

FOXT.

...Essential Security



FoxT BoKS Access Control for Applications

In the enterprise, business applications that process sensitive data or are subject to regulatory scrutiny must be appropriately secured and audited. Such high-risk applications typically include a mixture of ERP systems, modern Services Oriented Architecture-based programs and legacy applications. The dilemma many organizations are facing is how to define and deploy access controls on business applications in a structured, efficient manner. BoKS Access Control for Applications provides an application-agnostic framework to deliver access control, encryption, and auditing capabilities for networked applications. Using FoxT, organizations can achieve centralized enforcement of access controls, secure single sign-on to a range of applications, and streamlined IT audit reporting.



“Authentication, separation of duties, role management and enforcement, and reporting address the identity and access management requirements of regulatory compliance.”

~ Gartner Report

Business applications are critical elements in the data-to-day operation of your business, and it is vital that they work seamlessly and securely. With constant developments in technology, most enterprises are actively looking at how to use innovations within their business applications to leverage a competitive advantage. This means that most organizations are running a complex mixture of business applications based on different technologies, with different security and logging models. With an increased regulatory burden now demanding that organizations implement and document security controls on applications, finding a standard framework that will suit this mixture of applications is crucial.

The ability to standardize and centralize access control to diverse applications offers a number of benefits including making it much easier to collate information for both internal and external audits, more efficient user account administration, and reduced risk of fraud.

BoKS Access Control for Applications is an enterprise solution used to centrally manage, secure and monitor access controls across diverse enterprise business applications. The primary benefit is that organizations can centrally define and manage targeted, fine-grained access control policies, enabling strong authentication and encryption to be surgically applied where they are needed.

Since BoKS Access Control for Applications requires no changes to application logic, the solution is easy to implement and ideally suited to serve as a common framework for controlling access to a wide variety of applications. The solution's key functions include:

- Centralized definition of access control policies for all applications, enabling administrators to instantly provision application access, or block users from accessing an application, from a centralized, remote console.
- Ability to flexibly define how users should authenticate when accessing specific applications. For example: passwords for applications with a low level of risk, and stronger authentication for higher-risk applications.

- Support of hardware tokens, smartcards, and biometric devices enabling multiple-factor authentication for flexible implementation of your central security practices
- User logon information for multiple applications can be combined in one credential, giving users secure single sign-on (SSO), speeding the login process, and minimizing problems related to managing multiple passwords.
- Encryption of traffic between workstations and application servers, protecting information in transit from unauthorized access.
- All attempts by users to access applications are recorded in a central system log instead of having multiple, scattered audit logs across applications.
- Comprehensive segregation of duties (SoD) with true cross-application monitoring, analysis, enforcement and compliance reporting
- Compliant user provisioning featuring automated approval workflow and SoD testing
- Ability to securely extend application access beyond the traditional enterprise boundary and simplify the sharing of data with affiliates, partners and customers.

The solution comes out-of-the-box for most standard business applications and protocols, and also includes a Software Development Kit to create Agents for custom and legacy applications.

Centralized, Fine-Grained Access Controls For Applications

BoKS Access Control for Applications enables organizations to manage access rights to all applications from one central point in the network. Administrators have complete control over who can access applications, how much of the application can be accessed, and when applications can be accessed. Administrators do not need to log-in to all application servers to disable an account. Instead, the user is removed (or blocked temporarily) in the central security database.

Using BoKS Access Control for Applications, you can manage:

- *Which users can access what business application, 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 when they access a particular application.** Authentication can be set per host, application, user, and time of day.
- **How application users are grouped.** You can easily create common groups of Access Routes for similar users and add the routes to a user class. This creates roles-based access control. When you add a new user to the user class, the user automatically inherits all the application access they need.
- **Password policies.** BoKS automatically enforces password policies across all managed applications including complex password rules featuring password formats, password lifetime, password history, and banned words.
- **User identities.** You can map multiple application login credentials to one centralized user account so users can log into multiple applications using one login. This allows you to consolidate multiple user accounts into one identity, which is then traceable back to a physical user.
- **Application roles.** Users who must access applications for different purposes, for example, as an administrator, tester, or ordinary user, may need different user credentials for each type of session. FoxT's role mapping enables users to indicate which set of credentials they need for a given session by allowing each set of credentials to be mapped to a unique role.

Strong Authentication for Application Access

BoKS Access Control for Applications supports strong two-factor authentication of users by allowing the use of a variety of authentication devices, including: smart cards, one-time password tokens, and LDAP. Strong authentication ensures that only authorized users gain access to the network.

You can easily tailor your authentication policies to use stronger authentication for higher-risk application access and standard password authentication for everyday access. Organizations that want to continue using password authentication have the option of using randomly generated, frequently changed, passwords that the user never knows.

In addition to strong authentication for users, BoKS Access Control for Applications performs authentication of computers to make sure they have not been replaced by an unauthorized machine. All workstations and application servers are securely identified by means of digital certificates to prevent so-called "man-in-the-middle" attacks, a situation where an imposter clones a computer's IP address to illicitly collect data over the network.

BoKS Agent Method Name: TELNET
ORACLE_1

Authentication: User Certificate
 Standard Authentication

Encryption: High Security (DES)
 Medium Security (ND2)
 No Encryption

From Host: ALL
ORADM
SSODT
SSOSRV

or Specify From Host:

To Host: ALL
ORADM
SSODT
SSOSRV

or Specify To Host:

Days Effective: Workdays

Effective From: 12 am

Effective Until: 11:59 pm

BoKS Access Control for Applications enables you to apply a variety of authentication methods to manage access control including OTP tokens, biometric devices and LDAP

Encrypted Communications With Application Servers

In a typical workstation-to-application communication scenario, data, including sensitive information such as usernames and passwords, is transferred in clear text over a network. The lack of encryption can result in passwords being compromised or other sensitive information being obtained by unauthorized persons. Transferring information in clear text significantly increases the risk that business applications become compromised and is likely to be noticed by auditors.

BoKS Access Control for Applications encrypts communication between the workstation and the application host using strong encryption. BoKS Desktop (the client component of the solution) connects to the appropriate BoKS Agent using SSL. This protects the integrity of information as it crosses the network.



Select a user to add an Authenticator to.

Add to User:

or Specify a User:

Type of Authenticator:

- SecurID
- DES Gold
- SSH Public Key
- SSH Certificate
- SSH Hostbased

User Must Use Authenticator:

- Yes
- No

Comment

User-friendly administration interface makes it easy to set targeted encryption and strong authentication

Single Sign-On to Business Applications

Logging in to multiple applications at the start of the working day eats into users' valuable working time, and also requires them to remember multiple unique usernames and passwords. To help them remember their multiple passwords, users may store these in an insecure manner, or choose simple, easily-cracked passwords. In addition, forgotten login information can lead to helpdesk calls, resulting in increased operating costs and employee downtime for the enterprise.

The single sign-on (SSO) functionality provided by BoKS Access Control for Applications means that users perform just one login operation per day. They are then logged on to the various networked applications they are authorized to use transparently and automatically.

Set password parameters for user's passwords.

Passwords Format:

- User selectable passwords
- Randomly generated passwords
- Model passwords

Min number of digits:

Min number of lower case characters:

Min number of upper case characters:

Min number of non-alphanumeric characters:

Minimum Length:

Password Lifespan:

Time Limit For Expired Passwords:

Length of Password History:

Minutes Between Password Changes:

You can build detailed rules for password formats, lifetime, history and more to standardize and enforce your application password policies across the enterprise

Users no longer need to remember multiple passwords and security routines for applications because passwords are stored securely in the user credential. The SSO capability has been shown to greatly reduce help desk traffic by minimizing log-on related calls while improving overall application security.

Centralized Audit Logging

Preparing application access data for compliance and security audits requires security professionals to collate and cross-reference disparate application audit logs across the network...a labor intensive and error-prone process. Legacy applications may store log data in different formats from standard ERP systems, and users may have different log-in names for different applications, making the tracing of a specific application log-in session back to a physical user problematic.

The auditing function of BoKS Access Control for Applications provides a consolidated, centrally located audit log of all successful and unsuccessful user log-on attempts and access control configurations for all protected applications. Instead of obtaining separate logs from each application, the administrator can consult the BoKS Access Control for Applications central audit log for detailed tracking of all access activities. Consolidated audit logs and reporting makes it much easier for administrators to monitor system access and provide accurate, meaningful data to auditors.

Summary

FoxT extends centralized access control management across the applications that run your business. The ability to control access to both the server (using BoKS Access Control for Servers), and the applications that run on that server, through a common infrastructure, enables organizations to implement targeted, fine-grained access control policies, utilize strong authentication and encryption, improve productivity of end users with SSO, streamline user provisioning and administration, and greatly simplify audits.

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.



FOXT.

www.foxt.com • 883 North Shoreline Blvd. Building D, Suite 210 Mountain View, CA 94043 USA • 650.687.6300
