



MSK allows businesses to:

- Simplify user access administration
- Minimize exposure to network breaches
- Adhere to industry and government regulations
- Deploy and maintain with low total cost of ownership
- Enable secure workforce mobility

MSK Identity and Access Management

Overview

All businesses have sensitive data and must simultaneously protect it and provide access to it. To effectively do this, a proven system for user authentication, the reliable validation of users' identity, is required. The ideal system provides top-level security with cost-effective deployment and maintenance as well as ease of use.

MSK offers identity and access management solutions that meet these requirements. MSK delivers enterprise-grade user authentication that is more powerful than existing encryption-based technologies without the complexity, overhead and risk associated with these solutions that require key management and storage.

Because user acceptance is a critical part of the success of a security system, MSK is designed for maximum ease of use. Additionally, MSK streamlines administration by providing a single authentication method for accessing data and applications through networks, email, intranets and extranets, desktops, Web servers and other network resources.

To deliver powerful authentication with minimal overhead, MSK takes the proven two-factor method to a new level of ease of use and security. Unlike existing two-factor solutions, something you know (e.g., password) and something you have (e.g., token) provide secure access to multiple systems and applications. With MSK, administrators and users have a single point of control for all access needs.

MSK also adds another level of security by having users' authentication done directly between the client and the server. This direct connection authentication confirms that users are logging into the actual server rather than being spoofed.

Key Features

Lightweight Deployment and Maintenance

MSK's lightweight deployment and maintenance model is built on a token-based system that provides access to multiple applications and systems from a single token assigned to an individual user. The token validates to the server that the users are who they say they are and access is controlled by the MSK application.

Through a central server, tokens are issued in real time, access rights are granted and revoked, and users are authenticated. This means that user access to multiple applications can be added or deleted from a single point.

The MSK architecture is designed for maximum scalability. It can grow with current systems and applications as well as easily support additional ones.

User Set Up

When a new token is issued, user profiles can be drawn from applications' and systems' rules databases. Once issued, tokens are delivered to users' individual systems or pushed through a network. The token can be downloaded to the user's computer or stored on portable media, such as CD or USB drive. This eliminates the need for costly one-time password (OTP) systems. To limit use to a specific system, tokens can be assigned to IP address to prevent users from accessing from other systems.

User Access Management

With MSK, it is easy to set up and retract access rights. When user rights need to be modified or revoked completely, a token is simply disabled and the user's access to any number of systems or applications is completely cut off – all in a single step.

Robust Reporting

MSK provides a wide range of reports to meet all audit and regulatory requirements. All data can be easily accessed and aggregated to create custom reports or exported to other systems. Among the regulatory requirements supported by MSK are: FFIEC, Sox, HIPAA, FDA 21, CFR Part 11, GLBA, CA Notice of Breach, NERC Cyber Security Standards and PCI.

Attack Prevention

Because of its unique authentication methodology, MSK dramatically reduces attack surface. MSK eliminates the possibility of common attacks, including SQL injection, Phishing, key loggers' attacks on the login, DNS poisoning/Pharming and man-in-the-middle attacks. MSK also dramatically reduces the risk of denial of service.



Contact MSK
9518 Ninth St., Suite C-2
Rancho Cucamonga, CA 91730
Phone: 818-974-4400
E-mail: info@multipleshiftkey.com
URL: www.multipleshiftkey.com