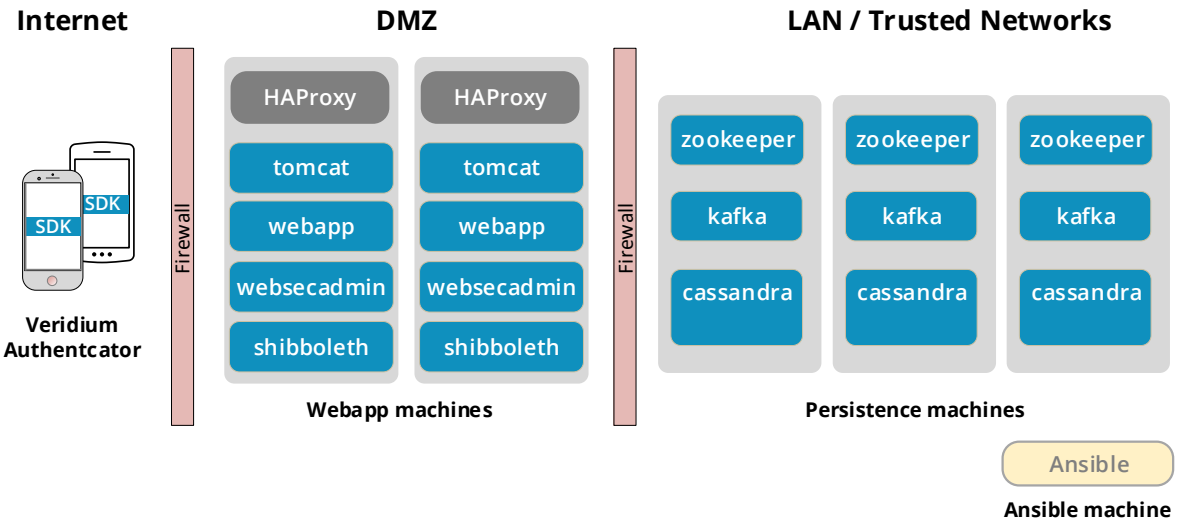
VeridiumID 1.8 Server Specifications

Example Deployment

A typical production deployment requires up to six machines in a single data center.

Two WebApp machines:	WebApp machines run web applications and load balancers to provide the administration dashboard UI and handle interactions with Veridium Authenticator and other possible Veridium client apps.
Three Persistence machines:	Persistence machines host the Cassandra database and supporting software used to store administration, configuration, and account parameters used by the system.
One Ansible machine:	The Ansible machine stores and runs ansible scripts for provisioning VeridiumID software. A deployment needs only one ansible machine even when multiple WebApp and Persistence machines are deployed.

VeridiumID Infrastructure Example



Machine Resources Required

Resource name	WebApp machines	Persistence machines	Ansible machine
CPU	4 cores	4 cores	2 cores
Memory	8 Gb	8 Gb	2 Gb
Disk	40 Gb	80 Gb	20 Gb
Operating System	RedHat 6/Centos 6	RedHat 6/Centos 6	RedHat 6/Centos 6

VeridiumID Base Software Installation

All machines require the following base packages from the RHEL official repository.

- apr-devel
- openssl-devel
- libstdc++-devel
- curl
- unzip
- wget
- zlib
- zlib-devel
- nc
- openssh-clients
- perl

Deployment Types

- On-premises and cloud deployments.
- VeridiumID supports most clouds including Amazon Web Services (AWS) EC2, Rackspace Cloud, and Microsoft Azure.

Licenses and Certificates

- Licenses required for your specific configuration.
- A globally resolvable SSL certificate.

Connections Required

- Internet accessible (direct or indirect) for authentications outside your network.
- Internet access for sending OTPs (SMS or SMTP) and Push Notifications.
- Apple Push Notification service (APNs) and Firebase Cloud Messaging (FCM) required for push authentication client workflows.

Biometrics Support

- 4 Fingers TouchlessID (provided)
- vFace (provided)
- Utilizes native phone biometrics
- 3rd party biometrics (must be separately licensed)
- Veridium InMotion Behavioral Biometrics

Services Required in your Environment

- Certificate Authority – Required to issue internal certificates for passwordless authentication to Citrix VDAs and AD domain-joined PCs.
- Identity system – Required to host the user directory.

Integrations Supported

VeridiumID supports these environments out-of-the-box.

- Citrix Application Servers and VDIs
- Windows PCs in an Active Directory domain
- We support most VPNs using RADIUS
- SAML Workflows
- Provide identity authentication for IAM environments

Standards Supported

- IEEE Std 2410- (2015, 2017, 2019) Biometric Open Protocol Specification

Veridium has a leadership role in these standards bodies

- IEEE Std 2418-6 - Blockchain for Healthcare and Life Sciences
- ISO SC 27/WG 5
- W3C Decentralized Identifiers
- W3C Verifiable Credentials

Certifications

- FIPS 140-2 (self-assessed)
- EPCS certified as a biometric subsystem for electronic prescription of controlled substances.
- FIDO UAF Certified
- FIDO2 (pending 3Q 2019)
- Citrix Ready
- National Registry of Identification and Civil Status (Peru)

Veridium Authenticator

- Android 5.0 and higher
- iOS 9.0 and higher for any iPhone

Tools and Utilities Required

- A file transfer utility like WinSCP or scp to transfer files.
- An ssh client like PuTTy to access the machine command line.