# Adobe® Zero-Trust Enterprise Network Platform

**Benefits of ZEN**

- Improves user experience by removing VPN requirements and improving authentication
- Improves security by restricting network level access to infrastructure
- Nearly eliminates lateral movement during compromise
- Protects internal applications while enabling a cloud-like experience

## Adobe Security

At Adobe, we take the security of your digital experience seriously. Security practices are deeply ingrained into our internal software development, operations processes, and tools and are rigorously followed by our cross-functional teams to help prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, security research institutions, and other industry organizations helps us keep up-to-date with the latest threats and vulnerabilities. We regularly incorporate these innovations into our internal enterprise security services as well as the products and services we provide to our customers.

This white paper describes the Adobe® Zero-Trust Enterprise Network (ZEN) Platform, an Adobe Security initiative that aims to securely enable access to the Adobe corporate network and resources based on the posture of the user and device.

## Background

You are likely familiar with the cumbersome process for accessing critical, on-premise applications, which first requires the user to log into the VPN followed by multiple additional authentications and authorizations. Not just complicated and annoying, the process may also lead to incomplete device security. What's more, inconsistent or unenforceable application authentication and authorization standards may permit unauthorized devices to join the network. Certificate-based mutual authentication is one technique to help avoid this problem.

As users became increasingly accustomed to the seamless experience of using cloud-based applications, Adobe set out to create an easier, more transparent application access experience that simultaneously helped to improve network security.

## What is Adobe ZEN?

The ZEN platform transforms the Adobe network and internal applications to a "cloud-like" state, enabling users to access applications from anywhere without requiring a VPN to the corporate network. With ZEN, Adobe employees with properly configured devices have a better, more seamless experience, while application owners can be more confident that trusted devices gain access to their resources. In addition, ZEN restricts lateral movement within the network.

## How Does ZEN Work?

Adobe ZEN uses certificate technology, rather than usernames and passwords, for authentication in order to deliver a better, more seamless user experience as well as improved network security through stronger two-factor authentication.

For any application accessible through the ZEN platform, Adobe evaluates the security posture of each device attempting access. All managed devices automatically receive a unique ZEN certificate, which is used for authentication, reducing the need for employees to provide their username and password multiple times to access the resources they need. Certificates are renewed and re-issued on a regular basis to devices to help maintain a solid trust chain.

Based on the details collected about a device, including whether the device is protected with anti-malware software or has been lost or stolen, Adobe can determine if the device is allowed to safely access a particular resource. With ZEN, managed computers are quickly recognized as trusted assets.

## Adobe ZEN Platform Architecture

The ZEN Platform architecture includes the following key functions:

- **Device Management** – Leveraging the AirWatch by VMWare device management solution, ZEN helps establish the authorization chain by securely generating and distributing ZEN certificates to each managed device and configuring the device for the ZEN environment. The device management solution is responsible for certificate lifecycle management.
- **Authentication and Posture Check** – Integration of Okta and VMWare Workspace One (vIDM and AirWatch), enables web applications to allow resource access using certificate-based authentication (CBA) and conducts a security posture check.
- **Access Proxy** – Allows users with devices containing a ZEN certificate to access on-premise applications outside the corporate network without VPN. The access proxy forces encrypted communication, authenticates the user, and makes control checks to the Access Policy Engine, helping to ensure only authorized devices can reach an internal application.
- **Identity and Access Management** – Authenticates the user based on their credentials (first and second factor) and authorizes access to an application by making a control check to the Access Policy Engine.
- **Access Policy Engine** – Acts as the central authorization service, providing an authorization decision based on the device and user posture.

**LEGEND**

1. Client challenged for certificate
2. Active Directory
3. Compliance check to Access Policy Engine

4a. AuthN request to IdP

4b. Client challenged for certificate

4c. Compliance check to Access Policy Engine

5. Allow access if all conditions met

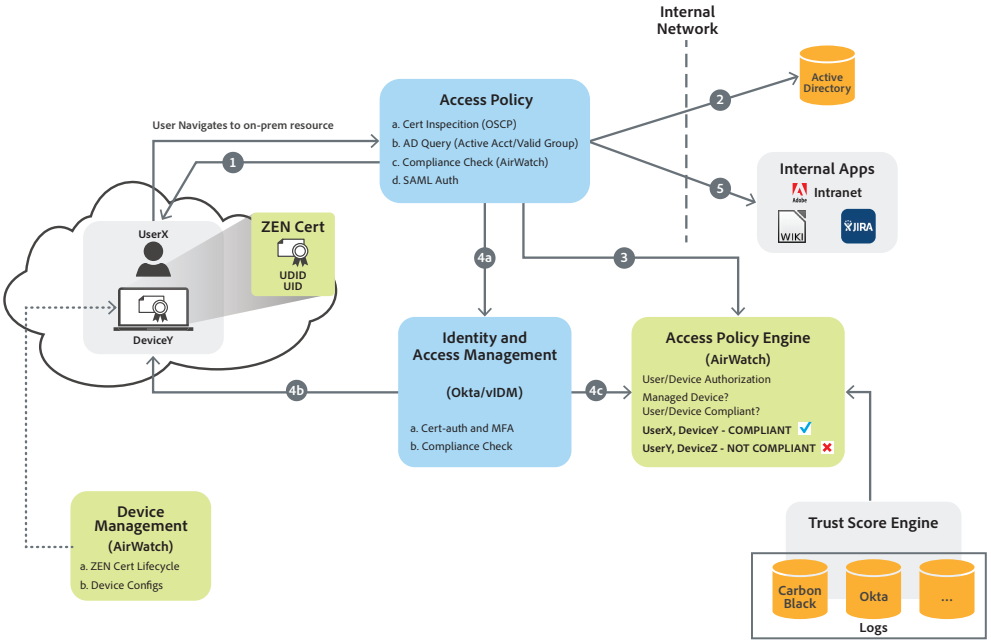


Figure 1: Adobe Platform Architecture

## ZEN Device and User Authentication

When a device enrolls in AirWatch, it automatically receives the following:

- **ZEN certificate** – AirWatch automatically and silently pushes a ZEN certificate to the device (similar to how WiFi certifications are deployed via AirWatch). The ZEN certificate includes the device's unique identifier (UDID) and the user associated with the device (UID), and is used to authenticate the user and make a device posture check to the AirWatch server.
- **ZEN configuration** – In addition to the ZEN certificate, AirWatch automatically pushes ZEN configuration settings that ensure the ZEN certificate is automatically selected when authenticating to a ZEN-enabled application. If the ZEN configuration was not deployed to a device, the user sees a certificate pop-up window, asking them to select a certificate from their machine certificate store.

If a device is not yet managed and does not have a ZEN certificate, the employee can use existing secure authentication methods (such as username/password + MFA) to access internal or on-premise resources. However, as an added layer of security they must be on the corporate network either physically or through VPN.

Once configured, the ZEN certificate is presented to the Access Proxy and Identity and Access Management functions. If authorized, the user can access internal applications from outside the Adobe corporate network.

**LEGEND**

1. Request goes to web app
2. App makes AuthN request to Okta
3. Okta delegates AuthN request to vIDM
4. vIDM challenges client for certificate
5. Certificate sent for authentication
6. CRL/OCSP Check
7. CRL/OCSP Response
8. Compliance Check
9. Response (Compliant)
10. If cert valid, vIDM generates SAML response and send to Okta
11. Okta validates SAML, challenges for MFA generates new SAML response and sends to app
12. App validates SAML and if valid, redirects user to protected application content

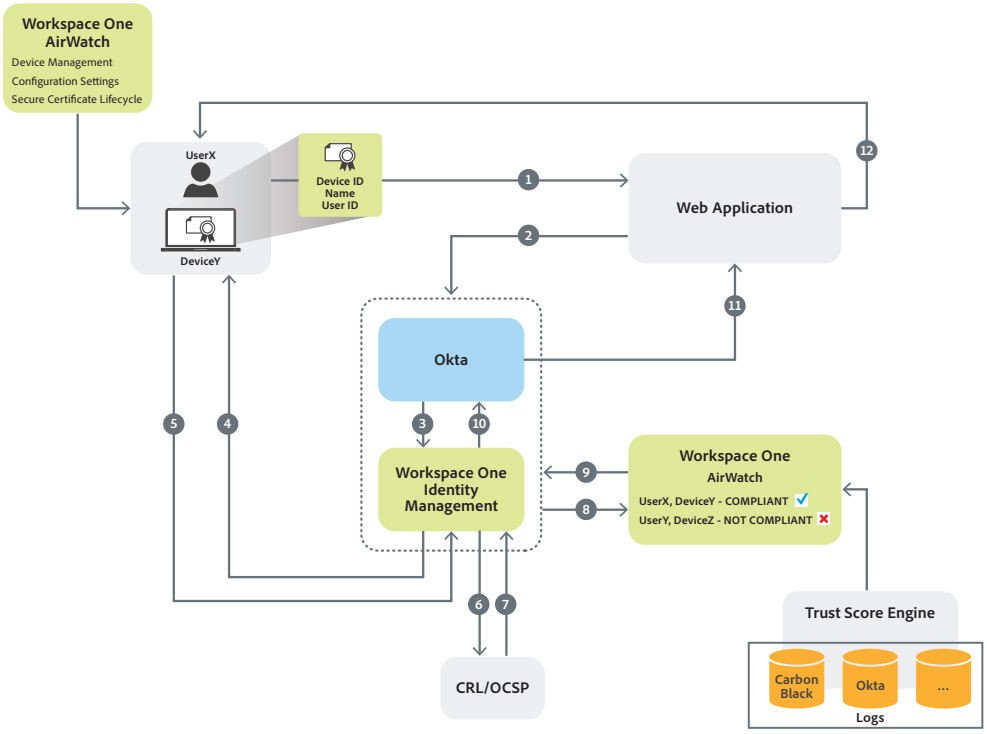


Figure 2: User Authentication and Posture Check Flow

## How Does ZEN Fit into Adobe's Wider Security Framework?

With a company-wide culture of security, Adobe is committed to building security into all aspect of our business, from application and operational security to network and enterprise security. Our goals for security include automating and standardizing as much as possible, thereby helping to reduce risk, helping to meet compliance standards and regulations, and improving experiences for both our customers and employees.

Combining reputable security technologies in a novel approach that builds upon our existing investments, instead of replacing them, ZEN is an important step toward meeting Adobe's enterprise security infrastructure goals.

## A Novel Implementation Approach

Identity is at the core of everything in Adobe's network. When devices join the network, it is to perform functions, and these functions require authentication to communicate with or deliver that function to the device. After determining that we could combine user and device identities in the authentication workflow, we embarked on an implementation that would rely on a single checkpoint to determine both access and authorization.

One of the key requirements for the new access and authorization model was that it could not impact the traditional authentication and VPN access methods. So, ZEN was designed with coexistence in mind, in order to make the migration seamless: Users with ZEN-enabled devices could access ZEN-enabled applications without the need for VPN or their username and password. At the same time, non-ZEN-enabled devices could fall back to the traditional authentication workflow, requiring a username and password as well as VPN when the user was not on the corporate network.

Another key requirement was that the new approach needed to leverage Adobe's existing technology investments. In addition to the money and time required to build a new approach from scratch, the ensuing user migration could cause user downtime and productivity impacts. Adobe instead worked with our existing vendors in order to deliver the end-to-end workflows in ZEN.

Finally, we wanted our application teams to feel zero impact in order to support and move to ZEN. Almost all of our applications already used OKTA as part of the multi-factor authentication workflow. After working with OKTA to make a back-end change in their code, our application teams didn't need to make any configuration changes in order to take advantage of the ZEN platform. To help ensure compatibility once implemented, all application teams participated in a beta rollout of ZEN.

## Conclusion

The Adobe ZEN platform is an Adobe Security initiative which aims to enhance the user experience when accessing web applications, while simultaneously helping to improve network security. Using certificate-based technology to enable access to the Adobe corporate network and resources based on the posture of the requesting user and device, ZEN helps ensure that trusted devices can access on-premise and internal applications from outside the Adobe corporate network. At the same time, ZEN makes the user experience seamless by eliminating the need for multiple authentications and re-entry of their username and password.

As with all of Adobe's security initiatives, we will continue to evolve ZEN based on lessons learned, emerging technologies and capabilities, and new service offerings.

Adobe

**Adobe Systems Incorporated**
345 Park Avenue
San Jose, CA 95110-2704
USA
*www.adobe.com*