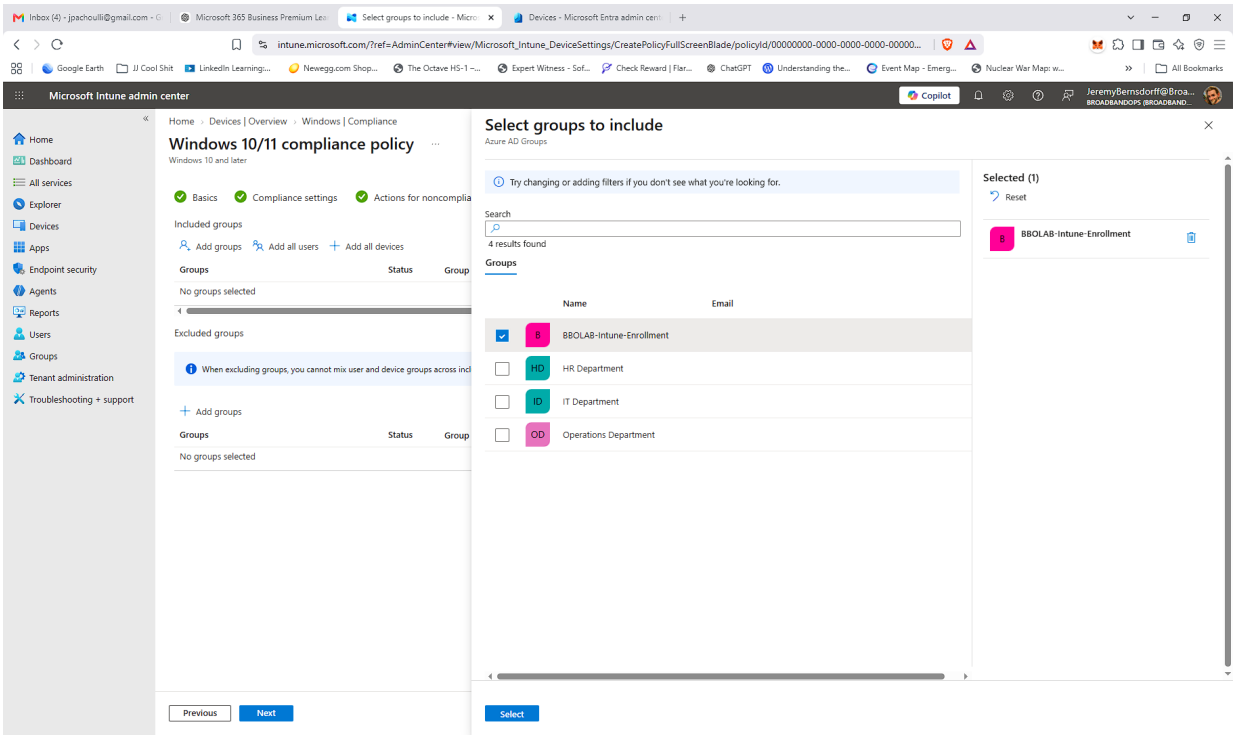

Figure 9 - Intune compliance policy assignment to BBOLAB-Intune-Enrollment.

What this demonstrates: The policy is actually targeted to the enrollment group rather than merely existing unassigned.

[RECORDED] The endpoint phase included an Intune compliance policy named "BBO - Windows Baseline Compliance". The final device-level policy view showed the baseline policy alongside the Default Device Compliance Policy.

16.1 Baseline settings validated

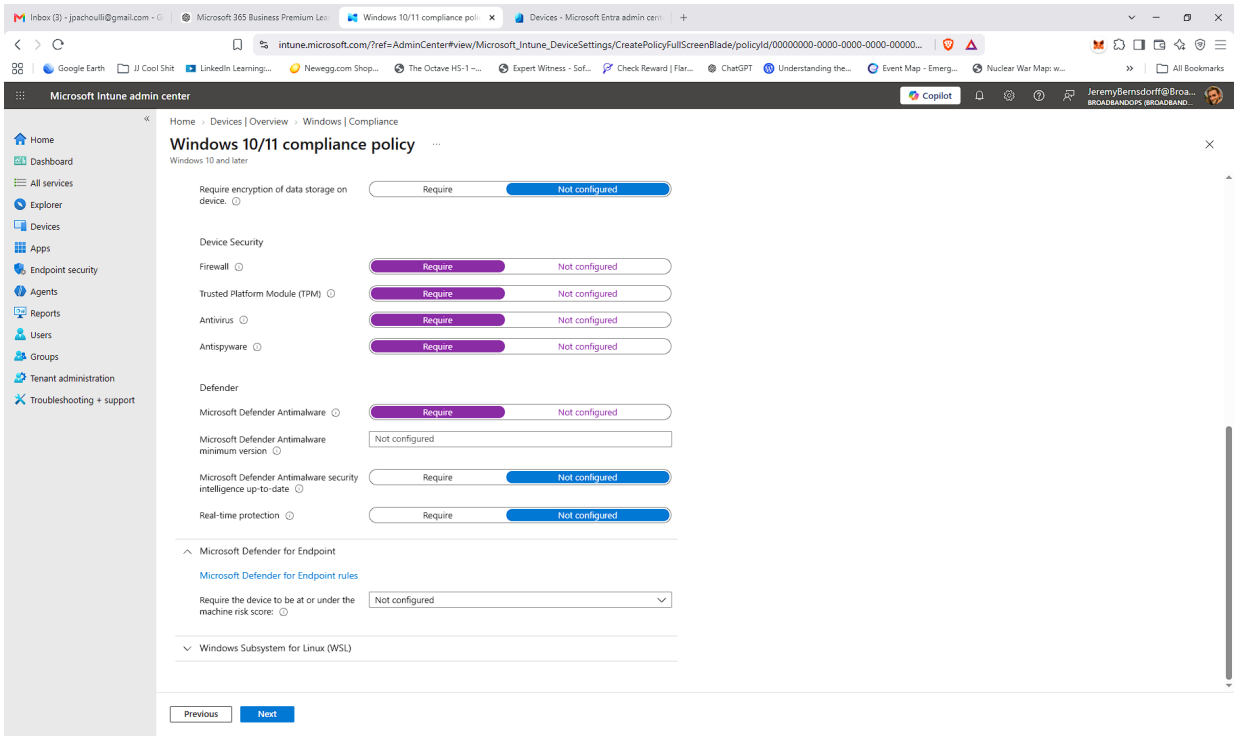

Figure 10 - Windows 10/11 baseline compliance requirements.

What this demonstrates: Firewall, TPM, antivirus, antispyware, and Microsoft Defender Antimalware are explicitly set to Require.

Compliance setting	Final observed state
Firewall	Compliant
Anti-Spyware	Compliant
Antivirus	Compliant
Microsoft Defender Antimalware	Compliant
Trusted Platform Module (TPM)	Compliant

These checks formed a practical minimum endpoint-health baseline: host firewall, anti-malware/anti-spyware protection, Microsoft Defender antimalware state, and TPM presence.

16.2 What the policy result means

A green device result means Intune received enough current device state to evaluate the assigned policy successfully. It is not the same thing as merely seeing the device object in Entra ID or Intune. Enrollment, check-in, policy assignment, device health reporting, and compliance evaluation are separate stages.

17. Client Sync and Compliance Evaluation

The final lab work demonstrated an important operational behavior: Intune is asynchronous. A device can be powered on, online, enrolled, and even able to accept a sync request while the portal still shows an older or intermediate compliance state.

17.1 Manual sync from Intune

22. Open Microsoft Intune admin center > Devices > Windows > Windows devices.
23. Open the target client record.
24. Choose Sync.
25. Watch the Sync status pane for Notifying device, Policies, and Applications.
26. After the sync request completes, allow time for device processing and cloud-side reporting before judging the final compliance result.
27. Refresh the device record and open Device compliance to inspect the evaluated policies/settings.

17.2 BBO-CL04: apparent sync failure that cleared

[RECORDED] On BBO-CL04, the first manual sync attempt showed Notifying device = Failed while Policies and Applications had not started. The VM was already booted and had network connectivity.

[RECORDED] A subsequent attempt completed the Notifying device stage. The device record later showed BBO-CL04 as Compliant, with Nina Patel as primary user.

Troubleshooting and Resolution

What went wrong: The first CL04 sync notification reported Failed even though the machine was online.

Symptoms / evidence: The failure occurred at the notification stage; it was not accompanied by evidence that the entire enrollment or network stack was broken.

What was done: The client was left online and the sync was retried rather than immediately rebuilding enrollment or changing configuration.

What resolved it: The next notification completed, and the device subsequently evaluated as compliant.

Operational lesson: Treat a transient Intune sync/notification state as evidence to investigate, not automatic proof of a broken endpoint. Retry and allow propagation time before escalating.

18. Final CL02-CL04 Compliance Validation

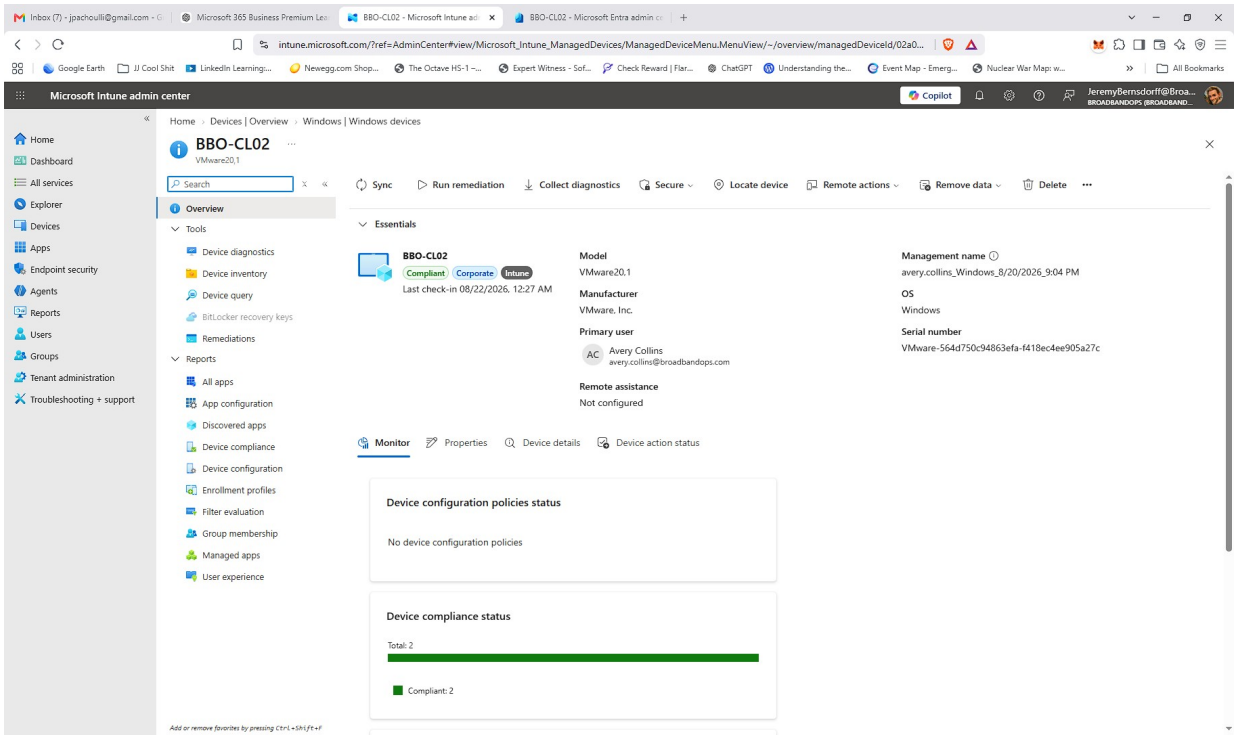

Figure 11 - BBO-CL02 final Intune overview showing Compliant status.

What this demonstrates: The managed endpoint has checked in, is associated with Avery Collins, and the compliance summary is green.

[RECORDED] By the end of the lab, the later client fleet was reporting compliant in Intune. The screenshots retained from the final checks show CL02 and CL04 in compliant state, and CL03 had already transitioned to compliant during its sync/check-in sequence.

Client	User shown during final work	Final observed state / note
BBO-CL02	Avery Collins	Compliant; both BBO baseline and Default Device Compliance Policy showed compliant.
BBO-CL03	Jordan Blake	Compliant after sync/check-in; sync notification/policy processing completed quickly.
BBO-CL04	Nina Patel	Compliant after an initial transient notification failure cleared on retry.

18.1 CL02 baseline detail

[RECORDED] BBO-CL02's policy-setting view showed all five baseline requirements compliant: Firewall, Anti-Spyware, Antivirus, Microsoft Defender Antimalware, and TPM. The device compliance page showed both the BBO baseline and Default Device Compliance Policy as compliant.

18.2 CL03 sync behavior

[RECORDED] BBO-CL03's Intune sync completed rapidly: device notification completed, policy processing succeeded, and no application updates were required. The device record displayed Jordan Blake as the primary user.

18.3 CL04 final result

[RECORDED] BBO-CL04's final baseline-setting view showed the same five settings compliant, and its device-compliance page showed both policies compliant. This confirmed that the earlier red/noncompliant state was an intermediate evaluation state rather than a permanent configuration failure.

Troubleshooting and Resolution

What went wrong: The endpoint phase repeatedly produced red or incomplete portal states before the final green state appeared.

Symptoms / evidence: CL02 took substantially longer to settle; CL04 briefly showed a failed notification; CL03 processed much faster.

What was done: Devices were kept online, sync/check-in was triggered where useful, and portal state was refreshed after allowing processing time.

What resolved it: The clients converged to compliant state without unnecessary destructive remediation.

Operational lesson: Cloud management has propagation and evaluation latency. 'Wait, verify, then change' is often better operations practice than repeatedly changing a configuration that may already be correct.

19. Intune Windows Security Configuration Profile

[RECORDED] The continuation lab created a Settings catalog configuration profile named BBO - Windows Security Configuration. Its purpose was to establish a centrally managed Windows security baseline for BroadbandOps-managed Windows 10/11 endpoints.

The profile began with two Microsoft Defender SmartScreen controls, was assigned to BBOLAB-Intune-Enrollment, and was then edited to add the Windows PowerShell execution policy that had been omitted during the first creation pass.

Configuration item	Final value
Enable Smart Screen In Shell	Enabled
Prevent Override For Files In Shell	Enabled
Turn on Script Execution	Enabled
Execution Policy	Allow local scripts and remote signed scripts
Scope tag	Default
Included group	BBOLAB-Intune-Enrollment
Excluded groups	None

19.1 Create and assign the profile

Microsoft Intune admin center > Devices > Configuration > Create > Windows 10 and later > Settings catalog.

Name the profile BBO - Windows Security Configuration and enter the baseline-security description.

Add SmartScreen settings: Enable Smart Screen In Shell = Enabled; Prevent Override For Files In Shell = Enabled.

Leave the default scope tag.

Assign BBOLAB-Intune-Enrollment under Included groups.

Review the settings and create the profile.

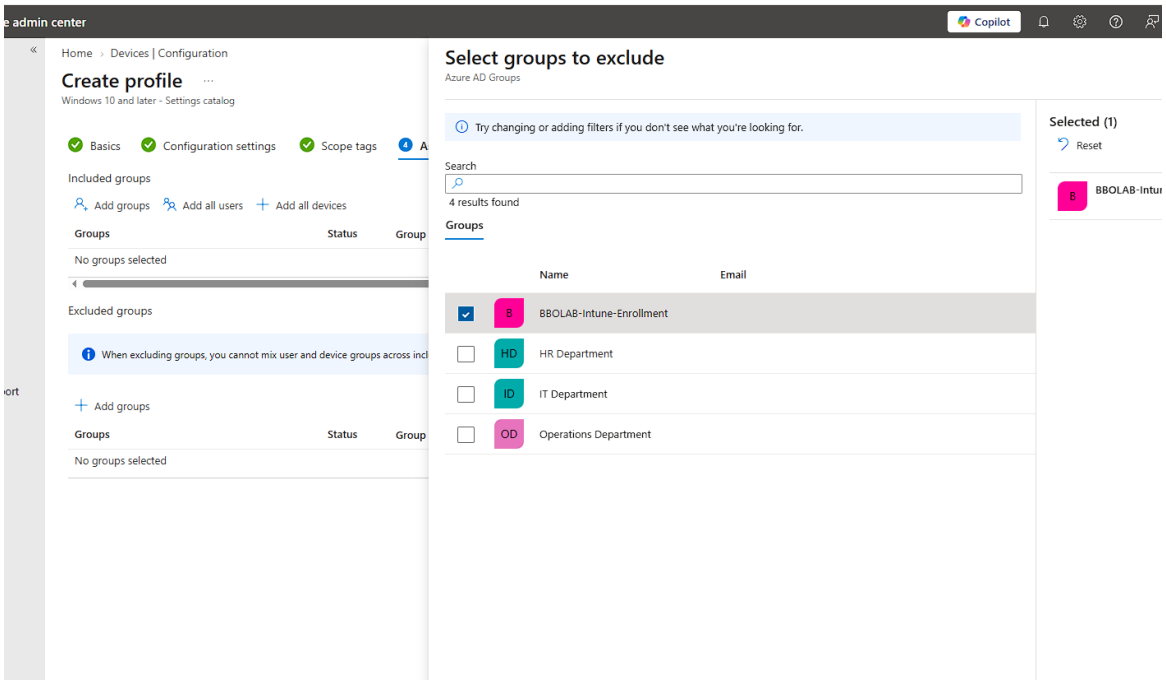

Figure 12 - Incorrect assignment attempt with BBOLAB-Intune-Enrollment selected under Excluded groups.

What this demonstrates: The intended target group was placed in the opposite assignment control. Had it been saved this way, the profile would have been prevented from applying to the very group it was meant to target.

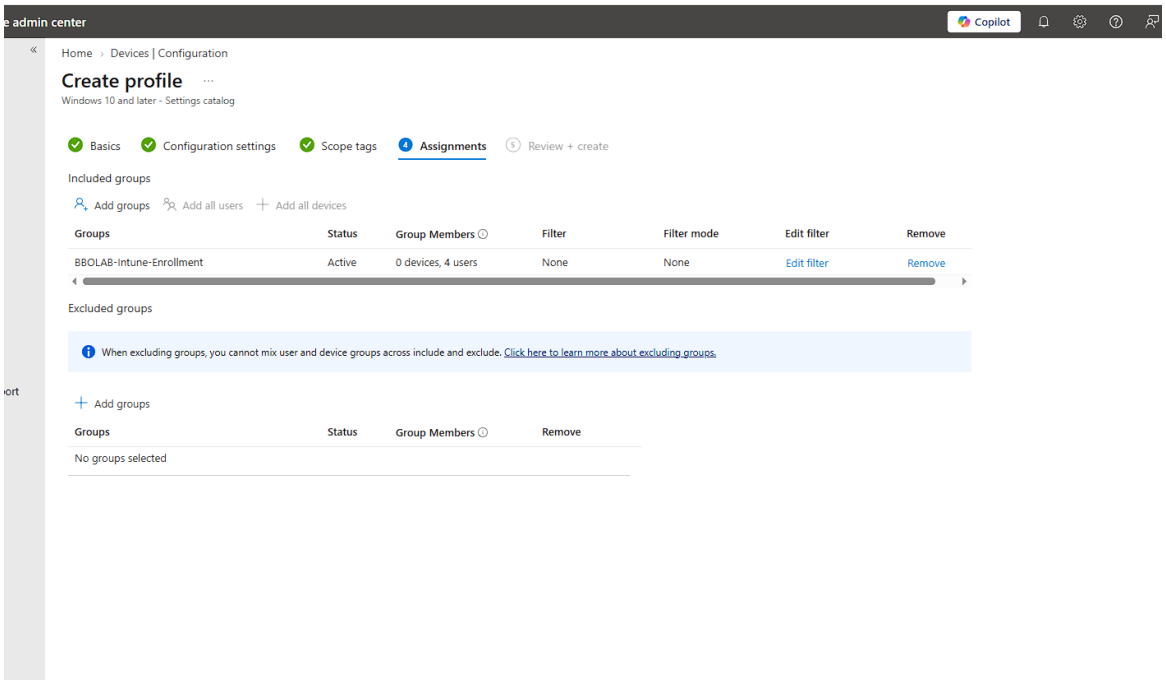

Figure 13 - Corrected assignment with BBOLAB-Intune-Enrollment under Included groups and no excluded groups.

What this demonstrates: The target group is Active and appears under Included groups, while Excluded groups remains empty. This is the correct assignment direction for the lab.

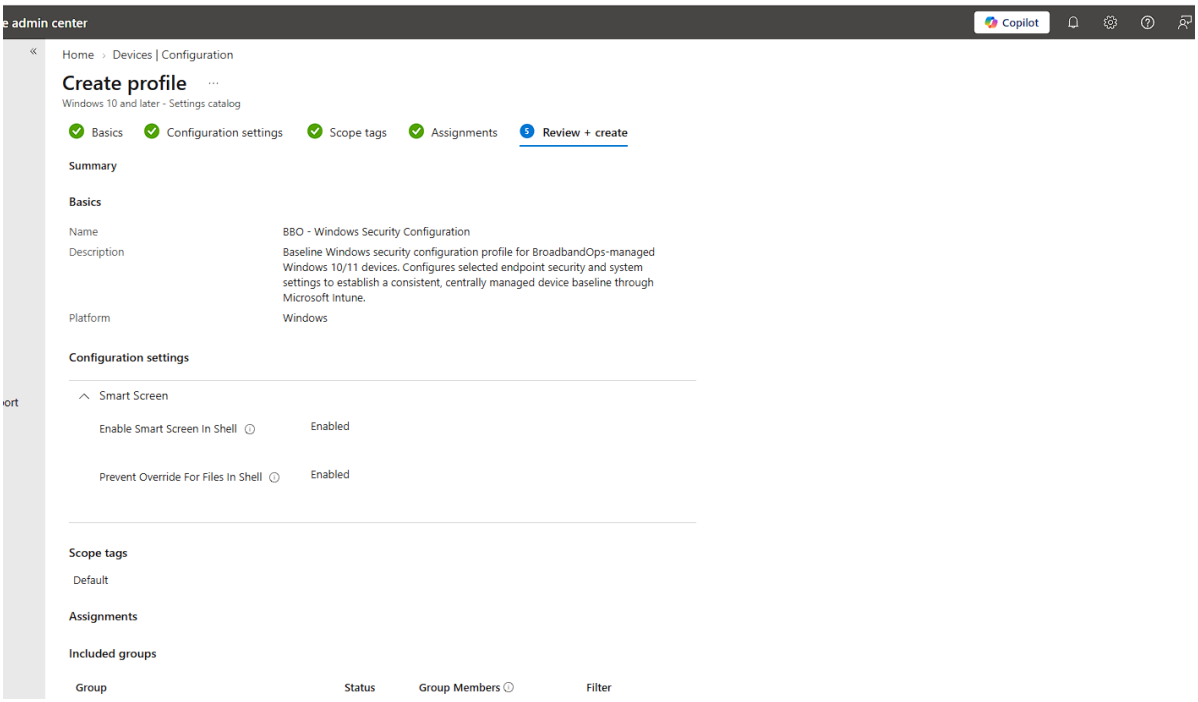

Figure 14 - Initial profile review showing both SmartScreen controls and the BBOLAB-Intune-Enrollment assignment.

What this demonstrates: The first complete review correctly showed Enable Smart Screen In Shell and Prevent Override For Files In Shell as Enabled and confirmed the intended group assignment.

19.2 Edit the existing profile to add PowerShell

Before endpoint synchronization, the omission of PowerShell was caught. The existing profile did not need to be deleted or recreated. The profile was reopened, Configuration settings was edited, and the device-level Administrative Templates > Windows PowerShell > Turn on Script Execution setting was added.

The selected execution policy was Allow local scripts and remote signed scripts. This provides a practical lab posture: locally created scripts may run while scripts obtained from remote sources are expected to be signed.

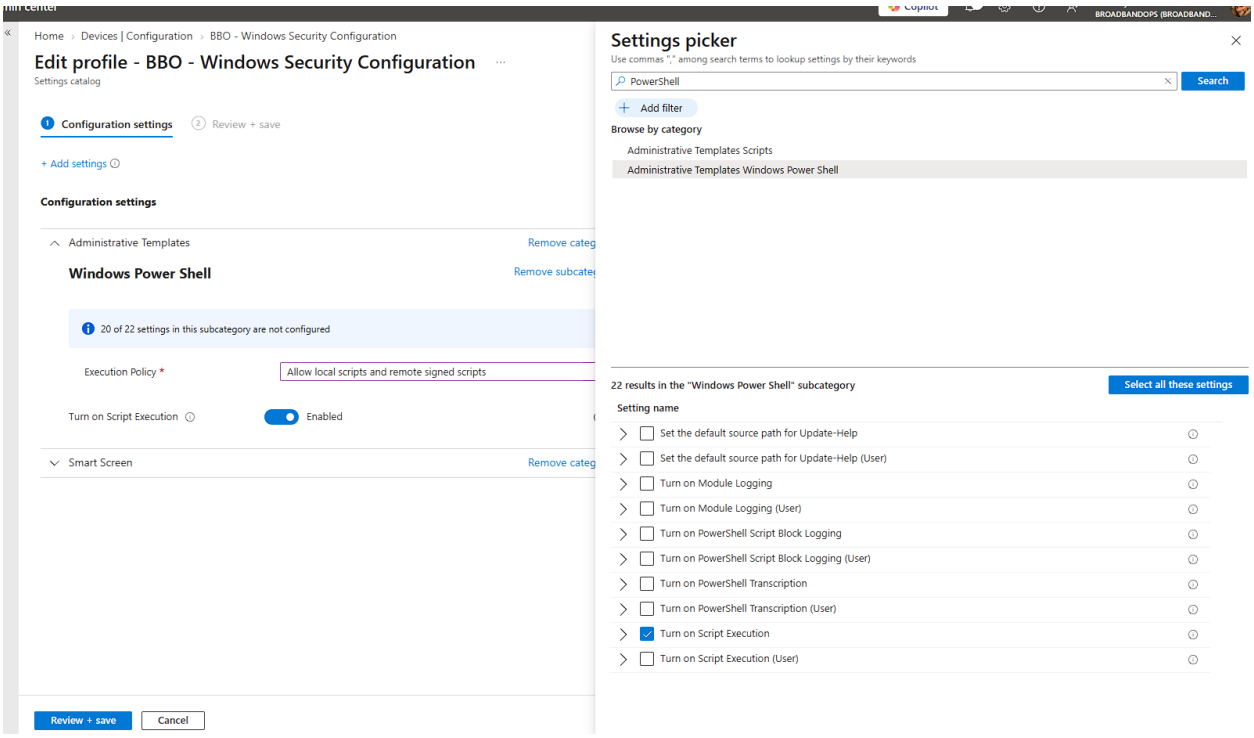

Figure 15 - Windows PowerShell Administrative Templates setting added to the existing Intune profile.

What this demonstrates: The device-level Turn on Script Execution control is selected, enabled, and paired with Allow local scripts and remote signed scripts. The SmartScreen category remains in the profile.

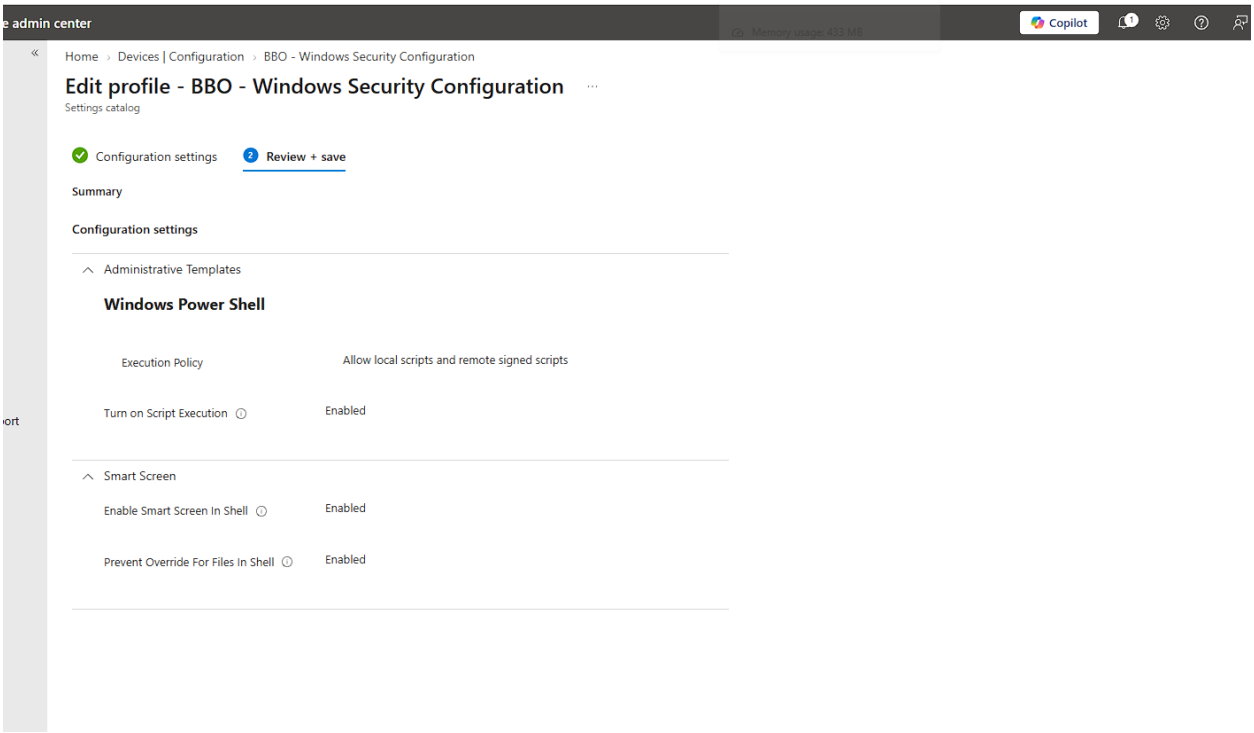

Figure 16 - Final Review + save state showing PowerShell execution policy and both SmartScreen controls together.

What this demonstrates: All intended configuration controls are visible in one review screen before the edited profile is saved.

19.3 Profile creation and initial reporting state

[RECORDED] After creation and the PowerShell edit, the policy appeared in Devices > Configuration as a Windows 10 and later Settings catalog profile. The first policy-summary view initially showed zeros across Succeeded, Error, Conflict, Not applicable, and In progress.

That all-zero state was treated as an intermediate reporting condition, not as proof that the profile had failed. Intune configuration deployment requires assignment, endpoint check-in, local processing, and cloud-side reporting; those stages do not always complete at the same moment.

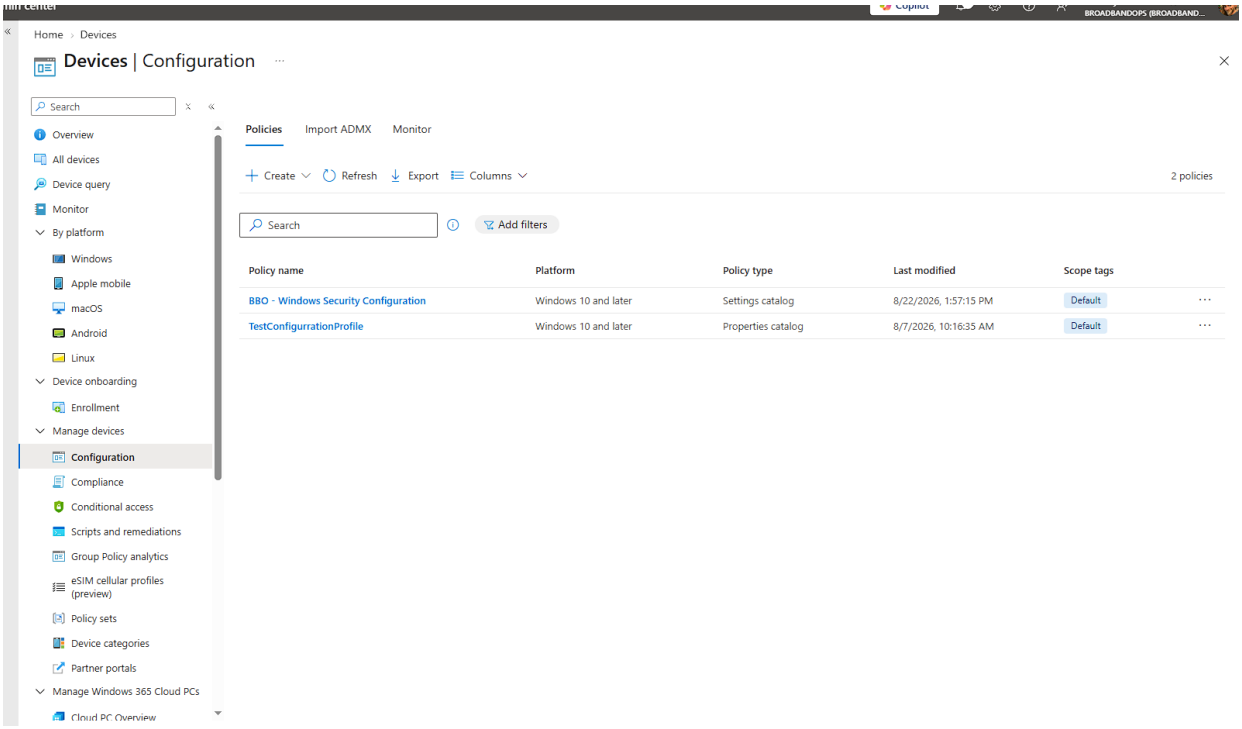

Figure 17 - BBO - Windows Security Configuration listed as an active Windows Settings catalog profile.

What this demonstrates: The configuration object exists in Intune after creation and can be reopened for monitoring or further editing.

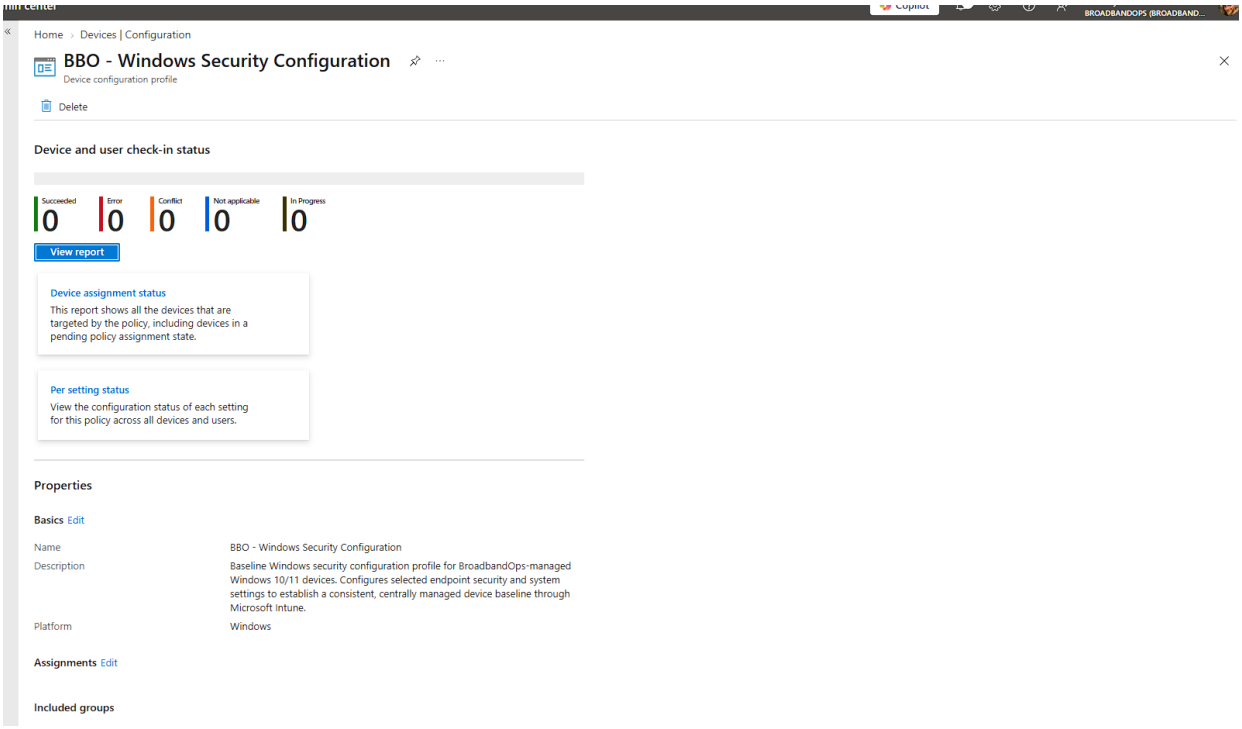

Figure 18 - Initial policy-summary view before managed endpoints had reported configuration results.

What this demonstrates: All status counters were still zero immediately after deployment. This was an incomplete reporting state rather than a confirmed failure.

19.4 Endpoint-side synchronization and policy visibility

[RECORDED] BBO-CL01 was used as one of the managed Windows 11 lab clients for configuration testing. The VMware context confirms that the endpoint is part of the same BBO virtual fleet built earlier in the lab.

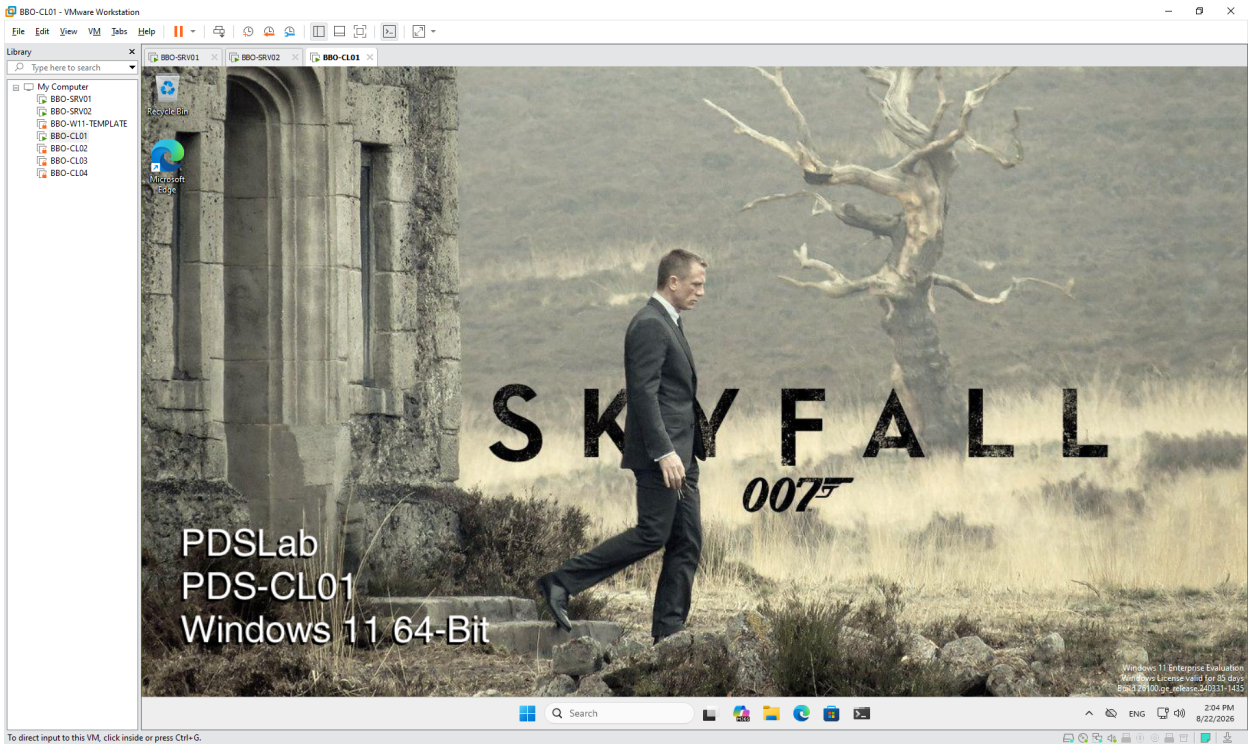

Figure 19 - BBO-CL01 running as a Windows 11 client VM in the VMware Workstation lab.

What this demonstrates: The endpoint used for the configuration test is one of the original cloned Windows clients, tying the later Intune work back to the virtual infrastructure established at the beginning of the lab.

On the Windows client, Settings > Accounts > Managed by BroadbandOps displayed the management policy areas ADMX_PowerShellExecutionPolicy, Security, and SmartScreen. A manual Sync action was used to force an immediate MDM check-in for validation.

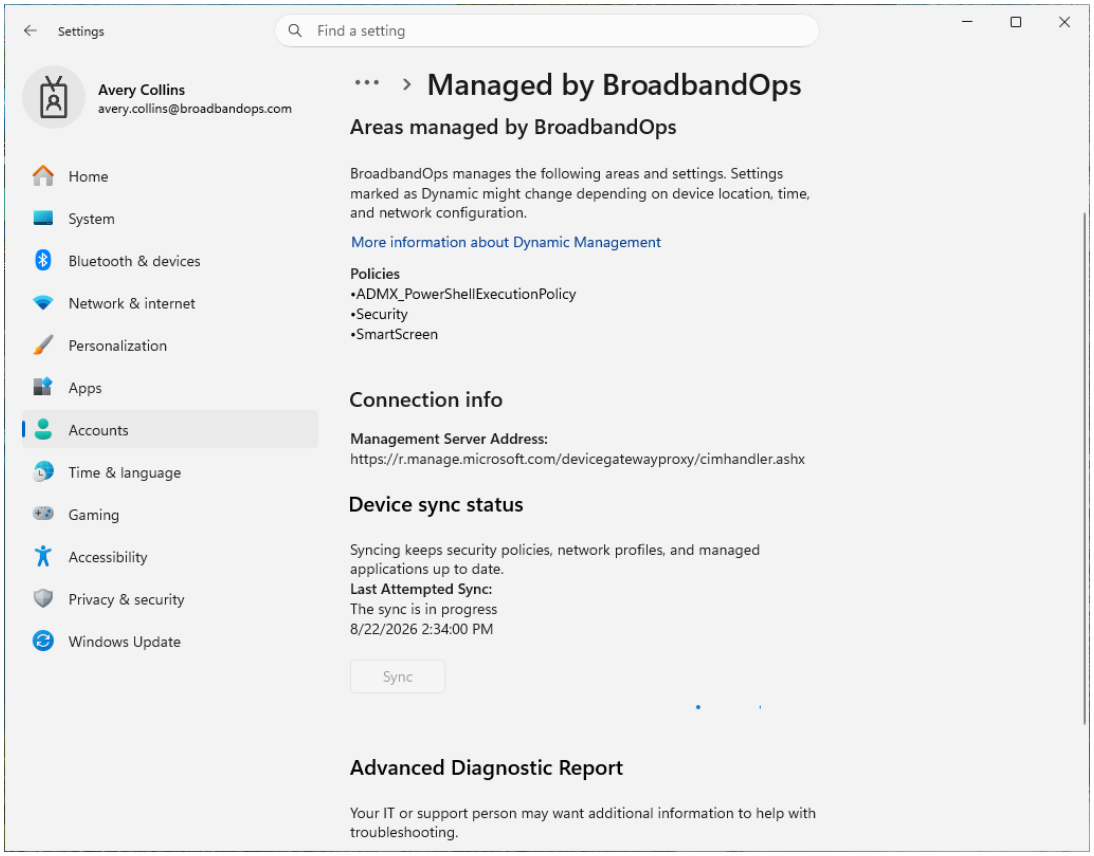

Figure 20 - BBO-CLxx actively synchronizing managed policies with Microsoft Intune

What this demonstrates: Windows shows Managed by BroadbandOps and lists the PowerShell, Security, and SmartScreen policy areas while the device sync is actively in progress.

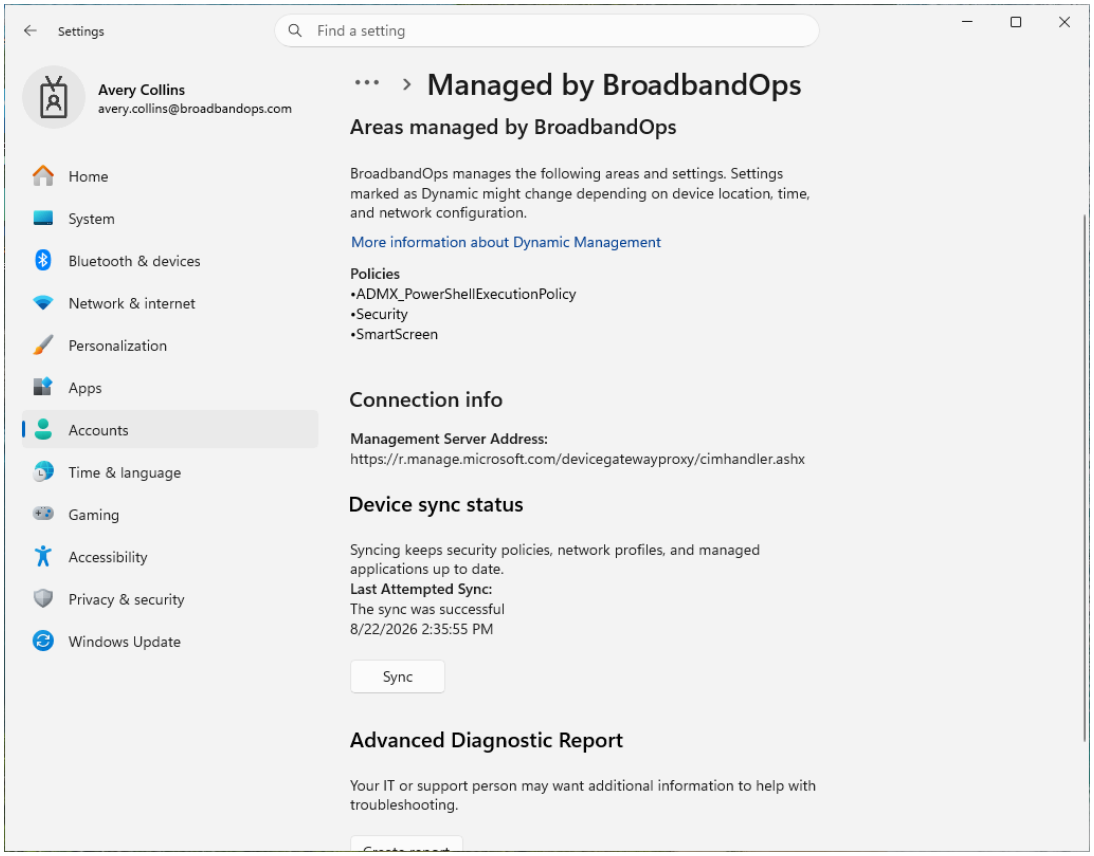

Figure 21 - BBO-CLxx confirming successful synchronization with Microsoft Intune

What this demonstrates: The same endpoint view reports that the sync was successful, producing a clean before-and-after record of the client-side management cycle.

19.5 Automatic/background check-in observation

[RECORDED] A separate managed client session under Nina Patel was intentionally left without manually pressing Sync after sign-in. The Windows page already showed a successful recent management sync, and the Intune configuration profile subsequently advanced to four successful results.

This supports an important operational distinction: manual Sync accelerates testing, but normal Intune management also performs background/scheduled check-ins. The evidence does not prove that sign-in itself was the exact trigger; it proves that the endpoint checked in successfully without a manual Sync action during that test sequence.

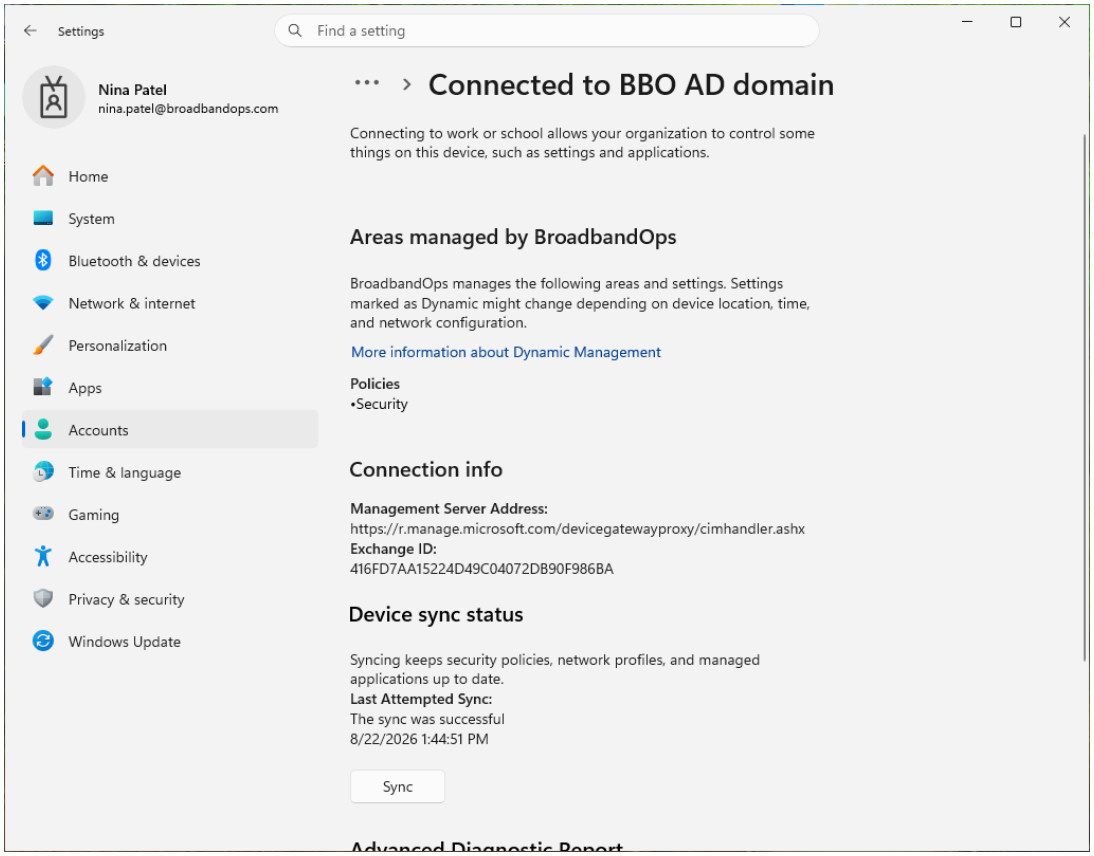

Figure 22 - Managed Windows client under Nina Patel showing successful BroadbandOps management without a manually initiated Sync action in the test sequence.

What this demonstrates: The client reports a successful recent synchronization while remaining under BroadbandOps management. This supports automatic/background Intune check-in behavior.

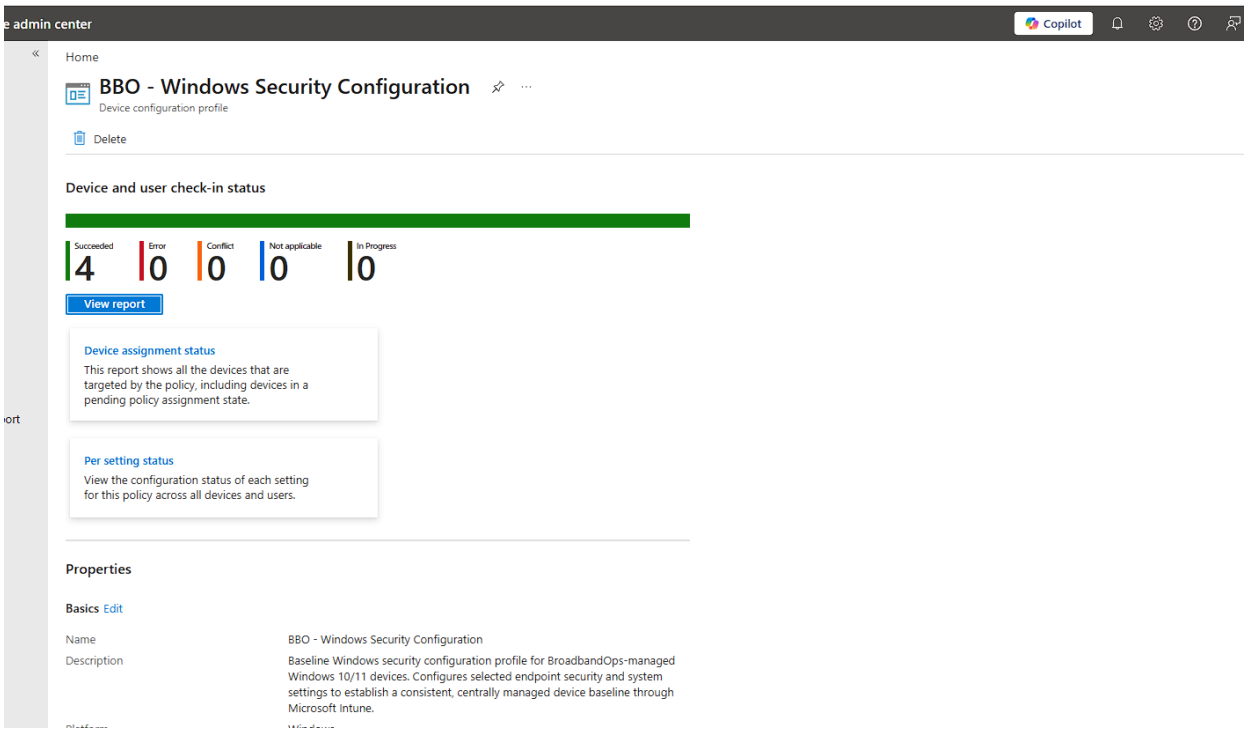

Figure 23 - Intune configuration profile reporting four successful check-ins with zero errors, conflicts, not-applicable results, or in-progress results.

What this demonstrates: The cloud-side configuration summary confirms successful convergence across the targeted lab users/endpoints after sufficient check-in and reporting time.

Troubleshooting and Resolution

What went wrong: Three operational mistakes or false alarms appeared during the configuration-profile work: the target group was initially selected under Excluded groups; the PowerShell execution policy was omitted from the first creation pass; and the Intune summary initially showed all zeros.

Symptoms / evidence: The first assignment would have blocked the intended target group; the initial review contained only the SmartScreen settings; the first profile-summary view contained no reported device results.

What was done: The group was removed from Excluded groups and added to Included groups. The existing profile was edited to add the PowerShell setting. Managed clients were left online and allowed to check in, with manual Sync used where immediate validation was useful.

What resolved it: The corrected assignment, saved profile edit, endpoint check-ins, and cloud-side propagation produced visible policy categories on Windows and a final Intune result of four successes with no errors or conflicts.

Operational lesson: Intune configuration is a staged process: create, assign, endpoint check-in, device processing, and cloud reporting. Verify assignment direction and intended settings before saving, then allow time for reporting before treating an empty dashboard as a deployment failure.

20. End-to-End Validation Checklist

- [ ] VMware VMnet8 NAT is functioning and the lab subnet is reachable.
- [ ] BBO-SRV01 has stable networking, AD DS, DNS, and the bbo.test forest.
- [ ] AD users, groups, and computers can be queried and administered.
- [ ] BBO-SRV02 can reach Microsoft cloud endpoints and Entra Connect synchronization is functioning.
- [ ] On-premises UPNs align with the verified broadbandops.com cloud namespace where intended.

The Windows 11 template is patched, generalized, decrypted before Sysprep, and preserved as a clean snapshot.

BBO-CL01 through BBO-CL04 exist as independent client VMs.

Clients use AD DNS when discovering/joining bbo.test and show successful domain membership after restart.

Hybrid Microsoft Entra device identity is verified separately from local AD membership.

Intune/MDM enrollment exists and managed devices appear with the expected primary users.

BBO - Windows Baseline Compliance is assigned and the validated firewall, anti-spyware, antivirus, Microsoft Defender Antimalware, and TPM requirements report compliant.

BBO - Windows Security Configuration exists as a Windows Settings catalog profile and is assigned to BBOLAB-Intune-Enrollment.

Enable Smart Screen In Shell and Prevent Override For Files In Shell are enabled.

Turn on Script Execution is enabled with Allow local scripts and remote signed scripts.

Managed Windows clients display the expected PowerShell/Security/SmartScreen management areas.

Manual Sync is understood as an immediate check-in action rather than the only way Intune communicates with a managed device.

Automatic/background Intune check-in was observed without manually pressing Sync during the Nina Patel test sequence.

Final configuration-profile reporting shows four successes with zero errors, conflicts, not-applicable results, or in-progress results.

Final state is verified from both the endpoint and Intune rather than inferred from one side alone.

21. Commands Used or Referenced

The following commands were used or explicitly referenced across the reconstructed lab. Commands that represent a GUI-equivalent action rather than a verbatim recovered command are identified as reconstructed in the relevant section.

```
Get-NetIPConfiguration
Get-DnsClientServerAddress
Resolve-DnsName bbo.test
Resolve-DnsName -Type SRV _ldap._tcp.dc._msdcs.bbo.test

Test-NetConnection BBO-SRV01 -Port 53
Test-NetConnection login.microsoftonline.com -Port 443

Get-ADDomain
Get-ADForest
Get-ADUser -Filter *
Get-ADGroup -Filter *
Get-ADComputer -Filter *

Get-ADGroupMember -Identity "Production-Users"
Get-ADPrincipalGroupMembership -Identity "alice"

Get-ComputerInfo
gpupdate /force
dsregcmd /status

Get-ScheduledTask | Where-Object {
$_.TaskPath -like "*EnterpriseMgmt*" -or
$_.TaskName -like "*enrollment*"
} | Select-Object TaskPath,TaskName,State

manage-bde -status C:\nmanage-bde -off C:

Invoke-WebRequest <Microsoft-login-URL> -UseBasicParsing
AzureADConnect.exe /InteractiveAuth
```

22. Evidence Gaps and Lessons Learned

22.1 Exact items not recovered

BBO-SRV01 first-day static IPv4 configuration method/timestamp; the later recorded address is 192.168.219.10.

Exact original PDS-SRV01 vCPU, RAM, and disk sizing.

Exact BBO-SRV02 hardware/IP values.

Exact text of the original failed New-ADUser command.

Exact GUI-versus-PowerShell method for every server role, join, and enrollment action.

Every individual final Get-ComputerInfo and dsregcmd transcript for BBO-CL01 through BBO-CL04.

Every intermediate Intune timestamp/state for every client.

A per-setting Intune status screenshot for the final Windows Security Configuration profile was not captured; the profile-level success state and endpoint-side policy visibility were captured instead.

22.2 Major operational lessons from the complete lab

DNS is foundational to Active Directory. Internet connectivity is not enough for domain discovery.

Directory distinguished names must match the real object path and class; CN and OU are not interchangeable.

Network reachability and authentication are separate failure domains.

Golden images should be generalized only after encryption state and removable media are checked.

AD domain membership, Microsoft Entra device identity, Intune enrollment, Intune compliance, and Intune configuration deployment are separate states.

Cloud management is asynchronous. Intermediate red, failed, empty, or all-zero states can clear after device processing and service propagation.

Included and Excluded groups are opposite controls; verify the target location before saving.

An existing Intune Settings catalog profile can be edited when a setting is omitted; recreation is not automatically required.

Manual Sync is useful for immediate validation, but Intune-managed Windows endpoints also check in automatically in the background.

Collect evidence before changing state. A retry plus time can be safer than rebuilding a working enrollment.

Always validate the original symptom after a fix; a successful command or green portal tile is not, by itself, proof that the original problem is resolved.

END OF REVISED COMPLETE LEARNING REFERENCE