

Access Controls for Servers

BoKS Access Control for Servers Feature Overview

A FoxT White Paper
04.18.2008

About the FoxT Solutions

FoxT solutions provide identity and access management, security with strong authentication and time-saving, simplified administration:

- BoKS Access Control for Servers (UNIX/Linux servers)
- BoKS Access Control for Applications
- BoKS Access Control for Workstations

FoxT solutions enhance existing Identity and Access Management infrastructure. Features that can be integrated include centralized user administration, centralized policy management, centralized audit logging, access control with strong authentication, single sign-on, encrypted communication, file encryption, credential management and secure messaging.

● Introduction to BoKS Access Control for Servers

BoKS Access Control for Servers is a comprehensive management solution for large enterprises whose networks include multi-vendor UNIX or Linux platforms. BoKS Access Control for Servers is designed to meet the administrative and security needs of financial institutions, government organizations and global corporations who operate in dynamic, diverse and security-sensitive environments.

BoKS Access Control for Servers has a small footprint on the managed UNIX and Linux systems and does not affect the operating system kernel. It can be installed in a heterogeneous UNIX environment to provide added value while all the native UNIX features remain unaltered.

Primary components are a BoKS Manager server that maintains a central security database, Replication servers for backup and failover, and client packages installed and remotely maintained on each UNIX/Linux server.

Configuration, maintenance and daily administration are highly customizable through a flexible, modular command line interface as well as a user-friendly graphical user interface. Management of users, credentials, hosts, access rights, logs, backups and so on are all delegable to individual administrators with configured rights. Administrators can run under their own identities and credentials, thus protecting root account passwords and limiting root passwords to a limited number of individuals. Support for major two-factor and strong authentication technologies and corresponding third-party hardware and software allows direct out-of-the-box installation of a BoKS Access Control for Servers solution that dovetails with existing infrastructure.

BoKS Access Control for Servers customers include prominent worldwide banks, large hospitals, tax authorities, police systems, and major industrial corporations, as well as medium-sized businesses with intensive computing services to be managed and protected.

This feature overview includes:

- Main Functions
- Terminology
- Deploying BoKS Manager
- The BoKS Manager GUI
- BoKS Manager Functions For BoKS Access Control for Servers
- BoKS Manager Documentation

● Main Functions

BoKS Manager's features provide for management and security needs within the following main functional areas:

Identity and Access Management in a Domain

- Authentication by multiple means, configurable for users and hosts, with internal BoKS and external servers and external devices.
- BoKS internal CA and external CAs for issuing and managing user certificates
- Single point for user administration
- Single point for access control to all hosts and applications
- Managing common password policy
- Central auditing for the entire domain
- Logging
- Checking file and system integrity
- Monitoring files for changes
- Applying system-wide security policies
- Maintaining Accounts, Access Rules, Logs and Backups
- Delegated sub-administration

BoKS Access Control for Servers (with BoKS Client for UNIX)

- Distribution of user accounts to hosts across platforms
- Defining allowed access methods and restrictions per user and User Class
- Specifying required authentication methods per user and/or host or access method.
- SSH with centrally managed Hostbased authentication
- Granting privileges to execute programs as other users including root
- Keystroke logging of individual commands and entire login sessions
- Monitoring user inactivity

● Terminology

To use BoKS Manager, you need to be familiar with the following concepts and terminology:

Security database

The database contains the security information vital to managing the network, including user accounts, passwords, host accounts, access rules and rights, and logging parameters.

Host

A host is any computer included in the BoKS Manager security database. Hosts may include computers within the local network and non-local computers such as dial-in computers. Hosts that have the Fox Technologies security products installed are called:

- BoKS Manager Master and Replicas (sometimes called BoKS servers).
- BoKS Clients for UNIX (sometimes called BoKS Clients)
- BoKS Agent Hosts
- BoKS Desktops

Master

The BoKS Manager Master is the server that controls central security functions and contains the only writable copy of the database. The Master (or a Replica, see below) responds to a request for authentication and access to a BoKS Client for UNIX, BoKS Desktop Windows workstation or protected application based upon information in the security database.

Domain

A BoKS Manager Domain is a collection of computers controlled by one specific Master with its security database. A Domain may span over subnet or LAN borders. There may be several Domains, each with its own Master and database, running on a single subnet.

Replica

A Replica is a host on which is installed BoKS Manager set up in Replica (previously called server) mode and that is registered in the BoKS database as a BoKS Replica. A Replica holds a read-only copy of the security database which is only written to by the Replica itself when the Master announces that updates are available. A Replica responds to requests for authentication, reducing the load on the Master, and acts as a backup in the event that the Master fails. Depending on network size, the Domain may have many Replicas, which retrieve updated information automatically from the Master several times a minute.

Server

Server is an older term used to denote either the Master or a Replica, that is, a host with a copy of the BoKS Manager database that can respond to requests for authentication and access from BoKS Clients for UNIX, BoKS Desktop Windows workstations and BoKS Agent-protected applications.

BoKS Client for UNIX or “Client”

A BoKS Client for UNIX is a UNIX/Linux host that is protected by BoKS Manager software. The software installed can be either BoKS Client for UNIX or BoKS Manager set up in Client mode, depending on platform. The host is registered in the BoKS database as a BoKS host. A BoKS Client for UNIX host can be registered in only one domain as a Client, where the Master controls access to it. It can be registered in other BoKS domains as host type Other Host, thereby allowing access from it to the other domain(s).

Terminal

A terminal is an IO unit connected to a host by a physical wire. A terminal can also be a text window on one host connected to another host over the network. A terminal is distinguished from the console on a host by the fact that there is

only one console and that console may not be exported. The concept of terminal versus console plays a major role in the two access methods, login and su.

Host Group

A Host Group is a collection of hosts defined by your organization for ease in managing access rights or users. Individual hosts are normally, but not necessarily, members of one or more Host Groups. Host Groups may not contain other Host Groups.

Pre-registered Host

A pre-registered host is a host definition that is held in BoKS Manager, but is not part of the BoKS database, and is not included in the normal access management and protection services provided by BoKS, until BoKS Client for UNIX is installed on the host. Once BoKS Client for UNIX is installed, the host can be automatically added to the BoKS database and configured to automatically be disconnected or de-registered when it cannot contact the Master. Host pre-registration is useful for machines that are used sporadically in your network.

Authentication

Authentication is the process of verifying that users or hosts are who they claim to be, for example, by requesting that the user present his or her password or SecurID passcode.

Authentication method

The means by which an authentication is performed. Examples of authentication methods are ordinary passwords and one-time password generators. One-time password generators are virtually impossible to falsify and are called two-factor authentication. BoKS Manager supports a range of one-time password and other authentication methods that can be configured for specific access needs.

Authenticator

In BoKS Manager, an authenticator is a means of authentication (such as a token, smart card, mobile phone, certificate or LDAP server) that is registered for a user and gives them the right to use that means of authentication for identification (or if so configured, the enforced need to use it). Use of BoKS authenticators allows you great flexibility in tailoring authentication method to meet varying security requirements for different users, different servers and different types of network access.

Token

In BoKS Manager, a token is a physical authentication device such as a key-fob token, smart card or mobile phone that generates one-time passwords (also

called passcodes) that a user uses to log in.

Certificate Authority (CA), CA Certificates

A Certificate Authority (CA) is an entity that issues and signs digital certificates. Digital certificates are signed using the private key of a CA certificate. This signature on a certificate is a stamp of authenticity to prove the legitimacy of the certificate. A certificate hierarchy can contain many levels of CA certificates. This is known as a certificate chain.

BoKS Manager contains functionality to produce internal CA certificates. In BoKS Manager you can work with both the internally generated CA certificate hierarchy (BoKS CAs) and imported external CA certificates.

Virtual Card

A virtual card is a digital carrier of secrets that can be used to give users and hosts access to protected system resources. Among other things, the virtual card contains a digital certificate and the corresponding private key that can be used to prove the identity of a user or host. Virtual cards are used in BoKS Manager to authenticate users and hosts when using BoKS Desktop, BoKS Agents and for remote administration in the BoKS Manager GUI.

Access Method

An Access Method is a program that is used to access a resource in the BoKS Manager domain. For example a BoKS Client for UNIX may be accessed using programs such as telnet, ftpd and login. Depending on option choices at installation, BoKS Manager exchanges some or all of the original access programs in the operating system with its own counterparts. (The kernel is untouched.)

Access Route

An Access Route specifies how, from where, and when a user may access a particular resource, for example a host or group of hosts, in the BoKS domain. An Access Route includes:

- The access method (telnet, ftp, login, BoKS Agent etc.)
- The source and destination computers (“from host”, “to host”)
- The day of week and time of day when access is granted

BoKS Manager allows you to control access by assigning Access Routes to users individually or by User Class.

Restricted Access Route

A Restricted Access Route is an Access Route that disallows, that is, denies, access. In all other regards, a restricted Access Route is specified by the same parameters as and treated as an ordinary, non-restricted, Access Route.

User Class

A User Class is a group of users that you define for ease in managing access rights, Group Encryption Keys and security parameters. User Classes can be given Access Routes and Group Encryption Keys that are made available for all users in the class. An individual user can be assigned to one or more User Classes, or none, thereby inheriting the access rights associated with each of their classes. One of a user's assigned classes can be designated the primary User Class, which means that the user also inherits the class values of BoKS Manager security parameters that are set for the class (in addition to any Access Routes and encryption keys that may have associated with the class).

UNIX Group

Every UNIX user account must have one UNIX group assigned at creation in BoKS Manager, called the primary UNIX group. Optionally, other groups can be assigned to a user. These are called secondary UNIX groups.

Node Key

A Node Key is a special password given to each BoKS-protected host. Node Keys are used to secure internal communication between hosts and to authenticate a BoKS Client for UNIX when it communicates with the Master or Replicas. Node keys are also required for Agent Hosts running BoKS Agent software for BoKS ApplicationControl.

HostID

A HostID is an identifier given to BoKS Clients for UNIX having dynamic IP addresses in order to identify them in the BoKS domain. Other hosts are identified by means of their IP address.

Administrator, Sub-Administrator

An administrator in BoKS Manager is anyone whose user account is registered in the database as having rights to use some or all of the BoKS Manager GUI menus. BoKS Manager makes a distinction between Administrators and Sub-Administrators. An Administrator has unlimited access to all the BoKS Manager menus. A Sub-Administrator has access to only menus, functions and user accounts that have been assigned specifically to that Sub-Administrator.

Integrity Check

An Integrity Check is a specification for checking a UNIX host system for vulnerabilities. You can configure checks on aspects such as file writability and root permissions depending on your security needs.

File Monitoring

File Monitoring is an intrusion-detection tool that looks for changes in file attributes such as owner, modification date and checksum. It includes pre-configured monitoring of the BoKS Manager or Client for UNIX software itself, and Custom File Monitoring that you can set up on any directories and files on these hosts.

Performance Monitoring

BoKS Manager includes tools for monitoring how many UNIX authentications (successful and failed) are handled by BoKS UNIX hosts (Master, Replica and BoKS Clients for UNIX) per time period. This graphically-presented information can be useful for managing load-balancing and troubleshooting in the domain.

Keystroke Logging

BoKS Manager features a powerful keystroke logging function that can be used to record user activities within UNIX and Linux operating systems in great detail. You can log single commands or entire sessions, and optionally display a warning message when keystroke logging is activated for a particular user.

● Deploying BoKS Manager

Initial Deployment

If you are deploying BoKS Manager for the first time or in a new domain, you need to plan the best way to set up user IDs, User Classes, Host Groups and Access Routes to fit your security management needs. You can find guidance on these and other planning issues in the BoKS Manager Installation Guide, after you have become familiar with the BoKS Manager concepts and terminology covered in this chapter.

Another issue that needs planning is importing users.

Installation and Upgrade

Installing BoKS Manager on a single server is in itself a simple process. Installing a whole domain or upgrading an existing domain with a Master, Replicas, BoKS Clients for UNIX, BoKS Desktops and BoKS Agents requires more planning.

Initial Configuration

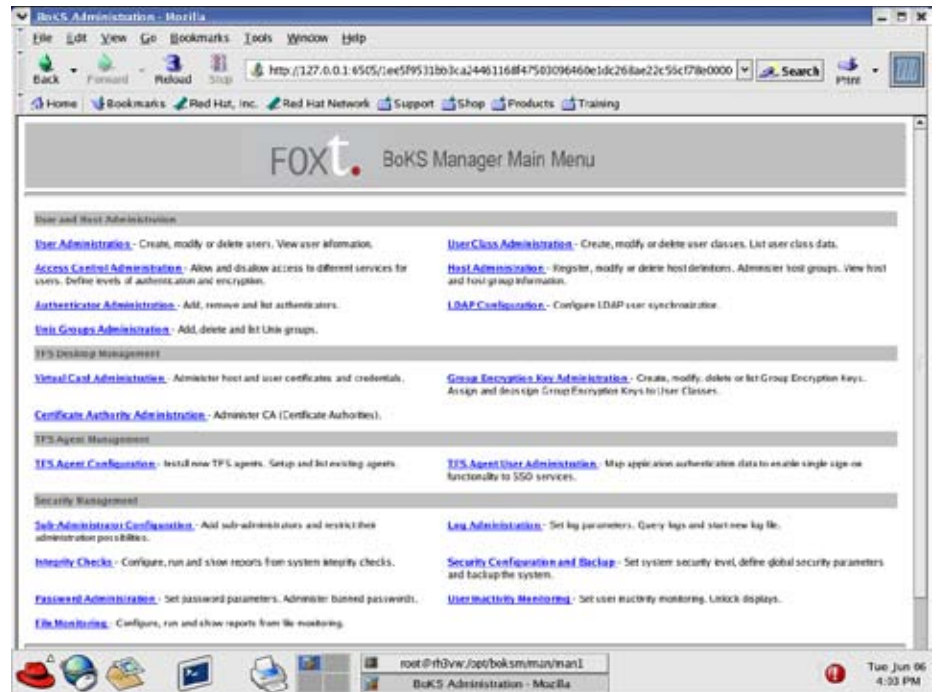
Configuration of BoKS Manager is an ongoing process to continually meet the needs of current security policy and surrounding world events. When you

deploy a new system or upgrade a domain, you need to make initial settings to start in a safe and secure manner.

● The BoKS Manager GUI

BoKS Manager can be managed through either a standard browser window or from the command line, in both cases either remotely or locally on the Master.

The BoKS Manager Administration GUI



The main menu functions are organized into groups for:

- User and Host Administration
- BoKS Desktop Management
- BoKS Agent Management
- Security Management

User and Host Administration

This section contains menus for managing user accounts, host definitions, authentication methods and access rights.

BoKS Desktop Management

This section contains the menus you use to work with PKI including CAs, virtual cards and group encryption keys.

BoKS Agent Management

This section contains the menus you need to configure and manage BoKS

Agents.

Security Management

This section contains menus for configuring Sub-Administrators, setting security parameters, managing auditing and logs, and backing up the database.

The top-level menus correspond to BoKS Manager's key objects (Users, User Classes, Hosts, CAs etc.) and key functions (Access Control, Logs, Inactivity Monitoring, etc.). The menu Security Configuration and Backup includes many of BoKS Manager's configurable parameters. Some other menus, for example Log Administration and User Inactivity Monitoring, contain their own "Parameters" sub-menus, where parameters for those functions can be set.

Depending on your job and task, you may be primarily concerned with and/or have access to only some of the menus in the BoKS Manager browser window.

● BoKS Manager Functions For BoKS Access Control for Servers

BoKS Manager functions used by BoKS Access Control for Servers are as follows:

General Functions

- User Administration
- Host Administration
- Host Administration > Pre-registered Host Administration / Pre-registration Classification Administration
- User Class Administration
- Sub-Administrator Administration
- Log Administration
- LDAP Configuration
- Security Configuration and Backup > Set Security Level
- Security Configuration and Backup > Backup/Restore
- UNIX Groups Administration
- Managing UNIX Password Policies
- Authenticator Administration
- User Inactivity Monitoring
- Access Control Administration > Access Routes
- Access Control Administration > Access Routes > SSH
- Access Control Administration > suexec Program Group Administration
- Access Control Administration > Authentication/Encryption
- Access Control Administration > Block users
- Integrity Checks
- Keystroke Logging

- File Monitoring
- Security Configuration and Backup > Activate/Deactivate
- CA Administration (Used for Host virtual cards only)
- Virtual Card Administration (Used for Host virtual cards only)
- Access Control > Access Routes
- Access Control > Authentication and Encryption

● BoKS Manager Documentation

BoKS Manager documentation is divided into the following parts:

- BoKS Manager Administration Guide
- BoKS Manager Installation Guide
- Online Help System, accessible from the BoKS Administration GUI

The two manuals are available in pdf form and online HTML versions from the Fox Technologies web site. The HTML versions, together with the HTML online help system are available from the BoKS Manager browser interface (click Online Manuals, and the Help links on each GUI page).

In addition, there are man pages available directly from the command line.

A README file in the installation package contains last minute information.

The Fox Technologies web site (<http://www.foxtechnologies.com>) provides a continuously updated README file containing last minute information. Usage notes, white papers and information on patches can also be found on the web site.

● Identity and Access Management with BoKS

BoKS Manager together with other Fox Technologies products allows you to manage a heterogeneous network of UNIX hosts, Microsoft Windows servers and workstations (together with BoKS Desktop) and application servers (together with BoKS Agents). BoKS Manager includes tools for ensuring stringent security on all of the hosts protected by BoKS Manager software, including the Master and Replicas that contain the security database.

Topics include:

- Authentication Basics in BoKS Manager
- User Administration Basics in BoKS Manager
- Using Host Groups for User Administration
- The User Administrator's Menus and Tasks
- Using LDAP Directories for User Account Data
- Auditing Basics in BoKS Manager
- Maintenance of Accounts, Logs and Backups

- Domain-Wide Security Policies
- Delegated Administration with BoKS Manager

Authentication Basics in BoKS Manager

The authentication method is the means by which a user is identified during an access request. You can configure different authentication methods for different user accounts, access to specific hosts, times of day and so on. The default authentication method for BoKS Access Control for Servers is password.

Authentication Methods for BoKS Access Control for Servers

For BoKS Access Control for Servers, BoKS Manager supports the following authentication methods for UNIX/Linux access:

- Passwords
- Authenticator devices: tokens, smart cards and password generators
- Secure Shell (SSH) methods: Public Key, Hostbased and x509 certificate
- Certificate (PKI) (for GUI browser login and on platforms with PAM support)
- An external authentication server (requires a module for each specific server type)

Authenticator Devices

The user carries a physical device such as a token or smart card that generates a one-time password. The user must also know the password or PIN for the token, hence, this method is an example of two-factor authentication. Further, the authenticator device must be registered for the user as an authenticator in the BoKS database. Using RSA SecurID tokens or Secure Computing SafeWord authenticators requires that you have the corresponding server up and running and configured to work with BoKS Manager. Whatever tokens you have in use, you can then assign tokens to some or all users in BoKS Manager and make their use optional or mandatory, depending on security needs.

Ways to Configure Authenticator Requirements

Authenticator usage can be required on a user or Access Route basis:

- By requiring specific users to always use their authenticators. Set this in Authenticator Administration > Add Authenticator to User, selecting the User must use authenticator option.
- By requiring a specified authentication method for a specific Access Route. Set this in Access Control Administration > Define Authentication and Encryption Methods in one of two modes:
 - Enforced: requires all users to authenticate by the specified method on the given Access Route.
 - Not enforced: requires the specified authentication method for those users who have that authenticator assigned, and allows password for other users.

User Administration Basics in BoKS Manager

Centralized User Administration

Centralized administration is one of the most outstanding features of BoKS Manager. From one browser window, authorized system administrators can configure, manage, and audit the BoKS system, including user accounts. The same functions are also available from the command line for those who prefer to use that interface.

BoKS Manager propagates user accounts and user password changes to all relevant BoKS hosts. BoKS Manager propagation includes UNIX primary and secondary groups. Propagation of data eliminates time-consuming and error-prone manual updates.

If your organization uses an LDAP directory to maintain user accounts, you can synchronize this directory with BoKS Manager for ease of use. This avoids you having to maintain user data in two places.

If your organization uses NIS/NIS+, you can configure BoKS Manager to synchronize with this directory.

User administration basics includes:

- Using Host Groups for User Administration
- The User Administrator's Menus and Tasks
- Using LDAP Directories for User Account Data

Using Host Groups for User Administration

To simplify management of user accounts on UNIX hosts, hosts can be gathered into Host Groups. These need not be the same Host Groups as are used for access control, but one Host Group can often serve both purposes. Host Groups can also contain groups of hosts that share similar access restrictions, making it easier to configure and manage user access rights.

In BoKS Manager, each user is assigned to a host or Host Group. If the user is assigned to a host, BoKS Manager creates that user's account on that host. If the user is assigned to a Host Group, then the user account (with UID, password and primary and secondary UNIX group memberships) is created on all UNIX hosts included in the Host Group.

This is a significant benefit. For example, if a Host Group contains 100 BoKS hosts, the user would be created on all 100 hosts at once. Without the BoKS Host Group, the user would have to be added manually to each host. Adding, removing, and modifying users this way is simple when Host Groups are defined along organizational lines.

Example:

For example, say the Host Group ACCOUNTING contains 50 hosts. You have just hired a new accountant who needs access to all these hosts. To accomplish this, the system administrator can simply assign this user to the ACCOUNTING Host Group, and the user's account will be created across all 50 hosts with one click. (Propagation to all hosts can take a few seconds, depending on BoKS Manager and network traffic).

Unique Usernames within a Host Group

BoKS Manager identifies a user with the notation `host:username` or `hostgroup:username`. BoKS Manager requires unique usernames within each Host Group, but allows non-unique names otherwise. Since overlapping Host Groups are also allowed, and frequently used, Fox Technologies recommends keeping both usernames and user IDs unique throughout the domain, in order to minimize the risk of administrative errors that could lead to security breaches. See "Unique Usernames within a Host Group" on page 193 for details.

The User Administrator's Menus and Tasks

You can perform all user administration tasks in the BoKS Manager browser menu or, if you prefer, from the command line. For your convenience, some tasks can be performed from more than one sub-menu. Many of these tasks require only one or two clicks.

Working with User Accounts

- User Administration > Create User lets you add new users to the security database.

When you add a new user account, you are also creating a UNIX user account on all of the hosts and Host Groups you select. Therefore, most of the fields in User Administration > Create User are identical to UNIX account fields. The BoKS Manager fields are:

Username
User's real name
UID
Primary User Class
Secondary User Class(es)
Primary UNIX group
Secondary UNIX group(s)
Home directory
Shell
Password

Note that if you add user accounts by editing files or through programs such as `admintool`, users cannot access the system unless you also import them into BoKS Manager.

- User Administration > Import User Data lets you move users from the system's `/etc/passwd` file or NIS password maps to the BoKS database. You can load existing user data into the database at any time.

- User Administration > Modify User lets you make changes to existing user accounts.

Removing User Accounts

- User Administration > Delete Users lets you permanently remove a given user account. Removing a user account from BoKS Manager removes it from all BoKS-protected servers in the domain.
- Access Control Administration > Block User lets you immediately disallow all UNIX and BoKS Agent access by a user account without removing it.
- Virtual Card Administration > Block BoKS Desktop Domain User immediately blocks a BoKS Desktop user.

Working with Passwords and Locked Displays

- User Administration > Set User Password lets you set or change user passwords.
- Access Control Administration > List Blocked User lets you see any users who are blocked from accessing the system because of an invalid, empty, or expired password.
- User Inactivity Monitoring > Unlock Displays lets you unlock a locked user display without the root password.
You can also unlock a display by using the superuser login name and password separated by a slash at the locked display.
If a user was authenticated using an RSA SecurID token, the display must also be unlocked using the token.

Delegating User Administration Tasks

- Sub-Administrator Configuration > Add Sub-Administrator lets you delegate limited security administration tasks to other support administrators by giving them limited access to the BoKS Manager GUI.

Obtaining Reports

- View who is currently locked out from BoKS-protected UNIX hosts in User Inactivity Monitoring > Unlock Displays.
- View who is currently logged on to BoKS-protected UNIX hosts in User Administration > List Users Logged On.
- List all currently blocked users in Access Control Administration > List Blocked Users.
- List detailed information for one or more user accounts in User Administration > List User Data.
- List users by User Class in User Class Administration > List Users in User Class.
- List the Access Routes assigned to a user or User Class in Access Control Administration > List User Access Routes or Access Control Administration > List User Class Access Routes.
- List all Sub-Administrators and their administration rights in Sub-

Administrator Configuration > Show Sub-Administrator.

- Display the current Inactivity parameter settings for a host or Host Group in User Inactivity Monitoring > Show User Inactivity Parameters.

Assigning/Unassigning Authenticators

- Authenticator Administration > Add Authenticator to User lets you assign a special (non-password) means of authentication to a user.
- Authenticator Administration > Remove Authenticator from User lets you remove a particular special (non-password) means of authentication from a user.

Using LDAP Directories for User Account Data

The LDAP synchronization feature in BoKS Manager allows you to set up automatic or manual synchronization between the BoKS Manager user database and a user database maintained on an LDAP server. Synchronization means that users who are added, deleted and modified in the LDAP database are added, deleted and modified respectively in the BoKS Manager database. Changes in the BoKS Manager database are not propagated back to the LDAP server.

Setting up automatic synchronization with an LDAP server in your network is straightforward and can be done quickly in the BoKS Manager GUI. However, before importing users in full scale or automating the synchronization, you need to carefully test your configuration set up.

Configuring LDAP Synchronization

Define the LDAP server to use in LDAP Configuration > LDAP Server and Directory Definitions. This is mandatory set up. Enable here Modify BoKS users, if you want not only creation of new users and deletion of old users but also BoKS data modified for existing users.

Set up default BoKS Manager parameter values to be used when LDAP data is missing or not mapped, in LDAP Configuration > Configure Default User Values. Host Group is a mandatory parameter.

Specify how to map LDAP user attributes to BoKS user parameters in LDAP Configuration > Map LDAP Attributes to BoKS User Parameters. Mapping is optional for creating new users but required for modifying existing BoKS users. When you do not use mapping, all new users get assigned the same default parameter values.

Enabling Creation of Virtual Cards

To enable automatic creation of virtual cards for new BoKS Manager users, you need to:

- Select a CA in LDAP Configuration > Configure default user values.
- Export the CA virtual card to the correctly named file:
\$BOKS_data/sso_creds/ca_creds/keypkgs/<CA Dname>.kpg
- Provide the CA password in the file (by default):
\$BOKS_data/sso_creds/keys/<CA Dname>.psw
You can also enter the password directly in the GUI during a manual run.

To disable automatic creation of virtual cards, edit the configuration file \$BOKS_etc/ldapsync/ldap.cfg and remove the line that begins with “CADNAME=”.

Running LDAP Synchronization

- Test run a synchronization from the command line using the program \$BOKS_lib/ldapusersync with the -n flag that makes no changes to the BoKS database.
- Run a synchronization one time, as configured, using LDAP Configuration > Manually Synchronize BoKS with LDAP.
- Set up automatic synchronization by choosing a time interval in LDAP Configuration > LDAP Server and Directory Definitions.

Using Logs and Synchronization Results

You can follow up and modify the results of runs in a number of LDAP log files, all in the \$BOKS_var directory (default /var/opt/boksm/):

- View successful creations, deletions and modifications in the file usersync_ldap.log.
- View unsuccessful creations, deletions and modifications in the file usersync_ldaperr.log.
- Provide unique BoKS Manager usernames for users that had name clashes, in the file usersync_ldapdn2user.map. This file is read, if it exists, during every synchronization.

Auditing Basics in BoKS Manager

Audit facilities are a key component of any security system. Auditing includes UNIX logins, BoKS Desktop workstation and application logins, and any administrative activity on the BoKS Manager Master or Replicas.

BoKS Manager has a robust facility for producing reports on successful and failed access, alarm events, and integrity checking. Integrity checking includes file checksumming and a variety of other checks. These facilities can provide security administrators and auditors with the information necessary to:

- Keep BoKS Manager and other network servers safe from unauthorized access
- Provide timely awareness of non-secure configurations
- Meet reporting and accountability requirements

Audit Logging Overview

All security-related events in a BoKS Manager domain are logged and sent to the Master. The log includes:

- Changes to the BoKS system
- Access attempts by all users
- Alerts from the file monitoring daemon on changes to the UNIX operating system, BoKS Manager and other critical files
- Changes to host system clocks

The audit log is separated for convenience into the system log and the session or user log. The system log contains changes to the BoKS system. The session (or user) log contains login attempts, etc. Both of these are different from the error log, which logs process errors (see Error Log Overview below).

The BoKS Manager logging facility allows the administrator to query logs for specific events by date, time, host, terminal, user and service. You can query for success, failure or other message type. Using the command line, you can also query per access method. Log data can be viewed on a historical or real-time basis.

The BoKS audit log also keeps information on changes made to the security database and who made the changes. This provides accountability, required at the UNIX system level.

For the audit log, BoKS Manager uses the local time at the Master/Replica servicing a request, not the local time at a Client or Agent Host (that is used for Access Routes and which is calculated from the time zone specification for the Client or Agent host).

Keystroke Logging Overview

BoKS Manager also allows you to log keyboard input and, optionally, screen output for specified commands or even entire user sessions. This enables you to record exactly what a particular user did when performing a specific operation or during a login session, giving forensic traceability of system activity.

Error Log Overview

The error log, in contrast to the audit log, is updated when some process fails (or the machine and/or BoKS Manager are rebooted). For example, failure might be due to no certificate available, wrong certificate or incorrect node key.

The error log is different from the audit logs (system log and session or user log), which keep track of security-related events such as user logins.

Performance Monitoring Overview

BoKS Manager includes tools to monitor the performance of the security domain and of individual Master or Replica servers. You can monitor the number of authentications to the Master or Replicas on a per-hour basis, and get detailed or summary reports containing authentication information.

This can be useful in determining if load-balancing in your domain is properly configured, and for early detection of any problems with authentication servers.

Integrity Checks Overview

You can set up Integrity checks that run through the UNIX file system on the Master and Replicas and look for known security vulnerabilities. Checks may be set up on specified hosts and files, and run both automatically and manually. By default, a check is run on the Master and Replicas once per month. Depending on your specification, Integrity Checks examine things such as:

- File permissions, ownership and contents
- Deletion of files
- Password integrity
- The mail system

Configure and run Integrity checks in the Integrity Checks menu. You can also view reports in this menu.

File Monitoring Overview

The File Monitoring daemon computes checksums and compares attributes on vital files and directories. By default it runs at 120 minute intervals on the Master, Replicas and BoKS Clients for UNIX, monitoring BoKS Manager system files and sending any discrepancies that are discovered as alert messages to the audit log.

You can optionally configure Custom File Monitoring on directories and files of your choice on specified hosts or Host Groups, in a configuration file that resides on each host (`$BOKS_etc/filmon.conf`). Once configured, you set the frequency and time of day to do monitoring in the menu File Monitoring > Configure Custom File Monitoring.

You can optionally run file monitoring from the command line manually at any time.

File Monitoring Sub-Menu	Description
Enable/Disable BoKS File Monitoring	BoKS file monitoring is enabled by default at installation. It can be disabled (not recommended) on a host or Host Group basis. If disabled, it can be enabled at any time.
Configure Custom File Monitoring	Set up Custom File Monitoring to run automatically. Requires a configuration file.
View Reports	Display log files from Custom File Monitoring in the GUI. (Log messages from BoKS File Monitoring can be viewed in the audit log.)

Maintenance of Accounts, Logs and Backups

Daily, weekly and other periodic maintenance routines are essential to good security management. In addition to setting security s and examining log and integrity reports, the single most important management area and the basis for all security management is careful upkeep of user accounts and access privileges.

The BoKS Manager browser menu provides options for performing many routine update tasks with just a few clicks:

- Access Control Administration > Block User lets you immediately disallow access for a user account, system-wide.
- User Administration > Delete Users lets you permanently remove a given user account simultaneously from all hosts across the BoKS domain. This function lets you choose whether or not to delete the user's home directory, but does not otherwise remove files owned by the user.
- Access Control Administration > Remove Access Routes lets you quickly remove one specific, or all, Access Route(s) from a given user or a User Class.
- Log Administration > Start New Log lets you change log files in a one-click operation.
- Security Configuration and Backup > Backup or Restore backs up the database and necessary BoKS files, or restores them.

From the command line you can do all of the above and many other tasks, including scheduling periodic system monitoring using BoKS Manager tools or your own. One such simple tool for the Master, Replicas and Clients for UNIX is boksinfo, which checks that the host can connect to the Master or a Replica, then takes a snapshot of domain and system information.

Domain-Wide Security Policies

BoKS Manager allows you to quickly set and apply security policies that apply

to the BoKS Manager Master and Replica, as well as to any Clients for UNIX in the domain. These range from simple, across-the-board settings to detailed and advanced settings for individual users, hosts, subnets, terminal types, times of day, and so on. This ensures that the BoKS Manager Master and Replicas and the database are secured, as well as any Clients for UNIX (if deployed). These settings make BoKS Manager comfortable for the less-experienced UNIX user as well as for more experienced UNIX administrators (who can use the command line when they wish).

Predefined Security Levels

The easiest way to configure BoKS Manager is the Security Configuration and Backup menu:

- Security Configuration and Backup > Set Low/Medium/High Security Level

This simultaneously sets up basic configurations for logging, integrity checking, login requirements, user password restrictions and timeout monitoring. By choosing a low, medium or high setting for all of these, you have an initial configuration that you can use until time and/or experience allow you to adjust the individual parameters separately.

Configurable Customized Parameters

For more granular UNIX security policies, BoKS Manager provides a large number of configurable security parameters. Some are system-wide and some may be set on specific hosts, Host Groups or User Classes. Still others can be set for individual users. You can set many of the system-wide parameters quickly and easily from the BoKS Security Configuration and Backup > View/Modify Current Settings menu. What you configure on this menu applies to all hosts and users, system-wide.

Others can be set, or set in more detail such as on a host or user basis, in the following menus:

- Password Administration > Password Parameters and Password Administration > Ban Password(s) (set up requirements on user passwords)
- User Inactivity Monitoring > Set User Inactivity Parameters (configure inactivity timeout for users)
- Sub-Administrator Configuration > Modify Sub-Administrator (set Sub-Administrator rights)
- Log Administration > Log Parameters (set up logging as you want it)
- Integrity Check > Setup Integrity Check (configure Integrity Checks)
- Integrity Check > Exclude Warnings (define content of Integrity Check reports)
- File Monitoring (configure monitoring on directories and files of your

choice on BoKS Manager-protected hosts)

Still other parameters are set by editing configuration files on chosen hosts or by running BoKS Manager's command line programs. You define the access rules that you want, specifically or in general, using a set of browser menus or command line functions that are called Access Control in BoKS Manager.

Delegated Administration with BoKS Manager

The BoKS Manager GUI, through which you manage your BoKS domain including all your hosts and users, is available only to users that have been granted administrative access.

Administrators

An administrator is any user whose account has access to the BoKS Manager GUI or command line (CLI) by having been assigned Access Routes to the BoKS Manager GUI or UNIX root access to the Master. By default, access to the GUI gives unlimited access to all menus and functions and to all hosts and users.

- You grant full GUI access by providing the BOKSADM Access Route to a user. You can assign it directly to them or add them as a member of a User Class that has that route (for example, the pre-defined class ADMIN).

To limit an administrator's access to GUI menus and functions or to hosts and users, you can configure them as a Sub-Administrator (see below).

Access to the BoKS Manager GUI is controlled by a special Access Route, separately from access to the CLI.

Sub-Administrators

In order to delegate administrative tasks, you can configure Sub-Administrator limitations to user accounts. A Sub-Administrator is an administrator whose access to the GUI is limited by BoKS Manager built-in restrictions and by specific permissions, which you assign in the BoKS Manager GUI. Besides specifying which menus are allowed, you can limit the scope of the Sub-Administrator's privileges to sets of users who are defined by UID range, a name template, Host Group and User Class. This gives you the ability to delegate responsibility while maintaining access on a "need-to-know" basis.

- To configure a Sub-Administrator, use the menu Sub-Administrator Configuration.
- BoKS Manager has built-in restrictions which exclude the menus Hosts, Host Groups, User Classes and others. These menus are not assignable to Sub-Administrators.

● BoKS Access Control for Servers in Overview

BoKS Access Control for Servers uses BoKS Manager on the Master and

Replicas together with BoKS Client for UNIX to centrally manage and control access to UNIX/Linux hosts in your organization.

Topics include:

- Centrally Managed UNIX Password Policies
- Controlling Root in BoKS Manager
- Centralized, Granulated Access Control with Access Routes
- User Inactivity Monitoring Menus
- BoKS Client for UNIX Features
- SSH (Secure Shell) Access
- Using BoKS Manager with NIS and NIS+
- Activating BoKS Protection Menus

Centrally Managed UNIX Password Policies

BoKS Manager provides you a number of options and parameters to implement UNIX password policies across the board on all UNIX/Linux platforms. UNIX policies apply to any user logging in to the Master, Replicas and BoKS Clients for UNIX.

Options and parameters include the following:

- Password format options include specifying a minimum number of upper or lower case characters, digits, and non-alphanumeric characters.
- Length of the expiration warning period, the grace period, and the minimum time between changes.
- Rules based on regular expressions, whereby you can specify regular expressions that passwords must or must not match.
- A list of words that are not allowed to be used in passwords, called banned words.

To define UNIX password requirements, use one or several of the following:

- To set individual password options and parameters for format, time between changes, grace period, etc., use Password Administration > Password Parameters.
- To specify rules based on passwords matching or not matching regular expressions, use Password Administration > Add regular expression.
- To change a regular expression rule, use Password Administration > Modify regular expression.
- To remove a regular expression rule, use Password Administration > Delete regular expressions.
- To list regular expression rules, use Password Administration > List regular expressions.
- To ban individual words from being used in passwords, use Password Administration > Add Banned Passwords.
- To remove words from your list of banned words, or view the list, use Password Administration > View or Delete Banned Passwords.

- To select one of the predefined packages of password settings, use Security Configuration and Backup > View/Modify Current Settings, and choose from:
 - None
 - Low
 - Medium
 - High
 - Random Generated (Model) and Random Generated. The Random Generated options (not available on platforms where BoKS protection is implemented via PAM, i.e. Solaris, RedHat Linux and SuSE Linux) provide the user a randomly generated password, rather than placing requirements on the user's own creation.

The model and random generated passwords features may not be supported in future versions of BoKS Manager.

Controlling Root in BoKS Manager

- Control of root requires careful planning and systematic implementation of a security policy. BoKS Manager provides you with a number of effective tools to implement your policy and control the root account:
- Define certain users as BoKS Manager Administrators and BoKS Manager Sub-Administrators, so that all security administration can take place under user accounts, without having to change to root identity.
- Allow only login from console, and define an Access Route with the privilege to su to root only to the administrators (or class) who need it.
- Use BoKS Manager's suexec utility to allow other users (or classes) to execute specific programs on specific hosts with root privileges.
- The option exists to log all keyboard input and system output for users performing operations as other users, including root, using suexec.
- Run integrity checks regularly. BoKS Manager discovers any incorrect system configurations that could result in a user gaining root access.
- Use BoKS Manager's inactivity control to automatically lock any unattended (root) windows, thus limiting the risk of an intruder using an unattended terminal or workstation.
- Regularly examine logs that show all root activity including root itself, su to root and suexec usage.

Access as Root with suexec

The suexec utility lets you allow a user to run a program as another user. This means a user can be allowed to run programs with root privileges without needing to know the root password. To allow a user to execute specific programs with root privileges on specified hosts, use one of the following:

- In the BoKS Manager browser, Access Control Administration > Add Access Routes, selecting the access method SUEXEC
- From the command line program, ttyadm

Note that this privilege by itself covers only local access. For remote access, the

user must also have an Access Route to the host. Root is doubly protected.

The user runs a program with root privileges by typing `/opt/boksm/bin/suexec` (if `suexec` is installed in the default location) followed by the program name. The user is prompted for a password, and must respond with his or her own password or SecurID passcode.

When a user runs `suexec`, keyboard input and screen output can be logged to provide extra forensic traceability for privileged access.

Centralized, Granulated Access Control with Access Routes

An Access Route is the means in BoKS Manager by which you authorize access to protected UNIX hosts and application servers. In addition to access, you can control authentication method and privileges to execute programs as other users such as root, described in other sections.

An Access Route consists of the following components:

- A user or a User Class
- An access method (telnet, ftp, BoKS ApplicationControl service etc.) used to access a host
- A source and a destination, that is, from which host and to which host the access is granted
- The times of day and days of the week during which access is granted

An Access Route is always associated with a single user or a single User Class. Thus, if two User Classes require the same access, then you need to set up two Access Routes that are identical except for the User Class. This makes possible the exact control of access for a given User Class, through adding and removing its Access Routes, independent of other User Classes.

Work with Access Routes in the Access Control Administration menu.

Alternatively, you can use the command line programs `routeadm` and `ttyadmin`, described in their respective BoKS man pages.

Source and Destination

The source and destination in an Access Route definition are usually specified as a single hostname or Host Group. For `login` and `su`, source is a terminal or terminal type.

To simplify construction of Access Routes, you can define Host Groups with similar access requirements and use the groups as the sources and destinations in Access Routes. Host Groups can be overlapping (but not nested), that is, created for specific access needs without modifying other existing Host Groups.

In the Customized Access Route option on the Access Control Administration > Add Access Routes page, or from the command line, you may specify names that include wildcards and IP addresses.

The Customized option also allows use of BoKS Manager's host prefixes ANY/, KNOWN/, BOKS/ and NONBOKS/ which are useful in allowing access to users from different categories of hosts.

Using the command line to define Access Routes allows even greater flexibility in specifications.

Restricted Access Routes

Restricted Access Routes let you specifically disallow certain accesses. This is useful when, for example, a user has been authorized more access than you want to grant by his or her assignment to a User Class. You assign the user to the class that most closely fits his or her access needs, then remove any unwanted access by defining a restricted Access Route for that user.

User Inactivity Monitoring Menus

Terminals or hosts with unattended active sessions are a security risk. Any passer-by can take over the session and do anything the original user could have done. To minimize this danger, you can set BoKS Manager to monitor user activity and either log out or lock out users after a specified period of inactivity. You can check the current status of network users by displaying both logged-on users and locked-out users.

Set up Inactivity Monitoring in the following menus:

- Security Configuration and Backup > Set Low/Medium/High Security Level or View/Modify Current Settings, for predefined timeout period and default actions, that apply to all hosts and users. Note that the two options Timeout Monitoring for Root Only and No Timeout Monitoring override any settings made in other menus for specific hosts or users.
- User Inactivity Monitoring > Set User Inactivity Parameters, to enable/disable timeout and X-lock, and to set the X-lock mode, for a given host or Host Group.
- User Administration > Modify User, to set the timeout period and action taken (logout or lockout) for a particular user.

Locked-out users can unlock their own display with their password or SecurID passcode, or call a System Administrator (or Sub-Administrator) to be unlocked.

View user activity in the domain in the following menus:

- Display who is currently locked out or unlock a display in User Inactivity Monitoring > Unlock Displays.
- Display who is currently logged on in User Administration > List Users

Logged On.

BoKS Client for UNIX Features

A BoKS Client for UNIX looks and feels like a regular UNIX machine for users, but is protected by a centrally managed server with a single GUI and a flexible command line administrative interface (CLI) available to Helpdesk personnel and administrators.

Key features provided for a Client are:

- UNIX access daemons, such as telnetd, sshd and ftpd, are replaced by BoKS versions of the same programs so that you can control their access and use through BoKS Manager. All access to BoKS-protected Clients for UNIX can be controlled uniformly and audited centrally, regardless of platform.
- User accounts on BoKS Clients for UNIX are centrally managed across multiple platforms using BoKS Manager, making everyday tasks such as deleting an account simple and immediate.
- For Clients on certain operating systems, BoKS adds a number of additional user authentication options including smart card authentication and SSH with certificate authentication.
- Clients that are pre-registered hosts can be configured to automatically disconnect from the BoKS Master or de-register from the BoKS database, and if disconnected automatically re-connect to the Master, to minimize the queuing of updates to non-contactable clients and enable more automation for machines used sporadically in your network.

SSH (Secure Shell) Access

BoKS Manager supports Secure Shell (SSH) based on OpenSSH. The primary documentation for OpenSSH is the documentation included in the OpenSSH distribution. See www.OpenSSH.com.

SSH is implemented in BoKS as an Access Method just like telnet, ftp and others, and SSH access is granted in the same way as, for example, telnet access using BoKS Access Routes. There are a number of settings for SSH that can be configured separately.

Using BoKS Manager with NIS and NIS+

BoKS Manager supports NIS and NIS+ by propagating information to the NIS or NIS+ database, for installations that use them.

Adding a New User

When a user account is added through BoKS Manager, BoKS Manager updates the local `/etc/passwd` and `/etc/shadow` files and if configured, the `/etc/group` file, on all BoKS Hosts (Replicas and BoKS Clients for UNIX) in the user's Host Group (or host, if the user is defined on a single host rather than a

Host Group). Note, however, that the `/etc/passwd` and `/etc/shadow` files are not used for authentication, for which BoKS Manager uses its own database.

All data entered into the User Administration > Create User menu, with the exception of User Class, is propagated to the NIS or NIS+ Master.

Propagation of Password Changes to NIS and NIS+

- NIS: A password that is changed on a local machine is propagated to BoKS Manager, which in turn propagates the change to NIS.
- NIS+: Propagation of a local password change is platform-dependent:
 - On Solaris with PAM active, PAM updates BoKS Manager and NIS+.

On Solaris with PAM active, users must be entered in the `/etc/passwd` file. Even though `/etc/passwd` is not used by BoKS Manager for authentication, if the user is not present in the file, PAM will block access for that user.

- On Solaris with PAM replaced by BoKS Manager, BoKS Manager attempts to update NIS+.
- On other platforms, BoKS Manager does not propagate local password changes to NIS+.

Note that you must configure BoKS Manager to support NIS and NIS+. In addition, propagation of certain information from BoKS Manager to NIS or NIS+ is platform-dependent.

Activating BoKS Protection Menus

You can activate and deactivate BoKS Protection on the Master, Replicas and BoKS Clients for UNIX from the BoKS Manager GUI. Activating BoKS Protection means that the UNIX operating system access programs on a host are replaced by the BoKS versions of those programs, and BoKS Manager takes over access control to and logging of activity on the hosts.

Work with BoKS Protection activation/deactivation in the following menus:

- Security Configuration and Backup > Activate or Deactivate BoKS Protection to activate or deactivate on Master, Replicas or BoKS Client for UNIX.
- Security Configuration and Backup > Hosts with BoKS Protection Activated to display a list of hosts with BoKS Protection activated, any of which you can deactivate.
- Security Configuration and Backup > Hosts with BoKS Protection Deactivated to display a list of hosts with BoKS Protection not activated, any of which you can activate.

● Access Control Tutorial

This section provides you a working understanding of the basics of access con-

trol based on Access Routes in BoKS Manager. Access Routes are used for controlling access to BoKS Manager Administration, to UNIX hosts and to BoKS Agent-protected applications.

Topics include:

- Access Control in BoKS Manager
- Using Host Groups for Access Control
- Using User Classes for Managing Access Rights
- An Access Example (Telnet to Dallas)
- Reading Access Route Basics
- More Access Route Examples
- Customized Access Routes Basics
- Maintenance of Access Routes
- Access Route Basics
- Access Control Menus and Tasks

Access Control in BoKS Manager

When BoKS Manager is initially installed and activated, default access is no access. In BoKS Manager, every access requires an account in BoKS Manager and for UNIX and BoKS Agents, a positively configured Access Route set up by an administrator. No access is ever allowed simply by default (except on BoKS Desktop workstations where it is sufficient to have an account).

Access Route

Access Routes are the means by which you authorize access for specific users on specific hosts for specific days and times of day. Access Routes may be set up for individual users, but for most purposes it simplifies management to use User Classes as a basis. Similarly, an Access Route may be set up for a single pair of hosts (source and destination), but use of Host Groups greatly simplifies management of access rights.

Access Routes are always tied to either a user or a User Class. No Access Routes exist “freely” or “floating” in the BoKS Manager system.

User Class

A user can belong to one or more User Classes. When you assign a user to a User Class, the user acquires the Access Routes of that class. When you add a new user to the BoKS Manager database, you therefore assign that user the User Class or classes that most closely resembles his or her access needs (which usually correspond with job duties). You may then add (define) any individual Access Routes assigned directly to the user that this user needs over and above those provided by the User Class(es) that you assigned.

BoKS Manager comes with predefined User Classes, each with predefined Access Routes. Your organization can use these classes if it wishes, and can

modify the Access Routes associated with each.

At installation, these classes exist but are not assigned to any users; they are available, but provide no access until you assign them to users.

User Account

Besides an Access Route, a user requires an account on the destination host. To simplify management of accounts, BoKS Manager uses Host Groups that enable you to easily create accounts in a heterogeneous UNIX environment.

su, suexec and Access Routes

In BoKS Manager, you can grant the privilege to su to other accounts, and to run specific programs as other users including root. In the BoKS Manager GUI, su and suexec access can be granted in Access Control Administration > Add Access Routes.

Note, in addition, that both su and suexec privileges require the user to have an Access Route to the host in question. Therefore, remember when you grant these privileges that these are not Access Routes, but are privileges above and beyond host access, and check that the necessary Access Route exists.

Authentication

Password authentication is the default for most UNIX Access Routes in BoKS Manager (default for BoKS Agents is Certificate). You can optionally require two-factor authentication with other authenticators, for example, RSA SecurID tokens or SSH Public Keys, for individual users or for Access Route types.

Summary

- Every access authorization requires an Access Route, assigned either individually to the user or via his or her User Class(es).
- Privilege to execute as root requires separate definition (SU or SUEXEC Access Route) in addition to an Access Route to the specific host (for example TELNET Access Route).
- A user account is always required on the destination host, and is normally provided by means of Host Groups.
- Authentication may be by BoKS password or optionally required to be by special (non-password) methods that are assigned to specified users or for an Access Route type.

Using Host Groups for Access Control

Creating logical Host Groups simplifies management of access rights. A Host Group allows you to assign one Access Route to many hosts, rather than creating separate, identical Access Routes for each host. A Host Group can be used as the source or destination, or both, in an Access Route.

Since a host may belong to multiple Host Groups, you can define new Host Groups without disturbing the old, as the need arises for new access rights or for other purposes, such as user accounts administration.

View what Host Groups a particular host belongs to using the following menu:

- Host Administration > List Host Information (displays each host's type, IP address and home directory)

View what Access Routes provide access to a particular Host Group using the following menus:

- Access Control Administration > List User Access Routes
- Access Control Administration > List Class Access Routes

browsing through all User Classes or, if necessary, all users.

Using User Classes for Managing Access Rights

A User Class is a collection of users with common access needs, for which Access Routes, Group Encryption Keys and optionally security parameters may be associated. Once defined, a class may then be assigned to users who will then be able to use the Access Routes, group keys owned by that class, and whose security parameters will be controlled by their Primary User Class (when assigned to a user).

BoKS Manager provides a set of predefined User Classes that may be used as is or modified; other User Classes can be created to fit your organization's needs.

A user can be assigned to one or more User Classes. Through assignment, the user acquires the Access Routes of that class. If a user has no class assigned, the user's only Access Routes are those specifically defined for him or her. Without User Classes, it would be necessary to assign access rights to each user individually, making for an unmanageable number of Access Routes and an insecure situation.

A user who is assigned a class can have their own user (individually assigned) Access Routes in addition to those acquired through User Classes. A user's total access privilege is the sum of Access Routes owned by the user's User Classes and by the user individually. (For access to UNIX hosts, UNIX file rights naturally also apply, once access to the host is gained through BoKS Manager.)

A user's access rights (from both individual and User Class Access Routes) can be limited by:

- Restricted Access Routes.
- Blocking a user.

An Access Example (Telnet to Dallas)

Suppose there is a group of engineers in the development department in New York, who all need telnet access to a host named stingray, a server in Dallas.

To avoid having to create an Access Route from each of the engineers' workstations to stingray, you can create a Host Group (if it does not already exist) that contains all of their workstations.

To allow development engineers to access stingray from New York:

1. Make sure all of the IP addresses in the New York development subnet are defined as hosts in the BoKS database, using Host Administration > Register Host or Import Host Definition.
2. Create a Host Group called, for example, DEV_HOSTS, containing all of these workstations, using Hosts Administration > Add/Modify Host Group.
3. Create a User Class, if it does not already exist, called DEVELOPMENT, to give all developers who require it access to stingray. You can use the class to grant access to other hosts, too. Create the class using User Class Administration > Create User Class.
4. Add all users in the development department to the DEVELOPMENT class using User Class Administration > Modify User Class.
5. Decide what days and hours access is needed. For this example, say workdays, all hours. These are the default in BoKS Manager. (Workdays are defined locally on each installation in the /etc/acct/holidays file.)

You now have the components needed for an Access Route:

- The User Class DEVELOPMENT, including all users in development
- The access method of interest, telnet
- The source DEV_HOSTS and the destination stingray
- The days of week and times of day: workdays, all hours

Consider for a moment the User Class DEVELOPMENT to which the Access Route will belong. Without the User Class, you would need to create identical Access Routes for each of the engineers, perhaps ten or twenty routes instead of one. In addition, with this class now defined, you can later easily grant this group of users other access: other access methods on stingray, or to other hosts.

Similarly, the Host Group DEV_HOSTS makes it possible to provide access to or from the whole group with one Access Route, rather than to or from each individual host.

6. Create the route by selecting Access Control Administration > Add Access Routes, selecting the components as described above, and then clicking Execute.
7. Check what access you have created by selecting Access Control

Administration > List User Class Access Routes, which displays:

```
DEVELOPMENT TELNET:DEV_HOSTS->stingray 12 am 11:59 pm  
Workdays
```

In the listing, you see the User Class DEVELOPMENT as a heading, followed by all of its Access Routes (here, only one), each on a separate line. The route itself is displayed compactly: TELNET is the access method, DEV_HOSTS is the source, -> is the symbol for “to”, and stingray is the destination host. The times shown indicate the whole 24-hour day, 12 am to 11:59 pm, or midnight to midnight (workdays and times are defined locally on the Master, Replica or Client for UNIX host in the `/etc/acct/holidays` file).

Note that both source and destination in this example are single names, i.e., a single host or Host Group. To specify multiple names, use the Customized definition option in Add Access Routes. When multiple hosts or Host Groups are chosen as destinations, for example, they will be displayed as a list separated by commas.

A Restricted Access Route Example

Suppose now that in the Development department in the previous example, there is a consultant named Janet, and that she needs access to most of the same hosts that others in Development use, but that she is not to be allowed into the Dallas host stingray. How could you set up her Access Routes?

If her needs were very special, you would probably define one or several Access Routes and assign them individually to her, in Access Control Administration > Add Access Routes.

But since her needs closely resemble the rest of the engineers in Development, the easiest way is to assign her to User Class DEVELOPMENT, which we assume by now has a number of Access Routes, and then remove her access to stingray using a Restricted Access Route.

To set up an Access Route that denies her access to stingray:

1. Select Access Control Administration > Restrict Access Routes.
2. Select the user DEVELOPMENT;janet. Select the method Access over network (with password).
3. On the continuation page, select all of the methods in the Access Methods list (Telnet would do, if telnet were the only open access method for User Class DEVELOPMENT, but here we select all for safety's sake).
4. Select ALL as the source in the From Hosts list. We could have selected DEV_HOSTS since this is where she works from but, again, selecting all is safer.
5. Select stingray as the destination in the To Hosts list and click

Execute.

6. Check the access you have created by selecting Access Control Administration > List User Access Routes, which displays:

```
DEVELOPMENT:janet -RLOGIN,TELNET,XDM,FTP,REXEC:  
ALL->stingray 12 am 11:59 pm Any Day
```

The minus sign in front of RLOGIN that shows that this is a restricted route, that is, one that denies access under the specified conditions.

In Restrict Access Routes, the default for days is Any Day. For Add Access Routes (allowing access), the default is Workdays.

Reading Access Route Basics

You need to be able to read basic Access Route syntax in order to understand listings of Access Routes.

The syntax for Access Routes is:

```
Method[,Method]: [Prefix/]Source -> [Prefix/]Destination [From:] [To:]  
[Days:] [, Modifiers]
```

where:

- Method is the name of the access method (TELNET, FTP, RSH, etc.).
- Source is the source host, Host Group or terminal from which access is granted.
- Destination is the target host or Host Group to which access is granted.
 - Source and destination are sometimes written as IP addresses or tty numbers, for example, 120.13.22.01, tty12, etc.
 - The wildcard asterisk * means, as in standard UNIX usage, “any” (host, tty or IP address).
 - In terminal access methods, there are three special sources:

Source	Description
Console	from the console only
tty*	all terminals except console
*	from anywhere, including console

- Prefix is one of BoKS Manager’s host prefixes that qualify the source or destination. For example, the prefix BoKS means BoKS Manager host, so that BoKS/HG12 would mean BoKS Manager hosts within the Host Group HG12.
- From is the time of day when the access (or denial, for a restriction) begins.
- To is the time when the access (or restriction) ends.
- Days are the days of the week during which access is allowed (or disallowed, for a restriction).

- Any Day means all days. This is default in restricted Access Routes.
- Workdays means normal working days Monday to Friday, excepting holidays. This is default in unrestricted Access Routes.
- Numbers 1-7 indicate specific days of the week, where 1=Monday.
- Modifiers are additional specifications for the Access Route, including what Authentication/Encryption are specified:
 - Authentication: tells the type of authorization (default is password authentication). See the chapter Managing Authentication on Access Routes.
 - Encryption: Yes means encryption has been specified for this route (telnet only).
- Colon (:), comma (,) and right arrow (->) are separators.

More Access Route Examples

Access Route	Description
TELNET,FTP:DEV_HOSTS->stingray 8 am 5 pm Workdays	TELNET and FTP are allowed from Host Group DEV_HOSTS to host stingray, workdays, 8 am to 5 pm.
TELNET:robin->ALL 8 am 6 pm Workdays	TELNET is allowed from host robin to Host Group ALL during business hours, workdays. ALL is a pre-defined group that means ALL hosts in the database.
-FTP:123.45.*.*->seagull 12 am 11:59 pm Any Day	FTP usage is disallowed (indicated by the minus sign in front of FTP) from hosts in the 123.45.x.x network segment to the host seagull, any day, all hours. Note the asterisk wildcards.

Customized Access Routes Basics

When you create an Access Route in Access Control Administration > Add Access Routes, the Customized definition option allows greater flexibility in specifying source and destination. It lets you enter the source and destination in any of the forms acceptable in Access Route syntax, rather than only choosing hosts or terminals from a host list. This gives you the freedom to use the following forms:

- Terminal device numbers, for example, tty123
- IP addresses, for example, 10.115.46.3
- Host Prefixes: KNOWN, ANY, BOKS, NONBOKS
- username@hostname, for example cynthia@hh1
- Wildcards, for example, H*

For example, you can specify Access Routes such as the following:

- From terminal tty123
- From host IP address 1.2.3.4 to host IP address 5.6.7.8
- From hosts on the subnet 173.11. Specify the source as 173.11.*.*
- From ANY/*, allowing access from all hosts including hosts outside the domain.

Once you are familiar with the syntax, an effective way to add Access Routes is via the command line programs `ttyadmin` and `routeadm`, which allow the above features as well as other flexibility.

Maintenance of Access Routes

BoKS Manager has no separate command to modify an Access Route. When you want to change the conditions of an Access Route, add the new route, then remove the old route. Adding the new route first insures continuity of access.

Access Route Basics

Key elements of Access Route definition and usage are:

- Access that is not explicitly granted is not allowed.
- Access Routes can be created and assigned to a user or User Class – but not to a host or Host Group.
- Access Routes can be non-restricted (allow access) or restricted (deny access). In listings, a restricted route is indicated by a minus sign preceding the specification.
- Access Routes (non-restricted) authorize access. To actually gain access, a user must also authenticate him or herself.
- Authentication is granted separately. By default, authentication is by password.
- Once authorized and authenticated to a host, UNIX file permissions apply as usual.
- Individual routes dominate over User Class routes, and restricted routes dominate over non-restricted routes. Individual routes are examined by BoKS Manager first, and if a match is found, access is granted, even though there may be a User Class restricted route for that route and user.
- Multiple access methods may be included in a given Access Route as long as they all use the same kind of specification (host, terminal) for source and destination.
- Source and destination are mandatory. In a Customized definition they may include the predefined Host Group ALL, host prefixes KNOWN, BOKS, etc. and the wildcard asterisk (*).
- Times of day and days of week are optional. Default for non-restricted routes is workdays, all hours. Default for restricted routes is any day, all hours.
- Times of day that are used in Access Routes are by default relative to the Master or Replica that performs the authorization, unless another local time for the host being accessed is specified in the file `$BOKS_etc/`

timezones on the Master. Time zones apply to access to the Master, Replicas, BoKS Clients for UNIX and Agent Hosts. They do not apply to BoKS Desktop logon. See “Setting Time Zones” on page 131.

Work with Access Routes in the Access Control Administration menu.

From the command line, use `routeadm` and `ttyadmin`.

Access Control Menus and Tasks

Working with Access Routes

- Define a new Access Route in Access Control Administration > Add Access Routes.
- Use the Customized option to specify source and destination as IP addresses, terminal numbers or using wildcards.
- Deny access in Access Control Administration > Restrict Access Routes.
- List Access Routes in Access Control Administration > List User Access Routes or List Class Access Routes.
- Delete a route in Access Control Administration > Remove Access Routes. Deleting a route removes the access, or denial, that is specified in that route.
- Modify an Access Route by adding a new route with the desired specifications, then deleting the old route. Creating the new route first ensures continuity of access.
- Temporarily block all UNIX/BoKS Agent access for a user in Access Control Administration > Block User. Use List Blocked Users to display blocked users.
- From the command line, use `routeadm` for a route assigned to a User Class and `ttyadmin` for a route assigned to a specific user.

Authentication and Encryption

- Authentication requirements in a particular access request are determined jointly by the authentication requirements (if any) for the particular user and the requirements (if any) for the Access Route type.
- Specify non-password, two-factor authentication for a user in Authenticator Administration.
- Specify authentication for an Access Route type in Access Control Administration > Define Authentication and Encryption Methods.
- From the command line, specify authentication and encryption with `bksdef`.
- Communications between Master, Replicas and BoKS Clients for UNIX are always encrypted with RC5.

Solving Access Problems

Limiting access is one side of access management; seeing that user access needs are met on a daily basis is equally important. Many things can prevent a user from actually accessing the host, application or data to which you and the user

agree that he or she needs access.



FoxT
883 N. Shoreline Blvd.
Mountain View, California 94043
www.foxt.com
650.687.6300

Copyright © 2008 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.