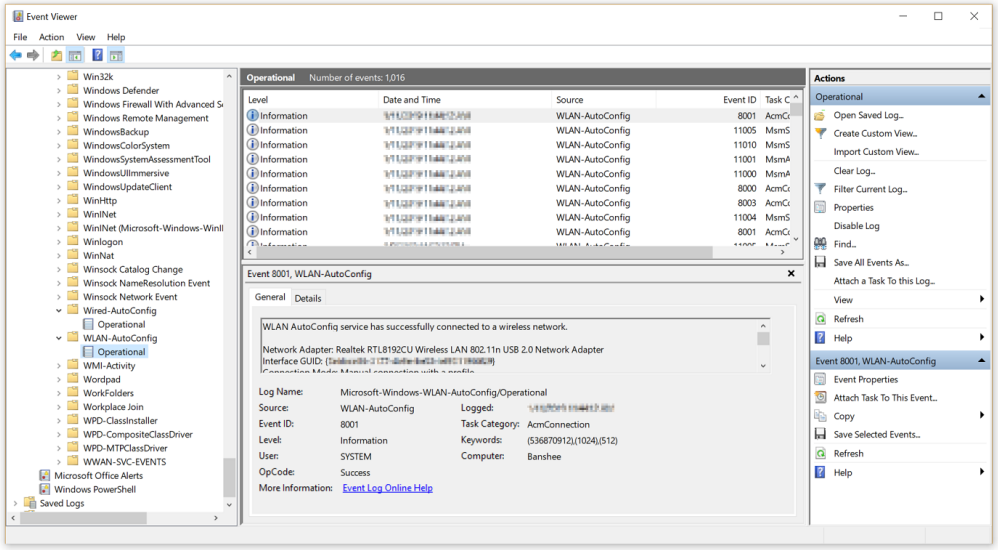
THREATVISOR RESEARCH

Validating Windows network-authentication changes before rollout

A practical acceptance method for a network change: preserve the access people need, verify the intended security restriction, and trace both results to the configuration tested.

TV-R03 · Technical analysis · Version 1.0

Last updated · November 7, 2026



Microsoft Windows Event Viewer shows the wireless connection event stream and the details behind a selected event. The report explains how to correlate these client observations with authentication decisions and a fresh application transaction. Source: Microsoft Learn: 802.1X authentication troubleshooting. Used with permission from Microsoft.

An independent ThreatVisor publication, not affiliated with, authorized, sponsored or approved by Microsoft Corporation.

Microsoft and Windows are trademarks of the Microsoft group of companies. All other trademarks are the property of their respective owners.

Prepared for

Windows endpoint engineers, network operators and security owners reviewing an authentication change.

Sourced analysis and proposed engineering practice, not original experimental results.

Executive summary

- Write two separate acceptance claims: the required workflow still works, and the behavior the change is meant to prevent is rejected for the intended reason.
- Pin the Windows configuration and authentication path before interpreting an update advisory. A fleet label or successful connection is too broad.
- Connect client and NPS evidence to a fresh application transaction. Keep missing observations and excluded configurations visible in the decision.

Method and scope

This report combines Microsoft documentation and one published operator advisory with a proposed acceptance method. It presents no ThreatVisor experiment or customer result. The method targets a representative Windows client using an NPS-backed Wi-Fi path. Other clients, wired access and VPNs need their own applicability review.

In this report

1. Start with the change behind the ticket
2. Define the path and the identity
3. Agree acceptance criteria before execution
4. Compare baseline, candidate and revision
5. Treat migration and recovery as different decisions
6. Make the decision no broader than the evidence

1 Start with the change behind the ticket

A network-access change has two jobs. It must alter a security property, such as which authentication behavior is permitted, while preserving the work that authorized users need to perform. A single ”connected” indicator cannot establish both. The useful unit of review is one proposed change, one defined access path and a small set of independently agreed outcomes.

Microsoft’s October 2026 credential hardening illustrates why configuration matters. For affected Windows systems with Credential Guard disabled and BlockNtlmv1SSO absent, the update changes the internal default from Audit to Enforce. This can interrupt single sign-on that relies on NTLMv1-derived credentials, including some MS-CHAPv2 network-access configurations. Manual credential entry remains possible in Enforce mode. The change does not mean every MS-CHAPv2 connection is disabled. [1]

York University reported affected AirYorkPLUS access after the October update, a Group Policy return to Audit, and unaffected Intune-enrolled devices using certificate authentication. That advisory documents a real operational consequence and a response. It does not establish what York tested beforehand, its financial impact, or a need for any particular vendor’s product. [8]

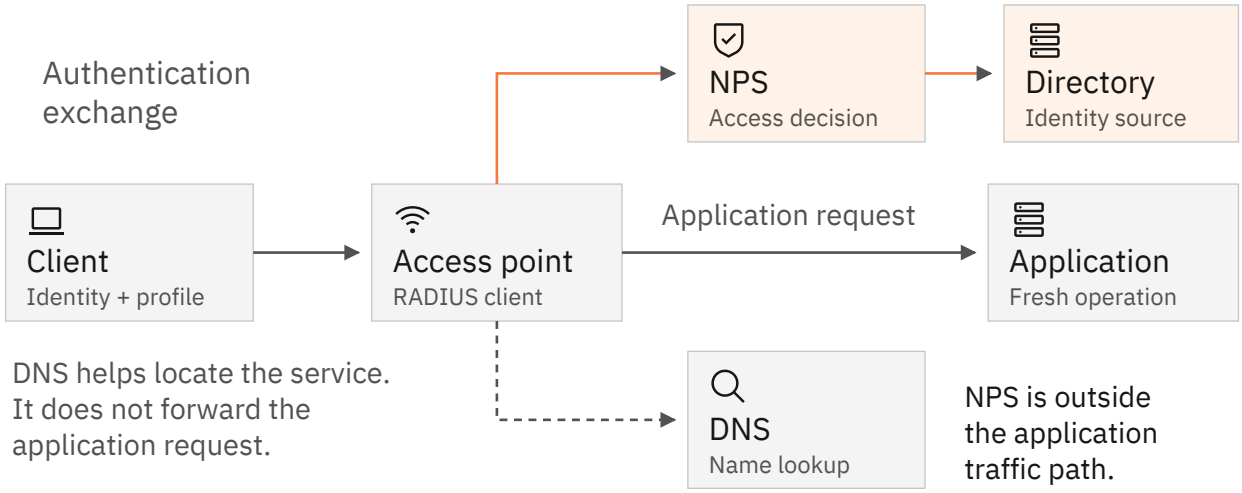
The engineering question is therefore specific: after this candidate change, can this authorized identity complete its required work through the intended network, while the behavior we intend to restrict is actually restricted? Answering that question requires more than checking whether an update installed.

2 Define the path and the identity

For an NPS-backed wireless path, separate the authentication exchange from the application traffic. The access point communicates with NPS as a RADIUS client. NPS makes the network-access authentication and authorization decision. The application request subsequently uses the network access that has been granted. Drawing the application behind NPS would obscure the distinction between these responsibilities. [5]

Record the client build, adapter and driver, selected Wi-Fi profile, authentication mode, identity, access point, NPS policies, certificate dependencies and target application. Record effective configuration, including where it came from, rather than relying only on a policy name. A user sign-in and a computer-authentication attempt may exercise different paths. PEAP alone is also insufficient as a method description because it can encapsulate different inner methods. [2]

Choose an application operation with an observable output, such as retrieving a newly created test record from an internal service. The record should be harmless and authorized for testing. Specify the expected identity, route and response before execution. A cached page or a response reached through another interface must not satisfy this requirement.



The access point participates in separate authentication and application paths. NPS makes the access decision and does not forward application traffic. DNS supplies name resolution. Conceptual topology. [5]

3 Agree acceptance criteria before execution

The operator and security owner should agree the expected behavior before inspecting candidate results. Otherwise, a test can accidentally define success around whatever the candidate happens to do. Distinguish the requirement from the observation and preserve the reviewer's authority to reject an apparently successful run.

For example, an approved certificate-authenticated client might need to reach a specific internal application. A separate test identity or profile might be required to fail because it uses a prohibited method. These are proposed checks, not a reproduction of the October SSO change. That historical mechanism requires its own eligible Windows configuration and evidence.

For each criterion, specify a positive observation, a relevant failure observation and the conditions that make the result inconclusive. This prevents "no error appeared" from becoming a substitute for evidence. Record a recovery procedure and stop condition before changing a test path, particularly where policy or certificate changes could affect other users.

An acceptance record for one change

Claim	Required observation	Limit
Approved work continues	Fresh application output from the intended identity and path	One operation does not cover every application workflow.
The intended restriction holds	A controlled attempt is rejected for the expected reason	Unreachable infrastructure is not proof of enforcement.
The result applies to this candidate	Recorded builds, profiles, policies and evidence times	Unrecorded differences leave applicability unresolved.

4 Compare baseline, candidate and revision

First establish the approved workflow on the recorded baseline. Preserve its observations before applying a candidate. Then run the same workflow and the security-specific checks against the candidate. If a revision is needed, record exactly what changed and repeat the affected checks. A revised candidate must not inherit a successful label from an earlier run.

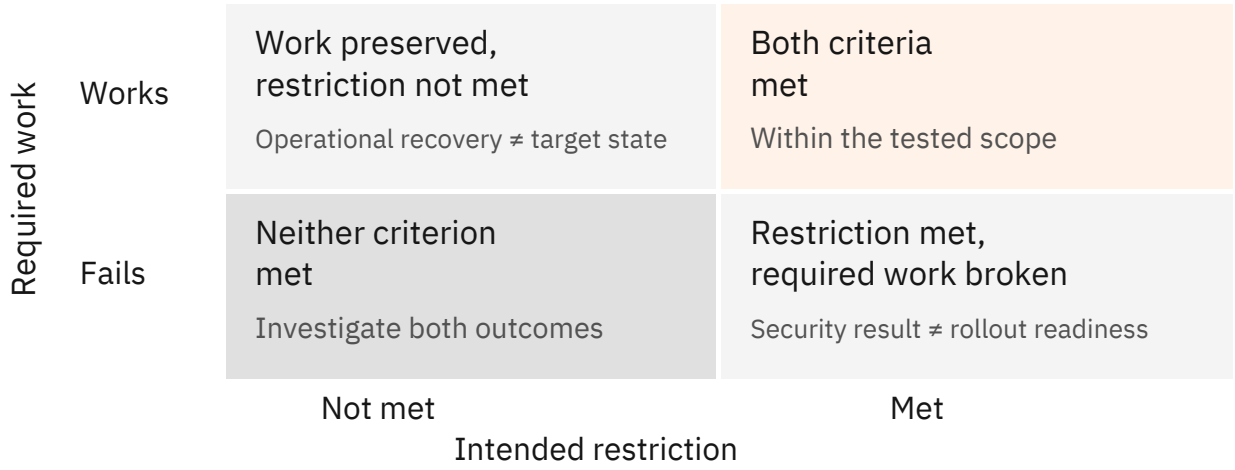
Collect client-side observations alongside the NPS decision where available. Microsoft documents NPS event 6272 for accepted requests and 6273 for rejected requests, with additional fields needed to interpret the policy and reason. Wireless client diagnostics are available in WLAN-AutoConfig/Operational. These sources should be correlated by identity, network context and a bounded time interval, not treated as if they share a universal test identifier. [6]

For the October credential change specifically, Microsoft documents Audit event 4024 and enforcement event 4025. Those events belong to that mechanism. They are not universal prerequisites for every certificate or NPS policy test. If the authentication attempt stops on the client before reaching NPS, the absence of a server event does not by itself locate the cause. [1]

After authentication, require the fresh application operation. Connectivity diagnostics can help establish interface, route and TCP reachability, but their success does not establish an application-level outcome. Preserve the application response and the evidence supporting its path. [7]

Two criteria create four possible outcomes

Classify only when both observations have enough supporting evidence.



Missing or ambiguous evidence → inconclusive, outside this outcome map.

Assess the required workflow and intended restriction independently for each tested state. Place a result in the map only when both outcomes have adequate evidence. Missing or ambiguous evidence remains inconclusive. No measured outcomes are plotted.

5 Treat migration and recovery as different decisions

Recovering access is an operational achievement, but it may not establish the intended security improvement. Returning an eligible system to Audit, for example, can restore behavior that Enforce restricts. That response needs an explicit owner, bounded scope and follow-up decision. It should not be reported as successful completion of a stronger authentication policy. [1]

A certificate-based migration also needs more than a certificate installation check. Client and server certificates serve different purposes. Trust, certificate usage, identity mapping and the selected authentication mode affect whether the intended exchange can succeed. Microsoft documents these requirements separately. [2] [4]

Windows version matters when assessing server validation. Microsoft's Windows 11 guidance distinguishes trust through a stored server-certificate thumbprint from trust through a certificate chain and a trusted-root thumbprint in the profile. Server-name matching matters when name validation is enabled. Record the actual profile and applicable OS behavior instead of copying an older validation rule into a new test. [3]

The acceptance owner should separately decide whether a recovery state is tolerable and whether the target state has enough evidence for rollout. A temporary exception can have a legitimate operational purpose without satisfying the original security criterion.

6 Make the decision no broader than the evidence

The useful output is a change record that another engineer can inspect: what was proposed, what was tested, which observations support each criterion, what remains missing and who accepts the remaining uncertainty. A green summary without those links is difficult to challenge or reuse.

One representative path is a starting point for learning, not fleet coverage. Before expanding, identify configurations that may change the outcome, such as machine versus user authentication, certificate enrollment, Windows build, profile delivery and application route. Choose the next test group because it exercises a meaningful difference, not because a device count looks reassuring.

Use the companion acceptance worksheet to separate approved requirements, execution receipts and the release decision. A result can support rollout within a stated scope, require more evidence, or justify a different response. None of these decisions establishes universal safety. The value lies in making the relationship between a change, its security purpose and dependent work explicit enough to review.

References

Sources reviewed November 7, 2026.

[1] Microsoft: Upcoming changes to NTLMv1-derived credentials

Documents the conditional October 2026 default change, Audit and Enforce behavior, and events 4024 and 4025.

https://support.microsoft.com/kb/5066470

[2] Microsoft: EAP for network access

Describes EAP methods and authentication modes. PEAP can contain different inner methods.

https://learn.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/network-access

[3] Microsoft: EAP changes in Windows 11

Windows 11-specific server-certificate validation behavior takes precedence over older general guidance.

https://learn.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/windows-11-changes

[4] Microsoft: Certificate requirements for PEAP and EAP

Describes distinct server and client certificate requirements, including purpose and identity checks.

https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-manage-cert-requirements

[5] Microsoft: Network Policy Server overview

Establishes the role of NPS and RADIUS clients in network-access authentication and authorization.

https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top

[6] Microsoft: Troubleshoot 802.1X authentication

Documents NPS acceptance/rejection events and client-side wireless, wired and certificate diagnostics.

https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/802-1x-authentication-issues-troubleshooting

[7] Microsoft: Test-NetConnection

Documents connectivity and route diagnostics. A successful TCP check is not an application transaction.

https://learn.microsoft.com/en-us/powershell/module/nettcpip/test-netconnection?view=windowsserver2025-ps

[8] York University: October 2026 update advisory

Operator-reported AirYorkPLUS impact, return to Audit through Group Policy, and unaffected certificate-authenticated Intune devices. No inference about prior testing or cost.

https://www.yorku.ca/uit/2026/10/service-advisory-microsoft-patch-tuesday-october-2026-kb5127648/