

FOXT.

...Essential Security



FoxT BoKS Access Control for Desktops

Desktop computers are the user's gateway into enterprise information and applications. Unauthorized access to the desktop presents a major risk factor in today's business world. Recognizing the security risk at the desktop, many organizations have made efforts to control access to end-users' PCs and Linux workstations with PKI deployments, biometric mechanisms, and other strong forms of authentication and encryption. As desktop security deployments mature, however, organizations are seeing the need to better manage access to desktops across the enterprise, consolidate the security infrastructure, and simplify PKI deployments in order to extend the use of PKI across and beyond the enterprise. FoxT's BoKS Access Control for Desktops provides a comprehensive framework for managing desktop security, and streamlining authorization and authentication procedures for your workforce. Using FoxT, organizations can achieve centralized management of desktop access controls, secure sign-on to networks, and secure file storage and sharing.



The BoKS Access Control for Desktops solution provides comprehensive protection for workstations in a domain and gives administrators complete control over who accesses those workstations. The solution provides the ability to apply a range of protection mechanisms such as passwords, SecurID tokens, smart cards, and USB tokens to protect user credentials. Regardless of which protection mechanism is used, legitimate users are welcomed to their workstations with the same streamlined authentication process. Individual users can be assigned different protection mechanisms, which makes it possible to tailor the protection level according to each user's needs. Protection mechanisms can be easily exchanged over time without losing user credentials.

In addition to greatly enhancing your control over who is accessing your desktops and how, BoKS Access Control for Desktops will also enable you to:

- Manage access to all desktops and terminal servers from a central console
- Implement easy-to-use, secure communications between user workstations and the data center
- Centralize and streamline distribution and management of user credentials such as symmetric keys, RSA keys, certificates, and user data
- Extend the potential of smart cards
- Protect sensitive files with encryption and secure deletion

Manage Desktop Access From a Central Console



The BoKS Desktop Login screen provides control over who is accessing desktops and provides a structured approach for managing credentials across the enterprise.

BoKS Access Control for Desktops enables organizations to manage access rights to all Windows and Linux desktops and terminal servers from one central point in the network. Administrators have complete control over who can access desktops and when desktops can be accessed. Administrators can block user access from a central point, disabling desktop logins system-wide.

Using BoKS Access Control for Desktops, you can manage:

- **Access to desktops across the enterprise via centralized policies.** Administrators can define settings to enforce your company's security policies for accessing Windows and Linux desktops, as well as terminal server applications, on one machine, and then distribute them automatically to end-user workstations.
- **How users authenticate when they access their desktop.** Administrators can specify how users should authenticate, choosing between passwords, SecurID tokens, smart cards, and x.509 certificate-based authentication where stronger methods are required for more high-risk accounts.
- **Smart card assignments.** If you are using smart cards and a user loses or forgets their smart card, you can instantly assign them a temporary smart card, or even temporarily switch their authentication requirement to password, ensuring a minimum loss of productivity.
- **How users can securely share files.** Create group encryption keys so users can securely share files within a group. Only users who belong to the group can read the files encrypted with the group key.
- **Login policies.** Define complex login rules for desktop login, including password formats and history, screen locking, and allowed login attempts. BoKS automatically enforces your login policies across all managed desktops.
- **Desktop login roles.** Select which users can log in and modify their desktop security settings, and which users can only log in to the desktop to perform normal work tasks.
- **The ability to expand and restrict user access.** Administrators can expand and restrict system access in several ways, including using the information in a user's certificate to determine access rights. Administrators can define the extent of user roaming to control workstation access within the domain.

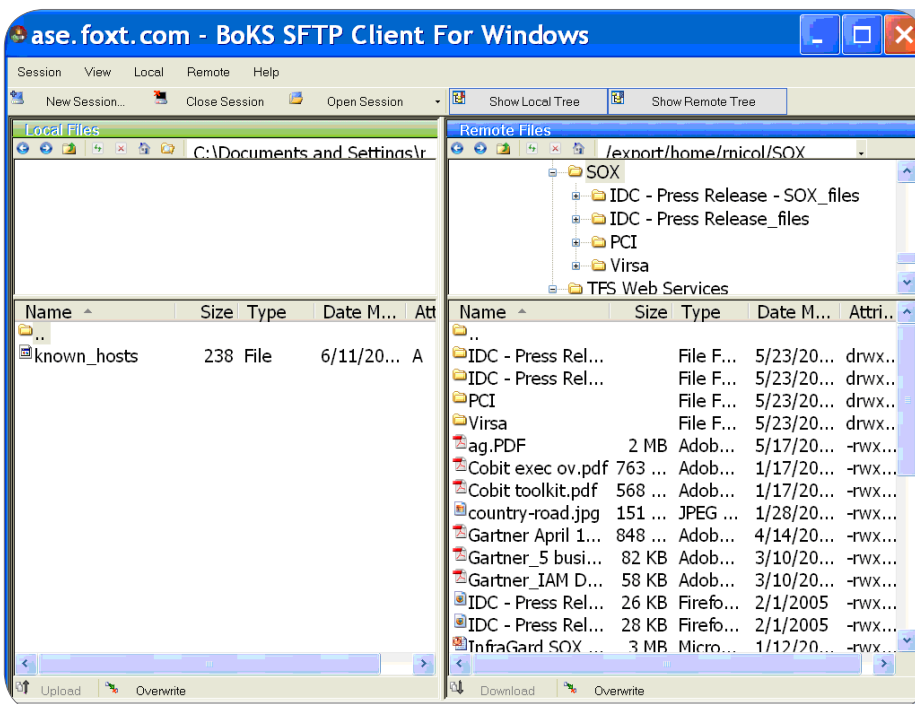
Secure Access To The Data Center

Data stored in your data center is usually crucial to the running of your business, and is often sensitive in nature. You need to ensure that users can readily access the data and perform work tasks without compromising the integrity of that data. Linking end-user workstations to servers in the data center using secure protocols has become imperative. But without a structured approach to managing access controls and credentials, you may find your organization is unable to efficiently provide secure access from workstations to the data center.



BoKS Access Control for Desktops includes a Secure Shell (SSH) client, the BoKS SSH Client for Windows, which enables users to securely connect to servers. The easy-to-use client includes support for SSH interactive sessions, secure copy, and secure file transfer. Port forwarding is also included so that users can securely pipe remotely run programs to their local desktop.

BoKS SSH Client for Windows also includes a graphical file transfer interface, BoKS SFTP Client for Windows, enabling users to easily move files between the desktop and the remote server. The interface has a Windows Explorer look and feel, and features drag-and-drop file transfer.



BoKS SFTP Client for Windows enables users to easily and securely move files between the desktop and the remote server.

BoKS SSH Client for Windows can be operated with any SSH server. Using the BoKS SSH client in conjunction with BoKS Managed SSH on the server side enables your administrators to control user access to the protected servers using fine-grained BoKS Access Routes. In BoKS you can restrict user access to one SSH sub-service, for example, giving a user secure copy access to a specific server but denying interactive SSH or sftp access.

Extending The Potential Of Smart Cards

The use of smart cards as a method of enhancing user access to both physical and digital enterprise resources is becoming more and more widespread. Smart cards provide strong authentication based on PKI certificates and can remove the need to remember multiple complex passwords. In some applications, smart cards can even be combined with physical access mechanisms to enhance security for premises such as data centers.

However, many organizations that have deployed smart cards are finding limitations in this technology are stopping them from getting the most out of their investment. For example, it is difficult to centralize key and certificate management, and there are severe memory limitations on the cards for storing data and keys. Loss of smart cards is another problem; all user login data is lost if the card is lost. In addition, developing new drivers for smart cards as technology moves forward is a difficult, expensive process.

BoKS Access Control for Desktops solves the disadvantages of smart cards by introducing the concept of extended smart cards. Extended smart cards are locked with a digital credential that can be centrally managed by administrators. This concept offers the following enhancements for smart cards:

- Keys and certificates can be managed centrally in a secure database.
- The limited storage space on the smart card is only used to store a key pair that unlocks the digital “virtual card”. New data and credentials for the user can be added to the unlimited virtual card, so your organization has no need for expensive upgrades of the physical smart cards to increase their storage space.
- If smart cards are lost, the only data lost is the key pair used to unlock the virtual card. An administrator can easily and quickly assign a new smart card to unlock the virtual card, where all the relevant user credentials are stored.
- Smart card driver development becomes less of an issue, as your organization can keep using the same smart cards for years, since they are only used for unlocking.

Extended smart cards are the ideal solution for organizations looking to control the costs of their smart card investment while extending the number and kind of applications they use for smart cards in their enterprise.

Streamlined Certificate Management

Using PKI and certificates is a sensible, secure approach to controlling access to enterprise data assets. However, PKI deployments have in the past been plagued by complex technology platforms and labor-intensive processes for the ongoing management of user certificates.

BoKS Access Control for Desktops helps streamline the management of user certificates and the Certificate Authority (CA) certificates that validate them. BoKS Access Control for Desktops includes its own internal CA for deploying PKI to your organization’s desktops, and also works with external CA’s if you already have a PKI implementation.

BoKS Access Control for Desktops includes the following features to streamline user certificate management:



- **Eliminate per-user certificate management.** BoKS Access Control for Desktops tracks the expiration date of user certificates and provides configurable messages to users to warn them that their certificate is about to expire. The message can include a link to your CA enrollment site so the user can enroll immediately; administrators and users do not need to track certificate expiration manually, and administrators are spared the task of communicating certificate expiration information to users individually. Furthermore, certificate management can be fully automated with procedures for secure certificate renewals configured to run as a background service server-side, which means that no user-interaction whatsoever is required.
- **Eliminate incorrect logon certificate choices.** BoKS Access Control for Desktops automatically evaluates a user's valid logon certificates and selects the appropriate one based on default or configured selection criteria. This reduces help desk calls from users who cannot log on because of a valid, but incorrectly selected certificate.
- **Allow administrators to delegate responsibility.** BoKS Access Control for Desktops includes a utility that allows users to be a partner in the certificate management process. Users can view certificates in their user credentials and respond to administrator requests to delete obsolete certificates and add new ones.

Secure File Storage, Sharing And Deletion

Ensuring the integrity of data at rest is a prime concern for the enterprise. With regulatory mandates stipulating that growing amounts of data be stored and protected, using the right tools for data encryption can be vital when it comes to secure access to, and sharing of, sensitive corporate information.

BoKS Access Control for Desktops includes easy-to-use file encryption and secure deletion features to help your organization manage sensitive data. Users can encrypt files easily via the familiar Windows Explorer interface using either a password or a key. Users can be assigned to groups that use the same key to encrypt files that can be shared within the group. Obsolete information that remains sensitive can be securely deleted, rendering it unrecoverable.

After an authorized user is admitted to the safe working environment afforded by BoKS Access Control for Desktops, he or she has access to the file encryption feature, which is a flexible, easy-to-use tool. Users can then encrypt files and share them with other users who may or may not be BoKS Access Control for Desktops users.

File encryption ensures that only people with specific authorization can view sensitive information. To protect files from interception over the network, all encryption is performed locally, even if the file or directory resides on a server. The files are never exposed in clear text on the network, which protects data from intruders who may be listening in on the network. Even authorized system administrators who are not authorized to view sensitive information cannot read encrypted files stored on public file systems, even if they take ownership of them. Only the properly authenticated file owner can decrypt the file.

This powerful functionality is made available via the familiar Windows Explorer interface. In addition, command line utilities are available with which users can create protected folders, manually encrypt files, and delete files securely. Administrators can use command line utilities to carry out administrative tasks on protected folders and encrypted files, as well as recover encrypted files.

BoKS Access Control for Desktops file encryption technology is based upon the use of symmetric keys. Users can have both personal encryption keys and group encryption keys.

- **Personal encryption keys:** This unique key, which is created in the BoKS Manager, is stored on the user's credential and is never shared with other users. This means that a user can encrypt sensitive files on which he or she is working. These files cannot be shared with other users unless they are first decrypted.
- **Group encryption keys:** Group encryption keys protect data in shared folders (directories) on network file servers. These folders are accessed by workstations running BoKS Desktop. Group encryption keys can also be used on local hard drives. Group encryption keys are created, stored, and managed in the BoKS database and are assigned to a User Class. The keys are then downloaded to members of the User Class when the user logs on to a BoKS Desktop anywhere in the BoKS security domain. When the user needs to work with a document offline, a group encryption key can be stored locally in the user's virtual card. When User Classes or policies change, group keys can be added and removed from the virtual card.

Summary


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

- Provide easy-to-use, secure communications between user workstations and the data center
- Centralize and streamline management of smart cards and certificates
- Extend the potential of smart cards
- Protect sensitive files with encryption and secure deletion.

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
