



# Privileged Access Management with ConsoleWorks

A unified in-band and out-of-band solution

## Solution Brief



# Privileged Access Management with ConsoleWorks

**A unified in-band and out-of-band solution**

## ConsoleWorks Privileged Access Platform

ConsoleWorks offers organizations a single tool that can manage all privileged access in the organization. From operating systems to configuration ports, ConsoleWorks can control access, enforce permission models, and record (down to the keystroke) all privileged user activity for virtually any asset in the IT infrastructure.

## Access Management

Access management is the practice of controlling the IT resources each person in the organization has access to along with the permissions they are granted for each resource they can access. In simpler terms, access management determines who can go where, and what they can do when they get there.

From a security perspective this is normally discussed in terms of role-based access and control. In a role-based access and control security model, each role is assigned a specific list of access permissions (what the role has permission to access) and the associated privileges (what a person is allowed to do for each access permission granted). People are then assigned to one or more roles in order to grant them the access and privilege they need to perform their work.

## Privileged Access Management

Privileged access management is a specific subset of access management where the interfaces being managed have an inordinately high level of privilege associated to them. The most common example of a privileged interface is an account on an operating system.

For example, having permission to access a shared drive has a relatively low level of privilege with a limited set of permissions like read, change and full control. Access to an operating system can offer thousands of commands, many of which can have broad reaching affects on operations, security, and compliance.

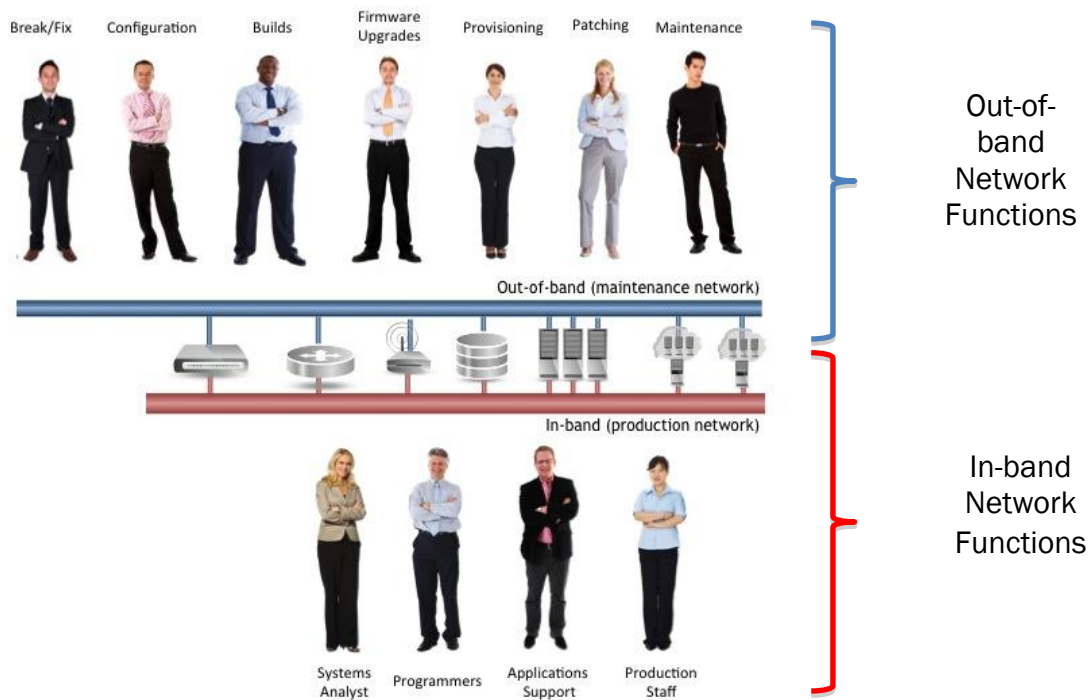
ConsoleWorks addresses privileged access management, which is further broken-down into two broad functional groups: in-band access and out-of-band access.

## In-Band Access

System analysts, programmers, production staff, application support, and others need regular access to the operating system accounts to support business operations. These people access operating systems over the normal network, also called the in-band network. This is the primary scope of most privileged access management programs.

## Out-of-Band Access

IT systems and infrastructure management teams support the actual devices for break/fix, configuration, build, firmware upgrades, provisioning, patching, and maintenance. These people typically access those same servers through configuration ports<sup>1</sup>, often over a separate network commonly termed the maintenance or out-of-band network.



## Different Network, Different Interfaces

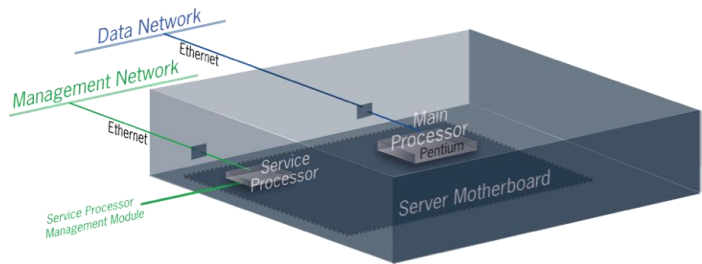
These two networks use different network interfaces. The in-band network uses one or more of the NIC ports on the server for network connections. The out-of-band network uses

<sup>1</sup> Configuration ports are on baseboard management controllers including HP iLO, Dell DRAC, Sun ALOM, etc.

configuration ports that are connected to dedicated service processor computers in almost all servers on the market today. These service processors run completely independently – accessible at any time and under any condition as long as power is connected to the server chassis.

## Production (Data) and Maintenance Networks

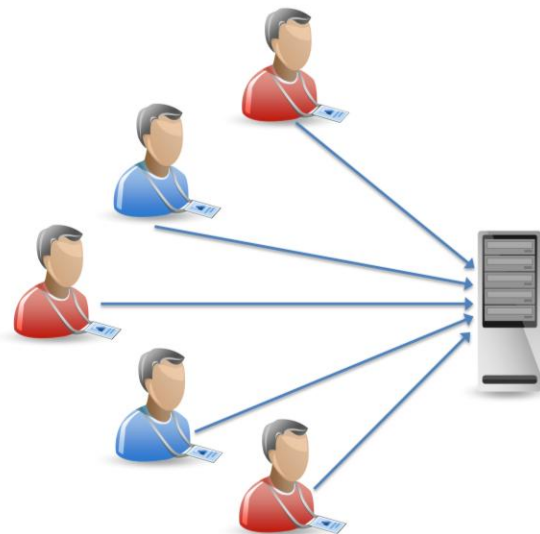
- 1) Maintenance Network
  - Service Processor built in to servers (on Motherboard)
  - Is a computer in the computer
  - Is live (external communications) anytime power is applied to chassis
  - Has dedicated (maintenance) TCP/IP connection
- 2) Production (Data) Network
  - Uses normal Network Interface (NIC)



Both groups are accessing interfaces with extremely high privileges where mistakes can directly result in service disruption, compliance failure, and data breaches. They both need to be under privileged access management control. If they are not, the business is placed under a high degree of risk.

The use cases are quite different though. In-band access is typically a many people to one interface scenario. Least privilege plays a very important role with in-band access, as the people accessing operating system accounts often touch sensitive data and their activity must be tightly controlled.

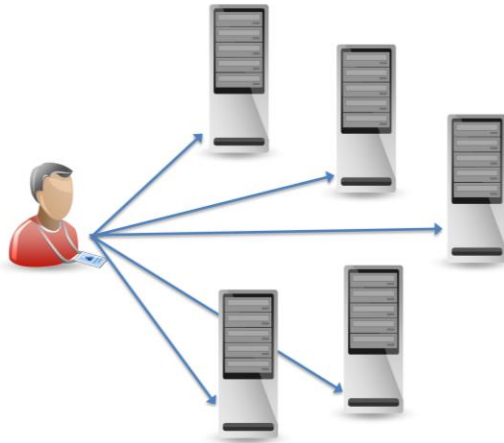
In-band Privileged Access is Many People to One Device



ConsoleWorks manages the many people to one interface within its Privileged Access Platform module that can create, and manage, an unlimited number of private user sessions to operating system, database or application interfaces.

Out-of-band access is typically a one user to many interfaces scenario. Least privilege

Out-of-Band Privileged Access is One Person to Many Devices



remains important with out-of-band access but there are typically more privileges granted for out-of-band access as they are needed for break/fix operations, patching, device configuration, firmware/bios updates, and device build.

ConsoleWorks manages the one person to many interfaces within its Privileged Access Platform module that can create, and manage, multiple user device sessions for a single ConsoleWorks user.

## Privileged User Risks

The risk associated with user access to operating systems over the in-band network is compounded by the fact that so many people in the organization require some form of privileged access. Maintaining control over an environment where many people are accessing devices at the operating system level is best achieved through tightly defined permissions that often include specific set of commands users can execute (and nothing else).

ConsoleWorks already has a robust permissions model built into its role-based access and control functions this capability being augmented with explicitly defined commands sets for each role. The next release of ConsoleWorks includes this additional functionality.

The risk associated to configuration port access over the out-of-band network is actually higher than the risk of operating system access because the configuration port has “command and control” over the operating system and every other component of the server. Configuration ports are the highest privileged interface that exists on every modern server.

This makes control (access, permissions, limiting permission to specific commands) over out-of-band interfaces even more important as most organizations have limited controls in place to address this security risk.

Several of the more prominent high-risk capabilities provided by out-of-band interfaces are:

- Mount media devices and copy data
- Install malware at multiple levels (Bios, Firmware, OS)
- Add, change or delete user accounts and privileges
- Change device and component configuration
- Execute operating system commands without an OS account
- Open, close or reconfigure network ports

## Summary

Providing a unified security approach across the in-band and out-of-band networks ensures that privileged interfaces are controlled and risk is mitigated. A unified approach dramatically simplifies the security practice and addresses the vulnerabilities with privileged interfaces that present an extremely high security issue today.

## About TDi Technologies

TDi Technologies is the leader in IT Foundation Management, delivering IT Foundation Management solutions to a global customer base with key verticals including Utilities, Financial Services, Telecommunications, Healthcare, and Government. The company's solutions help customers reduce operating costs, meet foundational compliance requirements, secure the IT foundation, and improve IT Service delivery.