

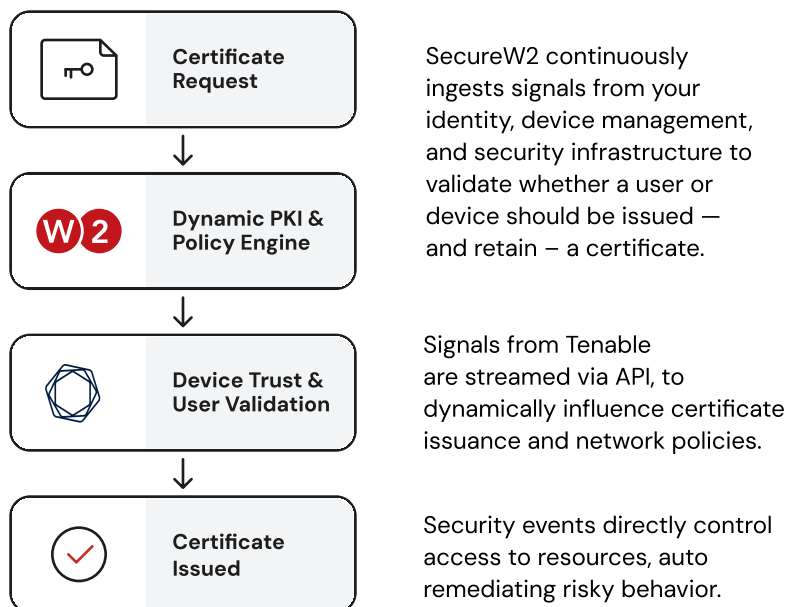


Automating Network Access with Dynamic Trust

SecureW2's Dynamic PKI delivers a modern, adaptive approach to securing network and application access. By continuously ingesting real-time security signals from sources like Tenable, it ensures certificates are issued only to verified devices, and stay only with those that remain compliant.

By leveraging your Tenable with SecureW2, you gain access to dynamic security signals, ensuring access is tied to trusted devices, not outdated assumptions.

How the Integration Works



BENEFITS

Modern, Flexible Enrollment

Use Dynamic SCEP, ACME, OAuth, JSON, self-enroll via dissolvable clients, and more.

High-Assurance Policy Engine

Build adaptive workflows that validate identity through limitless integrations.

Continuous Trust Enforcement

Tenable intelligence keeps certificate issuance and access retention decisions aligned with real-time security posture.

Instantly React to Threats

Revoke certificates immediately after critical threats surface.

Continuously Monitor Risk

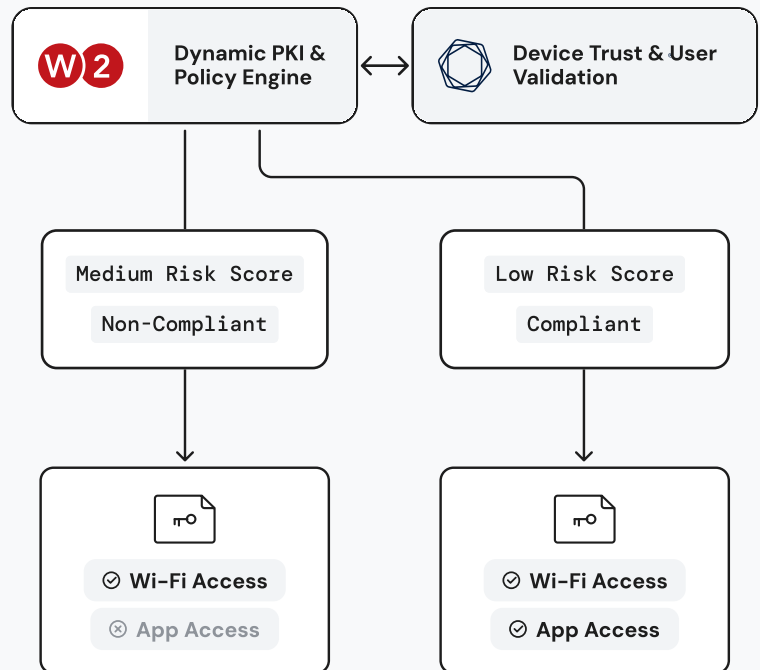
De-risk system access by dynamically issuing certificates for different levels of authentication, based on current risk exposure.

Adaptive Access Policies via Tenable Asset Exposure

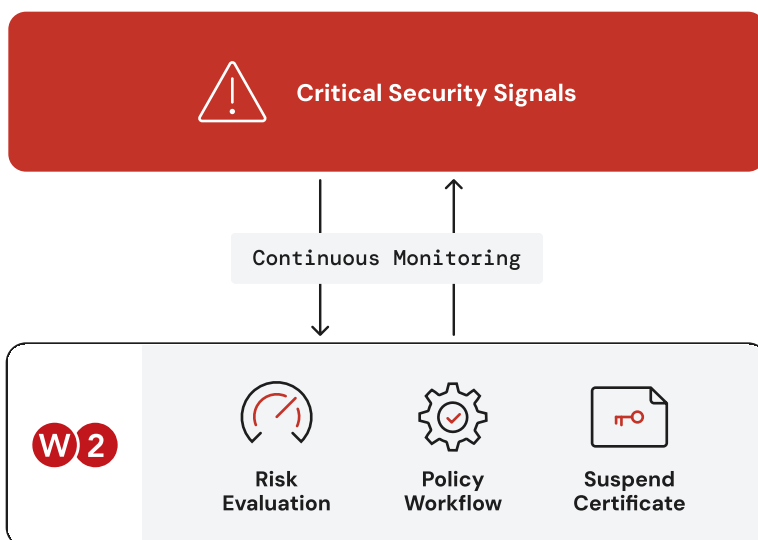
Access decisions should dynamically align with the risks they are intended to protect against. SecureW2 continuously incorporates security signals from **Tenable**, issuing certificates that adjust access levels based on the device's risk profile

Higher-risk devices might face quarantine, whereas lower-risk ones continue seamless access, ensuring authentication policies adapt in real time.

- ✓ **Manage Certificate Lifecycles:** Throughout the certificate lifecycle, SecureW2 uses Tenable API to assess the device's Asset Exposure level to ensure trusted and verified access.



Mitigate Risks Instantly via Continuous Monitoring



SecureW2 implements predefined remediation actions via continuous monitoring before threats can escalate. The workflow below demonstrates SecureW2 real-time enforcements as a reaction to critical threat events from **Tenable**, maintaining sync between security policies and threat intelligence.

- ✓ **Critical Threat Response:** SecureW2 immediately suspends or revokes the affected certificate as information from Tenable or other sources is received.