

FOXT.

...Essential Security



FoxT BoKS Access Control for Servers

Large data centers store and process the information you need to keep your business going. Managing and securing these crucial server environments requires intensive administration resources and detailed policy definition and enforcement. FoxT BoKS Access Control for Servers delivers an integrated set of capabilities to control, monitor and audit user access and security across large server environments running heterogeneous operating systems. Using FoxT, you can centralize enforcement of access controls, control delegation of privileged and root accounts, and streamline IT audit reporting.



“Organizations should proactively develop & implement security-related controls...instead of waiting for auditors to identify the problem areas.”

~ Gartner - The Top 10 Risk and Security Audit Findings to Avoid

Most organizations are running a complex mixture of server platforms. Even before the latest developments in virtualization technologies, keeping track of user accounts and access rights across a diverse mix of servers with disparate operating system security models has been a tremendous challenge. Ensuring compliant and secure authorization across multiple servers accessed by thousands of users, controlling the users of privileged accounts, and effectively securing inter-server communication have become time consuming and difficult tasks. Adding to the pressure, regulatory compliance now requires organizations to prove that user access changes within their server environments do not introduce new risk or control issues into the IT infrastructure.

To ensure security over IT assets without impacting responsiveness to business change, organizations need powerful, flexible, management tools that enable them to administer user access rights to their servers without losing control of security configurations and falling foul of auditors.

BoKS Access Control for Servers enables companies to better control who has access to their servers. The solution's key functions include the ability to:

- Centrally define access to Unix, Linux, Windows, and Virtual servers using access policies; instantly provision server access, or block users from accessing a server, through a remote console.
- Flexibly define how users should authenticate when accessing specific servers.
- Control delegation of privileged and root accounts including integrated keystroke logging.
- Encrypt traffic between servers to ensure that all information in transit is protected from unauthorized access.
- Centralize management of SSH and passwords.
- Proactively monitor security & troubleshoot access control across the entire server estate.
- Consolidate audit logs and reporting

Using a common infrastructure to manage user access controls and authorization across your server environment greatly simplifies both day-to-day administration and IT audits. FoxT's BoKS Access Control for Servers is available for all major UNIX, LINUX, z-Series LINUX, and Windows Servers, including virtualized infrastructures from HP, IBM, SUN, and VMWARE.

Centralized, Fine-Grained Access Controls Across Heterogeneous Servers

“The need for effective monitoring and enforcement of the identity and access management (IAM) process — which can be defined as controlling who has access to what — is a longstanding concern for enterprises, especially those in highly regulated industries.”

~ Gartner - The Top 10 Risk and Security Audit Findings to Avoid

Defining and enforcing access control policies across diverse server platforms, the reality in most data centers, is difficult. Different native security models, user provisioning procedures, and privileged account handling methods make it hard to devise a consistent approach to data security. The proliferation of virtualization technologies, far from

making this task simpler, is in fact compounding access control challenges. While potentially reducing the number of servers required, the ease with which new virtual machines and user populations can be created creates more accounts to manage, more machines to secure, and more headaches for administrators and auditors alike.

BoKS Access Control for Servers enables you to centralize access controls for Unix, Linux, Windows and Virtual servers. Entire domains of servers running heterogeneous operating systems can be securely managed from one central, web-based administration console.

Using BoKS Access Control for Servers, you can manage:

- **Which users, can access what network or local service on a server, when, and from where.** The BoKS concept of Access Routes facilitates fine-grained access rules that BoKS makes sure are applied and enforced consistently across the managed network.
- **How users authenticate.** Authentication can be set per host, service, user, and time of day. BoKS Access Control for Servers supports a variety of authentication methods including: password, one-time password token, LDAP, certificate, and SSH keys. You can tailor your authentication policies to use stronger authentication for higher-risk access and standard password authentication for everyday access.
- **Password policies.** Define complex password rules for the entire managed domain, including password formats, password lifetime, password history, and banned words. Again, BoKS automatically enforces your password policies across all managed servers.
- **Host and user groups for ease of management.** Group hosts into logical groups to simplify access configuration and collect users into roles for role-based access controls. Host groups can include physical and virtual servers, and sporadically-used servers can be set to automatically become part of the BoKS domain when they come online. If you set up access rules by role, a user automatically inherits access and authentication rules when added to a role.

Protected Delegation of Privileged Accounts

“Administrator accounts have privileges to access any data and execute any application or transaction, typically with little or no tracking or control. These accounts — which in some enterprises number in the hundreds — are frequently not tied to specific individuals, so the accounts can be used to do virtually anything, with little or no possibility of detection.”

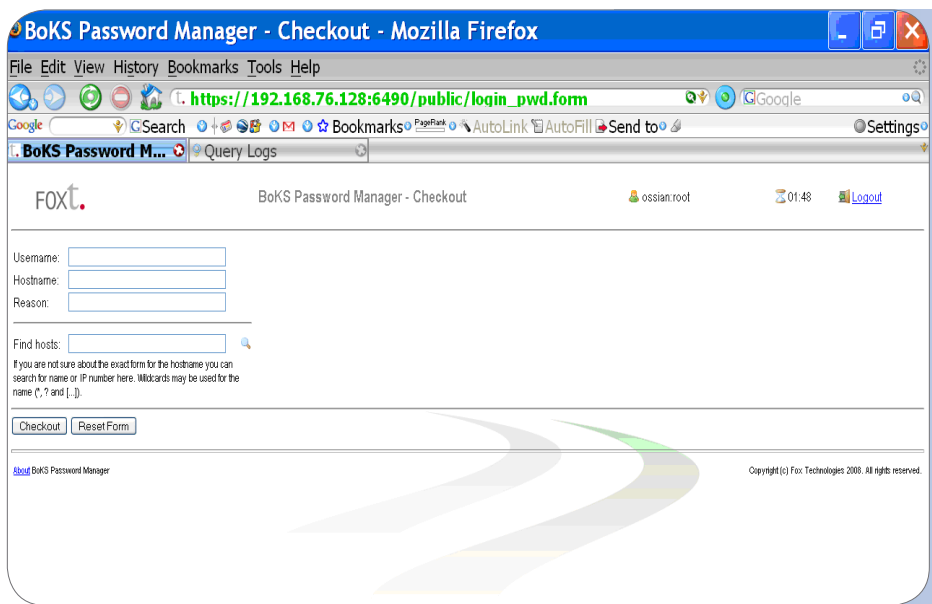
~ Gartner - The Top 10 Risk and Security Audit Findings to Avoid

Managing the use of privileged and root accounts has been identified by analysts as one of the key audit issues organizations are facing today. In Unix and Linux environments particularly, containing the superuser or root account is vital to controlling the wide-ranging privileges this account has in the system. The problem is that many standard network operations require root access, and to ensure the smooth day-to-day running of their business, many organizations end up sharing root passwords among a group of administrators. Furthermore, in order to minimize disruptions to vital operations, some organizations fail to change the root passwords with sufficient regularity to safeguard against the password being compromised.

Another problem with sharing root passwords is that it becomes impossible to trace which physical user has actually performed specific operations. If more than one administrator knows the password, any of those administrators could have logged in and performed the operation. The lack of control over privileged accounts is of great concern to auditors and prevents organizations from effectively controlling their IT assets and data.

Given the importance of controlling access to crucial data and transactions, it is no surprise that a number of point solutions for privileged account protection exist on the market. BoKS Access Control for Servers, however, brings together a unique and powerful combination of functionality to deliver the most effective control over privileged and root accounts.

- First, many of the common management functions in your server domain can be performed using the secure BoKS administration interface via a Web browser. This greatly reduces the amount of operations requiring administrators to know privileged passwords. You can also define sub-administrators who are allowed to work on certain tasks or on specific portions of your server environment and track their actions.
- On BoKS-protected servers, SU can only be performed if the user has a specific Access Route allowing him or her to do so. Even if a user knows a privileged account password, they cannot use it to become the privileged user unless they have been granted permission to run SU.
- BoKS Access Control for Servers includes programs that enable your administrators to delegate privileged command execution. SUEXEC (for UNIX and Linux servers) and BoKS Run As (for Windows servers) allow users to perform specific operations as another user. Again, users can only perform SUEXEC/BoKS Run As controlled operations if they have explicitly been assigned permissions to do so. For ease of management, you can specify, down to program argument level, exactly what operation the user can carry out as another user, and group the program command permissions.
- You can also configure the system so that users can run SU and SUEXEC using their own passwords or tokens, which removes the need for any of your administrators to know privileged account passwords.
- If you decide to keep using privileged account passwords, BoKS Password Manager, an optional add-on module, is a password vault that manages the checkout of privileged account passwords and automatically changes passwords after the configurable checkout period has ended. BoKS Password Manager removes the need to share passwords, and helps you avoid having privileged account passwords active in the system too long.



With BoKS Password Manager, you can easily manage which privileged and root account passwords can be checked out and automatically change checked out passwords after the configurable check out time period has ended.

- SUEXEC operations can be keystroke logged, with a configurable level of keyboard input and on-screen output recorded for reference. Keystroke logging provides a forensic level of traceability, and ensures that no user in your organization can perform any subversive activity in the guise of a privileged user.

Organizations using BoKS Access Control for Servers can avoid sharing privileged account passwords, and indeed, once the system is configured, there is no need to use these passwords in day-to-day activities. When operations are traceable back to a specific, physical user, you significantly improve the security over your IT assets and greatly simplify your IT audits.

Role-Based User Account Provisioning

Provisioning user accounts across heterogeneous servers can be a time-consuming task. And this task is compounded by the proliferation of virtual servers, the fast-changing nature of business (including mergers, acquisitions and consolidations), and compliance requirements dictating that organizations have full control over user access permissions. Equally important and labor-intensive is the process of de-provisioning users, to ensure that staff who have left the organization no longer have any access to crucial systems and data.

Many organizations are using directory tools such as NIS/NIS+ and LDAP to provision and manage user populations across the data center; both of these methods have come under increased scrutiny from auditors in recent years due to their inherent lack of security.

NIS/NIS+ and LDAP do not provide organizations with control over how users authenticate, or what resources users can access. In addition, there is no central logging facility with these directory management tools, so getting a complete picture of what has happened in the network is extremely problematic. As well, local functional accounts, which application managers are highly reluctant to hand over to external LDAP systems, can remain outside centralized control.

BoKS Access Control for Servers provides a robust provisioning model whereby user accounts can be provisioned to multiple servers running different operating systems with a couple of mouse clicks. You can add users to one or more User Classes, instantly granting them appropriate authorization and authentication requirements.

In contrast to other solutions based on Active Directory technology, BoKS Access Control for Servers is developed to utilize the native security models on the target provisioning systems. This means that, instead of only controlling accounts at host level, you can control the Unix and Linux user accounts at the level of the Unix/Linux services that can be used on specific machines or groups of machines. In addition, BoKS Access Control for Servers provides robust controls for privileged account operations, so you can safely provision local accounts from a central point knowing that they are protected within the BoKS security framework.

The solution also features easy integration with LDAP and NIS/NIS+ for organizations looking to quickly deploy a more secure user provisioning and de-provisioning solution with their existing corporate directories.

Centralized SSH Management

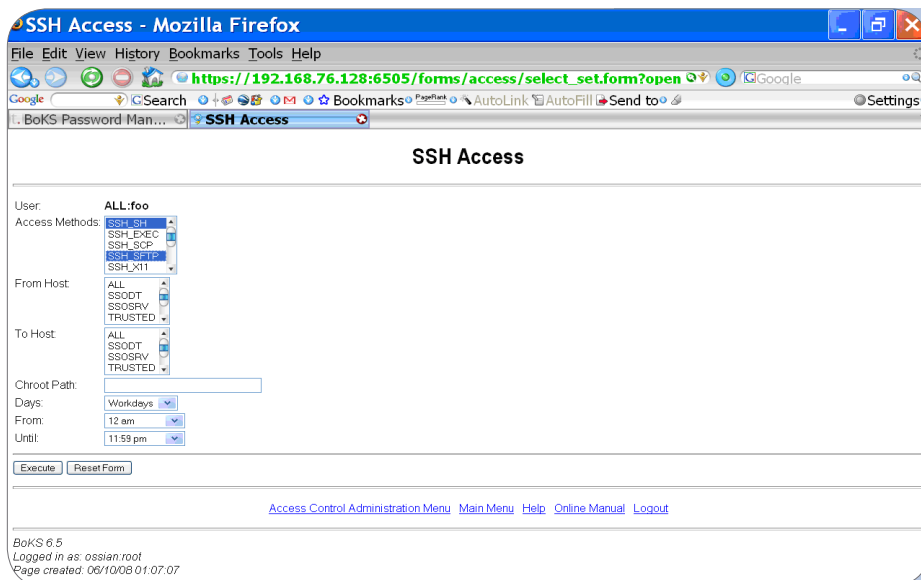
Data flowing across your enterprise network is the lifeblood of your organization, and transferring it over insecure channels is a risk that fewer and fewer businesses are willing or able to take. Fortunately, recent years have seen the development of new security protocols such as Secure Shell (SSH). SSH is a multi-service protocol used to establish a secure, encrypted communication tunnel between two computers. Strong authentication of users can be achieved as well.

Once a secure connection has been established, multiple services are offered as secure options to corresponding conventional, but poorly protected, connectivity tools such as telnet, ftp, and UNIX r-commands. Thus, SSH-based solutions can meet the increasing demands for strengthened authentication, authorization, and privacy protection schemes that many organizations are facing today.

However, SSH is a peer-to-peer-based concept. Configuration and deployment requires very complex and vulnerable procedures to make sure all parties involved, users and machines alike, can exchange their respective public keys used for encryption and identification purposes.

Without centralized management of public keys, SSH can hardly be thought of as a realistic general-purpose replacement for the conventional but insecure access methods on which many organizations still heavily depend.

BoKS Access Control for Servers provides network administrators with centralized administration of users and managed hosts. It adds the concept of Access Routes to server administration, which gives an administrator centralized and precise instruments to grant or refuse access to individual services on individual hosts.



BoKS provides centralized management of public SSH keys and adds granular access control for individual SSH services.

BoKS SSH not only provides for central storage and management of public keys, but also adds granular access control for individual SSH services, thereby making SSH a realistic, flexible, user-friendly, and extremely secure option to conventional connectivity tools.

Consolidated Audit Logging and Monitoring

“The need to track user behavior — not just user access rights and privileges — has become a “hot button” issue for auditors. Activity tracking and analysis has tremendous value as a deterrent to inappropriate behavior and as a form of remediation.”

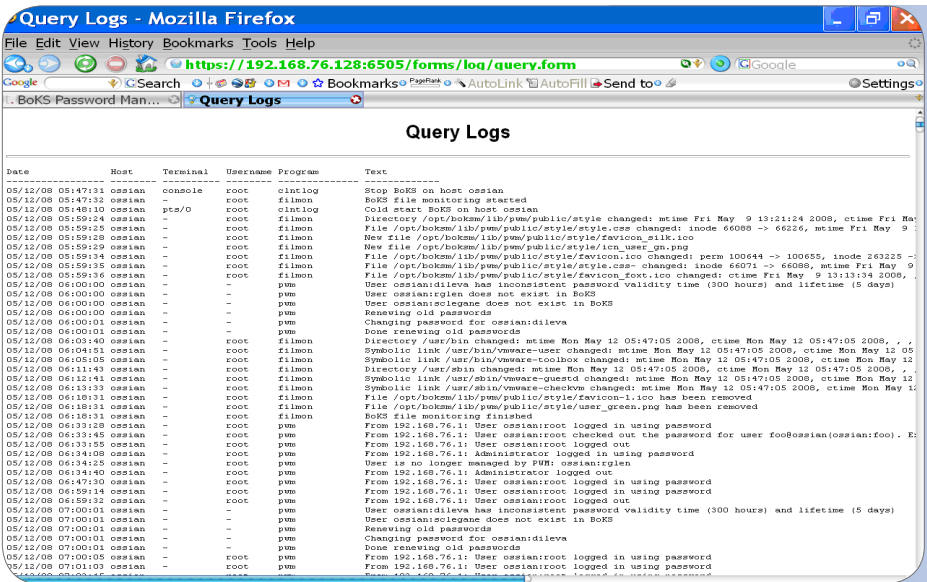
~ Gartner - The Top 10 Risk and Security Audit Findings to Avoid

For organizations running a large number of diverse servers, collecting and collating audit log information in preparation for compliance and security audits is no easy matter. Even when deployed in the enterprise network, Unix, Linux, Virtual and stand-alone Windows systems are still basically autonomous nodes where users are granted or denied access based on local security settings, and where access to and activities on the system are logged locally. For administrators responsible for hundreds or even thousands of these nodes, preparing for audits can be a daunting task.

One challenge is how to track effective user permissions. When every user account on a Unix, Linux or Windows machine is a local account, tracing these back to a physical user is not always easy. If identities are not managed domain-wide, it is difficult to maintain segregation of duties and present auditors with an accurate picture of effective user permissions.

Building the audit trail is another problem. This involves collating a number of local log files from each of the autonomous server nodes and, thanks to the ease with which users can hop from host to host, trying to cross-reference the logs to create a picture of what a particular user has done across the network.

Finally, auditing the use of privileged accounts creates additional complexity. Many Unix and Linux system tasks require superuser privileges, and any user with access to the password of a superuser account can switch to that account using the SU command. The consolidated log files will contain records of operations performed by privileged users, but no information as to which user switched to the privileged account and performed these operations, making it impossible to trace responsibility back to a physical, accountable user.



BoKS provides centralized audit logs and reporting across heterogeneous Unix, Linux, Windows and Virtual servers to greatly simplify IT audits.

BoKS Access Control for Servers includes a number of features that make it easier to prepare for, and pass, compliance and IT security audits:

- The centralized user identities provided by BoKS mean that a physical user can be granted the same account on numerous hosts, so you can trace operations performed by that user across the network. The centralized, fine-grained access control makes it easier to demonstrate to auditors that your organization's access control policies are actually being enforced.
- BoKS automatically collects information from all protected hosts in the domain into a searchable, exportable audit log, so you avoid the laborious task of collecting log data from each host in the network.
- When it comes to privileged access, BoKS Access Control for Servers only allows users to perform privileged operations if they have been given explicit permission to do so. All SU and SUEXEC (a sudo-like program for executing a command as another user) operations are logged to the BoKS audit log so you can trace privileged operations back to the physical user who initiated them.
- For sensitive operations that involve sessions using the SUEXEC program, you can also log the keystrokes performed and screen output to provide a forensic level of detail should auditors require this.

BoKS Access Control for Servers provides one place to go for administrators and auditors to get all the information they need on user access activities across your enterprise servers, and provides system wide monitoring for all protected servers, including:

- Monitoring of inactive user terminals
- Integrity checking to proactively scan for potential vulnerabilities
- File monitoring to check for changes to sensitive system files

Summary

By implementing FoxT BoKS Access Control for Servers, you can greatly enhance your control over who is accessing your servers and:

- Secure assets with encryption, authentication, and controlled delegation policies
- Improve audit results with centralized logging and reporting
- Reduce the annual costs for common administrative tasks such as managing SSH, passwords, sudo permissions, and general user provisioning.

About FoxT

FoxT's comprehensive Enterprise Access Control Management solution suite enables organizations to centrally manage and control access to operating system services, configuration services, business applications, and information on wired or wireless devices. The ability to centrally administer, authenticate, authorize, and audit the IT infrastructure enables organizations to simplify audits and compliance, strengthen security, and streamline IT operations. Headquartered in Mountain View, California, FoxT serves Global 1000 customers in 32 countries. For more information – www.foxt.com.

