



Access Control Excellence

## Proactively Controlling Access to Critical Windows Servers and Simplifying Audits with FoxT ServerControl

*FoxT ServerControl's Local Privileged Account protection offers a more effective way to secure your Windows systems from insider fraud. Using FoxT ServerControl, you can centrally provision and administer Windows Server local accounts, and easily implement and enforce security policies for the support staff controlling access to these privileged accounts. By consolidating the management of these accounts in one place, auditing and reporting also become extremely simple and cost effective.*





## Overview

In the last five years Windows 2003 and 2008 have become significant platforms for Intranet Web Applications and Corporate Transaction Processing. Overtime, the Microsoft Active Directory lifecycle experience has graduated into a highly scalable platform for user management, including the distribution, operation, and action of Group Security Policies. Your reliance on the data held inside these server environments, and the expectation of the correct use of the Active Directory security model has become essential.

Each Windows operating system install, however, continues to operate with a pre-delivered local administrator account. In Windows 2008 this account is deactivated by default, but can be activated easily by your support staff, exposing your business and customer data to duplication or attack.

FoxT ServerControl's Local Privileged Account protection offers a more effective way to secure your Windows systems from insider fraud. Using FoxT ServerControl, you can centrally provision and administer Windows Server local accounts, and easily implement and enforce security policies for the support staff controlling access to these privileged accounts. By consolidating the management of these accounts in one place, auditing and reporting also become extremely simple and cost effective.

## Security Challenges with Windows Server 2003 R3 and 2008 R2 as Platforms for Transactional Applications

The use of Windows Server platform for corporate applications is growing enormously. Microsoft has invested significant time, energy, and marketing dollars in promoting the use of Windows server outside the traditional area of file and print sharing. They have succeeded, taking market share from UNIX™ like platforms in the SMB sector, by providing management tools, services, and packaged applications and databases. They have further extended their presence by moving aggressively up into multi-national corporate data centres. For example, with Windows HPC Server 2008, Microsoft has targeted prospects with clustered compute-intensive supercomputer environments that have, most recently, been the province of Linux-based technologies.

The efficiencies gained by replacing the small number of UNIX and Linux like servers from the IT back office need to be balanced by the ongoing risk of insider fraud and the subsequent exposure of transactional and customer data outside the organization.

Each Windows Server install will typically have between three and six additional powerful accounts (in addition to Windows "Administrator"), controlling the operation of backup, monitoring software, and owning the files and data of application and database software environments. The setup, operation, and audit of these local accounts are outside the control of your Active Directory Group Policies. Core Transactional Applications often explicitly assume software is installed locally to each Windows Server, as a dependence on Active Directory availability is not acceptable.

Audit reporting of which support staff member accessed these local accounts on each server operating system is tiresome, repetitive, and not always amenable to automation. By default the operating system reports on actions taken in the past. Pre-emptive control, when not part of Group Policies, is almost impossible. For every audit report cycle, support staff will typically visit each server, "log trawling" for events that may have taken place weeks ago. Businesses are reporting that on average it is taking two hours per operating system install, per audit cycle, to collect basic access and command execution information.

Of even greater concern is that reporting only indicates what has happened. By then, inappropriate and fraudulent actions may have already occurred, resulting in significant risk to your corporate value.

Semi-manual mitigations to protect these "local privileged accounts" from your support staff include ad-hoc scripting, the use of shareware third party tools, or the implementation of Microsoft's PowerShell. Each has their weakness and failing:

- The installation, configuration, and operation of scripted solutions to control local accounts is not easily scalable, and makes your audit status totally dependent on the day-to-day actions of your Windows Support staff, and how that person is feeling on that day whilst carrying out that task.
- PowerShell requires significant preparation, with multiple steps of configuration required on each server operating system. Consistency of its configuration is very hard to achieve. Many banking and finance organizations refuse to allow PowerShell to be installed, as it is seen as both too powerful in scope and too much of an administration overhead. Operational efficiencies are very difficult to realize, as a PowerShell specific security team silo is created and added to your security departments.



## Challenges for Critical Application and Database Control

Over twenty years ago, the move to “client-server computing,” as in the movement of critical business applications from mainframes to UNIX platforms, was taking place. Exactly the same arguments about the suitability to host enterprise applications and the risks managing access to privileged accounts on each server (in the case of UNIX, the “root” account) for critical system administration are now being made in a similar way about the local “Administrator” account delivered with each and every copy of Windows Server 2003 and 2008.

- Over-privileged authority in a server-specific primary account that **must be there**.
- Poor operational practices, where support staff assumed a quick “flip” to the admin account is **a fast and easy way to “get the job done”, without regard to the risk to business data**.
- Uncontrolled trust relationships between servers. **If a support team member can become the admin account on one server, it is easy to jump to or run commands on another system in the same cluster with god-like privilege.**

In the same timeframe, relational databases were also installed on UNIX platforms, and ERP applications later layered on top of the databases. Here additional and more troubling control issues became apparent:

- Database software had complete control of the data inside the database files. To the operating system administrator, databases were black boxes. **However “flipping” to installed Database Administrator account gives the privileged user access to the RDBMS tools including free access to change (or copy) any data inside the database.**
- ERP and JAVA application servers manipulate transactional data in memory before posting back to the underlying database, and the technical change management processes available in the product. **“Flipping” to the installed Application Administrator account gives privileged users access to the live application with open and free access any data inside the active application module and the underlying database. In addition, Application Change Management workflow processes can be superseded, usurping the flow of software, and master data management that affects the correct execution of transactions.**

In many ways privileged application and database accounts have a significantly higher compliance and risk profile than bare operating system control. Potential data manipulation is more subtle, and not as obvious. Often it can be unnoticed over multiple accounting periods. Standard accounting rules do not allow you to “reverse” transactions, only to “post” updates to reconcile them. Without pre-emptive access controls, you are unable to prevent one of your support team from carrying out forbidden actions and commands, greatly increasing the risk to your overall business value.

Back to the present, the latest phase of migrations of UNIX or Linux core applications onto the Windows Server platforms does *not* mitigate the access risks outlined above. The requirement for pre-emptive access controls to protect you from your own staff remains a very real and potentially costly security risk.

### FoxT ServerControl: Proactive Windows Local Account Protection

For more than two decades FoxT has been providing a multi-platform software solution for pre-emptive control to “root” or “administrator” accounts, as well as operational, database, or application management functional accounts residing in UNIX, Linux and Windows Server platforms.

For an organization that must comply with a regulatory environment, your auditors will be pushing you to deal with your “**Privileged Account Protection Controls**”. The kinds of characteristics and actions auditors are looking for include:

- Removal of home-built scripts that require are maintained by specific staff members without guarantee of consistent deployment.
- Removal of non code-reviewed, internally-developed tools, that require expensive in-house development teams.
- Installation of centrally managed security and access management policy platform.
- Implementation of software that requires no local configuration.
- Deployment of software without restarting the Operating System.
- Automatic updates of software release changes.



FoxT ServerControl provides centralized administration, fine-grained authorization, contextual authentication, and consolidated audit of privileged accounts across server platforms.

Specifically for Windows 2003 R2 and 2008 R2, FoxT ServerControl supports the following capabilities:

- Central definition of local Windows Server Groups.
- Central import and assumed control of local accounts from each Windows Server.
- Support team groupings, and capabilities for local account access defined by role.
- Policy-based access controls for account transitions from Active Directory users to local server accounts.
- Graduated stricter controls for those support staff who need to transition to local server privileged accounts to carry out maintenance.
- Pre-emptive control of Windows command execution by your administration staff.
- A enhancement to Windows RUNAS for improved command control.
- Compatibility and interoperability with no modification to your existing Active Directory Group Policy framework.
- Automatic local account provisioning as new servers are created (or cloned from Virtual Machine templates).
- Either local interactive or central software agent install.
- Central logging of all events using local accounts.
- Central and standard reporting.
- Secure Remote Desktop protocol (Secure RDP).
- A complete Secure SHell (SSH) server built in, for SSH remote access.
- The ability to mix Windows Server and UNIX/Linux-like servers in common policy groups, with the equivalent controls in place.

## Conclusion

Transitioning your core applications and databases to Windows Server 2003 R3 or 2008 R2 can provide operational savings. However, if it is required that some of your critical applications must be installed with local accounts, Active Directory cannot provide you with the global security assurance and access control you need to protect your business.

Foxt ServerControl, in harmony with your existing Active Directory Policy framework, can proactively control the access by privileged users to the operating system and your key applications or databases. In addition to significantly reducing the risk of insider fraud, you will also be able to dramatically streamline audits with automatic consolidation of user activity logs from across your servers, enabling you to concentrate on running your business. Implementation is rapid, cost effective, and the ROI payback will pay dividends both to the business and IT support teams.

For more information please visit [www.foxt.com](http://www.foxt.com) or call us at 1-650-687-6300.

Copyright © 2010 FoxT. All rights reserved.

The document is provided for informational purposes only and the contents herein are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior permission.

FoxT logo is a trademark of FoxT, Inc. Other product and company names herein may be registered trademarks and trademarks of their respective owners.

