nma.com/zsentry/

Request a ZSentry trial

ZAuthority™ Administration Authority for ZSentry™ Credentials

Easily issue ZSentry credentials with centralized user administration and control delegation.

ZAuthority offers enterprises a **cost-effective** and **secure** system to deploy, audit, activate, suspend and revoke ZSentry credentials, with:

- ✓ Automated and self-service administration of ZSentry credential generation, activation, suspension and revocation from an existing user database
- ✓ Manager direct access interface
- ✓ Built-in translation tables for ZSentry *Authorization Information*, providing easy interfacing for credential generation from back-end access control systems
- ✓ Support for common architectures, such as RADIUS, LDAP and Active Directory
- ✓ Automated updates and synchronization from changes in the user database, by database trigger events or by direct polling from ZAuthority

Key Benefits

- Manages the entire process of deploying and auditing ZSentry credentials
- Does not retain credential copies
- Built-in fault tolerance
- Centralized user administration with control delegation
- Multi-level credential management
- Credentials can be immediately activated, suspended or revoked per credential type, management level and user
- User self-service interface

Optional three-factor authentication with:
Smart cards
USB tokens
Biometrics

About ZSentry™

ZSentry is an access control system with five credential types for maximum usage and control granularity:
DTC™, Password, Return Code, Authorization Information, User ID

The credentials are linked by cryptographic keys. The *Password* is private, known only by the user. The *DTC* and the *Return Code* are given to the user. The *Authorization Information* and the User ID are not given to the user.

Four security services, that reinforce each other, are directly available with ZSentry:
Authorization, Spoof Prevention, Authentication and Access Control.

Non-repudiation, trust development and control delegation are also supported. ZSentry operates without databases, shared secrets and PKI, significantly reducing costs and complexity, improving scalability and strengthening security.

ZSentry is the most cost-effective solution for secure and flexible access control.

Very Simple to Use

With ZAuthority, users and managers can request, activate, suspend, revoke and automatically bind ZSentry credentials to specific access control information. Managers have approval authority on all matters. Approval authority can be conditionally delegated to users and sub-managers. Events can be securely audited, developing trust and supporting non-repudiation.

Very Simple to Deploy

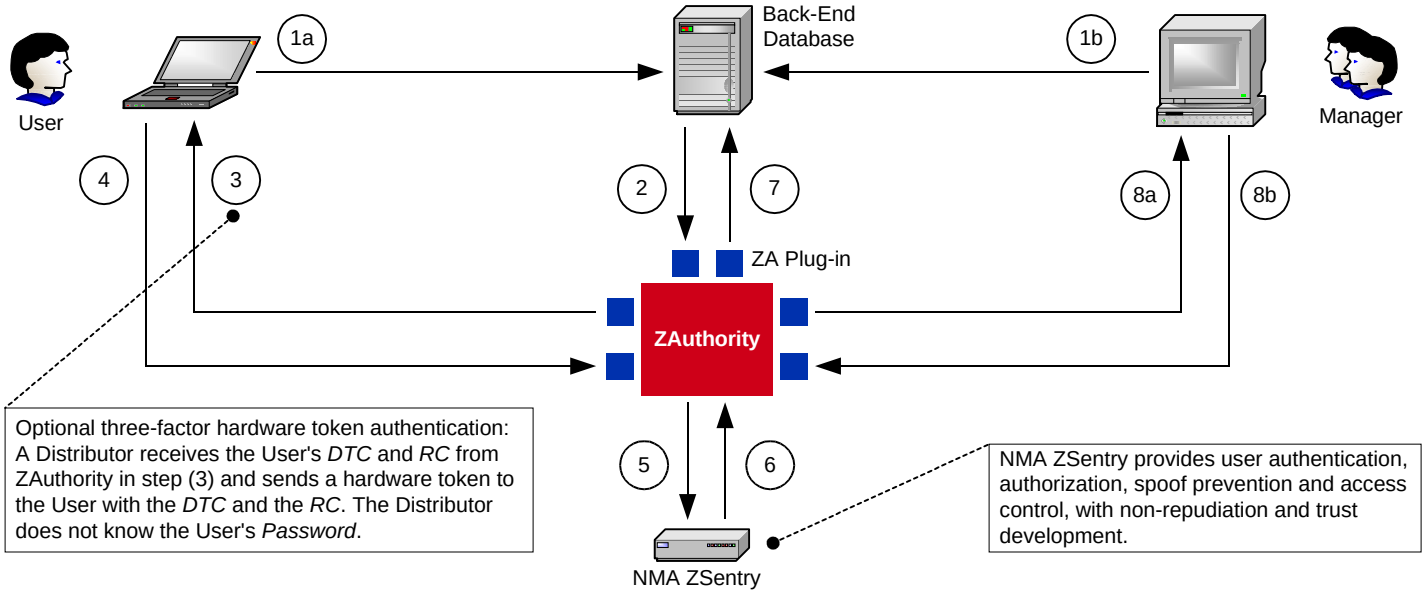
ZAuthority functions are handled via a browser that accesses a Web server within an intranet or on the Internet; no additional software is required on the client.

See the reverse side for a ZAuthority example of ZSentry credential deployment.

NMA ZAuthority™

ZSentry Administration Authority

ZAuthority Architecture



The **ZAuthority Architecture** shown above supports a variety of administration needs and policies, with multi-level credential management. ZAuthority plug-ins are provided for easy interfacing with diverse systems and communication modes. There are no plug-ins for the User, Manager and back-end systems. Fault tolerance is built in by data replication. Redundant ZAuthority systems can work together to further increase fault tolerance. Customized protocols can be efficiently defined, providing enterprises with specific solutions for access control. The table below shows one example of a ZAuthority administration protocol for ZSentry credential deployment.

(1a, 1b) Request to Back-End Database: User or Manager submits a request to a back-end database for ZSentry credential generation. The User's data can be supplied by the User, by the Manager, and/or by the database itself.

(2) Request to ZAuthority: The back-end database sends the request to ZAuthority. For "push" synchronization purposes, a trigger event at the back-end database can also automatically send a request to ZAuthority. Additionally, for "pull" synchronization purposes, ZAuthority can automatically query (7) the back-end database at pre-specified time intervals, prompting the database to send a request to ZAuthority.

(3) Credential Generation: ZAuthority requests approval (8a) by the Manager. If the credential request is authorized (8b), ZAuthority issues a *DTC* and *Return Code (RC)* and sends them directly to the User. No credential copies are retained and only the User knows the *Password*. Translation tables in ZAuthority can be used to allow credential generation directly from back-end data formats. Confirmation of transmission and/or confirmation of receipt (4) are provided with auditable feedback to the back-end database (7) and/or Manager (8a).

In addition to credential generation, the events (1a), (1b), (2) and (3) can be used for credential activation, suspension and revocation requests. A configurable, auditable session linking the control events is maintained by ZAuthority for all requests.

(4) User Self Service: User may be authorized by the Manager to request generation, activation, suspension or revocation of credentials.

(5) Notification to ZSentry: ZAuthority sends activation, suspension and revocation notices to ZSentry, with ZSentry feedback (6). There is no credential generation notification.

(6) ZSentry Alarm, Auditing and Response: ZAuthority receives alarms from ZSentry and can also query for confirmation and auditing of credential use, failed attempts, activation, suspension and revocation. ZAuthority can command ZSentry to directly respond to threats; for example, automatic credential revocation (or suspension during a given time interval) can be internally triggered after a pre-defined number of failed sequential authentication attempts.

(7) ZAuthority Auditing and Data Replication: ZAuthority reports events to the back-end database for auditing and fault tolerance purposes, including ZSentry events and generation, activation, suspension and revocation of credentials.

(8a, 8b) Manager Direct Access: Manager has approval authority on all matters. Approval authority can be conditionally delegated to Users and sub-managers. Manager can directly configure ZAuthority and ZSentry audit reports, and can also directly control the generation, activation, suspension or revocation of credentials.