virtel
a syspertec group company

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

VANGUARD ez/Token ™

What is Multifactor Authentication?

Multifactor authentication is a system for identifying and granting access to a computing resource that utilizes two or more independent credentials. They might be something the user knows (like a password), something the user has (a security token) or perhaps something physically unique to the user (biometric verification). The goal of multifactor authentication (MFA) is to create a layered defense and make it more difficult for an unauthorized person to access a target resource. If one factor is compromised or broken, a hacker still has at least one more barrier to breach before successfully breaking into the target.

Data Breaches and Why MFA is a Security Best Practice

Becoming headline news for a data breach has caused more than one CEO/CISO to wake up in the middle of the night in a cold sweat. It's not an unfounded fear. The outbreak of recent high-profile corporate breaches has been a wake-up call for executives. CEOs and CISOs are now tasked with overseeing the elements that contribute to their organization's success in today's high-risk world, and that includes taking an active role in the company's data and infrastructure security strategy. Failing to do so often involves fines and visits from regulators, a loss of reputation and revenue, angry customers fleeing to rivals, not to mention in some instances, executives losing their own positions. Weak or stolen user credentials remain the primary entry point for hackers, which is why authentication must be included in the overall security plan. Multifactor authentication is the best-practice approach to help keep user data secure and keep your company out of the headlines.

Vanguard's ez/Token Two-Factor Authentication Solution

VANGUARD ez/TOKEN is a two-factor authentication solution that allow users to authenti- cate through either RSA SecurID, SafeSign, ActivIdentity, and other tokens to the z/OS Security Server or any other application currently using RACF authentication. The ez/Token solution provides a more secure alternative than the usual RACF user ID/password combination. With ez/Token, users substitute a new, one-time passcode in place of or in addition to their password.

Vanguard ez/Token Key Capabilities

There are basically two types of authentication methods used by EZ/Token. Authentications that go through a windows server (RSA Token / Active ID) and authentications that go directly through the LINOTP server.

1. RSA Token (SECUREID) or ActiveID (SAFESIGN) agents and Tokens are handled very similarly and their features below are grouped together. ActiveID has two different servers and both are supported (the 4tress and ActiveID AAA Server are both supported and selectable during installation)
2. 2. LINOTP (LINOTP) agents and any token supported by LINOTP are handled separately and it's features below have been separated

- Authenticate through either an RSA, SafeSign or ActivIdentity token to log on to the Mainframe via TSO, CICS, IMS, or any other application using RACF authentication.
- Perform New PIN and Next Token Code operations through a Web interface.

2025 Vanguard Integrity Professionals - Nevada All Rights Reserved.

VANGUARD ez/Token ™

Enabling Password Reset

The ez/Token authentication exit authenticates users logging on to the z/OS Security Server or any other application that uses RACF security, through either an ActivIdentity, RSA SecurID tokens or LINOTP.

Vanguard ez/Token Components

Security on Demand Host Server

The Security on Demand host server (VIPMAIN) runs as a started task on an IBM mainframe server.
The Security-On-Demand host server is integrated with the Vanguard Security Solutions product installation.

RSA, Active ID or Secure ID (only)

Vanguard ez/Token Agent Daemo

The ez/Token Agent Daemon provides remote clients, such as the ez/TOKEN Website and ez/ TOKEN Authentication Exit, the ability to authenticate either an RSA, SafeSign or ActivIdentity tokens change PINs and get the Next Token Code by redirecting requests from these remote clients to the token server via an API.

Vanguard ez/Token Mainframe Authentication Exit

The ez/TOKEN Mainframe authentication exit selectively redirects certain RACF users to authenticate using RSA, ActivIdentity or SafeSign two-factor tokens instead of a RACF password. This exit talks to the ez/Token Agent Daemon.

Vanguard ez/Token Website

The ez/TOKEN Website communicates with the ez/TOKEN Agent Daemon to allow users to perform New PIN and Next Token Code operations. The ez/TOKEN authentication exit on the mainframe does not have the capability to provide these interfaces therefore the website provides these functions.

Key Differentiators

- With ez/TOKEN, users substitute a new, one-time passcode in place of a password. Passcodes are generated randomly every 60 seconds. For enhanced security, the passcode can be combined with a pin number. The ez/ Token solution provides a more secure alternative than the usual RACF user id/ password combination.
- Authenticate to the Mainframe through multiple token technologies like: ActivIdentity, RSA SecurID, YUBiKEY, or OAUTH Tokens via TSO, CICS, IMS or any other application that utilizes z/OS Security Server authentication
- Selectively include or exclude applications from multifactor authentication.
- Easy User Management, users can be migrated to multifactor authentication individually or by groups.

2025 Vanguard Integrity Professionals - Nevada All Rights Reserved.

VANGUARD ez/Token ™

Virtel et ses partenaires

L'assurance d'un expert, la garantie de solutions logicielles efficaces

Depuis 1993, la société Virtel représente des éditeurs majeurs en France et dans les pays francophones. Elle offre ainsi des solutions logicielles novatrices et fiables destinées tant aux grandes entreprises qu'aux PME.

Contact

302 Bureaux de la Colline
92213 Saint Cloud
Tél: 01 41 06 92 00
Email: **info@syspertec.com**
Site: **www.virtelweb.fr**

2025 Vanguard Integrity Professionals - Nevada All Rights Reserved.