helpsystems

Installation Guide

BoKS Manager

7.2

Copyright Terms and Conditions

201909131148

Preface

BoKS Manager 7.2 Installation Guide describes how to install BoKS Manager and BoKS Server Agent for Unix/Linux in a network as part of the FoxT ServerControl solution.

> **NOTE:** See the HelpSystems Community Portal for updated versions of product documentation. Revision: September 2019.

A parallel guide, the BoKS Manager 7.2 Administration Guide, covers how to configure and use BoKS Manager and BoKS Server Agent for Unix/Linux. The *Administration Guide* covers domain concepts, the BoKS Command Line Interface, and most configuration issues. It also covers initializing the BoKS CA, which is necessary for remote administration. It provides detailed usage of many settings that may be necessary for installation. References to many of these topics are found here in the Installation Guide at appropriate places.

Use the *Administration Guide* and *Installation Guide* interchangeably, employing the references between them and their separate indexes to find what you are looking for. Topic matter overlaps considerably.

Audience

This guide is intended for security administrators and network administrators who are responsible for security management. Only users with root permission and users given security administration rights can manage this security software.

You should be familiar with essential Unix concepts and know how to use basic Unix commands from the command line.

About User Interfaces for Managing BoKS Manager

The old BoKS Administration GUI is no longer included in the BoKS Manager package.

BoKS Manager 7.2 includes the following user interfaces for managing BoKS Manager:

- FoxT Control Center, a separate management component with an updated web interface
- the BoKS command line interface.
- BoKS password checkout interface, that can be used to check out password for BoKS-protected accounts.

The procedures in this guide describe how to manage BoKS Manager using the command line interface and FoxT Control Center. For further information on how to manage BoKS Manager using FoxT Control Center, also see the FoxT Control Center online help system.

Modified and Removed Functionality in This Version

For a list of modified and removed functionality in this version, see the *BoKS Manager 7.2 Release Notes*. Note that the Release Notes are updated periodically, so it is recommended to check the FoxT Customer Support website for the latest version.

How This Guide Is Organized

This guide includes the following chapters:

- *Planning Installation* covers preparation for implementing BoKS Manager in your network.
- *Installing BoKS Manager* provides step-by-step instructions on how to install the product, initialize and do basic configuration as a Master or Replica.
- *Upgrading BoKS Manager* describes how to upgrade from a previous version of BoKS Manager with a BoKS domain
- *Deploying BoKS Server Agents for Unix/Linux*

Product Documentation

The BoKS Manager documentation is available from the Fox Technologies Support web site:

- *BoKS Manager 7.2 Installation Guide* – BoKS72ins.pdf
- *BoKS Manager 7.2 Administration Guide* – BoKS72adm.pdf

> **NOTE:** BoKS Server Agent for Unix/Linux has no separate documentation, but is instead included in the BoKS Manager documentation.

Reference Materials

Following are the primary product documentation for the Fox Technologies products. You can obtain these from your Fox Technologies Representative, from the product download package, or in some cases online from the product itself after the product is installed.

BoKS Manager 7.2 Administration Guide (includes BoKS Server Agent for Unix/Linux)

BoKS Manager 7.2 Installation Guide (includes BoKS Server Agent for Unix/Linux)

BoKS Manager Administration Workshop Notes (available to workshop participants)

BoKS Manager Deployment Workshop Notes (available to workshop participants)

BoKS SSH Client for Windows Administrator's Guide and Readme

BoKS man pages for BoKS programs (from the command line)

The FoxT Control Center online help system

Recommended Reading

Recommended reading for getting started with BoKS Manager

- The chapter "A Guided Tour" in the *Administration Guide*. A detailed overview of the product.
- The chapter "BoKS Manager Administration" in the *Administration Guide*. An introduction to using FoxT Control Center and the command line interface (CLI).
- The appendix "Command Line Interface" in the *Administration Guide*. An introduction to the BoKS command line for the advanced UNIX user.

Tip: "Basics" topics give a quick summary of key concepts, common tasks and important details within a particular area.

Recommended further reading for getting started with installation

- The chapter *Planning Installation*. Includes system overview, network architecture with planning Master and Replicas, system requirements, overview of deployment and/or upgrade paths.
- The chapter "System Configuration" in the *Administration Guide*. Details on communication settings and many other domain-wide issues, many of which are part of basic configuration of a domain.
- Other chapters that are relevant for your installation, such as LDAP Synchronization or Token Administration.

Terminology in the Documentation

UNIX and Linux

The term UNIX is used throughout this manual in the generic sense to mean the operating systems that are supported for installation of BoKS Manager and BoKS Server Agents for Unix/Linux, which include a wide variety of **UNIX** and **Linux** platforms. The terms UNIX passwords, UNIX access methods, UNIX hosts, etc. thus include those items on or in the operating system that is installed, including both **UNIX** and **Linux** varieties.

See also:

- *Terminology* in the chapter *A Guided Tour* in the **Administration Guide**

IP Version

BoKS Manager supports IP version 6 & 4. The majority of the IP addresses described in the documentation are in IP v4 format. BoKS Manager 7.2 features full support for IP version 6, and it is supported to have an IPv6 address as the primary IP address for BoKS hosts as long as the Master and Replicas are running BoKS Manager 7.1 or later and the BoKS hosts are also running BoKS 7.1 or later.

Other Terminology

Terminology has changed during development of successive versions of the product over the years. Some of the key terms and their older synonyms or names are listed in the following:

Term	Description or older terms
FoxT Server Agent for Unix/Linux, Server Agent	Known in the documentation and some menus and man pages variously as BoKS Client for Unix/Linux, BoKS Client for Unix, BoKS Client and Client. A Unix host with BoKS Manager software installed and set up as a Client. Previously called simply **Client**, in contrast to a Master and a Replica. The actual software installed may be the Master/Replica/Server Agent (MRA) package, or the Server Agent (A) package.
server	Ordinary meaning, but sometimes also used to mean a BoKS Manager Master or Replica that provides services such as authentication, authorization and audit logging.
FoxT ServerControl, BoKS ServerControl or BoKS Protection	The services delivered in and controlled by BoKS Manager that protect UNIX access programs and daemons. When activated, these services protect the Master and Replicas, and any BoKS Server Agents for Unix/Linux. Previously called UnixControl. For details, see "Managing and Configuring the Domain in Overview" in the Administration Guide.

Getting Support and Service

Fox Technologies, a HelpSystems company	www.helpsystems.com

Before You Call for Technical Support

Note: Technical support is not provided during the warranty period unless a valid Software Service Contract is in force.

Please have the following information available when you call:

- Your Fox Technologies Customer/License ID.
- Fox Technologies software version number.
- The make and model number of the computer on which the problem occurs.
- The name and version of the operating system under which the problem occurs.
- The resulting tar archive from running the command:

```
BoKS # boksinfo
```

which includes parts of the BoKS log, the error log (err_log), a complete dump of the BoKS ENV file (which shows version and installed hotfixes and patches) and other info. For usage details, see *System Snapshot with the Program boksinfo* in the appendix "System Monitoring Tools" in the *Administration Guide*.

Planning Installation

With BoKS ServerControl, you turn your network into a centrally managed security domain that offers advanced and simplified system administration, improved security, and replicated and distributed authentication servers that provide your users with fast and secure access.

Before deploying the BoKS ServerControl software, you should read relevant parts of this guide and of the Administration Guide. You need to be thoroughly familiar with BoKS terminology and with the major components of the system, their functions and how they interact.

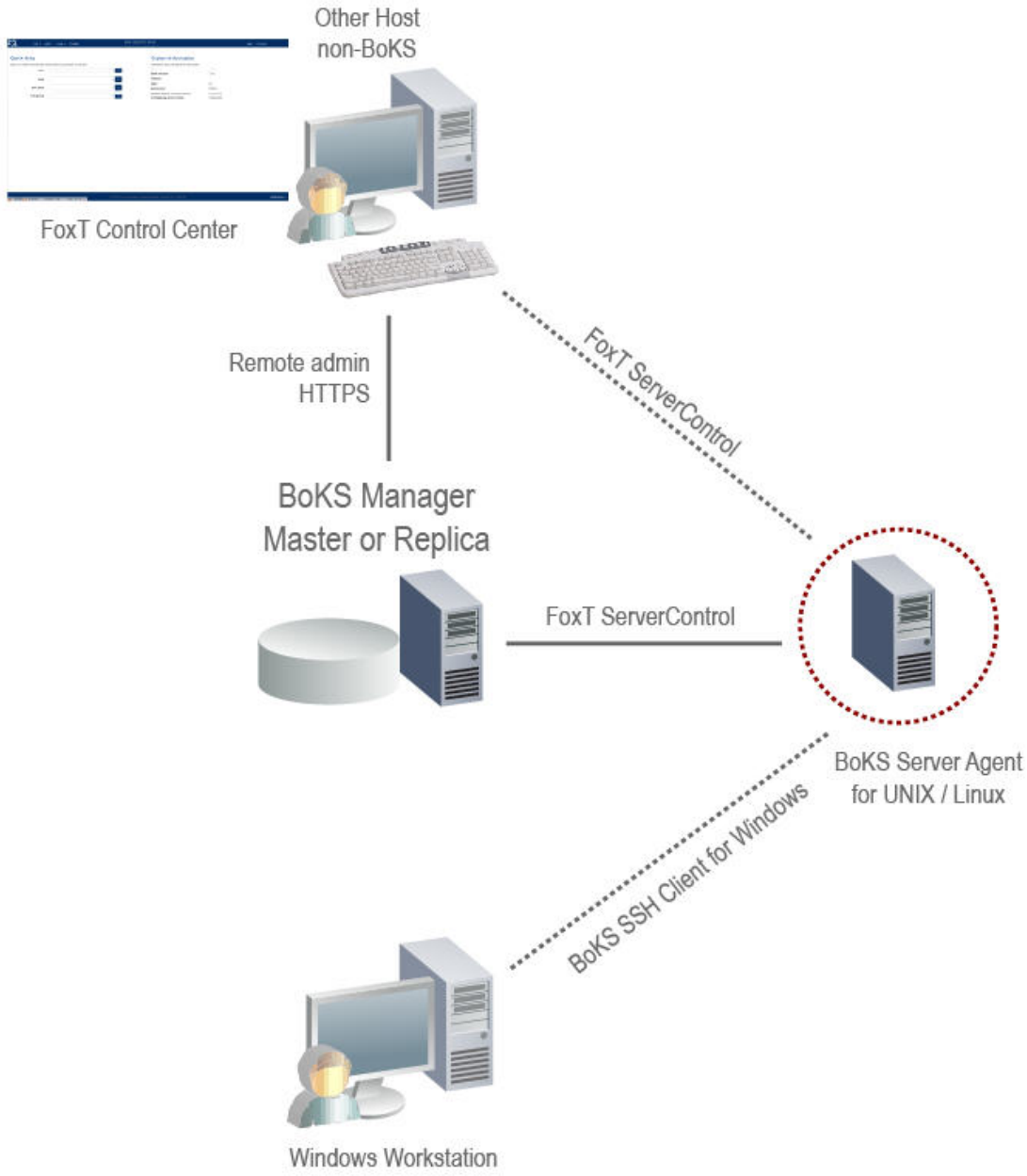
Planning Installation includes the following topics:

See also:

- The chapter "A Guided Tour" in the *Administration Guide*
- The appendix "System Architecture" in the *Administration Guide*
- The chapter "System Configuration" in the *Administration Guide*
- The chapter "Host" in the *Administration Guide*.
- The chapter "User Administration" in the *Administration Guide*
- The Readme and Release Notes, which contain late-breaking platform-specific installation information.
- Using Learn Mode

BoKS ServerControl Overview

The BoKS ServerControl security domain is a network in which at least one **Master** has been installed. In addition to the Master, one or several **Replicas** can be installed to help service BoKS Server Agents.



Each domain has only one Master, on which the security database is maintained. The database is a central repository for data about all hosts, user accounts, their access permissions and other important security-related information. All administration is performed on the Master.

For large networks it may be useful to deploy multiple BoKS domains independent of each other. See Multiple BoKS Domains.

The Master responds to user login requests forwarded by BoKS Server Agents in the domain.

Each Replica has a read-only copy of the BoKS Manager database and can also respond to login requests. Replicas thus provide for both load balancing and fault tolerance. In a network with Replicas, operation continues uninterrupted even if the Master fails.

A BoKS Server Agent for Unix/Linux is a Unix or Linux host on which the BoKS Server Agent software has been installed. This Server Agent makes calls to the Master/Replica whenever a user attempts to log in using one of the access methods (such as **telnet**, **ssh**) that are included in BoKS Protection.

The Master and Replica servers also protect themselves by using the same BoKS Protection modules as are installed on BoKS Server Agents for Unix/Linux.

For a full introduction to BoKS Manager, see the chapter *A Guided Tour* in the *Administration Guide*.

See also:

- Defining Masters, Replicas and Domain Architecture

Registering Hosts

You define the hosts in the domain and their different roles in the BoKS security domain using the BoKS Manager web-based administration program FoxT Control Center, where you provide the Host Type (Replica, BoKS Server Agent, Other) and the IP address. Once defined, the various hosts will be linked and their access controlled from a single point within the network.

Hosts that are not running BoKS protection software can be registered in the database to allow access *from* them to hosts that are protected. Such hosts are registered as “Other Hosts”

Note: The hostname on BoKS hosts (as returned by the **hostname** command) should always be the FQDN rather than the short name of the host, to ensure correct communication both internally and with other systems outside BoKS.

Pre-Registering BoKS Server Agents for Unix/Linux

Hosts do not need to have BoKS Server Agent for Unix/Linux installed to be registered as BoKS Server Agents in the BoKS database. You can pre-register hosts and they are then automatically added to the BoKS database when BoKS Server Agent for Unix/Linux is installed and they contact the BoKS Master.

The pre-register host function is useful for organizations that want to separate the tasks of registering and managing Server Agents in the BoKS database and installing BoKS software on hosts, and can be used to ensure machines in virtualized environments that are only used as and when needed are automatically managed and protected by BoKS.

Other Hosts

You can register a host as the type Other Host in the BoKS domain so that you can grant access *from* it (from a specified, known IP address) to the BoKS Master, Replicas or to BoKS Server Agent for Unix/Linux hosts. Access *to* such Other Hosts is not protected by the BoKS Master.

“Other hosts” may be protected by another BoKS Master in another domain, where they are registered as the appropriate type of host for that domain, for example, Server Agent for Unix/Linux. “Other host” allows a host to be included and known in several domains, while only one domain Master controls access to it.

One use of Other Host would be to allow remote administration of BoKS Manager from a workstation that was not protected by other Fox Technologies software.

See also:

- *Host Types* in the chapter "Host" in the *Administration Guide*

Prerequisites for BoKS Manager

Topics include:

- System Requirements
- Web Administration Requirements
- Installation Paths and Deployment Scenarios

System Requirements

See also:

- The Readme and Release Notes, which contain late-breaking platform-specific installation information.
- Master Basics
- Replica Basics
- BoKS Server Agent for Unix/Linux Basics.

Licensing Requirements

BoKS software is controlled by a licensing system that regulates the number of servers you can register per BoKS domain. The license details are normally agreed between your organization and your Fox Technologies representative.

You should ensure that the license(s) issued to your organization is in line with your requirements regarding the size of your BoKS domain(s). Licenses are activated as part of the Master install and setup procedure with the help of Fox Technologies customer support.

For more details on this procedure, see Licensing Background.

Supported Platforms

The following table lists the platforms supported by BoKS Manager 7.2 / BoKS Server Agent for Unix/Linux 7.2. Note that platform coverage may change and you can see the currently available platforms at the download page on the HelpSystems Community Portal.

Operating System	MRA
IBM AIX 7.1, 7.2	MRA
IBM VIOS 3.1	A
CentOS 6	MRA
CentOS 7	MRA
Debian 8 & 9	A
HP-UX 11iv3	A
Oracle EL 6	MRA
Oracle EL 7	MRA
Oracle Solaris 10 x64 & SPARC	A
Oracle Solaris 11 x64 & SPARC	MRA
Red Hat EL 6 x64	MRA
Red Hat EL 7 PowerLinux (Power 8) / Red Hat EL 7.5 PowerLinux (Power 9)	A
Red Hat EL 7 x64	MRA
Red Hat EL 8 PowerLinux (Power 8)	A
Red Hat EL 8 x64	MRA
SuSE 11 x64	A
SuSE 12 s390	A
SuSE 12 x64	MRA
SuSE 15 x64	MRA
Ubuntu 14 x64	A
Ubuntu 16 x64	A
Ubuntu 18 x64	A

NOTE: Due to differences in the operating systems, there are separate packages for Oracle Solaris up to 11.3 and Oracle Solaris 11.4.

NOTE: Support for CentOS and Oracle EL 6 and 7 is included in the packages for Red Hat 6 x64 and Red Hat 7 x64 respectively.

NOTE: Oracle Linux 7 is supported on Red Hat Compatible Kernel (RHCK) for MRA and Unbreakable Enterprise Kernel (UEK) 5 for A.

RAM and Shared Memory

Recommended **RAM** memory for a Master or Replica is at least 4 GB.

Recommended **shared memory** for a Master or Replica is at least 32 MB.

Semaphore Sets

The required number of semaphore sets for BoKS Manager are

- Master: 2
- Replica: 2

Semaphore Undo Structures

Semaphore undo structures are used to reset the semaphore state if a process holding the semaphore dies. For early versions of Solaris 10 that require static configuration of semaphore undo structures use the following as a minimum setting:

- Master: 600
- Replica: 600

For details on configuring the number of semaphore undo structures, see your operating system documentation set.

Note: It is possible to stop bridge processes in BoKS from using a semaphore for locking by setting the BoKS ENV variable `BRIDGE_CACHE_NOSEM` to `on`, in which case a file is used for locking instead.

Disk Space

Recommended free disk space is:

- Master: at least 700 MB
- Replica: at least 600 MB
- Server Agent installation of the MRA package: at least 400 MB
- Server Agent-only package installation: at least 300 MB.
- In addition to these “permanent” space requirements, during installation you need approximately 300 MB of temporary storage in the directory **/tmp** (or another configurable directory) where patches will be temporarily unpacked by the install program.

The Server Agent installation of the MRA package requires more space than that of the Server Agent-only package since it includes files used if converting the Server Agent to a Replica.

Disk space recommendations are platform dependent. The figures above cover the largest platform requirement. Requirements also depend on domain size, number of hosts and users, etc. Requirements here are minimum recommendations.

For installations from tar archives, the product is stored by default in the following default directories:

- **/opt/boksm ($BOKS_DIR)**
- **/etc/opt/boksm ($BOKS_etc)**

- **/var/opt/boksm ($BOKS_var)**

For installations from native packages, the product is stored by default in the following default directories:

- **/opt/boksm ($BOKS_DIR)**
- **/opt/boksm/etc ($BOKS_etc)**
- **/opt/boksm/var ($BOKS_var)**

If these directories are located on different partitions, 280 MB may be needed for **$BOKS_DIR** and 2 MB for **$BOKS_etc**. See also Install Directories.

The database on a Master or Replica is located in **$BOKS_var** and will grow depending on the size of your system.

Qualified Display Managers on Different Platforms

The table below lists the display managers used during BoKS qualification for each platform. On platforms where multiple display manager choices are available, other display managers than the one indicated in the table might work with some limitations to the functionality.

Operating System	dtlogin	gdm	lightdm
AIX 7	X		
Debian 8 & 9		X	
HP-UX 11v3	X		
Red Hat EL 6 & 7		X	
Oracle Solaris 10	X		
Oracle Solaris 11		X	
SuSE 11 & 12		X	
Ubuntu 14			X

Inet Services Support

The legacy UNIX services **telnet**, **rlogin**, **rsh**, **rexec** and **ftp** are traditionally started via the **inetd** daemon. Modern UNIX/Linux systems sometimes offer alternative startup methods.

The BoKS **sysreplace** command can optionally enable/disable these services when BoKS is activated or deactivated. The **sysreplace** service enable/disable function is only supported for one service startup method for each platform and service.

The table below lists the supported service startup method per platform and service. Some platforms offer alternative **ftp** daemons and for these platforms the **ftp** daemon used during qualification is listed.

OS - startup method	telnet	rlogin	rsh	rexec	ftp	vsftpd	vsftpd standalone	proftpd standalone
AIX 7 - inetd	x	x	x	x	x			
Debian 8 - xinetd with inetd_compat option	x	x	x	x			x	
HP-UX 11v3 - inetd	x	x	x	x	x			
RedHat 6 - xinetd	x	x	x	x			x	
RedHat 7 - systemd	x	x	x	x	x		x	
Solaris 10 - smf	x	x	x	x	x			
Solaris 11 - smf	x	x	x	x				x
SuSE 11 & 12 - xinetd	x	x	x	x		x		
Ubuntu 14 - xinetd with inetd_compat option	x	x	x	x	x			

Token Requirements

If you use RSA SecurID Tokens, you need to deploy the corresponding SecurID-related modules. For details, see the chapter "Managing Authenticators" in the *Administration Guide*.

To use RSA SecurID tokens with BoKS Manager, you also need to configure each BoKS Manager Master, Replica and Server Agent for Unix/Linux for integration with RSA Authentication Manager (RSA ACE/Server), which is described in the installation procedure for these types of hosts.

Note: In order to run BoKS debugging on Unix and Linux hosts, certain programs also need to be installed on the host. For details, see the section "Monitoring Daemon Processes" in the BoKS Manager Administration Guide.

Web Administration Requirements

You can manage your BoKS domain using the web-based administration program FoxT Control Center.

Note: You must use FoxT Control Center 7.2 with BoKS Manager 7.2.

FoxT Control Center has a separate installation program. The host where FoxT Control Server is installed is known as the presentation server. The presentation server can be either the BoKS Master, a Server Agent for Unix / Linux host, or another host in the BoKS domain.

Regardless of where you install FoxT Control Center, cookies must be enabled in the browser as FoxT Control Center stores authentication and timeout information in an encrypted cookie.

FoxT Control Center also includes a separate GUI for BoKS password checkout, where authorized users can check out the passwords of other user accounts. This GUI has a separate URL and login page.

Running FoxT Control Center

The following has to be set up:

- The user may authenticate using:
  - Password
  - RSA SecurID token
  - Kerberos password
  - Radius password
  - LDAP authentication
  - YubiKey token as secondary factor
- Master must have a **host certificate** (https - server side SSL)
- User must have a valid Access Rule for the **BCCAS** method, or for BoKS password checkout password checkout access, the PWMGR method.
- The browser must support https
- Cookies must be enabled in the browser

The procedures Installing the Master and Quick Start for FoxT Control Center cover password authentication, host certificate and a BCCAS Access Rule. Support for https and enabling cookies are the only steps you must prepare in advance.

See also:

- Web Browser Requirements
- *Using FoxT Control Center* in the chapter "BoKS Manager Administration" in the *Administration Guide*.

Web-based Administration and Failover

The FoxT Control Center presentation server (BCCPS) can be installed either on the BoKS Master, on another BoKS Server Agent within the domain, or on another host.

The failover procedure in the event that the Master stops responding and you need to convert another host to the Master is different depending whether you have installed the presentation server on the Master or on another host.

If you are running the presentation server on the Master, it is vital that you install the presentation server software on your failover Replica(s) to ensure minimal downtime. For a full description of setting up a failover Replica, see Failover Replica For Disaster Recovery.

However one measure you can take in advance to help minimize any downtime in the event of failover is to add the Master and failover Replica(s) to the same Host Group and ensure that **BCCAS** and, if used, **PWMGR** Access Rules for administration have this Host Group as their destination. This way, **BCCAS** / **PWMGR** Access Rules will continue to work without any changes.

To reconfigure FoxT Control Center presentation server at Master failure (Master installation):

1. Convert your failover Replica to become the Master. See "Recovery Procedures" in the Administration Guide.
2. If required, on the new Master, activate the administration server and ABAC controls. If you have pre-configured these on your failover Replica, the admin server will be started automatically when you convert to the new Master.

   To do this, set the variables `BCCASD=on` and `BCCASD_ABAC=on` in the BoKS **ENV** file and restart the BoKS processes with `Boot`.
3. Ensure that the FoxT Control Center presentation server software is installed on the new Master and that the correct hostname (for the new Master) is specified in the property `AdminServerURL` in the file **bcc.properties**.
4. In the BoKS database, ensure that **BCCAS / PWMGR** Access Rules giving users and/or User Classes access to FoxT Control Center and the BoKS password checkout GUI include the new Master in the **To** part of the Access Rules.

   This is easier if you have defined these rules to a Host Group that contains the Master and failover Replica(s) (see above).
5. Start the presentation server on the new Master.

   On Red Hat use the command:

   ```
   # /etc/init.d/bccps start
   ```

   On Solaris use the command:

   ```
   # svcadm enable bccps
   ```
6. Advise users to point their browsers to the new Master address in order to access FoxT Control Center.

To reconfigure FoxT Control Center presentation server at Master failure (non-Master installation):

1. Convert the new host to the Master. See "Recovery Procedures" in the Administration Guide.
2. If required, on the new Master, activate the administration server and ABAC controls. If you have pre-configured these on your failover Replica, the admin server will be started automatically when you convert to the new Master.

   To do this, set the variables `BCCASD=on` and `BCCASD_ABAC=on` in the BoKS ENV file and restart the BoKS processes with `Boot`.
3. In the BoKS database, ensure that **BCCAS / PWMGR** Access Rules giving users and/or User Classes access to FoxT Control Center and the BoKS password checkout GUI include the new Master in the **To** part of the Access Rules.

This is easier if you have defined these rules to a Host Group that contains the Master and failover Replica(s) (see above).

4. On the presentation server, redirect FoxT Control Center to the new Master.

   To do this, edit the property `AdminServerURL` in the file **bcc.properties**. This file is located by default in **/etc/opt/bccps**. `AdminServerURL` has the format `https://master_hostname:4343/bccas` and you can redirect the presentation server to the new Master by specifying the new Master name in the `master_hostname` part and saving the file.

5. Restart the presentation server.

   Enter the following commands:

```
# /etc/init.d/bccps stop
# /etc/init.d/bccps start
```

Web Browser Requirements

For web browser requirements see the FoxT Control Center Installation Guide for the version of FCC you are installing.

See also:

- Web Administration Requirements
- *Using FoxT Control Center* in the chapter "BoKS Manager Administration" in the *Administration Guide*.

Installation Paths and Deployment Scenarios

This Guide includes two basic procedures for installing BoKS Manager:

- The chapter "Installing BoKS Manager"
- The chapter "Upgrading BoKS Manager"

In addition to the BoKS Manager, or Server, part, this guide also includes instructions for deploying the Server Agents, or Clients:

- *Deploying BoKS Server Agents for Unix/Linux*

Full distribution or patch

BoKS Manager 7.2 is released as a full distribution.

For installing patches, see Installing a BoKS Manager Patch and the patch Readme.

See also:

- Deploying FoxT ServerControl with BoKS Manager

Defining Masters, Replicas and Domain Architecture

This section describes considerations for deciding on where to place Replicas in the network. It also discusses the use of multiple BoKS domains, each with their own Master and Replicas. Topics include:

- Domain Communication Basics
- Placing Replicas for Availability and Load Balancing
- Multiple BoKS Domains

Domain Communication Basics

Communication between BoKS hosts includes the use of IPv4 UDP broadcast and IPv6 UDP link-local multicast by default.. The network must be able to pass BoKS-related traffic between hosts in the domain, regardless of where they reside.

Two key configurations are needed to ensure correct and available communication:

- When the Master, Replica(s) and Server Agent(s) reside on different subnets, Server Agents must have the addresses of at least one Master and/or Replicas, specified in the **$BOKS_etc/bcastaddr** file on Unix/Linux Server Agents. Replicas should have the address of the Master, specified in the **bcastaddr** file on the Replica.
- When two or more BoKS domains operate on the same subnet, they must use different ports, as configured in the **/etc/services** file on the Master, Replica(s) and any BoKS Server Agent for Unix/Linux host(s).

Other configurations that may be needed are:

- All hostnames must be resolvable. BoKS Manager has the capability to use common hostname resolution applications, such as local **/etc/hosts** files, Domain Name Server (DNS), and Network Information Services (NIS/NIS+).
- If BoKS-related traffic will be communicated on networks utilizing firewalls (that is, Server Agents residing outside the firewall), the appropriate ports for this traffic must be opened.
- When a BoKS Server Agent for Unix/Linux host needs to be available in more than one domain, register that host as a BoKS Host in its own domain, and as an Other Host in other domains. Other domains will recognize it as a known, acceptable source host, but will not respond to its requests for authorization from a Master or Replica.

Identify the host's IP address. If nothing else has yet been decided, this will be referred to as the system's primary IP address, the IP address configured for the system's Network Interface Card (NIC). If a host has more than one NIC, the primary NIC must be registered unless you indicate a secondary NIC by adding the settings BRIDGE_ADDR_USE=*IP Address* and NO_IP_CHECK_ON_CALLS=*on* in the **$BOKS_etc/ENV** file on that host.

See also:

- *Communication Basics* in the chapter "System Configuration" in the *Administration Guide*
- *Name Resolution and Firewall Openings* in the chapter "System Configuration" in the *Administration Guide*

Communication Ports

Identify a set of ports to be used for BoKS Manager communication in this domain. By default, BoKS uses 6500 as the base port, plus the next three ports.

If you use non-default ports, the base port must be entered in the **/etc/services** file of all BoKS Server Agents for Unix/Linux within the same domain, or alternatively, you must configure the ENV variable on all Server Agents for Unix/Linux within the domain. See "Setting Base Port" and *Ports for Multiple BoKS Manager Domains* in the chapter "System Configuration" in the *Administration Guide*.

See also:

- *Port Assignment Basics* in the chapter "System Configuration" in the *Administration Guide*

Placing Replicas for Availability and Load Balancing

Replicas are used both for failover backup to the Master and for load balancing.

BoKS Server Agents send their requests for service to their list of BoKS Manager authentication servers (Master and Replicas). They complete the process of authentication and connection to the requested service with the first Master or Replica that responds, if the request is broadcast or sent to more than one configured server (see Domain Communication Basics). Since the Master or any of the Replicas can service a request from any Server Agent, the servers cooperatively manage Server Agent access and continuously implement system load balancing across the security domain.

Failover Replica For Disaster Recovery

To plan for the event that the Master becomes unavailable for a substantial period of time, Fox Technologies strongly recommends that you designate at least one of your Replicas as a failover Replica to back up the Master. In the event that the Master needs to be replaced, it would be this Replica that you would convert to become the new Master, perhaps only until the old Master can be brought back online.

> **NOTE:** All Replicas have copies of the security database and can provide the same authentication and authorization services that the Master provides. However, you can only update the database on the Master. So if you need to do administration, such as adding and deleting user accounts, while the Master is down, you will need to convert a Replica to Master. For details on converting, see *Recovery Procedures* in the chapter "Backup, Restore and Recovery" in the *Administration Guide*.

Failover Replicas require a number of preparatory steps to ensure they can be quickly brought into production as the Master if needed.

The failover Replica should:

- Have an identical BoKS **$BOKS_etc/ENV** file as the Master, with the exception that the `BOKSINIT` variable should be set to `replica` rather than `master`. In addition, the variable `ISMASTER` must NOT be set on the failover Replica.
- Have the same hotfixes installed as are installed on the Master to ensure a smooth transition and equal operation after converting the Replica to the Master.
- If the FCC presentation server is installed on the BoKS Master, the presentation server should also be installed on the failover Replica. The file **/etc/opt/bccps.properties**, should use the hostname for the Master for the `AdminServerURL` attribute and the hostname for the Replica for the `FailoverReplicaURL` attribute. This will ensure automatic failover of FCC services in the event of a Master failure. Note that you can have multiple failover Replicas defined in a comma-separated list for the `FailoverReplicaURL` attribute.

  > **NOTE:** If you have installed the FCC presentation server on a host other than the Master, you need to update the file **/etc/opt/bccps.properties** with the name of the failover Replica in the `FailoverReplicaURL` attribute if it is converted to become the Master.

- Have the following BoKS **ENV** variable settings: `BCCASD=on` and `BCCASD_ABAC=on`. This will ensure that the BoKS admin server is automatically started if the Replica is converted to become the new Master.
- The shared memory size `SHM_SIZE` should be the same and large enough to provide a sufficient amount of free space. Preferably 50% or more recommended. You can check the available space using the command `dumpbase -m`.
- Have a copy of the directory **$BOKS_var/ca** that is identical to the directory on the Master on the failover Replica. This directory contains the PKI infrastructure for BoKS. You can configure the program **push_files** to copy this directory (and other files) to the failover Replica by adding the following lines to the file **$BOKS_etc/distrib.cfg**:

  ```
  SERVERS name_of_failover_replica
  $BOKS_var/ca/*
  ```

  For more information see the BoKS man page **push_files** and the comments in the **distrib.cfg** file.
- The Replica must have a host certificate.
- The **root** account on the Replica must be properly protected - see Root Account on Failover Replica.
- If you are using BoKS password checkout, the Replica must have a copy of the password encryption key **$BOKS_etc/pwm/keys/pwmd.key** identical to the key on the BoKS Master.

In addition, Fox Technologies recommends following these best practices for your failover Replica:

- This Replica should match the configuration of the Master.
- This Replica should be as far removed from the Master as possible, so as not to be affected by the same disaster.
- Define disaster recovery procedures.

- Plan for multiple types of disaster, for example the Master being out of commission, the Master and Replicas being separated for an extended period.
- Practice disaster recovery regularly.
- Use backup to create an archive copy of the database, making sure you follow your organization's record retention policy with the backup.

Root Account on Failover Replica

Plan to protect the root account on this Replica just as you do for the root account on the Master. This might include:

- Restrict knowledge of the **root password** on this Replica to a limited number of administrators.
- Consider creating a **Host Group** for administration that includes only the Master and the Replica that is designated as backup to the Master, so that Access Rules for administration can be easily set up and will already be in place if the Replica needs to be quickly converted to Master.

You need to have a BoKS account for the **root account** on this backup Replica. A BoKS account is needed for administration on any host, but is particularly important to have in place for the backup Replica, since access as root is required during and after conversion, and at a time when you cannot use the Master to add the account to the database. With no local root account in the database, you would need to either work locally on the console or deactivate BoKS Protection.

See also:

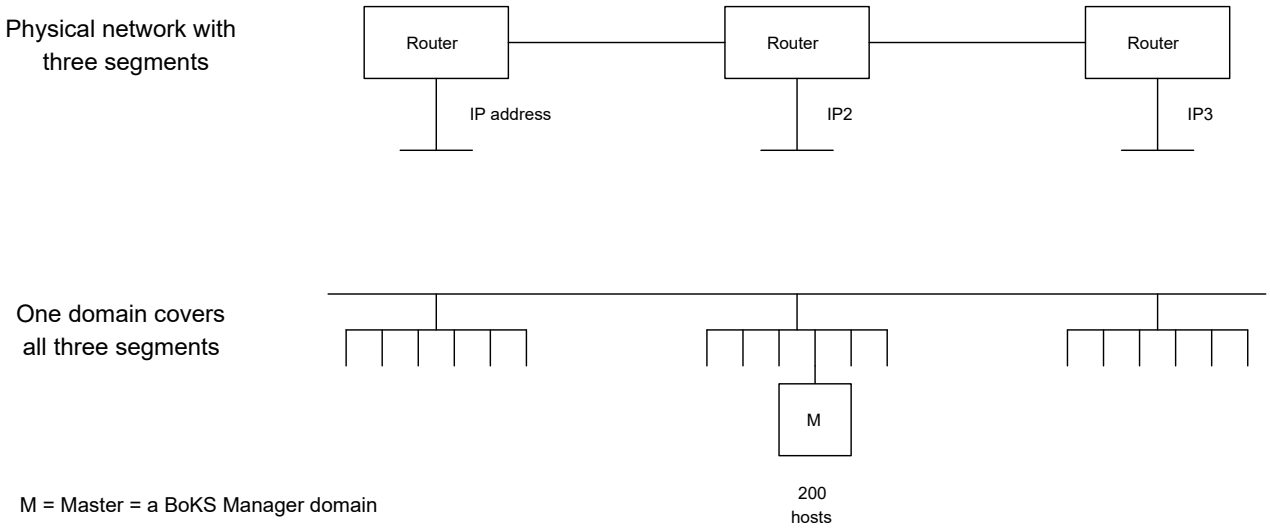
- *About Importing Unix System Accounts* in the chapter "User Administration" in the *Administration Guide*
- Master Basics
- Replica Basics

Load Balancing

This section includes examples on Master / Replica configurations in different network configurations.

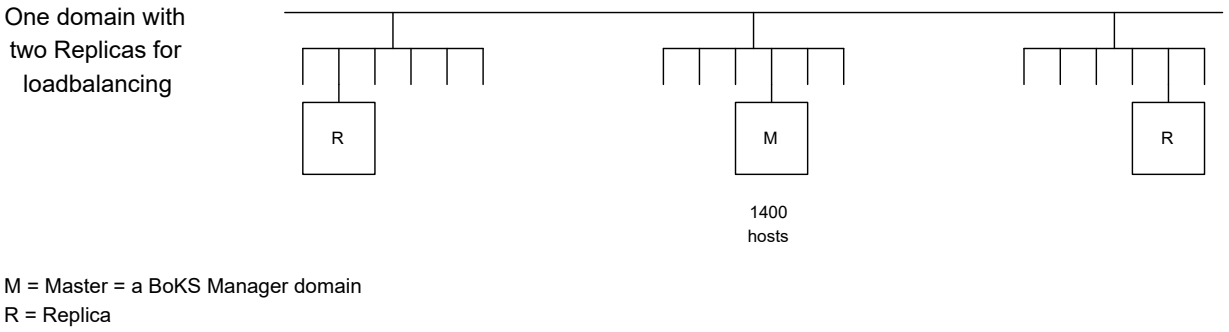
Example: One Master, No Replicas

The network in the example below consists of three segments, with one Master servicing login requests from Server Agents in the entire network.



Example: One Master, One Replica on Each Subnet

The network in the second example, below, includes two Replicas and one Master, each servicing requests from its own network segment. If any Replica or the Master is saturated with requests, a BoKS Server Agent for Unix/Linux may contact a remote Replica or Master for authentication.



As long as at least one Replica is up and running, the security management system is functional. Any Replica can assume the responsibilities of the Master, should the Master fail, ensuring that there are multiple backups available to service user access requests. Both high availability and load balancing become increasingly critical as intranets continue to grow, supporting up to thousands of users logging in to a large security domain.

See also:

- *Configuring the bcastaddr File* in the chapter "System Configuration" in the *Administration Guide*

Multiple BoKS Domains

A BoKS Master with sufficient resources and a sufficient number of Replicas is capable of handling a very large domain. Domain size might eventually become unmanageable with only one domain.

Other reasons to set up multiple BoKS domains include:

- The need for decentralized responsibility
- Interfacing with existing software or organizational structures
- Geographical spread (with both bandwidth and organizational considerations)
- Compartmentalized security, whereby hosts need to be isolated from other users and hosts, or require completely different levels of auditing and control

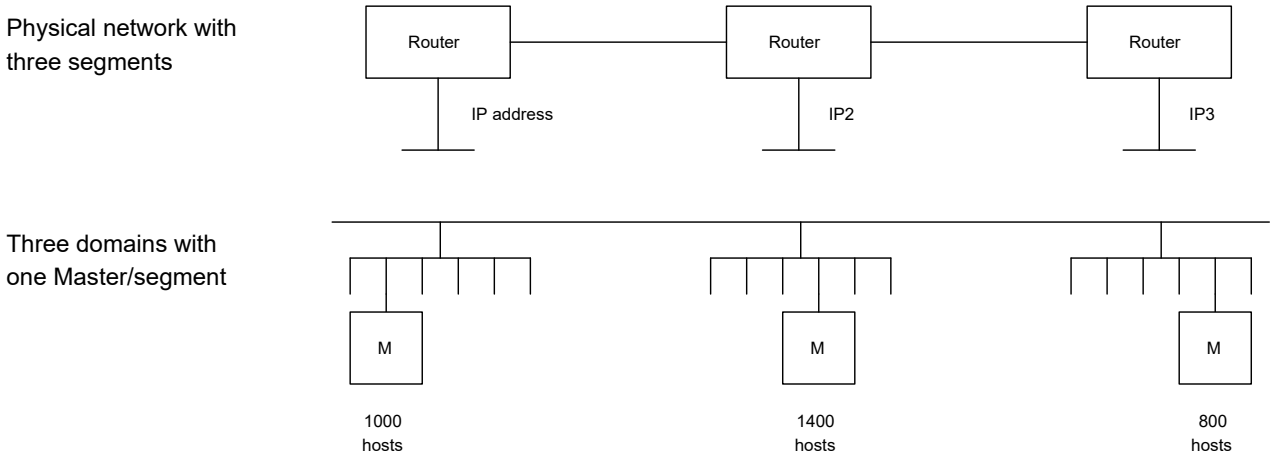
There are no limitations on how to set up BoKS Manager domains, but two key configurations are needed to ensure correct and available communication:

- When a single domain's Master, Replica(s) and BoKS Server Agent for Unix/Linux host(s) reside on different subnets, they must have each other's addresses, which are stored in the **$BOKS_etc/bcastaddr** file on the Master, Replica(s) and BoKS Server Agent for Unix/Linux host(s).
- When two or more domains operate on the same subnet, they must use different ports, as configured in the **/etc/services** file on the Master, Replica(s) and BoKS Server Agent for Unix/Linux host(s).

Fox Technologies recommends that different ports **always** be used for different domains even when the domains operate on separate subnets. This creates a failsafe environment for the different BoKS Masters and their respective domains in the event of router programming mishaps, network cables being inadvertently plugged into the wrong connector, and so on.

Example: One Master on Each Subnet

Each subnet in the example below is a domain with its own Master servicing requests from Server Agents within the subnet. No address or port configuration is necessary although it may be recommended.



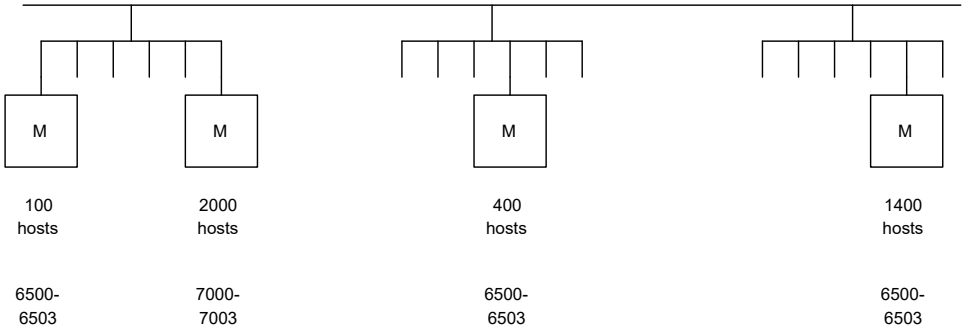
M = Master = a BoKS Manager domain
R = Replica

If you are defining multiple domains (with one Master per domain) on the same subnet, you must assign different communication ports to the hosts located in each separate domain. In other words, you will have different ports per domain, but the same port will be assigned to the Master, Replicas and all Server Agents within each Master's domain. For example, if you have two Masters, you would assign one port for the first Master and all its Server Agents, and one port for the second Master and all its Server Agents.

Example: Two Masters on the Same Subnet

One of the subnets in the example below contains two BoKS domains, possibly for decentralized management or for compartmentalized security. All BoKS hosts in one of the domains must be configured to use a set of ports different from the default ports (6500-6503), so that their communications do not collide.

Four domains, including two domains on one segment



M = Master = a BoKS Manager domain
R = Replica

In summary, set up BoKS domains first according to organizational needs and existing infrastructure, and secondly for availability.

See also:

- *Configuring the bcastaddr File* in the chapter "System Configuration" in the *Administration Guide*
- *Ports for Multiple BoKS Manager Domains* in the chapter "System Configuration" in the *Administration Guide*

Preparing Node Keys, User Accounts and Host Groups

Topics include:

- Node Keys
- Host Groups Planning
- Local Root Account in BoKS Manager
- Preparing User Accounts

See also:

- Basic Configuration of BoKS Manager
- Importing Users and Hosts into the Database

Node Keys

Each Master, Replica and BoKS Server Agent for Unix/Linux host has a node key. Node keys are used to encrypt security-related communication between these hosts and for encrypted communication using Telnet between UNIX hosts.

You create node keys when you set up BoKS Manager to be a Master, Replica, or BoKS Server Agent for Unix/Linux host. When the host is added (registered) in the security database you must provide the node key. The node key defined at installation (setup) and the node key specified later for registering in the security database must be identical. See To install BoKS Manager on the Master:.

Node Key Reminders

- It is vital to keep node keys secret.
- Node keys are only needed during installation and upgrade and when you register the host in BoKS Manager.
- Best are long, random sequences of characters. If the nodekey is changed it must be updated both locally on the Server Agent using the **hostkey** command and in the BoKS database using FoxT Control Center or the **hostkey** command on the Master.

See also:

- *Node Keys* in the chapter "Host" in the *Administration Guide*.

HostIDs

For environments featuring DHCP support and dynamic IP addresses, BoKS Server Agents have HostIDs. These are used instead of the IP address to identify the host. HostIDs should be unique identifiers for a host within the BoKS domain.

See also:

HostIDs in the chapter in the chapter "Host" in the *Administration Guide*.

Host Groups Planning

In BoKS Manager, each user is assigned to a host or Host Group. If the user is assigned to a BoKS Server Agent for Unix/Linux 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 group memberships) is created on all BoKS Server Agent for Unix/Linux hosts included in the Host Group.

Hosts can be gathered into **Host Groups,** based on common access needs, to simplify access control and user management. For example, when hosts are grouped by access needs, you can specify an

Access Rule by simply specifying the group instead of all the individual host members. See the chapters *A Guided Tour* and *Host* in the *Administration Guide*.

You can use UNIX groups and other host or user groupings that currently exist in your network as a basis for defining the Host Groups you want to set up for your BoKS domain.

See also:

- *Using Host Groups for User Administration* in the chapter "A Guided Tour" in the *Administration Guide*
- *Using Host Groups for Access Control* in the chapter "A Guided Tour" in the *Administration Guide*
- *Node Keys* in the chapter "Host" in the *Administration Guide*

Host Root Account Necessary

When you register a UNIX host in BoKS Manager, you often import some of the system accounts, especially the root account, into BoKS. This is necessary in order to do administration on that host.

See also:

- *About Importing Unix System Accounts* in the chapter "User Administration" in the *Administration Guide*
- Root Account
- Root Account on Failover Replica
- BoKS Server Agent for Unix/Linux Basics

Local Root Account in BoKS Manager

Fox Technologies recommends that you have a BoKS Manager account for the **root account** on any Replica or BoKS Server Agent for Unix/Linux. A BoKS Manager account is needed for administration on the host.

As with all BoKS accounts, you can prefix the root account with either the local hostname or the Host Group name. While there are advantages to using Host Group for many user accounts, Fox Technologies recommends you use the local hostname as prefix for system accounts and particularly the root account. That is, create the root account as *hostname*:root, where *hostname* is the hostname of the host.

See also:

- root as a role on Solaris
- *About Importing Unix System Accounts* in the chapter "User Administration" in the *Administration Guide*

Preparing User Accounts

User ID Synchronization

BoKS Manager identifies a user with the notation host:username or hostgroup:username. BoKS requires unique usernames within each host or Host Group, but allows non-unique names in Host Groups that have no hosts in common, that is, that are disjoint. 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.

In BoKS Manager 6.6.2 and later you can configure checking for overlapping user accounts that could potentially be created by various operations. For details, see the *BoKS Manager Administration Guide*.

Group ID Synchronization

Synchronization concerns regarding UIDs also apply to UNIX GIDs. Before BoKS Manager is implemented, a common **/etc/group** file should exist, including all UNIX platforms in the domain. If the UNIX group information is stored in NIS or NIS+ instead of **/etc/group** this synchronization is applied automatically.

See also:

- *Using Host Groups for User Administration* in the chapter "A Guided Tour" in the *Administration Guide*.
- *Unique Usernames within a Host Group* in the chapter "User Administration" in the *Administration Guide*

Deploying FoxT ServerControl with BoKS Manager

This section applies to initial installation. For upgrade, see the chapter *Upgrading BoKS Manager*.

To Deploy a FoxT Solution with BoKS Manager:

1. Prepare for the domain deployment process by reviewing and completing your plans, including selection of hosts to be the BoKS Manager Master (Master) and Replica(s), definition of user accounts, User Classes, Host Groups, and security policies. You can use the checklist in Pre-Deployment Checklist.
2. Install the Master and configure the BoKS Manager domain. See Installing BoKS Manager on a Master.
3. Install the Replica(s). See Installing BoKS Manager on a Replica.
4. Install the BoKS Server Agent host(s). For details, see the chapter *Deploying BoKS Server Agents for Unix/Linux*.
5. Test communications and troubleshoot access from the various Server Agents. For tools and

procedures, see:

- The appendix "Troubleshooting" in the *Administration Guide*
- The appendix "System Monitoring Tools" in the *Administration Guide*
- Using Learn Mode

6. After you are convinced that everything is working correctly, enable highest BoKS security on each respective host by **activating BoKS Protection**. Note that this applies to the Master and Replicas as well as to Server Agents.

Optionally, you may wish to allow users to temporarily access hosts without Access Rules. See Using Learn Mode .

Groupwise Deployment

During deployment, a common approach to maximize availability is to install one network segment at a time, first testing communications and configuration with a test host acting in conjunction with the Master or Replica. Once the test Server Agent works with the Master or Replica, then the other Server Agents can be installed using the same configuration.

See also:

- Pre-Deployment Checklist
- Installation Paths and Deployment Scenarios
- Installing Hotfixes, Patches and Upgrades using boks_upgrade

Pre-Deployment Checklist

Prior to deployment, perform the following tasks to ensure a smooth installation:

- Identify a machine to be used as the BoKS Master and note its IP address (unless otherwise noted, *IP address* refers to the system's primary IP address). See Master Basics.
- Identify one or more hosts to be BoKS Replicas, based on the initial deployment criteria, and list their hostnames and IP addresses.
- Ensure that all machines on which the BoKS Manager software is to be installed have sufficient disk space. See System Requirements.
- See Web Browser Requirements for details on supported web browsers for performing BoKS Manager Administration through the network and on Windows workstations in the domain. You can also run BoKS Administration using the command line programs, from a terminal window on the BoKS Master with the appropriate Access Rule to the Master and **su** to root privilege.
- Determine the format of the node keys. Node keys should be long and random, and kept in a secure location. See Node Keys.
- Develop a naming convention for Host Groups and User Classes to make it easier to distinguish hosts from Host Groups and users from User Classes.

Note: The name of the predefined Host Group `ALL` is in upper case letters, a convention also recommended for User Classes and Host Groups that you create.

- If you are using non-default ports, identify a base port for BoKS Manager communication. See Domain Communication Basics. Enter the base port in the **/etc/services** file of all UNIX systems within the same domain, for example:

  ```
  boks 7000/tcp
  ```

  where 7000 is the desired base port number.

- If any BoKS Server Agent for Unix/Linux hosts reside on the other side of a firewall, open two communication ports at the firewall, for example 6502 through 6503 if you are using BoKS Manager default ports, to allow both TCP and UDP traffic. See Domain Communication Basics.
- If Domain Name System (DNS) is to be used for name resolution, verify that it is working properly and able to perform accurate forward and reverse lookups.

  If DNS is not used for host resolution, then the **/etc/hosts** files on each UNIX system must be complete and consistent.

- If NIS or NIS+ is used for password or host file management on UNIX hosts, verify that it is working properly.
- If NIS is not used to manage the **/etc/passwd** file and users have accounts on multiple systems, clean up user accounts to ensure the following:
- Users should not have conflicting User Identifier (UID) numbers between systems. For example, a specific user with UID of 1500 should have a UID of 1500 across all systems.
- Group Identifier (GID) numbers and names should be consistent across all systems.
- Identify a person or group of people who will have full-time responsibility to manage the BoKS domain. Decide on other administrators who will be designated Sub-Administrators and have limited management rights, and specify those rights, including which hosts and users that they will manage.
- If SecurID authentication is to be used, ensure that the RSA Authentication Manager is up and running, and install the RSA authentication agent configuration file **AM_Config.zip** on each BoKS Master / Replica and Server Agent host that should use SecurID authentication. See *Configuring Hosts for SecurID Authentication* in the chapter "Managing Authenticators" in the *Administration Guide*.
- If Radius or Yubikey authentication is to be used, ensure that the appropriate servers are configured and operational, and that you have configured BoKS for communication with these servers. See the chapter "Managing Authenticators" in the *Administration Guide*.

Installing BoKS Manager

Installing BoKS Manager covers installing BoKS Manager on a Master or Replica, and doing basic configuration of these servers and the BoKS domain.

Topics include:

See also:

- The chapter "Upgrading BoKS Manager"
- The chapter "Planning Installation"
- The chapter "System Configuration" in the *Administration Guide*
- The Readme, which contains platform-specific installation information.

Install Background

Install Background includes the topics:

See also:

- The chapter "Upgrading BoKS Manager"
- The chapter "Planning Installation"

Package Contents

BoKS Manager and BoKS Server Agent for Unix/Linux 7.2 is delivered as a web download file from the Fox Technologies web site. Separate download files are available for each platform supported.

All packages are delivered as tar archives. In addition, BoKS Server Agent packages are also delivered in native package format that differs from OS to OS, for example RPM packages.

For the tar archives, you must unpack the package into an appropriate directory. For details, see Unpacking the Package Contents.

The unpacked tar archive packages for BoKS Manager and BoKS Server Agent for Unix/Linux contain the following:

BoKS Manager / BoKS Server Agent for Unix/Linux Package Directory Structure

Directory	Sub-directories and files	Description
root directory	install	Installation program for BoKS Manager 7.2
	platformname/ for example, Solaris	Directory used by the installation program. Contains full product program files for this platform, in archived format.
	/acknowledgments	Directory containing acknowledgment and license information for third-party products included in the distribution.
	upgrade_client	program that upgrades an older BoKS Server Agent to a specified later version of Server Agent for Unix/Linux.
	prog/	Contains upgrade utilities used by upgrade_client: **boks_uname, program that determines the operating system on the host** **pre_upgrade**, a script to back up data before upgrading **upgrade_version**, a script to upgrade files on an older BoKS Server Agent to format for BoKS Server Agent for Unix/Linux version 7.2
	README	An empty file. The Readme is now available on the Fox Technologies Support web site as a separate download. It is updated periodically and contains latest on-going information.
	License.txt	Fox Technologies License Agreement

Unpacking the Package Contents

Note that the information in this section applies only to the tar archive packages, not the native packages (RPM etc.).

Packages are delivered in archive format, and must be unpacked before installation can be run.

For information on the top level directory structure, including full distribution installation, licensing and documentation, see Package Contents. For information on the patch installation directory (for releases that include a patch level), see Patch Directory Structure.

To unpack the full package contents:

1. Save the archive file in a temporary directory. For example:

   ```
   hostname# cp BoKS72-Solaris-2.11-sparc.tar.gz /tmp
   ```

2. Move to the temporary directory. For example:

   ```
   hostname# cd /tmp
   ```

3. Unpack the archive file. For example:

   ```
   hostname# gunzip BoKS72-Solaris-2.11-sparc.tar.gz
   ```

4. Unpack the archive. For example:

   ```
   hostname# tar -xvf BoKS72-Solaris-2.11-sparc.tar
   ```

   A directory structure is created.

The untarred directory varies somewhat by platform, but has the general contents described below:

Patch Directory Structure

Directory	Sub-directories and files	Description
boksm_patch/	backoutpatch	Program to roll back the patch installation to the previously installed version.
	fmode	Used by installpatch to check file modes.
	fsinfo	Used by installpatch to check that there is enough disk space for installation.
	installpatch	Installation program for the BoKS Manager 7.2 patch.
	boksm	Directory that contains new versions of the files to be patched.
	patchname .patchmap	List of files that are patched for this patch, *patchname*.
	patchinfo	Lists various parameters for the patch, for example version and size.
	boks_uname	Program that determines the operating system on the host.
	README	An empty file. Readme issues for all platforms are included in the top-level README available on the Fox Technologies web site.

Install Directories

BoKS Manager software resides in the major directories listed below, either user-specified or default directories. Once installed, you can use the **$BOKS** directory names in the command line to refer to the corresponding directory. These names are used throughout the documentation to refer to the directories.

- BoKS Server Agent for Unix/Linux has the same directory structure, although Server Agents do not contain all components.

For further detail, see *Directory Structure in BoKS Manager* in the appendix "System Architecture" in the *Administration Guide*.

Directory	Default Directory	Description
$BOKS_DIR	/opt/boksm	BoKS directory
$BOKS_bin	/opt/boksm/bin	Executable programs for non-administrators (for example **xdl** and **suexec**).
$BOKS_sbin	/opt/boksm/sbin	**boksadm** and other programs for managing BoKS Manager.
$BOKS_lib	/opt/boksm/lib	Various programs and scripts used internally by BoKS Manager, and some less frequently used CLI programs.
$BOKS_man	/opt/boksm/man	Man pages for BoKS commands. Make sure to have your MANPATH variable set to include /opt/boksm/man.
$BOKS_etc	/etc/opt/boksm (/opt/boksm/etc for native package installations)	The configuration directory
$BOKS_var	/var/opt/boksm (/opt/boksm/var for native package installations)	Includes the security database, logs and variable data such as temporary files for integrity checks, etc. Note that if you specify this as a mount point the uninstall program does not remove all files and directories and these must be removed manually.
$BOKS_data	/var/opt/boksm/data (/opt/boksm/var/data for native package installations)	The database files which grow
$BOKS_ unipc	$BOKS_var/unipc or /var/opt/boksm/unipc (/opt/boksm/var/unipc for native package installations)	UNIX domain IPC socket directory. Default location $BOKS_var/unipc changes if $BOKS_var path name is longer than 80 characters. See *$BOKS_ unipc* in the chapter *System Architecture* in the **Administration Guide**.

See also:

- *BoKS Environment Variables* in the chapter "BoKS Manager Administration" in the *Administration Guide*
- Install Parameters and Options
- BoKS Manager Package Directory Structure
- Unpacking the Package Contents

Install Parameters and Options

Note that the information in this section applies only to the tar archive packages, not the native packages (RPM etc.).

You can run the install program with no options:

./install

or you can use some of the optional flags and parameters as described below.

Install Usage and Options:

install [-<id> <path>][-patchdir <dir>][-s type]
[-bcastaddr <file> | -Bcastaddr "<addr1>, <addr2> ..."]

install [-<id> <path>]
[-p] [-u <uid>] [-g <gid>]
[-s <type> -n <nodekey> -i <interface> -h <%hostid> [-bcastaddr <file> | -Bcastaddr "<addr1>, <addr2> ..."] -q -f
[-r product_number] [product_and_OS_ARCH]

- `-<id><path>` sets Install Directory paths from the command line for the three BoKS install directories with **id's** of opt, var and etc. For example, using these flags, you might install in:

  ```
  -opt /usr/opt/boksm
  ```

  ```
  -var /usr/var/boksm
  ```

  ```
  -etc /usr/etc/boksm
  ```

  If you do not use the flags, the install program will prompt you individually for each directory and provide a default for each that you can simply accept.

- `-patchdir <dir>` sets the directory where patches are stored
- `-p` activates SSH privilege separation by setting the parameter `UsePrivilegeSeparation` to `yes` in the **sshd_config..active** and **sshd_config..inactive** files
- `-u <uid>` optionally specifies a uid for the sshd user account, a special user account needed by the sshd daemon when privilege separation is enabled and
- `-g <gid>` optionally specifies a gid for the sshd user account.

  Without `-u` or `-g`, the system takes the next available uid and gid, respectively.

For details and creating this account manually instead, see *Configuring Privilege Separation* in the chapter *System Configuration* in the **Administration Guide**.

- `-q` runs in quiet mode, i.e., non-interactive. This requires the `-s` and `-n` flags.
- `-s <type>` runs **setup** BoKS Manager after install with the specified type where `<type>` is one of **master**, **replica** or **client**.
- `[-bcastaddr <file> | -Bcastaddr "<addr1>, <addr2> ..."]` is used to specify either the path to a **bcastaddr** file containing address information for the Master / Replicas, or a list of addresses if using the `-Bcastaddr` option. For more information on **bcastaddr**, see Domain Communication Basics and "Configuring the bcastaddr File" in the Administration Guide.
- `-n <nodekey>` provides the node key `<nodekey>` when setting up BoKS Manager.

  Used together with `-s` and `-q`.

  > **NOTE:** Using "`-n <nodekey>`" is a security risk, as the node key can be captured in real time during install by, for example, `ps -ef | grep install`.

- `-f`, setup does not prompt whether to remove group passwords, but removes any existing group passwords automatically.

  For more details, see About Group Passwords on Unix/Linux.

- `-i <interface>` specifies the network interface to be monitored for changes in IP address.

  Used together with -s, for BoKS Server Agents with dynamic IP address only.

- `-h <%hostid>` provides the HostID for the host.

  Note that the HostID must start with a % sign.

  Use together with `-s`, for BoKS Server Agents with dynamic IP address only.

- `-Bcastaddr <IP address of the BoKS Master>` specifies where on the network the host can locate the Master.

  Used together with `-s`, for BoKS Server Agents with dynamic IP address only.

- `-r <product_number>` select the product to install in the options list presented during interactive install (usually 1 = the product name, 2 = Quit). Most common is to use `-r 1`, which saves the interactive question to install or quit.
- `<product_and_OS_ARCH>`, for example,

  ```
  ./install boksm_d-6.6-Solaris-2.10-i386
  ```

  (the first part of the name of the files on the OS directory you want). This can be used to force an installation on a later release of an OS than the one Fox Technologies supported when that BoKS Manager version was released.

- `-v` installs in verbose mode.

> **NOTE:** Options for installing hosts with DHCP only apply for BoKS Server Agents - it is not supported to have a DHCP Master or Replicas, which must have static IP addresses.

When installing and setting up a DHCP BoKS Server Agent, you must specify the `-i` and `-h` options so that communication works with the BoKS Master. Note that the HostID specified using `-h <%hostid>` must match the HostID specified for the host when it is registered in the BoKS database. An example command to register the host `host1` as a DHCP Server Agent is:

```
[root@host1 BoKS67]# ./install -s client -n host1 -i eth0 -h %host1
\
-q -Bcastaddr 10.131.112.34
```

See also:

- Install Directories
- Unpacking the Package Contents
- Setup Parameters and Options

Setup Parameters and Options

The **setup** program is used after installing the BoKS Manager software (either from the tar archive or using a native package such as RPM) to select the host's role in the BoKS domain: BoKS Master, BoKS Replica or BoKS Server Agent. BoKS Server Agents have traditionally been referred to as BoKS Clients or simply Clients. Thus the term "Client" is a synonym for Server Agent. For more detailed information about the program options, see the BoKS man page **setup**.

Setup Usage and Options:

setup [-f] [-g *gid*] [-h *hostid* -i *if*] [-k] [-n *nodekey*] [{ -O | -o } '*service1 service2* ...'] [-p] [-u *uid*] [-v] client
setup -a [-A *par=val*] [-f] [-g *gid*] [-h *hostid* -i *if*] [-k] [-n *nodekey*] [{ -O | -o } '*service1 service2* ...'] [-p] [-u *uid*] [-v] client
setup [-f] [-g *gid*] [-k] [-n *nodekey*] [-p] [-u *uid*] [-v] replica
setup [-f] [-g *gid*] [-k] [-N] [-n *nodekey*] [-p] [-u *uid*] [-v] master

The options you can use with the setup program are as follows:

- `-A par=val` are arguments to the boks_autoregister client program. The -A option can be given multiple times to enter multiple arguments. Arguments are parameter=value pairs. For details see Installing a Pre-registered Host.
- `-a` setup and register pre-registered host with boks_autoregister program.
- `-f` is used to force removal of any group passwords without prompting. For more details, see About Group Passwords on Unix/Linux.
- `-g gid` create the **sshd** group with the gid `<gid>`.
- `-h hostid` set hostid for Server Agents using dynamic IP address. Note that the HostID must start with a % sign.
- `-i if` set network interface name for Server Agents using dynamic IP address.
- `-k` don't create SSH hostkey.
- `-N` when setting up the Master, enforce the use of the automatically selected hostname and address without prompting.

- `-n nodekey` set host nodekey, so it is not prompted for during setup.

  > **NOTE:** This option is not recommended for use in multi-user production environments as arguments given on the command line can be seen by other users using the **ps** command while the **setup** program is running.

- `-O | -o 'service1 service2'...` Enable offline support for the listed services. Use -O to enable offline support for the root user and -o to enable offline support for ordinary users.
- `-p` set up sshd to run in privilege separation mode.
- `-u uid` create sshd user with uid *uid*.
- `-v` run setup in verbose mode.

> **NOTE:** Options for setting up hosts with DHCP only apply for BoKS Server Agents - it is not supported to have a DHCP Master or Replicas, which must have static IP addresses.

When setting up a DHCP BoKS Server Agent, you must specify the `-i` and `-h` options so that communication works with the BoKS Master. Note that the HostID specified using `-h <%hostid>` must match the HostID specified for the host when it is registered in the BoKS database.

See also:

- Install Directories
- Unpacking the Package Contents
- Install Parameters and Options

Licensing Background

In order to activate BoKS Manager, a valid Fox Technologies license is required. The license is delivered as a file from Fox Technologies after you have installed the BoKS Master. When you set up the Master a **domain id** is generated that uniquely designates the new domain. The domain id is then used by Fox Technologies customer support to create the license for your domain.

Your license specifies the number of hosts of each host type that are allowed in the domain, and may also specify the amount of time BoKS can be used (time-limited license). You can have more than one license in the BoKS database at any one time, and as long as there is at least one valid license in the database, and you are not exceeding the number of hosts of that type allowed, adding a host is allowed.

The license acquisition process works as follows:

1. You install and set up BoKS Manager on your Master. This provides you with the **domain id**.
2. Send the domain id to Fox Technologies customer support.
3. Fox Technologies customer support provides you with a license file based on the domain id.
4. Import the license file to your database using the program `$BOKS_sbin/bokslicense`.

You can also list licenses available in your domain using `bokslicense`. FoxT Control Center also displays information about licensing for the domain.

To retrieve the domain id:

1. Install BoKS Manager and run the Master set up.
2. Log in to the BoKS Master and become root.
3. Start a BoKS shell

   For example:

   ```
   # /opt/boksm/sbin/boksadm
   ```
4. Either:
   - Run the **bksdef** command.

     For example:

     ```
     BoKS # bksdef
     ```

     The domain id is displayed at the bottom of the informational listing about the BoKS global settings.
   - Open the file **$BOKS_etc/domain.id**, which contains the string for the domain id.

     For example:

     ```
     BoKS # cat $BOKS_etc/domain.id
     ```

To import a license file:

1. Log in to the BoKS Master and become root.
2. Ensure that a valid license file is available for import on the Master.
3. Start a BoKS shell.

   For example:

   ```
   # /opt/boksm/sbin/boksadm
   BoKS #
   ```
4. Run the **bokslicense** program with the `-i` option and path to the license file as arguments.

   For example:

   ```
   BoKS # bokslicense -i < /tmp/bokslic1.lic
   ```

   Where `bokslic1.lic` is the signed license file to be imported.

To remove a license file:

1. Log in to the BoKS Master and become root.
2. Start a BoKS shell.

   For example:

   ```
   # /opt/boksm/sbin/boksadm
   BoKS #
   ```

3. Run the **bokslicense** program with the `-r` option and path to the license file as arguments.

   For example:

   ```
   BoKS # bokslicense -r <signature>
   ```

   Where `<signature>` is signature of the license to be removed.

To list information about licenses in the domain:

1. Log in to the BoKS Master and become root.
2. Ensure that a valid license file is available for import on the Master.
3. Start a BoKS shell.

   For example:

   ```
   # /opt/boksm/sbin/boksadm
   BoKS #
   ```

4. Run the **bokslicense** program with either the `-l`, `-y` or -s option, where:

   - `-l` lists the license in a reading friendly format and
   - `-y` lists the license in yaml format
   - `-s` displays a summary of the current licensing status for the domain

   Note that if you have multiple licenses, the licenses are listed on after another.

   For example:

   ```
   BoKS # bokslicense -l
   Installed licenses
   ------------------
   <customer name>
   Signature: kY9Jhfe+/fro967Hl#jI...
   Expires: never
   Hosts          cur./max   (+ grace)
   -----          --------   ---------
   UNIXBOKSHOST     100/500  (+ 20) In compliance
   REPLICA           2/5     (+ 0)  In compliance
   ```

   or

   ```
   BoKS # bokslicense -y
   licensee: <customer name>
   comment: <A descriptive comment>
   domain_id: <domain id>
   expiry_date: <expiry date>
   hosts:
   - type: UNIXBOKSHOST
     amount: <number of unix hosts>
     grace_amount: <number of allowed extra hosts during
   ```

```
       grace period>
enforced: <yes or no>
grace_period: <grace period>
obsoletes: <base64 encoded signature or nil>
message_digest: <digest algorithm, e.g. sha512>
signature: <base64 encoded signature>
```

In the license listing, the following key parameters can be seen:

- `grace_period`: the number of days after the first violation of licensed number of hosts before license enforcement begins.
- `grace_amount`: per host type, the number of hosts allowed to be registered over and above the licensed amount during the grace period.
- `amount`: per host type, the number of hosts allowed to be registered under the license
- `obsoletes`: lists the signatures of older licenses that are replaced by the current license.

The BoKS Manager Default License

BoKS Manager includes a special default license that ensures you can install a limited number of hosts . This license is not tied to a domain id and is designed so that you can get the first few hosts in your basic domain up and running without licensing restrictions stopping this.

You do not have to import this license into the BoKS database.

The default license is named `boks_default_license.lic` and is stored in **$BOKS_etc** (by default **/etc/opt/boksm**).

License Enforcement

Licenses can be limited in the number of hosts allowed and can also be time-limited, i.e. they can expire at a certain date.

The licensing system counts the number of hosts of a particular license type in the database.

Adding a host is allowed if there is a license that, for that host type,

- is not expired, and
- allows for more hosts than the count found in the database (or is in grace period and the number of hosts is below the grace limit)

or

- is not enforced

Adding a User Class or a Host Group is allowed if, for each host type, there is a license that

- is not expired, and
- allows for more hosts than the count found in the database (or is in grace period and the number of hosts is below the grace limit)

or

- is not enforced

IMPORTANT: If you experience limitations in BoKS functionality due to licensing enforcement, contact your FoxT, a HelpSystems Company, representative for assistance in resolving the issues.

License Grace Period

Should you exceed the number of permitted registered hosts in the BoKS database as specified in your license, a grace period begins giving you time to purchase additional licenses as required. The grace period time depends on the specifics of your license, and is counted from the time the first additional host is registered, also known as the "date of first violation".

Important: The grace period does **not** apply to expired licenses. If the license has expired, even if it is within the grace period, adding new hosts, Host Groups and User Classes will be prohibited until the license is made current.

When you register the first additional host, the grace period begins. During the grace period, you can continue to register hosts within the number limit specified by your license, however each time you register a host you are notified that you have exceeded the number of licensed hosts.

At the end of the grace period, you can no longer register any new hosts until you either purchase additional licenses or remove some other hosts to free up license berths.

Upgrading, Restoring an Unlicensed Database

If you upgrade to BoKS Manager 7.2 from an earlier version that does not include licensing controls, the domain id which is generated when you install the version 7.2 BoKS Master is imported into the BoKS database from the file **$BOKS_etc/domain.id** when you restore your old database as part of the upgrade.

However, no licenses have at this stage been imported to the database, so you must first import the default license (**$BOKS_etc/boks_default_license.lic**).

Note that once you have restored the old database, you must send the domain id file to Fox Technologies customer support in order to obtain your license file that you can then also import into the BoKS database.

If at a later point you need to restore your earlier version BoKS database, the domain id for your license is again imported into the restored database from the file. You must then re-import the default license file and your license file into the BoKS database.

If you restore a database that has a different domain id from that in the **$BOKS_etc/domain.id** file, the file is overwritten with the domain id from the database in order to ensure that this file is kept up to date.

Licensing Logging

The following licensing-related events are recorded in the BoKS audit log:

- When a license is imported using **bokslicense**.
- When a license is removed using **bokslicense**.
- When a host is registered causing licensing limits to be reached (note that this and other registration operations can be an auto-registration of a host pre-registration or a change in host type for an already registered host).
- When a host is registered causing licensing limits to be further exceeded during the grace period.
- When a host is registered but the license is due to expire in 30 days or less.
- When a host is removed causing licensing limits to be reached (i.e. licensing limits are no longer exceeded).
- When a host is removed but the license is due to expire in 30 days or less.
- A daily message is written to the log when the license has expired or is due to expire in 30 days or less (this is the result of a **boks_cron** check on the license status set to run each night).

Note: Audit log messages relating to the license having expired or having 30 days or less to expiry are by default configured as alarmlogs.

See also:

- Installing the Master

Configuring Multiple Domains on the Same Subnet

All BoKS communication uses the TCP/UDP ports 6500 through 6503 by default. *See* Domain Communication Basics. With multiple domains, the IPv4 UDP broadcast and IPv6 UDP link-local multicast can cause problems. If you want to install a second or third domain on the same network, you must use another set of four consecutive ports for each domain by altering the **/etc/services** file, so that the UDP broadcasts/multicast from the different domains do not collide. Do this on all BoKS hosts that belong to the second, third, etc. domains (Master, Replicas, and BoKS Server Agent for Unix/Linux hosts).

See also:

- *Ports for Multiple BoKS Manager Domains* in the chapter "System Configuration" in the *Administration Guide*

To install a second Master on a network:

1. Add a line with the following syntax to the **/etc/services** file:

   ```
   boks portnumber/tcp
   ```

   Example:

```
boks 6530/tcp
```

You can use any available number that has at least four consecutive free port numbers; for instance, in the example above 6530, 6531, 6532, and 6533 must all be available. Note that this will not work if NIS or NIS+ is used for network service lookup.

2. Follow the instructions in To install BoKS Manager on the Master:.

To install Replicas in a second BoKS Manager domain:

1. Add a line with the following syntax to the **/etc/services** file:

```
boks portnumber/tcp
```

where portnumber is the same as in the **/etc/services** file on the Master

Example:

```
boks 6530/tcp
```

2. Follow the instructions in Installing a Replica.

To install BoKS Server Agent for Unix/Linux hosts in a second domain:

1. Add a line with the following syntax to the **/etc/services** file:

```
boks portnumber/tcp
```

where portnumber is the same as in the **/etc/services** file on the Master

Example:

```
boks 6530/tcp
```

2. Follow the instructions in Installing BoKS Server Agent for Unix/Linux.

NOTE: An alternative way of separating BoKS domain port usage is the `BRIDGE_DOMAIN` variable in **$BOKS_etc/ENV**, see the **ENV(4B)** man page.

About Group Passwords on Unix/Linux

BoKS Manager and BoKS Server Agent for Unix/Linux do not support the use of group passwords on Unix and Linux platforms. Therefore any existing group passwords must be removed from the **/etc/group** file before installing BoKS Manager / BoKS Server Agent for Unix/Linux. In addition, if shadowed group passwords are in use, in for example an **/etc/gshadow** file, the entire **gshadow** file must be removed.

When you run **setup**, you are prompted to confirm the removal of any group passwords configured on the host. If you opt not to remove group passwords, the setup procedure is not completed. This leaves the system in a state where BoKS is installed, but not set up. Setup can be performed at a later time.

You can stop **setup** from prompting whether to remove group passwords, and automatically remove them, by specifying the **-f** option to the setup program. You can also specify **-f** to the **install** program (tar archive install only), in which case the option is passed to the **setup** program causing it not to prompt asking whether group passwords should be removed, but removing them automatically.

See also:

- Install Parameters and Options

Installation Issues on Specific Platforms

This section describes issues that are only relevant on a limited number of platforms. For late-breaking platform-specific installation issues, see the BoKS Manager README, available for download from the Fox Technologies web site.

It includes the following topics:

- Installation Issues on Oracle Solaris
- Installation Issues on Linux
- Installation Issues on Red Hat With SELinux

Installation Issues on Oracle Solaris

Installation issues on Oracle Solaris includes the following topics:

- root as a role on Solaris
- BoKS tty lock Issues

root as a role on Solaris

BoKS versions earlier than 7.2 did not support having the root account defined as a role on Solaris hosts. In BoKS version 7.2 and later, root can be a role. When activated BoKS takes control of login, thus if a matching Access Rule exists it is possible to log in directly to the root account even if it is a role. Similarly since BoKS controls su access, BoKS Access Rules determine which roles a user can enter regardless of OS configuration.

> **NOTE:** To secure access to roles even when BoKS is deactivated it is important to keep the OS user role assignment configuration in synch with BoKS su to role Access Rules. This is especially true if the root account is a role.

BoKS tty lock Issues

The BoKS device driver used to implement the tty lock service allocates space for a fixed number of tlock pseudo devices when the driver is loaded into the kernel. The default number of devices is 64. This means that no more than 64 simultaneous tty lock sessions can be active in the system. See the BoKS man page tlock.conf(4B) for details on how to change the max number of tlock devices. A failed tlock invocation attempt will be logged in the BoKS audit log.

Installation Issues on Linux

Red Hat Linux by default maps the hostname to the loopback address `127.0.0.1` in the **/etc/hosts** file at installation even if an external network address is configured for the machine.

Similarly, SuSE Linux can append `127.0.0.2` to **/etc/hosts** for the hostname.

For BoKS to be installed correctly, the **/etc/hosts** file must map the external network address to the hostname registered on the BoKS Master and the loopback address `127.0.0.1` or `.2` must NOT be mapped to the hostname registered in BoKS. Before installing BoKS, check the **/etc/hosts** file and correct it if necessary to meet this requirement.

Installation Issues on Red Hat With SELinux

The following applies to BoKS on Red Hat Enterprise Linux. For general documentation on the SELinux support for Red Hat Enterprise Linux, see documentation provided by Red Hat.

SELinux is enabled by default on Red Hat.

Note: Only the targeted policy is supported. This is the default policy on Red Hat Enterprise Linux.

Installing

When installing BoKS in an SELinux enabled environment, the BoKS SELinux policy must be installed to get a fully functional system.

This policy is provided by a separate RPM which is available for download from the FoxT Customer Service website, named `boks-selinux-X.X-X.elY.noarch.rpm`, where `X.X-X` is the current version of the policy, and `Y` is the RedHat release number.

If you plan to activate SELinux after you have installed BoKS, you should install the SELinux policy RPM before activating SELinux.

Making suexec work for confined SELinux users

If SELinux users other than **unconfined_u** are to be able to use **suexec**, a custom module must be written to enable this. In order to build the new security module, the package **selinux-policy-devel** must first be installed.

The following example gives the SELinux user **staff_u** permission to run **suexec** with keystroke logging:

```
policy_module(staff_suexec, 1.0);
gen_require(`
type staff_t;
role staff_r;
')
boks_run_kslog(staff_t, staff_r)
boks_run_suexec(staff_t, staff_r)
```

Store this in a file called **staff_suexec.te** and copy the files in **$BOKS_DIR/install/selinux/src/** to the same location. Then run

```
make -f /usr/share/selinux/devel/Makefile staff_suexec.pp
```

The module can then be installed by running the command

```
semodule -i staff_suexec.pp
```

For details about writing policy modules, see your Red Hat documentation set.

Installing on Virtual Server Operating Systems

This section includes the following topics:

- Installing on Oracle Solaris Versions With Zone Support

Installing on Oracle Solaris Versions With Zone Support

BoKS Manager includes support for installation on the virtual server operating system Oracle Solaris 10 and later with zone support. This section contains information about special considerations that apply when installing BoKS Manager on Solaris versions with zone support.

This section includes the following topics:

BoKS Zone Support Basics

Solaris zones is Solaris technology for creating multiple virtual application environments on a single machine. From a BoKS perspective, each Solaris zone is a separate BoKS host. One instance of BoKS should be installed in each zone requiring BoKS protection. BoKS must be installed in the global zone to be able to install BoKS Manager in non-global zones. The normal BoKS constraints for multiple BoKS domains and subnets apply to BoKS installations on a multi-zone host.

See also:

- Multiple BoKS Domains

Installation Requirements in a Solaris Zones Environment

The following requirements apply for the installation of BoKS Manager and BoKS Server Agent for Unix/Linux in a Solaris zones environment:

- The zone must be assigned at least one external network address.
- On Solaris 10, non-global zones may be configured to share disk partitions with the global zone to reduce disk-space usage, but the following directories must NOT be shared:
  - /etc - Zone configuration files
  - /var - Zone data files
  - $BOKS_etc - BoKS configuration files
  - $BOKS_DIR - BoKS program files
  - $BOKS_var - BoKS data files
- BoKS Manager on Solaris uses kernel modules to implement tty lock functions. Kernel modules can only be loaded/unloaded from the global zone. A non-global zone BoKS Manager installation will depend on a BoKS installation in the global zone supplying the kernel modules. BoKS must be installed and set up in the global zone before installing BoKS in a non-global zone. However, BoKS protection does not need to be activated in the global zone.
- The tty lock function uses a BoKS-specific device driver tlock. Non-global zone configuration

must include access permission to the tlock device, see zonecfg(1M) for details on how to add device access permission to a non-global zone.

Note: To get a /dev/tlock device instantiated in a non-global zone, the tlock device must be available in the global zone when the non-global zone boots for the first time. If /dev/tlock is not available in the non-global zone even though added to the zone configuration, reboot the non-global zone after installing BoKS Manager in the global zone.

Uninstalling in a Solaris Zones Environment

Uninstalling BoKS Manager in the global zone unloads the BoKS kernel modules for tlock. Any BoKS installations in non-global zones are then not able to use these services. Starting the BoKS uninstallation program in the global zone while there are BoKS installations in non-global zones results in a warning message. It is possible to override the warning and proceed with the uninstall to be able to temporarily uninstall BoKS in the global zone during an upgrade of the BoKS installation, see Upgrading With Solaris Zones.

Applying Hotfixes and Patches With Solaris Zones

When applying a hotfix or patch to a zone environment, the global zone must be hotfixed/patched first before applying the hotfix/patch to non-global zones.

Upgrading With Solaris Zones

Similarly to applying hotfixes and patches, upgrading must be performed in the global zone first before upgrading non-global zones. During upgrade of a BoKS installation in a zone environment it is allowed to temporarily uninstall BoKS in the global zone while BoKS installations are still running in non-global zones. However, new tty lock sessions cannot be initiated in the non-global zones until BoKS is reinstalled in the global zone.

A possible workaround to keep tty lock operational while upgrading the global zone is to lock the tty lock kernel module in the kernel. This can be achieved by having at least one active tty lock session in a non-global zone. The downside to this workaround is that the new version of the BoKS kernel modules will not be loaded into the kernel until the operating system is rebooted.

Compatibility With Solaris Zones

Different versions of BoKS can be installed on different zones on a multi-zone host. BoKS Server Agents for Unix/Linux installed on a multi-zone host are compatible with BoKS Manager Master, Replicas and Server Agents installed on other hosts in the domain.

Patching the Operating System With Solaris Zones

The recommended procedure for applying operating system patches when using BoKS Manager is to deactivate BoKS protection while installing the patch to prevent operating system files replaced by BoKS from being overwritten by the patch. Some Solaris patches require that the patch is installed on all zones at once. This would require deactivating BoKS protection on all zones before applying the patch. The only operating system file on Solaris replaced by BoKS Manager is the /etc/pam.conf file. If it can be verified that an operating system patch does not modify the /etc/pam.conf file, the patch may be applied without deactivating BoKS protection.

BoKS tty lock

The BoKS device driver used to implement the tty lock service allocates space for a fixed number of tlock pseudo-devices when the driver is loaded into the kernel. The default number of devices is 64. This means that no more than 64 simultaneous tty lock sessions can be active in the system. In a zone environment, the maximum number of tlock devices is shared by all zones and the maximum number of tlock sessions might need to be increased. See the UNIX man page tlock.conf(4B) for details on how to change the maximum number of tlock devices. A failed tlock invocation attempt will be logged to the BoKS audit log.

zlogin

When BoKS protection is active, zlogin interactive and non-interactive sessions are logged to the BoKS audit log via the login(1) and su(1) PAM services respectively. See the UNIX man page zlogin(1). When zlogin is invoked in “safe mode” (-S option), the PAM system is bypassed and sessions are not logged to the BoKS audit log.

Location of the xinit Wrapper Script

The BoKS xinit wrapper script is no longer installed in the /usr/openwin/bin directory by default. The script is only needed on systems where the X-server is started from the command line, a method rarely used in newer systems. The script is now located in $BOKS_bin/X11/xinit. See the UNIX man page xinit (1B) for instructions on how to install the xinit wrapper script when needed.

Installing BoKS Manager on a Master

Installing on a Master includes:

- Master Basics
- Prerequisites for BoKS Master Installation
- Installing the Master
- Quick Start for FoxT Control Center
- Basic Configuration of BoKS Manager
- Using Learn Mode
- Importing Users and Hosts into the Database
- Advanced Configuration Overview

See also:

- Installing BoKS Manager on a Replica
- *Converting Between Master, Replicas and Server Agents* in the chapter "Backup, Restore and Recovery" in the *Administration Guide*

Master Basics

The BoKS Master does not need to be a dedicated computer, but must not have heavy applications running. BoKS need not run on the most powerful machine, as long as the machine meets the minimum requirements.

Shared Memory

For recommended shared memory, see System Requirements. Once you set shared memory, you must keep it the same on the Master and all Replicas. When you re-install during an upgrade, you must set the same value as set in the old installation.

Set shared memory in BoKS after you have installed BoKS. Set shared memory with the variable **SHM_SIZE** in the **$BOKS_etc/ENV** file.

If needed, shared memory settings can also be changed later. Restart BoKS after changing shared memory settings:

```
BoKS # Boot -k
BoKS # Boot
```

If your BoKS shared memory setting necessitates changing the shared memory for the operating system, refer to your system's documentation.

Disk Space Requirements

For recommended disk space, see System Requirements.

Keep in mind the following:

- Disk space is platform dependent. Some platforms can get by with less.
- Disk space required for the log files depends on the amount of activity.

Protection

The BoKS Master will be the main security server for some, if not all, mission-critical applications in your domain. It therefore needs to be highly protected. Measures you can take to protect it include:

- **Physical security**. Like all mission-critical machines, the Master should be located in a secure place. Physical security is often overlooked in an effort to strengthen logical security, although it is equally important, if not more so.
- **BoKS Protection**. Always activate BoKS Protection on the Master (and on Replicas), to protect it from intrusion over the network, even when you are not using BoKS Protection in the rest of your BoKS domain. This allows you to control access to the Master on a host level, restricting access to only individuals to whom you assign specific Access Rules.
- **Root password**. Restrict knowledge of the root password on the Master to a limited number of administrators.
- **Replica designated as backup**. Designate one Replica to be converted to a Master in the event the Master fails and cannot be brought online again quickly. Prepare for this eventuality, so that you can convert the Replica and begin administration of the domain on it. See Failover Replica For Disaster Recovery. See also *Recovery Procedures* in the chapter "Backup, Restore and Recovery" in the *Administration Guide*.

Root Account

Note: The root account on the Master is automatically added to the BoKS database when you install BoKS Manager and set it up as Master. The BoKS Manager username is *masterhostname*:root where *masterhostname* is the hostname of the Master.

See also:

- Preparing Node Keys, User Accounts and Host Groups
- Install Directories

Prerequisites for BoKS Master Installation

Before deploying the Master, review your plan and see that:

- All system requirements are met. See System Requirements.
- At least 2 semaphore sets are available for BoKS Manager. See System Requirements.
- Port numbers have been decided upon, if non-default ports are used. See Configuring Multiple Domains on the Same Subnet.
- Node keys have been decided upon for the Master and all hosts.
- The source for user accounts is consistent.
- Use of certificates or RSA SecurID tokens is prepared. These can be added later, but it is well to have your plan clear from the start.
- Shared memory size has been decided upon. It must be set the same on the Master and all Replicas. See recommended size in Master Basics.

See also:

- Prerequisites for BoKS Manager
- Master Basics
- The Readme, which contains platform-specific installation information.

Installing the Master

Before installing the Master, read relevant parts of both the *Installation Guide* and the *Administration Guide*. See Master Basics for a summary.

For details, see:

- System Requirements
- Prerequisites for BoKS Master Installation
- The Readme, which contains platform-specific installation information.
- Install Directories
- Install Parameters and Options
- Unpacking the Package Contents

Notes:

- Plan node keys in advance and **remember the node key you use during installation**. You will need it when you register the host and in the case of future upgrades of BoKS Manager. See Node Keys.
- BoKS uses a number of install directories for which you can specify paths or accept system defaults. These are referred to below by the BoKS directory names **$BOKS_DIR**, **$BOKS_etc** and **$BOKS_var**. See Install Directories for a list of these directories and their default paths.
- The install program provides options not used in the procedure below. See Install Parameters and Options.

To install BoKS Manager on the Master:

1. Download and save the BoKS Manager latest release package in a location accessible from the Master.

   For example in the **/downloads** directory on the Master.

2. If required, uncompress the release package. See Unpacking the Package Contents. A directory structure is created.

   The directory structure includes an **install** program, and binaries for specific platforms in sub-directories.

3. Become superuser:

   ```
   $ su
   ```

4. Run the **install** program.

   To install without any options, type:

```
# path to location of uncompressed package/install
```

To activate SSH privilege separation, type:

```
# path to location of uncompressed package/install -p [-u <uid>]
[-g <uid>]
```

where <uid> and <gid> let you optionally specify the uid and gid for the SSH daemon account, respectively. If you do not specify these, the next available UID and GID are instead used for the account, which is created automatically. You can also activate privilege separation at a later point using the command `sshd_setup -p` (see *Configuring Privilege Separation* in the chapter *System Configuration* in the **Administration Guide**).

For other install options, see Install Parameters and Options.

5. When prompted to install the product or Quit, select the product.

```
1) BoKS Manager 7.2
q) Quit install
```

Type **1** and press ENTER to install BoKS Manager.

6. If you did not use the **-opt**, **-var** or **-etc** flags, the install program will prompt you individually for each install directory and provide a default that you can simply accept by pressing Enter. Defaults are:

/opt/boksm
/etc/opt/boksm
/var/opt/boksm

Accept each of these with Enter, or else enter the directory that you want to use.

7. When asked:

```
Would you like to start the installation now? [y]
```

press ENTER to start the installation.

8. When the installation is finished, the following is displayed:

```
Setting up BoKS
1) Master
2) Replica
3) Client
q) Quit and run setup later
```

9. Before running **setup**, open a new terminal window and make any of the following configurations that are necessary for **communications** between this Master and Replicas, Server Agents, and Agent Hosts in the same domain:

- Set shared memory with the variable **SHM_SIZE** in the **$BOKS_etc/ENV** file to the value decided upon.

- If you using **non-default port settings** for BoKS, configure the base port by adding a line to the **/etc/services** file. For example, add the line:

```
boks 6530/tcp
```

10. Return to the terminal window with the BoKS Manager install process finished (which you left after install but before **setup**) and type the number 1 for **Setup Master**, then press ENTER to set up the Master.

    If you closed the window, **start the setup program** by typing:

    ```
    /opt/boksm/sbin/setup master
    ```

    (for a default installation directory), or use the path to your **$BOKS_sbin** directory.

11. When prompted to enter a node key:

    ```
    Enter BoKS node key:
    ```

    type the node key that you have planned and press ENTER.

    Remember the node key for later upgrading or converting the Master to become a Replica or Server Agent. See Node Keys.

12. When prompted to re-enter the node key, do so and then press ENTER.

    ```
    Re-enter node key:
    ```

13. The installation process is finished and you are returned to the list of available products. Exit the installation program by typing q for quit:

    ```
    q) Quit
    ```

14. Retrieve the **domain id** for the domain that will be managed by this Master.

    You can do this either by running the **bksdef** command in a BoKS shell, for example:

    ```
    # /opt/boksm/sbin/boksadm
    BoKS # bksdef
    ```

    which displays a number of parameters about BoKS including the domain id, or alternatively retrieve the file **$BOKS_etc/domain.id**.

    Send the domain id to Fox Technologies customer support immediately so that they can generate a license file for the domain.

15. If you use SSH, enable BoKS SSH by finding the `BOKS_SSHD` variable in the **$BOKS_etc/ENV** file and changing its value from **off** to **on**. For other optional SSH configuration, see *Configuring SSH* in the chapter "System Configuration" in the *Administration Guide*.
16. If you are using RSA SecurID tokens, configure this host for SecurID authentication as described in the chapter "Managing Authenticators" in the *Administration Guide*.
17. To relay audit log messages to a logging system external to BoKS, see "Configuring Log Relaying to an External Syslog Server" in the Administration Guide.
18. Restart the BoKS daemons by typing (assuming installation in the default directory /opt/boksm/):

```
# /opt/boksm/sbin/boksadm Boot -k
# /opt/boksm/sbin/boksadm Boot
```

19. Run the program **fccsetup**, as described in Quick Start for FoxT Control Center. This quickly sets up the FoxT Control Center administration server. Once you have done this and installed the FoxT Control Center presentation server, you can then access FoxT Control Center for further configuration and management of the domain.
20. Import the license file you receive from Fox Technologies customer support into the database by running the following command on the Master:

    ```
    BoKS # bokslicense -i < /tmp/bokslic1.lic
    ```

    Where `bokslic1.lic` is the license file for the domain.

See also:

- Installing BoKS Manager on a Replica
- *Recovery Scenarios with the convert Script Overview* in the chapter "Backup, Restore and Recovery" in the *Administration Guide*

Quick Start for FoxT Control Center

This procedure, using the command line program **fccsetup**, quickly sets up the administration server for web-based administration of your BoKS domain via FoxT Control Center.

Prerequisite: BoKS Manager has been installed and set up as Master. See Installing the Master.

Usage:

- You can run this script several times, creating one user each time, or changing the password login option.
- When you create a new user account, the user's physical home directory is not created by the script. If you need it, it must be created outside the script.
- The CA, .p12 and session log files created when you run **fccsetup** are saved in the directory **$BOKS_tmp** (by default **/var/opt/boksm/tmp**).

To do a quick start for remote administration:

1. Log in to the BoKS Master, become root and start the BoKS shell:

   ```
   # /opt/boksm/sbin/boksadm
   ```

   where **/opt/boksm/sbin** is the default **$BOKS_sbin** installation directory. If not default, use the directory where you installed.

2. If you are upgrading, make sure you have already restored your BoKS database. This will ensure the administration Access Rules used in step 5 below are available for FCC setup.
3. Start the remote administration wizard:

```
BoKS # fccsetup
```

A prompt is displayed:

==========

This is the BoKS 7.2 GUI setup wizard. It will guide you

through the steps neccessary to run the BoKS GUI.

The procedure is in short:

* Create a root CA certificate (includes naming the CA entity)

* Create a host certificate for the BoKS Master

* Update existing BOKSADM user classes with BCCAS access routes

* Update existing BOKSADM users with BCCAS access routes

* Create a non-root user as which to run the admin GUI (optional)

* Grant administrative privileges to the user created (optional)

* Extract certificate files for the FCC host

The wizard has two phases - one information collection phase

and one execution phase. The information collection phase

may be interrupted at any time and no action will be taken.

==========

BoKS # Do you wish to continue? yes

4. **If this is a new installation, you need to create a root CA and a host certificate for the Master. If these do not exist, you are prompted to create them:**

   Enter CA certificate data that will be used to sign certificates needed for remote administration. This CA can be but need not be your root CA later on.

   Root CA Country (e.g. "US"): < the two letter ISO 3166 country code as listed in the file $BOKS_ etc/countrylist>

   Root CA Organization: <your organization's name>

   Root CA Org. Unit (not required): <unit within organization, optional>

   Root CA CommonName: <a name for this root CA>, for example, "Root CA"

   Root CA key length (max 8192): <4096>

   The minimum value is 512-bit, maximum 8192-bit and the default value is 4096-bit.

   Validity in years (default is 10): <10>

   Password: <CA password>

Make a note of this password so that you can use the CA later on.

Retype password: <CA password>

Save password for automatic use? [n]: Type **y** if you want to save the CA password for use in certificate operations.

5. If you are upgrading, and have not defined Sub-Administrators in your existing domain, users and User Classes that previously had access to the old BoKS Administration GUI by means of a **BOKSADM** Access Rule are given **BCCAS** Access Rules so they can access FoxT Control Center. The **From** and **To** parts of the Access Rules, as well as the date and time definitions, are copied from the **BOKSADM** Access Rules.

   Note: If you have defined Sub-Administrators in your previous installation, these are NOT given access to FoxT Control Center. These users must be given access, and their privileges defined, manually using Access Rules and FoxT Attribute-Based Access Controls. In addition, if Sub-Administrators are present, User Classes with **BOKSADM** Access Rules are NOT given access to FoxT Control Center.

6. If this is a new installation, enter the username and, optionally, data for the user account that will be used for administration in FoxT Control Center. This can be an existing account in the BoKS database, or a new account that is created here.

   Do you want to assign a new GUI administrator?

   Enter name of GUI administrator: <a user account name> for example, “cgray”

   If you specify an existing account in the BoKS database, you continue to the next step. If this is an existing user on the Master, but has not yet been registered in BoKS, the wizard gives you the option of importing user data for the account from **/etc/passwd**:

   User “<user>” exists locally. Do you want to import user data from /etc/passwd [yn]

   If you answer `yes`, you need to provide the user’s password.

   If this is a new account or if you answer **no** to the previous question, the wizard asks for data to set up the user:

   Do you want to set Unix parameters for this user [yn]?

   If you are not interested in a “real” user account (that is, if this will be a temporary account that you remove after BoKS Manager is set up and running), you can answer **No** and let the wizard use default values. Otherwise, answer Yes and enter any of the following that you want to (or press return to accept the default value):

   Enter UID (leave empty for auto selection): for example, “13300”

   Enter GID [65534]: for example, “500”

   Enter shell [/bin/false]: for example, “/usr/bin/sh”

   Enter home directory [/]: for example, “/home/cgray”

   Enter comment [BoKS GUI admin]: <user real name>

   Password: <user password> MANDATORY FIELD

Retype password: <user password>

7. Now you need to define where you will install the presentation server for FoxT Control Center.

   At the prompt "**Will you install the GUI Presentation Server on the master?**", type `yes` if you want to install the presentation server on the BoKS Master.

   Note: Fox Technologies does not recommend installing the presentation server on the BoKS Master as this option does not provide maximum security and performance for domain management.

   Alternatively, if you want to install the presentation server on another host (which must be a BoKS Server Agent for Unix/Linux) press **Enter** to choose the default option of **no** and type the name of the presentation server host at the **Host name:** prompt.

   Note: If you want to install the presentation server on a BoKS Replica, you should install BoKS Manager on the Replica and register it in the BoKS database **before** you run **fccsetup**, otherwise **fccsetup** will register the host as a BoKS Server Agent for Unix / Linux in the BoKS database.

8. If the host is not yet registered in the BoKS database, you are prompted whether you want to register the host now. To register the host, type the IP address for the host.

   Note: The host is registered with a bare minimum of parameters, and you will likely want to add more information about the host in the BoKS database when FoxT Control Center is up and running.

9. Press **Enter** at the prompt **Do you want to extract the certificate files now?**

   This creates the CA and host certificate file for the BoKS Master, which you need when you are installing the presentation server. If you skip this step, you can also retrieve the necessary certificate files later by running the command **bccgethostcert**.

10. A summary of the configuration you have entered is displayed.

    Answer yes to "**Do you wish to go ahead and make the changes to BoKS** [yn]:

    The wizard goes to work and reports on the various steps of the configuration.

11. If prompted, type a node key for the presentation server host. This is only required if the host has not previously been registered in the BoKS database.

    Note: Remember the node key, as it will be required when you install BoKS Server Agent on the presentation server host.

12. If required, a host certificate must be created for the presentation server host. You need to select a CA to sign the host certificate from the list by entering the CA number at the **Select CA:** prompt.

    The settings for the certificate are displayed and you are prompted to accept the settings.

13. If a host certificate is being created, type a password for the certificate at the **PKCS#12 file password:** prompt.

    You also need to retype the password to confirm it.

14. If required, install BoKS Server Agent for Unix / Linux on the host where you want to run the presentation server.

15. Install the presentation server (BCCPS). You can install the presentation server either on the Master or on another BoKS Server Agent for Unix/Linux in the domain.

    For details, see the appropriate *FoxT Control Center Installation Guide*.

16. To launch FoxT Control Center, open a browser window and enter the URL: **https://presentationserver:8443/bcc**, where *presentationserver* is the name or IP address of the host where the FoxT Control Center presentation server is installed (which may or may not be the BoKS Master). Note that 8443 is the default port, but you may have installed FoxT Control Center on another port.

On the login page, log in using the user account name and user password that you specified earlier for the FCC GUI administrator.

You can now perform administration using FoxT Control Center from any host.

The next step is **Basic Configuration** as described in Basic Configuration of BoKS Manager. Basic configuration tasks are done working locally on the command line interface on the Master and using FoxT Control Center.

See also:

- *Setting Up Remote Administration for a User* in the chapter *BoKS Manager Administration* in the **Administration Guide**
- *Launching FoxT Control Center* in the chapter *BoKS Manager Administration* in the **Administration Guide**

Basic Configuration of BoKS Manager

Prerequisites for this procedure are successful completion of the procedures:

- Installing the Master

To Perform Basic Configuration of BoKS Manager:

1. Open FoxT Control Center in a browser window with the URL https://*presentationserver:port/bcc* (port 8443 by default) from a remote computer (which you have included in a BCCAS Access Rule).
2. Additionally, log in to the BoKS Master, become root, and start a BoKS shell.

   For example:

   ```
   # /opt/boksm/sbin/boksadm
   BoKS #
   ```

3. Set shared memory, if needed to handle a large number of users (> 1000) in the database, by altering the variable **SHM_SIZE** located in the file **$BOKS_etc/ENV**. The default setting is 1000 KB. Set the same size on the BoKS Master and Replicas.
4. Set the file monitoring interval on the Master, if desired, with the variable **FILEMON_INTERVAL** in the file **$BOKS_etc/ENV**. Specify time in minutes. Default value is 120 minutes.

5. If you want, set the Lockout of Unknown host variables to prevent access by unknown hosts or hosts with unresolved hostnames, which the expression ANY/* in an Access Rule would otherwise allow. For details, see *Lockout of Unknown Hosts* in the chapter "System Configuration" in the *Administration Guide*.
6. Set up an automatic scheduled backup of the database (optional), by doing as follows (see *Setting Up Automatic Backup and Restore* in the chapter "System Configuration" in the *Administration Guide*):
   - From the root shell prompt, type:

     ```
     hostname# crontab -e
     ```

     This command starts the editor according to the environment variable **EDITOR**.
   - Add the new line to the file:

     ```
     01 00 * * * /opt/boksm/sbin/boks_bru -p -d /backup-
     dir/boksm-$ \
     (date +\%Y\%m\%d\%H\%M\%S).sav
     ```

     If you installed BoKS in a non-default directory, replace the directory above with your $BOKS_sbin directory.
   - Save the file and leave the editor.

     This file will run **boks_bru** each night at 00.01 and back up BoKS to the directory *backup-dir*.

     > **NOTE:** A **boks_bru** backup only includes the database and configuration files. Audit log files and keystroke log files are not included and must be backed up separately.
7. Configure the BoKS Manager audit log that is maintained on the Master using the **Domain** page, **Audit log configuration** section in FoxT Control Center.
8. To configure optional email notification whenever a BoKS-protected host is activated or deactivated (Master, Replica or BoKS Server Agents for Unix/Linux), add the following line to the **$BOKS_etc/ENV file:**

   ```
   MAIL_NOTIFY=email address of alert recipient
   ```
9. Optional: For any Server Agent for Unix/Linux or Agent host that uses a time zone different from the Master or the host's configured Replica, specify the time zone for the host using the CLI option `hostadm -z` or the host details page in FoxT Control Center.

   This can also be done later when installing each Server Agent for Unix/Linux or Agent Host.
10. Optional: Activate BoKS Protection on the Master (and later on each Replica) with the **Get BoKS status** > **Activate BoKS** buttons on the hosts listing and host detail pages in FoxT Control Center. To do this from a command terminal on the Master (or Replica), type:

    ```
    BoKS # sysreplace replace
    ```
11. Finish configuration by restarting BoKS processes, by typing:

    ```
    # /opt/boksm/sbin/boksadm Boot
    ```

See also:

- The chapter "System Configuration" in the *Administration Guide*
- The chapter "BoKS Manager Administration" in the *Administration Guide*
- The chapter "Managing CAs and Certificates" in the *Administration Guide*
- *Activating BoKS Protection on the Master and Other Hosts* in the chapter "System Configuration" in the *Administration Guide*

Using Learn Mode

Learn Mode is intended for initial deployment and troubleshooting.

Learn Mode allows you to run BoKS Manager and BoKS Server Agent for Unix/Linux with BoKS Manager activated but without enforcing most Access Rules.

Note: Access using the methods **rsh**, **rlogin** without password, and any access to an account with UID 0 (for example root) still requires users to have Access Rules, even in Learn Mode.

For access using methods other than those specified above, BoKS Protection is still activated and BoKS still logs all access, but access is not denied when the user has no Access Rule. Instead, access is allowed as long as all other requirements are met (such as having an account and authenticating correctly with password or whatever is configured). Learn mode produces an extra log entry for each access. These entries may be sorted out and displayed to see which Access Rules are needed.

Learn mode simplifies a roll-out when it is not certain that the system is configured correctly. The intent behind this feature is to decrease the pressure on administrators during deployment by decreasing frustration for the end users.

Properties

- Users must exist in the BoKS Manager database. Users that are only defined locally, for example, in /etc/passwd, are not granted access.
- User must login with the correct password.
- User must login with any required (and assigned) Authenticator.
- Learn Mode is not applied to the root account and BoKS Manager administration (both from the command line and in the old GUI or FCC)– the root account is still fully protected.
- Learn Mode is not applied for access using the methods rsh, and rlogin without a password – users accessing using these methods still require Access Rules.
- Limit on maximum number of concurrent logins for a user (set with modbks) applies even under Learn Mode.
- In learn mode, a user who enters the wrong password too many times is still blocked.

Example Output in the Audit Log

Login with Learn Mode disabled:

10/19/04 08:14:11 cgray-pc1 pts/4 cgray login Successful login (rlogin from cgray-pc3:cgray)

Login with Learn Mode enabled and the user has a correct Access Rule:

10/19/04 08:14:31 cgray-pc1 - cgray noaccessctl success, RLOGIN:cgray@cgray-pc3->cgray-pc1, psw (RLOGIN,TELNET,XDM:KNOWN/*->*)

10/19/04 08:14:31 cgray-pc1 pts/4 cgray login Successful login (rlogin from cgray-pc3:cgray)

Login with Learn Mode enabled and the user does not have the needed Access Rule:

10/19/04 08:17:27 cgray-pc1 - mafh01 noaccessctl failure, RLOGIN:mafh01@cgray-pc3->cgray-pc1, psw

10/19/04 08:17:27 cgray-pc1 pts/7 mafh01 login Successful login (rlogin from cgray-pc3:mafh01)

Note that there are two entries for each access when learn mode is enabled. When the Access Rule was missing, the failure entry shows a minimum rule that would provide the access.

Usage

To enable Learn Mode:

1. Log in to the BoKS Master, become root and start a BoKS shell
2. Run the following:

   ```
   BoKS # bksdef -Z enable
   ```

   It is not necessary to reboot BoKS.

To disable Learn Mode:

1. Log in to the BoKS Master, become root and start a BoKS shell
2. Run the following:

   ```
   BoKS # bksdef -Z disable
   ```

   It is not necessary to reboot BoKS.

To view the current Learn Mode setting:

To find out whether Learn Mode is enabled or disabled:

1. Log in to the BoKS Master, become root and start a BoKS shell
2. Run:

   ```
   BoKS # bksdef
   ```

3. Review the BoKS settings that are displayed.

If Learn Mode is enabled, the listing shows the line:

BoKS access control: DISABLED!

If Learn Mode is disabled, the listing shows the line:

BoKS access control: ENABLED

Note: The setting “BoKS Access Control” has the opposite setting to Learn Mode. Learn Mode enabled means that Access Control is disabled!

To view Learn Mode output:

When Learn Mode is enabled, extra log entries are added to the BoKS log by the program **noaccessctl**. You can study the BoKS audit log itself, but it will contain double entries for every access attempt as well as entries other than those concerning Access Rules.To only view output from Learn Mode (events concerning Access Rules), use the CLI command **learnmodelog**, for example:

```
BoKS # learnmodelog -f $BOKS_data/LOG -p
```

Tip! Using the -p option formats the output in the same way that **bokslogview** formats output.

See the BoKS man page for **learnmodelog** for details and other options.

See also:

- The chapter "Managing Access Rules" in the *Administration Guide*
- *Activating BoKS Protection on the Master and Other Hosts* in the chapter "System Configuration" in the *Administration Guide*
- The chapter "Planning Installation"

Importing Users and Hosts into the Database

You can import a whole existing BoKS database, or build a database by importing user accounts, hosts and other data from other sources.

Importing User Data to the Security Database

User data can be imported from a number of different sources. These include:

- The /**etc/passwd** file on a UNIX host.
- A combination of a NIS **passwd** map and the **/etc/passwd** file.
- A local file on the Master.
- An LDAP database. See the chapter "LDAP User Provisioning" in the *Administration Guide*.
- A security database from a previous BoKS Manager version that you have saved as a backup. See the chapter "Backup, Restore and Recovery" in the *Administration Guide*.
- Third party certificates. See the chapter "Managing CAs and Certificates" in the *Administration Guide*

See also:

- *Creating User Accounts* in the chapter "User Administration" in the *Administration Guide*.

Importing Host Data to the Security Database

Host data can be imported from the local **/etc/hosts** file on the Master or from an external source (NIS host map or DNS) or from a combination of both. See *Hosts* in the chapter "Host" in the *Administration Guide*.

Advanced Configuration Overview

When you have finished the Basic Configuration of your BoKS Manager domain, you must configure the settings that provide and control user access to hosts and applications in the domain.

Configuration that may need to be done includes:

- **Access** to hosts protected by BoKS Server Agent for Unix/Linux is controlled by Access Rules defined and managed in the **Access Rules** section for users and User Classes in FoxT Control Center.
- **Assign privilege limits for working in FoxT Control Center**, creating sub-administrators, using FoxT Attribute-Based Access Controls (ABAC). For details, see the *FoxT ABAC Reference Guide*.
- If you are using the password checkout feature, you can if required batch enable password checkout for users with the **pwmimport** program.

For full information on these and other configuration topics, see the BoKS Manager 7.2 Administration Guide.

See also:

- The chapter "A Guided Tour" in the *Administration Guide* (an introduction)
- The chapter "Managing Access Rules" in the *Administration Guide*
- The chapter "System Configuration" in the *Administration Guide*

Installing BoKS Manager on a Replica

Installing on a Replica includes the topics:

Replica Basics

The BoKS Replica contains a read-only copy of the security database. The Replica must be added as a BoKS **Replica host** in the security database on the BoKS Master. The node key must also be added to the Master. For details, see *Node Keys* in the chapter "Host" in the *Administration Guide*.

When installing a BoKS Replica, remember that the Replica must have contact with the Master. If the Master, Replica and BoKS Server Agent for Unix/Linux are on different subnets, you may have to configure the **bcastaddr** file on the Replica and BoKS Server Agent for Unix/Linux hosts to supply the IP addresses of the Master and Replicas. See Domain Communication Basics.

A Replica must always have the same BoKS shared memory setting in the **$BOKS_etc/ENV** file as the Master.

The disk space requirements for the BoKS Replica are approximately the same as those for the BoKS Master. See System Requirements.

Since a Replica contains a copy of the security database, **Replica security** should be as high as on the Master, which includes physical security, activating BoKS Protection, and restricting the root password to few administrators.

At least one Replica in the domain should be designated as and planned for as a failover backup to convert to Master if the Master fails. See Placing Replicas for Availability and Load Balancing.

In order to do administrative tasks on the Replica when BoKS Protection is activated, the **root account** on the Replica must be defined as a BoKS user account, just like any other user account. You can import this account from the /etc/passwd file (at the same time as you import user accounts) using the **Import users** button on the host details page for the Replica in FoxT Control Center.

See also:

- Master Basics
- Install Directories

Prerequisites for BoKS Replica Installation

Before installing Replicas:

- See that all system requirements are met. See System Requirements.
- Set up FoxT Control Center and complete the basic configuration procedure (you can always modify configuration later). See:
- *Quick Start for FoxT Control Center*
- *Basic Configuration of BoKS Manager*
- If non-default ports are used, configure port numbers in the **/etc/services** file. See Configuring Multiple Domains on the Same Subnet.
- Before running **setup** on the Replica, the BoKS Manager Master must be set up and running, so that **setup** can contact the Master in real time.

Installing a Replica

The steps described here are almost the same as for the BoKS Master (as described in To install BoKS Manager on the Master:), except that here you select to set up a **Replica** instead of a Master.

See also:

- Prerequisites for BoKS Replica Installation
- Replica Basics
- Install Directories
- Install Parameters and Options
- The Readme, which contains platform-specific installation information.
- *Configuring Log Relaying to an External Syslog Server* in the chapter "System Configuration" in the *Administration Guide*
- *Converting Between Master, Replicas and Server Agents* in the chapter "Backup, Restore and Recovery" in the *Administration Guide*

Notes:

- Plan node keys in advance and **remember the node key you use during installation**. You will need it when you register the host and in the case of future upgrades of BoKS Manager. See Node Keys.
- BoKS uses a number of install directories for which you can specify paths or accept system defaults. These are referred to below by the BoKS directory names **$BOKS_DIR**, **$BOKS_etc** and **$BOKS_var**. See Install Directories for a list of these directories and their default paths.
- The install program provides options not used in the procedure below. See Install Parameters and Options.

To install and set up BoKS Manager on a Replica:

1. Download and save the BoKS Manager latest release package in a location accessible from the Replica.

   For example in the **/downloads** directory on the Replica.

2. If required, uncompress the release package. See System Requirements. A directory structure is created.

   The directory structure includes an **install** program, and binaries for specific platforms in sub-directories.

3. Become superuser:

   ```
   $ su
   ```

4. If the directory **/tmp** has less than 250 MB of space for use during install, then set the UNIX environment variable PATCH_TMP to a directory that has 250 MB, for example, /var/tmp/tempbokspatch, as follows:

   ```
   # PATCH_TMP=/var/tmp/tempbokspatch
   # export PATCH_TMP
   ```

5. Run the **install** program:

   To install without any options, type:

   ```
   # path to location of uncompressed package/install
   ```

To install and create the special user account required if you intend to use SSH privilege separation, type:

```
# path to location of uncompressed package/install -p [-u <uid>]
[-g <uid>]
```

where <uid> and <gid> let you optionally specify the uid and gid for the SSH daemon account, respectively. This account can be created manually instead (see *Configuring Privilege Separation* in the chapter *System Configuration* in the **Administration Guide**).

For other install options, see Install Parameters and Options.

6. When prompted to install the product or Quit, select the product.

```
1) BoKS Manager 7.2
q) Quit install
```

Type **1** and press ENTER to install BoKS Manager.

7. If you did not use the **-opt**, **-var** or **-etc** flags, the install program will prompt you individually for each install directory and provide a default that you can simply accept by pressing Enter. Defaults are:

/opt/boksm
/etc/opt/boksm
/var/opt/boksm

Accept each of these with Enter, or else enter the directory that you want to use.

8. When asked:

```
Would you like to start the installation now? [y]
```

press ENTER to start the installation.

9. When the installation is finished, the following is displayed:

```
Setting up BoKS
1) Master
2) Replica
3) Client
q) Quit and run setup later
```

10. Before running **setup**, open a new terminal window and make any of the following configurations that are necessary for **communications** between this Replica and the Master, other Replicas, Server Agents, and Agent Hosts in the same domain:
    - Set shared memory with the variable **SHM_SIZE** in the **$BOKS_etc/ENV** file to the same value as set on the Master.
    - If the Master is outside of the Replica's broadcast subnet, create a **bcastaddr** file in the **$BOKS_etc** directory (default **/etc/opt/boksm**), containing the keywords `DONT_BROADCAST`, `DONT_MULTICAST` and `ADDRESS_LIST` and then the IP address of the Master. For example, add the Master's address:

```
DONT_BROADCAST
DONT_MULTICAST
ADDRESS_LIST
10.10.10.100
```

You can also add any Replicas that communicate with this Replica. See *Configuring the bcastaddr File* in the chapter "System Configuration" in the *Administration Guide*.

- If you are using **non-default port settings** for BoKS, configure the base port by adding a line to the **/etc/services** file. For example, add the line:

```
boks 6530/tcp
```

11. Return to the terminal window with the BoKS Manager install process finished (which you left after install but before **setup**) and type the number 2 for **Setup Replica**, then press ENTER to set up the Replica.

    If you closed the window, **start the setup program** by typing:

    ```
    /opt/boksm/sbin/setup replica
    ```

    for a default installation directory, or use the path to your **$BOKS_sbin** directory.

12. When prompted to enter a node key:

    ```
    Enter BoKS node key:
    ```

    type the node key that you have planned and press ENTER.

    Remember the node key for registering the host in the BoKS database later.

13. When prompted to re-enter the node key, do so and then press ENTER.

    ```
    Re-enter node key:
    ```

14. The installation process is finished and you are returned to the list of available products. Exit the installation program by typing q for quit:

    ```
    q) Quit
    ```

15. If you are **reinstalling** BoKS on this Replica, run the **push_files** program on the BoKS Master to copy configuration files from the Master to the Replica. This is done to ensure that a Replica can be converted to a Master in case the normal Master fails.

    For example:

    ```
    BoKS # push_files replica1
    ```

    To copy configuration files to the Replica with the hostname `replica1`.

    The files that are copied are those configured in the file **$BOKS_etc/distrib.cfg**.

16. If you use SSH, enable BoKS SSH by finding the **BOKS_SSHD** variable in the **$BOKS_etc/ENV** file and changing its value from **off** to **on**. For other optional SSH configuration, see *Configuring SSH* in the chapter "System Configuration" in the *Administration Guide*.

17. If you are using RSA SecurID tokens, configure this host for SecurID authentication as described in *Configuring Hosts for SecurID Authentication* in the chapter "Managing Authenticators" in the *Administration Guide*.
18. Restart the BoKS daemons by typing (assuming installation in the default directory /opt/boksm/):

```
# /opt/boksm/sbin/boksadm Boot -k
# /opt/boksm/sbin/boksadm Boot
```

19. In FoxT Control Center, register the Replica in the menu **Add > Host** as follows:
    - Select the host type **Master/Replica**.
    - Provide the **Node Key** that you entered earlier during **setup**.
    - Provide the Primary IP address in the **Networking** box.
    - In the **Create home directories on this host at** box, type the name of the parent directory on this machine under which users' home directories are located, for example **/home** (default location depends on operating system).

      See *Home Directory Host Configurations for Unix Hosts* in the chapter "Host" in the *Administration Guide* for examples of Parent Home Directory and Physical Home Directory.

    - If BoKS Manager is to create the home directory on another host, type the hostname and directory in the **Map home directories to host** box, in the format *Host* at location *Directory*. For example:

      hostname at location /export/home.

    - Click **Save** to complete the registration.
20. Create a host certificate for the Replica as follows (as described in *Creating Host Certificates* in the chapter "Managing CAs and Certificates" in the *Administration Guide*):
    - Host certificates should be signed by the BoKS Root CA.
    - In the **Lifespan** list, select a lifespan for the new certificate. The default lifespan is five years.
    - Check the **Install on host** checkbox (checked by default).
    - Click **Add**.

      The certificate is now created in the BoKS database and will be automatically installed on the Replica in the **$BOKS_etc/keys** directory.

      > **NOTE:** It can take up to ten minutes before the host certificate is pushed out to the Replica.

21. Import the root account for the host into the database, using the **Import users button on the host details page in FoxT Control Center**. Fox Technologies recommends you use the local hostname as prefix for system accounts and particularly the root account. That is, create the root account as *hostname*:root, where *hostname* is the hostname of the host. See *About Importing Unix System Accounts* in the chapter "User Administration" in the *Administration Guide*. This is necessary in order to do administration while BoKS Protection is activated.
22. Test communications with the Master and trouble shoot. Check that all processes on the Replica

are working.

- Look at the log files.
- For a list of daemons, see *Daemons and Their Operations* in the appendix "System Architecture" in the *Administration Guide*.
- For use of the command line program **bdebug**, see the man page for bdebug, and the appendix "Command Line Interface" in the *Administration Guide*.
- See also the appendix "Troubleshooting" in the *Administration Guide*

23. Optional: In FoxT Control Center, activate BoKS Protection of the Replica using the buttons **Get BoKS status > Activate BoKS**. Alternatively, use the command line program **sysreplace**. From this point on, access to the Replica host from any other host requires an Access Rule.

Installing BoKS Manager Patches

Topics include:

- Installing a BoKS Manager Patch
- Backing Out a BoKS Manager Patch

See also:

- Installing OS Patches
- Uninstalling BoKS Manager
- Rolling Upgrade to BoKS Manager 7.2
- Installing the Master
- Install Directories
- Installing Hotfixes, Patches and Upgrades using boks_upgrade

Installing a BoKS Manager Patch

Before you install a patch you should ensure that you have sufficient shared memory set on the machine, and if necessary increase the setting. For details of how to do this, see "Setting Shared Memory" in the BoKS Manager 7.2 Administration Guide.

- For a patch to BoKS Server Agent for Unix/Linux, you can use the remote patch installation script **boks_upgrade** instead of the procedure below. See Installing Hotfixes, Patches and Upgrades using boks_upgrade.
- To upgrade, see Upgrading BoKS Manager.

CAUTION: When patching, all hotfixes are removed. You should be aware that a released patch might not include a removed hotfix, and, in that case, should contact Fox Technologies.
For information on which hotfixes are included in the patch, see the BoKS Manager README.

To install a BoKS Manager or Server Agent for Unix/Linux patch:

1. Log in to the machine and become root.
2. If the host is the Master, make a backup of the security database.
3. Move to the directory that contains the patch distribution for the appropriate platform. See Unpacking the Package Contents. For example:

```
hostname# cd /downloads/patches/boksm_patch
```

4. If the directory **/tmp** has less than 250 MB of space for use during install, then set the UNIX environment variable PATCH_TMP to a directory that has 250 MB, for example, /var/tmp/tempbokspatch, as follows:

```
# PATCH_TMP=/var/tmp/tempbokspatch
```

```
# export PATCH_TMP
```

5. To install the BoKS Manager patch, run the **installpatch** program:

```
hostname# ./installpatch
```

6. Follow the online instructions in the patch installation program to complete the installation.
7. To verify that the patch has installed correctly, you can check the **$BOKS_etc/ENV** file (by default /etc/opt/boksm), which contains version information, or run the following command:

```
hostname# /opt/boksm/sbin/boksadm boksversion
```

(assuming the default installation directory /opt/boksm)

Note: The **installpatch** program will restart the BoKS processes after the patch installation is successful, if the processes were running when **installpatch** was run. Otherwise, you will need to start the processes manually.

See also:

- Backing Out a BoKS Manager Patch
- Installing OS Patches
- Install Directories

Backing Out a BoKS Manager Patch

To uninstall a BoKS Manager or BoKS Server Agent for Unix/Linux patch, you can run the **backoutpatch** program, which is included in the original distribution directory.

- For a patch to BoKS Server Agent for Unix/Linux, you can use the remote patch installation script **boks_upgrade** instead of the procedure below. See Installing Hotfixes, Patches and Upgrades using boks_upgrade.

What version results from running backoutpatch?

Note that running **backoutpatch** returns you to the patch level that you previously installed manually, or if none, to the patch level included in the last full distribution that you installed. If you installed interim patches between the full distribution and the latest patch, these will be removed one at a time each time

you run **backoutpatch** until the level of the full distribution is reached, at which time **backoutpatch** returns you to the baseline patch level for that port (which may be 0, but is sometimes higher).

For example:

- If you installed a distribution that included patch level 3, then installed patch 6, running **backoutpatch** once will return you to patch level 3.
- If you installed a distribution that included patch level 3, then installed patch 5, then installed patch 6, running **backoutpatch** will return you to patch level 5 the first time, then to patch level 3 if run again, then to level 0 (or whatever level is the baseline level for that platform port) if run a third time.
- If you installed a platform port based on patch level 3, running **backoutpatch** successively will return you to patch level 3 and no further, since that is the baseline for that port.

To back out a BoKS Manager or Server Agent for Unix/Linux patch:

1. Log in to the machine and become root.
2. If the host is the Master, make a backup of the security database.
3. Move to the BoKS installation directory (**/opt/boksm/** by default). For example:

```
hostname# cd /opt/boksm/
```

4. Uninstall the latest patch by running the **backoutpatch** program:

```
hostname# Patches/backoutpatch
```

See also:

- Installing a BoKS Manager Patch
- Uninstalling BoKS Manager
- Install Directories

Installing OS Patches

Before installing a new OS patch, you must **deactivate BoKS Protection**. This is to ensure that the patch does not overwrite any BoKS binaries such as the login program which is replaced when you activate BoKS Protection.

After you have installed a new patch to the operating system, you need to **activate BoKS Protection** again.

CAUTION: If the OS patch changes the OS version to a version that is not supported by the installed BoKS package, you will need to upgrade BoKS Manager when you install the OS patch. See Installing OS Upgrades.

To install an Operating System patch:

1. Deactivate BoKS Protection on the BoKS Master, Replica or Server Agent for Unix/Linux on which the patch is to be applied.
2. Install the operating system patch according to vendor instructions.
3. Activate BoKS Protection.

See also:

- The chapter "Upgrading BoKS Manager"
- *NIS Integration with BoKS Manager* in the chapter "System Configuration" in the *Administration Guide*.
- Installing BoKS Manager

Installing OS Upgrades

If a new OS version is released, you may or may not need to upgrade BoKS Manager to a new version, depending on the scope of changes within the OS upgrade. A handy way to check this is to determine if there is a specific BoKS Manager package available for the new OS version you are upgrading to available for download on the Fox Technologies customer service website.

If in doubt, please check with Fox Technologies customer service before installing an OS upgrade on a BoKS-protected machine.

See also:

- The chapter "Upgrading BoKS Manager"
- *NIS Integration with BoKS Manager* in the chapter "System Configuration" in the *Administration Guide*.
- Installing BoKS Manager
- Installing OS Patches

Uninstalling BoKS Manager

This procedure applies to the Master, Replicas and BoKS Server Agents for Unix/Linux. The uninstall procedure is the same for all, with two exceptions:

1. It is only on the Master that you must make a backup of the security database.
2. On the BoKS Server Agent, the uninstall procedure is different depending on whether the installation was made using the tar package or using a native package such as RPM.

Remove BoKS Server Agent hosts first, then Replicas, and finally the Master.

See also:

- The man page **uninstall**
- About Deleting, Changing Host Type or Domain and Uninstalling Server Agents

Notes

- When you run the **uninstall** program on the Master, a backup of the security database is created automatically and stored in **/var/tmp/boksm.sav**. It is recommended that you immediately move this backup to a safe place.

  To manually create a backup, use the CLI program **boks_bru**. See the chapter "Backup, Restore and Recovery" in the *Administration Guide*.

  You can prevent the uninstall program from taking a backup of the BoKS database by running it with the option `-n`.

- Note that on some platforms, files that are running cannot be removed. This means that some files may still remain in the system after execution of the **uninstall** program.
- Note if **$BOKS_var** is a mount point, the **uninstall** command does not remove all files and directories from this location. These must be removed manually.
- For a way (using Access Rules) to ensure no access to BoKS-protected hosts in the domain via the uninstalled host during uninstallation, see the man page **uninstall**.
- If you uninstall BoKS from a host while there are **suexec** sessions with keystroke logging still running, the keystroke log files are not finalized and sent to the Master.

To remove BoKS Manager or BoKS Server Agent for Unix/Linux:

Note: Exit the BoKS Manager prompt before removing BoKS Manager software.

1. If this is a BoKS Server Agent for Unix/Linux and if the special upgrade OpenSSH daemon used by the **boks_upgrade** script is still installed (see the directory **/var/boks_upgrade** on the Server Agent), remove it by running **boks_upgrade** from the Master, as follows:

   ```
   BoKS # boks_upgrade cleanall -h <host>
   ```

   where `<host>` is the host to be uninstalled.

   Alternatively, log in to the Server Agent, find the upgrade OpenSSH daemon and kill it, then remove the **/var/boks_upgrade** directory on the Server Agent.

   The special upgrade SSH daemon and the directory **/var/boks_upgrade** on a Server Agent are not removed automatically by the BoKS uninstall routine.

2. Log in to the host and become root:

   ```
   $ su
   ```

3. If this is a BoKS Server Agent that was installed using a native package (not a tar archive package), uninstall BoKS using the native program:

   For example, to uninstall an RPM:

   ```
   # rpm -e boks-client
   ```

   Once this operation has completed you can jump straight to step 7.

> **NOTE:** When you uninstall the native package, some files are not automatically removed from the **/opt/boksm/etc** and **/opt/boksm/var** directories and must be manually removed.

4. Run the **uninstall** program:

```
# /opt/boksm/sbin/uninstall
```

   The following is displayed:

```
Do you wish to go ahead (y/n)
```

5. Type `y` and press ENTER to start the **uninstall** program.

   If this is the Master, a backup of the security database is created:

```
Database saved to /var/tmp/boksm.sav
```

6. When the uninstall process is finished the following is displayed:

```
Done
```

7. Delete the host from the BoKS database using the Delete button in the **host listing in FoxT Control Center** or change the host type to Other Host using the **Change host type** button. If you do not delete the host, error messages will be written to the log every time the Master tries to establish communication (for a Replica, every ten minutes).
8. If you use SSH and the operating system includes sshd, re-enable and start the original **sshd** to restore the system to its original configuration.

Uninstalling The Presentation Server

Note: If you have customized the interface in any way, for example if you have modified style sheets and images used in the interface, these should be backed up before uninstalling in case they are needed in future.

To uninstall the presentation server:

1. Open a terminal on the presentation server host.
2. Stop the presentation server processes:

```
# /etc/init.d/bccps stop
```

3. Run the **uninstall** program.

```
# /opt/bccps/sbin/uninstall
```

4. You are prompted whether you want to delete the configuration directory **/etc/opt/bccps**.

   To delete the directory, press **Enter**.

5. You are prompted whether you want to delete the var directory /var/opt/bccps.

   To delete the directory, press **Enter**.

6. An overview of the settings is displayed and you are prompted whether you want to delete the selected directories.

   To continue with the selected settings, type **y** and press **Enter**.

The presentation server software is removed, together with the directories you selected for deletion.

Upgrading BoKS Manager

This chapter describes how to upgrade the BoKS Manager Master and Replicas from version 6.7 and later and BoKS Server Agents from version 6.6.1 and later to 7.2.

> **NOTE:** It is possible to upgrade from BoKS versions earlier than 6.6.1 but only via an intermediary upgrade to, for example, BoKS 6.7. For information on this intermediary upgrade, see the documentation set for the target version, for example the BoKS 6.7 documentation set.

Upgrading BoKS Manager includes the topics:

- Upgrade Background
- Key Features and Issues of Upgrading
- Mixed BoKS Environments
- Prerequisites for Upgrading
- Overview of Upgrading a BoKS Domain
- Rolling Upgrade to BoKS Manager 7.2
- Upgrading the Master and Replicas
- Upgrading BoKS Server Agents for Unix/Linux
- Server Agent Upgrade Basics
- Upgrading a Server Agent for Unix/Linux

See also:

- Installing BoKS Manager Patches
- Installing Hotfixes, Patches and Upgrades

Upgrade Background

Topics include:

- Key Features and Issues of Upgrading
- Mixed BoKS Environments
- Prerequisites for Upgrading
- Overview of Upgrading a BoKS Domain

See also:

- Installing BoKS Manager Patches
- Installing Hotfixes, Patches and Upgrades using boks_upgrade
- The chapter “Planning Installation”
- The chapter “System Configuration” in the *Administration Guide*

Key Features and Issues of Upgrading

Key features and issues of BoKS Manager 7.2 that you need to be aware of while upgrading are:

- **Support for BoKS Server Agent for Windows removed**

  From BoKS Manager 7.2, support for BoKS Server Agent for Windows, and consequently Windows user types and access methods, is removed. When you restore a pre-7.2 database as part of upgrading:

  - Users of type **WINLOC** or **WINDOM** are removed.
  - hosts of type **WINBOKSCLIENT** or **WINDYNIPCLIENT** are converted to **NONBOKSHOST**.
  - The access methods that are no longer supported (**NETSHARE**, **WINLOGIN**, **WINNETSHARE**, **WINRDP** and **WINRUNAS**) are removed from Access Rules.
  - Program group members that refer to Windows programs are removed.

- **Support for SafeWord tokens removed**

  From BoKS Manager 7.2, support for authentication using SafeWord tokens is removed. Any Access Rules in the database that have the `desgold` or `harddesgold` modifiers for Safeword authentication are not restored when you upgrade. These Access Rules are instead listed in the file **$BOKS_tmp/deleted-access-rules-<**pid of boks_bru**>.txt**. You can review the Access Rules in this file, if any, and determine whether they need to be recreated with an alternative authentication method in the new BoKS database.

- **Support for xRBAC removed**

  From BoKS Manager 7.2, support for xRBAC is removed. When you upgrade a database from a previous version to BoKS 7.2, any xRolesets, xRoles and Access Rules in the database that use the access methods `SWROLE` to enter a role will be removed, and this access will not work on BoKS Server Agents.

  When you install BoKS Server Agent 7.2 or later on hosts, BoKS no longer plays a role within RBAC on AIX or Solaris, and the RBAC functionality is no longer included on Red Hat.

- **Support for virtual cards removed**

  In BoKS 7.2, support for virtual cards is removed. If you have user virtual cards in your BoKS domain, these are deleted when you upgrade. All host virtual cards and CA virtual cards are converted to PKCS#12 files. This is done automatically for host virtual cards and for CA virtual cards if you have saved the CA passwords. If you have not saved the CA passwords, the BoKS restore program boks_bru prompts you to rerun the CA conversion program in interactive mode and provide the relevant password(s).

- **Functional account support modified**

  In BoKS versions prior to 7.2, you could define which user accounts were functional accounts by adding them in the file **$BOKS_etc/funcacc.conf**. When you upgrade to BoKS 7.2 **boks_bru** updates any users in the **$BOKS_etc/funcacc.conf** file, making them functional accounts, when you restore a pre-7.2 database backup into 7.2. If this operation is successful, the **funcacc.conf** file is removed. This is done using the new tool **$BOKS_lib/funcaccupdate**. The template file

$BOKS_etc/funcacc-template.conf is no longer part of the BoKS 7.2 package. Any old **$BOKS_etc/funcacc.conf** is no longer backed up by **boks_bru**.

- **Upgrading with ABAC**

  If you are using BoKS Attribute-based Access Controls to define system administration privileges in FoxT Control Center, you may need to update your **$BOKS_etc/bccas-abac.yaml** configuration file if it contains references to areas removed from BoKS Manager version 7.2, such as xRBAC and Windows Server Agents. If the **bccas-abac.yaml** file does contain such references, **boks_bccasd** starts but logs error messages in **boks_errlog**. You can run the command **bccasabac** to check the file and print the error messages on standard error. Note that an updated template file for ABAC, **$BOKS_etc/bccas-abac-template.yaml**, which does not include the removed functionality, is installed when you upgrade to BoKS Manager 7.2 on the Master.

- **Password history length enforcement**

  The maximum length for password history is 20 passwords, but in BoKS 7.1 and earlier this limit was not enforced so it was possible to set a much larger value creating high load on Replicas when passwords are changed. BoKS 7.2 now enforces password history max length and on upgrade the password history length is reduced to 20 if it is set higher.

- **Changes to password lookalike check**

  Enancements made to the password lookalike checking function in BoKS 7.2 renders the BoKS ENV variable `CHANGE_PSW_DIFF` no longer relevant after you upgrade. Password lookalike checking can instead be configured using the ENV vars `CHANGE_PSW_ED_QUOTIENT` and `CHANGE_PSW_LCS_PERCENT` - see the BoKS man page ENV for details.

- **BoKS Password Manager upgrade**

  From BoKS Manager 7.1, BoKS Password Manager is no longer a separate module, but is an integrated part of the Master installation (referred to as BoKS password checkout), and does not need to be installed as a separate extension package.
  The encryption algorithm used to encrypt checkout enabled passwords is changed from RC6 to AES256 in version 7.1 and later. If you have been using an older version of BoKS Password Manager before you upgrade, the password encryption key on the Master (**$BOKS_etc/pwm/keys/pwmd.key**) must be backed up before you upgrade and copied to the same location on the Master after you upgrade. After copying the file, you must run the program **pwm-convert-old-db**, which is available as an add-on package for BoKS Manager 7.2.

  > **NOTE:** If any user does not have at least one password decrypted, the pwm-convert-old-db program will not convert any passwords and will return the message "pwm-convert-old-db: Failed to decrypt some users' passwords. Wrong key?" In this case you must either 1) restore the correct key if no passwords can be decrypted or 2) set new passwords using the new key if some passwords can't be decrypted.

- **Local and remote handling of keystroke logs**

  When you upgrade to BoKS 7.2 the default setting for handling keystroke logging is “local”. If you have applied hotfix HFBM-0173 in your BoKS 7.0 domain and have the global default set to “remote”, it is reset to “local” when you upgrade.

You can set the global default to “remote” using the command `bksdef -g remote`. Note, however, that remote logging in large BoKS environments can negatively impact domain performance.

- **Unix group format change**

  In BoKS Manager 7.0, the way Unix group management is implemented changed to such an extent that it is not possible to automatically transfer the Unix group information in a pre-7.0 database to a 7.2 database. Due to this change, when you restore a pre-7.0 database as part of the upgrade procedure, Unix groups are not restored, and any users with secondary Unix group management enabled in the database are set to not have secondary Unix group management enabled.

  In order to help you with the migration to BoKS Manager 7.0 and later Unix group management, FoxT provides a **Unix Group Migration Tool** which is available as a separate download from the FoxT customer support website. Note that Unix Group migration is best planned well in advance of the actual upgrade to ensure you have time to properly configure groups and assignments for the BoKS 7.2 domain.

  For more details of how the tool works, see the manual, *BoKS Manager 7.0 Unix Groups Migration Guide*, which accompanies the tool.

- **Audit log format changes**

  BoKS Manager 7.0 introduced a redesigned audit logging infrastructure with a different format for log messages and different name and location for log files compared with earlier versions. If you are upgrading from an earlier version than 7.0, you must back up your old and current log files pre-upgrade in order to be able to access them post-upgrade. This can be done using **boks_bru** (not recommended for large log files) or manually using another program. Note that if you use **boks_bru**, the active log file is not backed up, only the completed log files; The active log file must be backed up separately.

  If you back up log files using **boks_bru**, the log files are automatically saved to the new log file storage location **$BOKS_var/auditlog** when you restore the backup after upgrading. If you manually back files up, these must be manually copied to the new log file storage location.

  Once you have upgraded, if required you can use the program **boksold2newlog** to convert audit log files from the old format to the new format so that they are readable in FCC 7.2. All converted files must also be saved in the new log file storage location (default **$BOKS_var/auditlog**) and renamed to comply with the new filename format for 7.0 and later, which has the following format:

  ```
  yyyymmddTHHMMSS.microseconds-yyyymmddTHHMMSS.microseconds.
  ```

  For example, the old format log file `L140408_223729-140430_085457` could be renamed to `B20140408T223729.000000-20140430T085457.000000`.

  For more information on using the program **boksold2newlog** to convert log files, see the man page **boksold2newlog**.

- **Licensing controls**

  BoKS Manager 7.0 and later includes licensing controls. If you are upgrading from an earlier version, you need to request a license from FoxT Customer Support as part of the upgrade process in order for your upgraded domain to function correctly. See the relevant steps in the

procedure for installing the Master for information about how to do this.

For more details about licensing, see Licensing Background.

- **Modified default location on Master for keystroke log files**

  The default location for storing completed keystroke log files on the Master, `/var/opt/boksm/kslog`, changed in BoKS Manager 7.0 to `/var/opt/boksm/kslog/ok`. This is the location that BoKS 7.2 and FCC 7.2 search for keystroke log files. If you want to access older keystroke log files you should back these up to a secure location before upgrading, then copy them to the new location after upgrading. Note that the **ENV** variable used to configure the location for keystroke log files on the Master has changed from `KSLOG_MASTER_LOGFILES_LOCATION` to `KSL_LOGFILE_FDLOCATION`.

- **$BOKS_var as a mount point**

  Note that if **$BOKS_var** is a mount point, the **uninstall** command does not remove all files and directories from this location. These must be removed manually before you install the new version of BoKS as part of the upgrade.

- **DTHOST host type removed**

  In BoKS Manager 7.1 the host type `DTHOST` was removed, as was support for BoKS Desktop auto-registration. If you are upgrading from pre-version 7.1 and have hosts with the type `DTHOST` registered in the database, these hosts will be converted to type `NONBOKSHOST` when you restore the database after upgrading if the `DTHOST` has at least one IP address assigned. Hosts of type `DTHOST` without any assigned IP address are removed from the BoKS data when restoring the database and a message with the removed hostname is printed to standard error.

- **Protocol support for communication with RSA Authentication Manager**

  RSA Authentication Manager version 8.x can in addition to the traditional UDP based protocol also use a HTTP/TCP based protocol. BoKS 7.2 RSA Authentication Manager Agents use the HTTP/TCP based protocol for all platforms except Linux variants on the PowerPC platform where the traditional UDP based protocol is used.

  When upgrading a BoKS host that has previously used SecurID authentication with the UDP protocol (BoKS 6.7 and earlier) the node secret must be renewed before SecurID authentication with TCP protocol can be used.

  For full details, see *Authentication Manager Communication Protocols and BoKS Versions* in the Administration Guide.

- **The $BOKS_etc/brpf file is not automatically updated after upgrading**

  The **$BOKS_etc/brpf** file contains an encrypted version of the root password, enabling system administrators to log in as root from tty console in the event of a host with BoKS protection activated being unable to contact BoKS to authenticate users. The **brpf** file is not automatically updated when you reinstall BoKS Manager on a host, for example during an upgrade, and must be manually updated in order to ensure that emergency root access from tty console will work.

  The following command, run in a BoKS shell, can be used to update the **$BOKS_etc/brpf** file on all BoKS hosts in the domain, ensuring local login for root in case of a problem will work:

  BOKS # boksdiag updpasswdentry ‘lsbks '*:root''

- **The $BOKS_var/ssh_userpubkeys file is now automatically backed up and restored**

  The **$BOKS_var/ssh_userpubkeys** file, which is used to keep track of which SSH user Public Keys have been provisioned on a host, was not automatically backed up and restored when you upgraded Server Agents with the **upgrade_client** script. This file is now backed up and restored automatically by the upgrade script.

  Note that this is a new file introduced in BoKS Manager version 6.7 as part of the SSH user Public Key management feature.

- **Shared Memory for Replicas**

  When you restore the database when upgrading the Master, the new **$BOKS_etc/ENV** file will have the shared memory value you had in the previous installation. However, the shared memory value is not restored on Replicas. If you have been using a different value, you must reset the **SHM_SIZE** to the value it has on the Master, before you do setup on the Replica.

- **Keystroke log files**

  Keystroke log files on the BoKS Master are not automatically backed up by **boks_bru**, but are stored by default in a BoKS directory, so these must be manually backed up and restored after the upgrade. For details of files and locations, see "Managing Keystroke Logging" in the *Administration Guide*.
  In addition, if you are using encryption to protect keystroke log files, certain other files must be manually backed up and restored post-upgrade. For details, see "Keystroke Log File Protection Backup" in the Administration Guide.

- **Protocol logging variables in the BoKS ENV file**

  The following variables are written to the BoKS **ENV** file and set to `on` at installation of BoKS Manager 7.2, enabling protocol logging:

  - `BOKS_SSH_FTL`
  - `SSHD_CMD_LOG`

  Note that if you are upgrading, any of these variables that you did not have set before upgrading will be written to the BoKS **ENV** file and set to `on` when you restore your BoKS database.

- **Server Agent for Unix/Linux Upgrade**

  Server Agents are now upgraded with a special script that automatically backs up files, upgrades, restores the earlier configurations and activates BoKS Protection (if it was activated at time of upgrade), making the whole process quick and easy. See Upgrading BoKS Server Agents for Unix/Linux. Another script allows you to safely, easily and securely push out upgrades to multiple Server Agents, for example, to a Host Group. See Installing Hotfixes, Patches and Upgrades using boks_upgrade

See also:

- Upgrade Background

Mixed BoKS Environments

BoKS Manager 7.2 supports a mixed BoKS environment.

The only restriction is that the Master and all Replica(s) must be of the same version and patch level, to ensure correct operation of BoKS server functionality and replication. FoxT also recommends that you install the same set of hotfixes on the Master and all Replicas, unless the hotfix is labelled “Applies to Master / failover Master only”.

Version 7.2 Master/Replicas can co-exist with version 6.6 - 7.1 BoKS Server Agent for Unix/Linux hosts.

See also:

- Key Features and Issues of Upgrading
- Upgrade Background

See also:

- “Launching FoxT Control Center” in the chapter “BoKS Manager Administration” in the *Administration Guide*

Prerequisites for Upgrading

Existing Versions

You can upgrade to BoKS Manager 7.2 on a Master or Replica starting from one of these versions:

- BoKS Manager 6.6.x
- BoKS Manager 6.7.x
- BoKS Manager 7.0.x
- BoKS Manager 7.1.x

Compatibility with Other BoKS Components

BoKS Manager 7.2 is compatible with BoKS Server Agents for Unix/Linux 6.6, 6.7, 7.0 and 7.1.

BoKS Manager 7.2 is compatible with FoxT Control Center 7.2.

See also:

- Mixed BoKS Environments
- Installing Hotfixes, Patches and Upgrades using boks_upgrade.

Overview of Upgrading a BoKS Domain

A BoKS Manager domain consists of a Master, possibly one or several Replica(s), and BoKS Server Agent host(s) (previously called Clients in earlier versions of the product).

Upgrading includes the basic steps:

- backing up the security database
- removing old BoKS Manager software on the Master
- installing the new version on the Master
- restoring the previously saved database
- removing and installing new software on all Replicas
- upgrading any BoKS Server Agents that may be wanted or needed in later versions.

In addition, depending on your environment, you may need to reconfigure some settings and to configure BoKS Manager for new features and functionality that you intend to use in version 7.2.

Note: As part of the upgrade you must also upgrade FoxT Control Center to the appropriate version for web administration of your BoKS domain. For information on the correct version of FoxT Control Center for this version of BoKS Manager, see Web Administration Requirements. For detailed instructions on upgrading FoxT Control Center, see the FoxT Control Center documentation set.

For details, see Rolling Upgrade to BoKS Manager 7.2.

This basic rolling upgrade procedure allows you to maintain service during upgrade, with Replicas handling authentications while the Master is being upgraded. The only loss of service is that the audit log will be missing for the time that the Master is down. If you want the log to be continuous, you can convert a Replica to be Master during the period that the Master's is down (see *Converting Between Master, Replicas and Server Agents* in the chapter "Backup, Restore and Recovery" in the *Administration Guide*). Another option is to gather cached logs from pre-version 7.2 Replicas in your domain. To do this, run one of the following commands on the Replica before you uninstall the old version of BoKS.

For BoKS versions pre-7.0, run:

```
BoKS # boksdiag fque -bridge -printlogs > <outputfile>
```

For BoKS 7.x versions, run:

```
BoKS # bokslogadm -qv > <outputfile>
```

These commands extracts log messages from the Replica queue to a file where `<outputfile>` is the name of the file to direct output to.

If you are upgrading from a pre-7.0 version of BoKS, the output file has the same format as pre-7.0 audit logs, although there is no initiating header or terminating footer. However the file can be viewed using the pre-7.0 **bkslog** program, or saved to a secure location and converted to the new log format using the program **boksold2newlog** if you want to view it in the 7.2 domain.

If you can accept downtime for authentications, you can modify the procedure to do an offline upgrade, which may be even simpler.

See also:

- Upgrading BoKS Server Agents for Unix/Linux
- Installing Hotfixes, Patches and Upgrades using boks_upgrade.

Rolling Upgrade to BoKS Manager 7.2

The following sections give detailed instructions on performing an upgrade from BoKS Manager 6.6/6.7/7.0/7.1 Masters and Replicas to BoKS Manager 7.2 while maintaining continuous ability to handle authentications and almost continuous logging.

Topics include:

- Upgrading the Master and Replicas

See also:

- Installing BoKS Manager Patches
- Upgrading BoKS Server Agents for Unix/Linux
- The chapter "Installing BoKS Manager"
- Installing Hotfixes, Patches and Upgrades using boks_upgrade.

Upgrading the Master and Replicas

Note: The rolling upgrade procedure below allows you to continue to handle authentications, but there may be a loss of password changes and log updates during the time the Master is being upgraded. If necessary to minimize log losses, you can convert a Replica to be Master during the period that the original Master is down (see *Converting Between Master, Replicas and Server Agents* in the chapter "Backup, Restore and Recovery" in the *Administration Guide*). Note that to access log files produced in the old version after upgrading, they need to be converted - see Audit log format changes.

Before upgrading, read Upgrade Background, including Prerequisites for Upgrading.

To upgrade the BoKS Manager Master and Replicas to version 7.2:

Note: Make sure the new Master is registered.

1. Upgrade the **Master** as follows:
   - Log in to the Master and become root.
   - If you have been using BoKS SSH, backup SSH keys in the **$BOKS_etc/ssh** directory to a safe location.
   - If you have been using BoKS Password Manager, back up the encryption key **$BOKS_etc/pwm/keys/pwmd.key** to a safe location.
   - Start a new log file.

     If you are upgrading from BoKS 7.0 or later use the following command:

```
BoKS # bokslogadm -n
```

If you are upgrading from a BoKS version earlier than 7.0 use the following command:

```
BoKS # logadm -n
```

- Back up the database (for use if the upgrade fails) by typing from a BoKS shell:

  ```
  BoKS # boks_bru -p -l -d filename
  ```

  - The `-p` switch saves the database in shar format.
  - The `-l` switch signifies that the log files should be backed up (leave this switch out of the command if you do not want to back up the log files).
  - The `-d` signifies the device/file to back up to. See the man page on the **boks_bru** command for more information.

    Note: This command can be run while the Master BoKS processes are running. The **boks_bru** script will stop and restart BoKS as needed.

- Using FoxT Control Center, or the CLI, change the Host Type of all Replicas from Replica to **BoKS Host**. From the CLI use the following command:

  ```
  BoKS # hostadm -h <replicaname> -t UNIXBOKSHOST
  ```

  For earlier BoKS versions you must also specify the `-a` and `-i <primaryIPaddress>` options.

  For details, see the online help for FCC or the old BoKS Administration GUI as appropriate.

- Start a new log file and back up the database **again** for using to restore after the upgrade. Use a different file name than in the first backup. For details, see the backup above.

  To start a new log file you can use the following CLI command if upgrading from BoKS 7.0 or later:

  ```
  BoKS # bokslogadm -n [-f]
  ```

  Or the following CLI command if upgrading from an earlier version than BoKS 7.0:

  ```
  BoKS # logadm -n [-f]
  ```

  You can either back log files up using **boks_bru** or back them up manually, which is a better option for large log files. See also Audit log format changes.

- Uninstall BoKS on the Master, by typing:

  ```
  BoKS # uninstall
  ```

  Note that you can add the option `-n` if you do not want to create a backup of the BoKS database when you uninstall.

Note: At this point, you will no longer be able to perform BoKS Manager administration. Any further log information (on authentications) will be lost (unless you choose to convert a Replica to a Master). If users change their passwords, they will still have to use their old passwords and change passwords again when the Master is brought back on line.

- Log out of the BoKS shell by running **exit** until the BoKS prompt disappears:

```
BoKS # exit
```

- Install BoKS Manager 7.2 on the Master as described in Installing the Master.
- Restore the security database on the Master using the backup taken just before uninstall, by typing:

```
BoKS # boks_bru -u -d path to file or device
```

- If you are upgrading from a pre-7.0 BoKS version, convert any backed up log files that you want to access in the upgraded system and if required save them to the new location for log files. Note that log files backed up using **boks_bru** are automatically saved to the new log file location, but must be converted to be readable in version 7.2. For details on converting files, file names and locations see Audit log format changes.
- If needed, adjust any IP addresses in the **$BOKS_etc/bcastaddr** file or encryption settings in the **$BOKS_etc/bremotever** file. Reboot BoKS if any files were changed.
- Manually restore SSH keys and re-configure any SSH settings that you use (enabling SSH was included in the procedure Installing the Master). If you restore the original SSH key as described above the keys are already in the database and there is no need to run **ssh_keyreg**.
- If you are using password checkout (BoKS Password Manager), manually restore the backed up **$BOKS_etc/pwm/keys/pwmd.key** file, install the Password Manager conversion program which is available as an add-on package for BoKS Manager 7.2, and run the following command:

```
BoKS # pwm-convert-old-db
```

- Run the **fccsetup** utility on the Master to set up the administration server for FoxT Control Center. Then install the FoxT Control Center presentation server.

  For details, see Quick Start for FoxT Control Center.

  The FoxT Control Center is the administration interface in BoKS 7.2. The old BoKS Administration GUI is not included in this release.

- Activate BoKS protection on the Master by typing the following at the command line:

```
BoKS # sysreplace replace
```

- Exit the BoKS shell by typing:

```
BoKS # exit
```

- For any Server Agent for Unix/Linux or Agent host that uses a time zone different from the Master or the host's configured Replica, specify the time zone for the host using the CLI option `hostadm -z` or the host details page in FoxT Control Center.

2. Upgrade **Replicas**, carrying out the following steps for each Replica:

- Log in to the Replica and become root.
- If you have been using BoKS SSH, backup SSH keys in the **$BOKS_etc/ssh** directory to a safe location.
- Uninstall BoKS on the Replica, by typing:

```
BoKS # uninstall
```

- Logout of the BoKS shell by running `exit` until the BoKS prompt disappears:

```
BoKS # exit
```

- Install the new BoKS Manager 7.2 version software, including setting shared memory with the variable `SHM_SIZE`, adjusting any necessary IP addresses in **$BOKS_etc/bcastaddr** and creating a host certificate, all as described in Installing a Replica.

  Before you set the host up as a Replica, manually restore SSH keys and re-configure any SSH settings that you use (enabling SSH was included in the procedure Installing a Replica).

  If you restore the SSH keys after setting the host up as a Replica, publish the old SSH public host key for the Replica in the BoKS database, use the following command:

```
BoKS # ssh_keyreg -w -f <host key file>
```

  For example:

```
BoKS # ssh_keyreg -w -f $BOKS_etc/ssh/ssh_host_rsa_key.pub
```

- In FoxT Control Center or the CLI on the BoKS Master, change the Host Type of the Replica from **Unix/Linux server agent** to Master/**Replica**, if you did not do so during the procedure Installing a Replica.

  You can change the host type using the following CLI command:

```
BoKS # hostadm -t REPLICA
```

- Run the **push_files** program on the BoKS Master to copy configuration files from the Master to the Replica. This is done to ensure that a Replica can be converted to a Master in case the normal Master fails.

  For example:

```
BoKS # push_files replica1
```

  To copy configuration files to the Replica with the hostname `replica1`.

  The files that are copied are those configured in the file **$BOKS_etc/distrib.cfg**.

- Activate BoKS protection on the Replica by typing the following at the command line on the Replica:

```
BoKS # sysreplace replace
```

- When all Replicas have been upgraded, verify that they are in contact with the BoKS

Master by running the following command on the Master:

```
BoKS # boksdiag list-servers
```

3. If using SecurID tokens for the new remote administration, distribute and assign any **RSA SecurID tokens** that may be needed.

Upgrading is now complete.

Upgrading BoKS Server Agents for Unix/Linux

This section applies to upgrading Server Agents from 6.6, 6.7, 7.0 and 7.1 to 7.2.

Upgrading BoKS Server Agents for Unix/Linux includes:

- Server Agent Upgrade Basics
- Upgrading a Server Agent for Unix/Linux With a tar Install
- Upgrading a Server Agent for Unix/Linux With Native Packaging

If you have BoKS Server Agents for Unix/Linux in your BoKS environment, you can choose whether to upgrade these to level 7.2. BoKS Server Agent for Unix/Linux was previously known simply as a Server Agent installation of BoKS Manager.

It is possible to run older supported versions of BoKS Server Agent for Unix/Linux in your environment after you have upgraded the Master and Replicas. However, Fox Technologies recommends upgrading Server Agents successively as platform coverage increases to take advantage of functionality improvements and issue fixes.

For details of currently supported Server Agent platforms, see System Requirements.

Server Agent Upgrade Basics

About Server Agent Packaging

The Server Agent distribution package is delivered in 2 variants:

- tar archive
- Native package, for example RPM

The tar archives are delivered as package for for Master/Replica/Server Agent (MRA) on platforms where Master and Replica are supported, but a Server Agent only package (A) for other platforms. Native packages are Server Agent only for all platforms. Currently native package installation is not supported for Master and Replica installs.

The form and content of the distribution package will therefore depend on the platform you are installing BoKS Server Agent for Unix/Linux on and whether you choose the tar archive or the native package.

Upgrade Programs

The primary programs for upgrading Server Agents are:

- For installations with native packages, the upgrade mechanism of the native package, for example RPM, must be used. For details see Upgrading a Server Agent for Unix/Linux With Native Packaging.
- **upgrade_client** upgrades a single Server Agent, backing up and restoring settings. For details, see Upgrading a Server Agent for Unix/Linux With a tar Install. When you can, run this program indirectly by running **boks_upgrade**, since **boks_upgrade** has certain features that make it easier, safer and more secure than running **upgrade_client** directly. This only works for installations with tar archives.
- **boks_upgrade** upgrades multiple Server Agents remotely and automatically, by calling **upgrade_client** once for each host. For background on **upgrade_client**, see below. This only works for installations with tar archives. For using the program, see Installing Hotfixes, Patches and Upgrades.

Backed Up Files

The following files and directories are backed up from the old installation and restored when you perform the Server Agent upgrade:

File or Directory
$BOKS_etc/bcastaddr
$BOKS_etc/bokscron.conf
$BOKS_etc/bokspam.conf
$BOKS_etc/bremotever
$BOKS_etc/brpf
$BOKS_etc/filmon.conf
$BOKS_etc/keys/host.kpg
$BOKS_etc/profiles/*
$BOKS_etc/radiusclient/server
$BOKS_etc/ssh/ssh_config
$BOKS_etc/ssh/ssh_host_dsa_key
$BOKS_etc/ssh/ssh_host_dsa_key.pub
$BOKS_etc/ssh/ssh_host_key
$BOKS_etc/ssh/ssh_host_key.pub
$BOKS_etc/ssh/ssh_host_rsa_key
$BOKS_etc/ssh/ssh_host_rsa_key.pub
$BOKS_etc/ssh/ssh_host_ecdsa_key
$BOKS_etc/ssh/ssh_host_ecdsa_key.pub
$BOKS_etc/ssh/ssh_host_ed25519_key
$BOKS_etc/ssh/ssh_host_ed25519_key.pub
$BOKS_etc/ssh/ssh_host_key
$BOKS_etc/ssh/ssh_host_key.pub
$BOKS_etc/ssh/ssh_host_rsa_key
$BOKS_etc/ssh/ssh_host_rsa_key.pub
$BOKS_etc/X11/Xdefaults
$BOKS_var/bic/*.rep
$BOKS_var/spool/cleanupdata
$BOKS_var/ssh_userpubkeys

Notes on the table

- In addition some custom configuration options in **$BOKS_etc/ssh/sshd_config** are transferred to the new sshd_config file. For SSH config files, exceptions to migrating changed attributes are:
  1. any changes to the `PermitTunnel` attribute are not migrated as allowing this presents a security risk. This must be turned on manually after migration if it is wanted.
  2. The attribute `KerberosAuthentication` was set to `yes` in the BoKS 6.6 **sshd_config..active** file. This attribute is now ignored when BoKS is active (and kerberos authentication is controlled by flags to Access Rules), so it is not migrated.
- Some variables from the old ENV file are also transferred to the new ENV file.
- The BIC integrity check configuration in crontab is saved.

Files That Are Not Backed Up

The **upgrade_client** program does not back up and restore the following files. If you have made modifications to these files, make sure that you save a copy of them in another location before you run **upgrade_client** so that you can restore them after the Server Agent has been upgraded:

- The PAM configuration files:

  $BOKS_etc/pam.conf..ssm for Solaris and AIX platforms

  $BOKS_etc/pam.d/* for Linux platforms.

- **$BOKS_etc/errlog.msgs** and **errlog.ignore**

If these files contain any customized additions that you want to retain, then save the additions and edit them back into the files after upgrade.

Upgrading a Server Agent for Unix/Linux With a tar Install

This section describes how to upgrade a single BoKS Server Agent for Unix/Linux host using the program **upgrade_client**. This method can only be used for Agents that were installed using the tar package. Agents that were installed using the native package program must be upgraded using the native package program. For information on this procedure see Upgrading a Server Agent for Unix/Linux With Native Packaging.This procedure can be done either before or after you have upgraded the BoKS Manager Master and Replicas. Before you begin, read Server Agent Upgrade Basics.

> **NOTE:** You can automate the **upgrade_client** procedure to upgrade multiple Server Agents, using the program **boks_upgrade**. For details, see Installing Hotfixes, Patches and Upgrades using boks_upgrade and the man page **boks_upgrade**.

The upgrade_client Program

For installations using the tar archive package, upgrading a BoKS Server Agent for Unix/Linux involves running the **upgrade_client** program from the BoKS Manager or BoKS Server Agent for Unix/Linux

distribution package. The program **upgrade_client** is located in the root directory of the distribution, at the same level as the **install** program. The complete distribution should be either saved on the Server Agent or at a location accessible from the Server Agent.

Operations Performed

The **upgrade_client** program performs the following operations in order:

- Saves important system files and configuration information in a backup directory
- Uninstalls the existing BoKS Server Agent for Unix/Linux
- Installs the current latest version of BoKS Server Agent for Unix/Linux
- Sets up the installation as a Server Agent
- Restores the saved system files and configuration information
- If BoKS Protection was active on the host before you began the upgrade, it is automatically activated again by the upgrade program. If it was not active, you must manually activate BoKS Protection on the host after upgrading.

Upgrade Logging

The **upgrade_client** program logs its progress to the **/tmp/boks_upgrade_client."pid"/boks_upgrade_client.log** file. Here you can see in detail the outcome of the various steps of the upgrade procedure. The return code of the program is included in this file and helps you determine whether or not the upgrade has completed successfully. See *Return Codes* below.

Node Keys and Encryption

The **upgrade_client** program automatically uses the same node key for the Server Agent as it had before. This node key can be changed after the upgrade, if required. It is recommended to reset the node key after you upgrade to BoKS Manager 7.2 from an earlier version than 6.6.1 so that the Server Agents receive a 256-bit node key that can be used with AES-256 encryption.

The node key must be reset both in the BoKS database and locally on the Server Agent. To reset the node key stored in the BoKS database, use the **Set Nodekey** button in the expanded host listing in FoxT Control Center. To reset the local copy of the node key on the host, use the **hostkey** command line program on the BoKS Server Agent.

Although the default BoKS Manager 7.2 bridge encryption algorithm is AES-256, when upgrading a BoKS Server Agent with the **upgrade_client** program, if the program detects that the local nodekey is only 128-bit, the program adds `BRIDGE_CRYPT=CRYPT_AES_128` to the Server Agent **$BOKS_etc/ENV** file.

BoKS Servers should also be configured to use AES_128 when communicating with the Server Agent until a new (256-bit) nodekey has been set both locally on the Server Agent and in the BoKS database.

It is also possible to specify an encryption algorithm for the upgraded Server Agent using command line option `-c <cryptalg>` to the **upgrade_client** program, where *cryptalg* can be one of the following strings:

- AES256
- AES128
- RC5128

> **NOTE:** The RC5-128 algorithm is deprecated and will be removed in future versions of BoKS Manager. It should only be used if there is a need to communicate with pre-6.6 BoKS Manager.

Remember that if `AES256` is used, the node key must be reset both on the BoKS Server Agent and in the BoKS database on the Master.

See also Key Features and Issues of Upgrading.

Server Agent Environment Variables

The environment variables in the **$BOKS_etc/ENV** file of the old installation are saved by the program. It then restores any variables that differ from the default variables in the **$BOKS_etc/ENV** file of the new installation, excepting those specified by the `ENVDONTSAVELIST` variable.

Return Codes

The following table describes the different codes that the **upgrade_client** program can return, together with the appropriate action to take if they occur:

Code	Description	Action
0 - Client successfully upgraded	The upgrade has completed problem free.	None
1 - Failed: installation still intact	The upgrade failed, but the original installation is still usable.	Check where the upgrade failed in the **/tmp/boks_upgrade_client.“pid”/boks_upgrade_client.log** file.
2 - Failed: upgrade done but BoKS couldn’t be activated	The new software has been installed, but BoKS Protection has not been activated on the host.	Activate BoKS Protection on the Server Agent using the command line or from FoxT Control Center.
3 - Failed: new Server Agent partially installed, BoKS unusable	The installation of the upgrade was interrupted, and a partial installation of BoKS Server Agent for Unix/Linux has been done.	1. Check where the upgrade failed in the **/tmp/boks_upgrade_client.“pid”/boks_upgrade_client.log** file. 2. Do an **uninstall** of BoKS. 3. Do a manual install of the new Server Agent using the **install** program. See Installing BoKS Server Agent for Unix/Linux. 4. Reconfigure the Server Agent.
4 - Failed: new Server Agent installed but ‘setup’ not done	The new software has been installed on the host, but it has not been setup as a Server Agent.	Manually run **setup** to specify the host as a BoKS Server Agent for Unix/Linux host.
5 - Failed: new Server Agent installed but won’t boot	The new software has been installed and the host has been set up as a Server Agent, but reboot of BoKS failed. Reboot is necessary to get the Server Agent to use the proper node key.	Manually reboot BoKS on the Server Agent.

6 - Failed: upgrade ok but wrong node key is used	The upgrade was completed but the node key was not successfully set for the Server Agent	Update the node key for the host to the correct value in FoxT Control Center using the **Set Nodekey** button in the expanded host listing.
7 - Failed: New Server Agent installed but failed to restore data	The new software has been installed but configuration data has not been restored.	Reconfigure the Server Agent.
8 - Failed: Error in usage	The upgrade script cannot be run on the host.	Check where the upgrade failed in the **/tmp/boks_upgrade_client.“pid”/boks_upgrade_client.log** file.

WARNING: The Server Agent Upgrade program will **unlock** any locked X-sessions on the Server Agent you run it on. These user sessions are also removed from **bwho** and **btmp** file, so you cannot see that they are logged on. Have users log out before you run the Server Agent Upgrade, to avoid x-locked sessions becoming unlocked as a result of the upgrade

To upgrade a BoKS Server Agent for Unix/Linux host (tar package):

1. Make sure the distribution package is saved in uncompressed form on the host, for example in the **/downloads** directory or on a networked device.
2. Log in to the host, become root.
3. Add the Master's IP address in **$BOKS_etc/bcastaddr**, if it is not already there.
4. If you were in a BoKS shell, exit the BoKS shell before installing or upgrading.
5. Move to the directory where the uncompressed distribution package is stored.
6. Run the **upgrade_client** program, optionally specifying the encryption algorithms to use on the command line (for details, see Node Keys and Encryption):

   ```
   # ./upgrade_client
   ```

7. Check the upgrade log file, **/tmp/boks_upgrade_client.“pid”/boks_upgrade_client.log**.
8. If the upgrade has completed successfully, you will need to manually activate BoKS Protection on the Server Agent if you deactivated it before upgrading.

Server Agent upgrade is now complete.

See also:

- Installing Hotfixes, Patches and Upgrades using boks_upgrade
- Server Agent Upgrade Basics
- Prerequisites for Upgrading
- Mixed BoKS Environments

Upgrading a Server Agent for Unix/Linux With Native Packaging

This section describes how to upgrade a single BoKS Server Agent for Unix/Linux host using the native package program. Agents that were installed using the native package program must be upgraded using the native package program, and Agents that were installed using the tar package must be upgraded using **upgrade_client** or **boks_upgrade**. This procedure can be done either before or after you have upgraded the BoKS Manager Master and Replicas. Before you begin, read Server Agent Upgrade Basics.

Configuration Files and Server Agent Environment Variables

How the environment variables in the **$BOKS_etc/ENV** file of the old installation are handled when you upgrade the native package differs depending on whether you are upgrading with an RPM package or a DEB package.

Environment Variables Upgrading With RPM Package

When you upgrade an RPM package, the new **$BOKS_etc/ENV** file with default environment variables is saved as the new file **/opt/boksm/etc/ENV.rpmnew**. You must manually configure the existing **$BOKS_etc/ENV** file to add or update any new configuration variables.

Environment Variables Upgrading With DEB Package

When you upgrade a DEB package, you are prompted on how to handle the update of the **$BOKS_etc/ENV** file as follows:

```
Configuration file '/opt/boksm/etc/ENV'
==> Modified (by you or by a script) since installation.
==> Package distributor has shipped an updated version.
What would you like to do about it ?  Your options are:
Y or I  : install the package maintainer's version
N or O  : keep your currently-installed version
D     : show the differences between the versions
Z     : start a shell to examine the situation
The default action is to keep your current version.
*** ENV (Y/I/N/O/D/Z) [default=N] ?
```

You can use these options to either use the new or old file, or manually configure the variables as required.

IMPORTANT: When BoKS is activated, it changes /etc/pam.d to be a symbolic link into the BoKS tree. When later upgrading BoKS, rpm detects this, reports conflicts and refuse to continue. There are two options:
1. Deactivate BoKS before upgrading.
2. Use rpm -Uvh --force to force the upgrade.

Regardless, the system's /etc/pam.d is restored when deactivating BoKS.
Deb packages do not have the same issue, and can simply be upgraded without deactivating BoKS or forcing the upgrade.

To upgrade a BoKS Server Agent for Unix/Linux host (native packaging):

1. Make sure the native package is saved on the host, for example in the **/downloads** directory or on a networked device.
2. Log in to the host, become root.
3. Add the Master's IP address in **$BOKS_etc/bcastaddr**, if it is not already there.
4. If you were in a BoKS shell, exit the BoKS shell before installing or upgrading.
5. Move to the directory where the native package is stored.
6. Run the packaging program with the upgrade option.

   For example to upgrade with an RPM package:

   ```
   # rpm -U boks-client-7.2.0.0-0.99.el7.x86_64.rpm
   ```

7. If the upgrade has completed successfully, you will need to manually activate BoKS Protection on the Server Agent if you deactivated it before upgrading.

See also:

- Installing Hotfixes, Patches and Upgrades using boks_upgrade
- Server Agent Upgrade Basics
- Prerequisites for Upgrading
- Mixed BoKS Environments

Deploying BoKS Server Agents for Unix/Linux

This chapter describes how to install and deploy BoKS Server Agents for Unix/Linux, used together with BoKS Manager in the FoxT ServerControl solution. For all post-installation configuration, for example, concerning user accounts, authentication, access control and auditing, see the relevant chapters in the *BoKS Manager Administration Guide*.

Topics include:

See also:

- The relevant Readme, which contains platform-specific installation information.
- Deploying FoxT ServerControl with BoKS Manager
- Domain Communication Basics
- Mixed BoKS Environments

Server Agents for Unix/Linux Background

Topics include:

See also:

- *Home Directory Host Configurations for Unix Hosts* in the chapter "Host" in the *Administration Guide*

BoKS Server Agent for Unix/Linux Basics

About Server Agent Packaging

For the majority of platforms, Fox Technologies distributes a Master/Replica/Server Agent (MRA) package that includes the BoKS Server Agent for Unix/Linux software. However for certain platforms, a BoKS Server Agent for Unix/Linux is distributed separately.

The form and content of the distribution package will therefore depend on the platform you are installing BoKS Server Agent for Unix/Linux on.

BoKS Server Agent for Unix/Linux only packages are delivered both as .tar packages and as native installation packages. The native installation packages provided are:

- RPM for Red Hat and SuSE
- DEB for Debian and Ubuntu

The installation process differs slightly between the tar packages and the native packages.

For the tar packages the steps are:

1. Uncompress the package.
2. Run install.
3. Run setup.

For the native packages the steps are:

1. Install the package.
2. Run setup.

System Requirements

For disk space requirements, see System Requirements.

The space requirements for `$BOKS_DIR` and `$BOKS_etc` are the same as for a BoKS Manager Master.

bcastaddr

When installing a BoKS Server Agent for Unix/Linux host, remember that the host must have contact with the Master or a Replica(s). If the Server Agent is not on the same subnet as the Master and Replicas, you must configure the host's **$BOKS_etc/bcastaddr** file to supply the IP addresses to at least one of these servers. See also Domain Communication Basics.

About Deploying BoKS Server Agents for Unix/Linux

Deploy BoKS Server Agent for Unix/Linux after you have installed the Master and imported or set up users in the database. Make sure that the Master and any Replicas that will service a particular BoKS Server Agent for Unix/Linux host, are working properly.

To install a BoKS Server Agent for Unix/Linux host, follow the procedure Installing BoKS Server Agent for Unix/Linux.

- In **setup**, select **Server Agent** mode.
- In FoxT Control Center, add the BoKS Server Agent for Unix/Linux host to the database, selecting the Host type **Unix/Linux server agent**.
- In order to do administrative tasks on the Server Agent when BoKS Protection is activated, the **root account** on the Server Agent must be defined as a BoKS user account, just like any other user account. You can import this account from the **/etc/passwd** file (at the same time as you import user accounts) using the **Import users** button on the host details page in FoxT Control Center. See also Local Root Account in BoKS Manager.

Check that communications with the Master and relevant Replicas are working.

Enable BoKS Protection of the BoKS Server Agent for Unix/Linux host, using the **Get BoKS Status > Activate BoKS** buttons in the expanded host listing in FoxT Control Center.

- For a new domain, you can disable Access Rule Access Control while you study access patterns of users and set up your Access Rules. See Using Learn Mode for details.

Always **deactivate and uninstall** a Server Agent before **deleting** it from the domain or changing its host type to **Other Host**.

When **uninstalling** a Server Agent, delete the host from the BoKS database after uninstalling it. Until you delete the host, it will still be a part of any existing Access Rules, so that it may open up a security hole to *protected* Server Agents since it will now be unprotected itself. See About Deleting, Changing Host Type or Domain and Uninstalling Server Agents. Note that uninstalling BoKS Server Agent for Unix/Linux removes all BoKS protection!

When **moving a Server Agent to another domain**, register it in the new domain and then delete it or change the host type to Other Host in the old domain (depending on your purposes). Until deleted or changed to Other Host, it may open up a security hole to Server Agents in the old domain (see Uninstalling, above) and error messages will be written to the log every time the Master tries to establish communication (for a Replica, every ten minutes).

BoKS Manager 7.2 also supports BoKS Server Agents for Unix/Linux with dynamic IP addresses used with Dynamic Host Configuration Protocol. Dynamic IP Server Agents are configured with specific setup options and registered as a different host type (Dynamic IP BoKS Host) in the BoKS database.

Note that a BoKS Server Agent for Unix/Linux is only protected when it is registered as a BoKS Host in a domain and BoKS Protection is activated. A host registered as Other Host is not protected by the Master on which it is registered as Other Host!

See also:

- Master Basics
- Replica Basics
- Install Directories
- Install Parameters and Options
- The Readme, which contains platform-specific installation information.
- *BoKS Manager Protection Processes on Unix Hosts* in the appendix "System Architecture" in the *Administration Guide*

About Deleting, Changing Host Type or Domain and Uninstalling Server Agents

Always **deactivate and uninstall** a Server Agent before **deleting** it or changing its host type to **Other Host**. BoKS Manager is designed to protect and update Server Agents. BoKS Manager is not designed to protect or update the host type Other Host, or hosts that once were part of a BoKS domain, but now are deleted.

Not deactivating and uninstalling BoKS while deleting or changing it to host type Other Host on the Master, leaves the host in an unclear situation:

- If a Server Agent with BoKS Protection activated is **deleted** from the database, the host will no longer receive updates from the Master to the **/etc/passwd** and **/etc/group** files. The host will continue to contact the Master for authentication, but all such attempts will fail because the Master no longer has the host with its node key in the database, and thus does not recognize this host as a Server Agent. Users will be denied access, but there will be no entry in the audit log.
- If a Server Agent with BoKS Protection activated is changed in FoxT Control Center to host type **Other Host**, the host will not receive updates from the Master to the **/etc/passwd** and **/etc/group** files.

Note: Deleting a Server Agent or changing its host type to Other Host (meaning it is no longer a Server Agent from the Master's point of view), removes BoKS Manager protection from the host. If you want protection, consider the following alternatives:

- If your purpose in deleting is to block all access to a host, you can accomplish this by assigning the authentication method LOCKED to an Access Rule for each relevant access method from anywhere to the Server Agent host (leaving the Server Agent as a BoKS host), using the program **boksrule**. For example, to block all SSH access:

  ```
  boksrule -a --policy -m SSH_ALL -f locked -t 00:00/00:00 -w
  1234567 -S '*:ANY/*' -D hostname
  ```

- Alternatively, you can block all access by adding a set of Restrictive Access Rules to this host, one for each Access Rule type (as viewed in FCC).
- For a way (using restrictive Access Rules) to ensure no access to BoKS-protected hosts in the domain via a host changed to Other host or during uninstallation of BoKS, see the man page **uninstall**.

When **uninstalling a Server Agent** or **moving a Server Agent to another domain**, delete the host from the BoKS database or change the host type to Other Host in the old domain. If you do not delete the host and there are queued messages for the host on the Master, error messages will be written to the log every time the Master tries to establish communication.

See also:

- Master Basics
- BoKS Server Agent for Unix/Linux Basics

- *BoKS Manager Protection Processes on Unix Hosts* in the appendix "System Architecture" in the *Administration Guide*

Prerequisites for Deploying BoKS Server Agent for Unix/Linux

Requirements for deploying BoKS Server Agents for Unix/Linux in the BoKS Manager domain include:

- All system requirements are met. See System Requirements.
- BoKS Manager is installed, initialized and basic configuration has been completed on the Master.

Note: If authentication and other services are not needed, the absolute minimum requirement for installing a Server Agent is that before running **setup**, the BoKS Manager Master must be set up and running, so that **setup** can contact the Master in real time.

See also:

- BoKS Server Agent for Unix/Linux Basics

Scripts for Unattended Installation

Prior to deploying the software across a domain with many hosts, plan the deployment with regard to user access and phased deployment of network segments, for the BoKS Server Agents for Unix/Linux. Then develop scripts for unattended installations of Server Agents, to be used after the BoKS Master and Replicas have been installed and configured.

For unattended installation of patches, hotfixes and upgrades, see Installing Hotfixes, Patches and Upgrades using boks_upgrade.

Unattended installations of BoKS Server Agent for Unix/Linux

For unattended installations of BoKS Server Agent for Unix/Linux, develop a script that will do the following:

- Perform the installation from a network installation directory.
- Perform any sort of customizing to the BoKS Server Agent for Unix/Linux host, for example integration with RSA Authentication Manager or copying the **$BOKS_etc/bcastaddr** file.
- Run the **setup** command to
  - set the node key, or
  - for pre-registered hosts, provide the pre-registration secret and if using pre-registration types, also provide the type
  - if required, specify configurations for offline login support

    - for BoKS Server Agents with dynamic IP address, set the HostID and network interface to monitor.
- Add the machine to the database with host type BoKS host (this step is not required for pre-registered hosts, which are registered in the database automatically).
- Verify communication with the Master and Replicas.

See also:

- *Scripting and Efficient Batch Processing* in the chapter "Command Line Interface" in the *Administration Guide*.
- BoKS Server Agent for Unix/Linux Basics
- Install Directories
- Install Parameters and Options

Installing BoKS Server Agent for Unix/Linux

BoKS Server Agent for Unix/Linux is distributed in two different packages, depending on operating system:

- Master/Replica/Server Agent distribution package (MRA)
- Server Agent distribution package (A)

The Server Agent distribution package is delivered in 2 variants:

- tar archive
- Native package, for example RPM

The install procedure below is almost identical for both MRA and A packages, but in the Server Agent package the **setup** gives only one choice, Server Agent, while in the MRA package you are given the three choices: Master, Replica and Server Agent. In both cases, you choose **Server Agent**. For reference concerning the MRA package, see Installing the Master.

See also:

- System Requirements
- Prerequisites for Deploying BoKS Server Agent for Unix/Linux
- The Readme, which contains platform-specific installation information.
- BoKS Server Agent for Unix/Linux Basics
- Install Directories
- Install Parameters and Options
- Setup Parameters and Options
- About Server Agent Packaging
- Unpacking the Package Contents

For remote installation of hotfixes, patches and upgrades, see Installing Hotfixes, Patches and Upgrades using boks_upgrade.

Notes:

- Plan node keys in advance and **remember the node key you use during installation**. You will need it when you register the host and in the case of future upgrades of BoKS Manager. See Node Keys.
- BoKS uses a number of install directories for which you can specify paths or accept system defaults. These are referred to below by the BoKS directory names `$BOKS_DIR`, `$BOKS_etc` and `$BOKS_var`. See Install Directories for a list of these directories and their default paths.
- The **install** program provides options not used in the procedure below. See Install Parameters and Options.

To install BoKS Server Agent for Unix/Linux:

1. Download and save the BoKS Manager or BoKS Server Agent for Unix/Linux release package (depending on the platform, the Server Agent may be packaged together with the Master and Replica) to a location accessible from the Server Agent host.

   For example in the **/downloads** directory on the Server Agent host.

2. If you have downloaded the native package, install the native package.

   For example:

   ```
   rpm -i boks-client-7.2.0.0-0.99.el7.x86_64.rpm
   ```

   Once the package has installed jump to step 12.

3. If required, uncompress the release package. See Unpacking the Package Contents. Note that this only applies if you downloaded the tar archive. A directory structure is created.

   The directory structure includes an **install** program, and binaries for specific platforms in sub-directories.

4. Become superuser:

   ```
   $ su
   ```

5. If the directory **/tmp** has less than 250 MB of space for use during install, then set the UNIX environment variable `PATCH_TMP` to a directory that has 250 MB, for example, **/var/tmp/tempbokspatch**, as follows:

   ```
   # PATCH_TMP=/var/tmp/tempbokspatch
   # export PATCH_TMP
   ```

6. Run the **install** program:

   To install without any options, type:

   ```
   # path to location of uncompressed package/install
   ```

   If you intend to use SSH privilege separation, type:

```
# path to location of uncompressed package/install -p [-u <uid>]
[-g <uid>]
```

where

- `-p` activates SSH privilege separation by setting the parameter `UsePrivilegeSeparation` to `yes` in the **sshd_config..active** and **sshd_config..inactive** files
- `-u <uid>` optionally specifies a uid for the sshd user account, a special user account for the sshd daemon and
- `-g <gid>` optionally specifies a gid for the sshd user account.

Without `-u` or `-g`, the system takes the next available uid and gid, respectively.

For details and creating this account manually instead, see *Configuring Privilege Separation* in the chapter *System Configuration* in the **Administration Guide**.

For other install options, see Install Parameters and Options.

7. When prompted to install the product or quit, select the product. With the Master/Replica/Server Agent package, the product is called BoKS Manager 7.2. With the Server Agent package, the product is called Server Agent for Unix/Linux 7.2.

```
1) BoKS Manager 7.2
q) Quit install
```

Type **1** and press **ENTER** to install BoKS Server Agent for Unix/Linux.

8. If you did not use the `-opt`, `-var` or `-etc` flags, the **install** program will prompt you individually for each install directory and provide a default that you can simply accept by pressing **Enter**. Defaults are:

```
/opt/boksm
/etc/opt/boksm
/var/opt/boksm
```

Accept each of these with **Enter**, or else enter the directory that you want to use.

9. When asked:

```
Would you like to start the installation now? [y]
```

press **Enter** to start the installation.

10. When the installation is finished, the following is displayed (the Master and Replica choices are only displayed when installing from an MRA package):

```
Setting up BoKS
1) Master
2) Replica
3) Client
q) Quit and run setup later
```

11. Before running **setup**, check to see what patch level has been installed, by typing, for example

(assuming the default installation directory):

```
# grep PATCH_LEVEL /etc/opt/boksm/ENV
```

The variable `PATCH_LEVEL` displays the patch level currently installed.

If the latest patch was not included, download the latest patch release and install it either now or later. See Installing BoKS Manager Patches.

12. Before running **setup**, open a new terminal window and make any of the following configurations that are necessary for **communications** between this Server Agent for Unix/Linux and the Master, Replicas and other Server Agents for Unix/Linux in the same domain:
    - If the Master is outside of the Server Agent's broadcast subnet, create a **bcastaddr** file in the `$BOKS_etc` directory (default **/etc/opt/boksm**), containing the IP address of the Master. For example, add the Master's address:

      ```
      10.10.10.100
      ```

      You can also add any Replicas that communicate with this Server Agent. See *Configuring the bcastaddr File* in the chapter "System Configuration" in the *Administration Guide*.
    - If you using **non-default port settings** for BoKS Manager, configure the base port by adding a line to the **/etc/services** file. For example, add the line:

      ```
      boks 6530/tcp
      ```
13. If this version 7.2 Server Agent will be inter-operating with pre-6.6.1 version Master/ Replicas, set the **$BOKS_etc/ENV** variable `BRIDGE_CRYPT=CRYPT_RC5_128`.

    See also Configuring Encryption with Pre-6.6.1 Hosts and *Setting Encryption Levels for BoKS Host Communication in the Administration Guide*

    If you are **upgrading** the installation of BoKS Server Agent for Unix/Linux, there may be other important steps to perform before you run **setup**. See the chapter *Upgrading BoKS Manager*.
14. If you are installing from the tar archive, return to the terminal window with the BoKS install process finished (which you left after install but before **setup**) and type the number for **Setup Server Agent** (1 or 3, depending on the distribution package), then press **Enter** to set up the BoKS Server Agent for Unix/Linux.

    If you closed the window, or are installating from the native package, **start the setup program** by typing:

    ```
    /opt/boksm/sbin/setup client
    ```

    (for a default installation directory), or use the path to your `$BOKS_sbin` directory).
15. When prompted to enter a node key:

    ```
    Enter BoKS node key:
    ```

    type the node key that you have planned and press **Enter**.

    Note: **Remember the node key** for registering the host in the BoKS database later.

16. When prompted to re-enter the node key, do so and then press **Enter**.

```
Re-enter node key:
```

17. For tar archive installation only, the installation process is finished and you are returned to the list of available products. Exit the installation program by typing **q** for quit:

```
q) Quit
```

18. If you use SSH, enable BoKS SSH by finding the `BOKS_SSHD` variable in the **$BOKS_etc/ENV** file and changing its value from `off` to `on`. For other optional SSH configuration, see *Configuring SSH* in the chapter "System Configuration" in the *Administration Guide*.
19. Register the Server Agent using the menu **Add > Host in FoxT Control Center** as follows:
    - Set the host type to **Unix/Linux server agent**.
    - Provide the **node key** that you entered earlier during **setup**.
    - Either:
        - Provide the Primary IP address in the **Networking section**.
        - If the Server Agent has a dynamic IP address, specify a **Host ID** which will be used to identify the Server Agent instead of the IP address.
    - In the **Create home directories on this host at** box, type the name of the parent directory on this machine under which users' home directories are located, for example **/home**.

      See *Home Directory Host Configurations for Unix Hosts* in the chapter "Host" in the *Administration Guide* for examples of Parent Home Directory and Physical Home Directory.
    - If BoKS Manager is to create the home directory on another host, type the hostname and directory in the **Map home directories to host** box, in the format *Host* at location *Directory*. For example:

      hostname at location /export/home.
    - Click **Save** to complete the registration.
20. If you use RSA SecurID tokens, configure this host for SecurID authentication as described in *Configuring Hosts for SecurID Authentication* in the chapter "Managing Authenticators" in the *Administration Guide*.
21. Restart the BoKS daemons by typing (assuming installation in the default directory **/opt/boksm/**):

```
# /opt/boksm/sbin/boksadm Boot -k
# /opt/boksm/sbin/boksadm Boot
```

22. Import the root account for the host into the database, using the **Import users** button on the host details page in FoxT Control Center. Fox Technologies recommends you use the local hostname as prefix for system accounts and particularly the root account. That is, create the root account as *hostname*:root, where *hostname* is the hostname of the host. See *About Importing Unix System Accounts* in the chapter "User Administration" in the *Administration Guide*. This is necessary in order to do administration while BoKS Protection is activated.
23. If this host uses a time zone different from the Master or the host's configured Replica, specify the time zone for the host using the CLI option `hostadm -z` or the host details page in FoxT Control Center.

See also:

- *Converting Between Master, Replicas and Server Agents* in the chapter "Backup, Restore and Recovery" in the *Administration Guide*

Installing Pre-registered Hosts as BoKS Server Agents for Unix/Linux

For hosts that have already been pre-registered in BoKS, the installation procedure is slightly different. All of the relevant information for the host has already been entered and the registration of the host in the BoKS database is performed automatically.

Key points for installing pre-registered hosts as BoKS Server Agents for Unix/Linux are:

- The pre-registered host must have contact with the BoKS Master when the Server Agent is setup for the registration of the Server Agent in the BoKS database.
- You do not need to specify a node key for pre-registered hosts; a random node key is assigned to the Server Agent by the BoKS Master.
- No information needs to be entered for pre-registered hosts in FoxT Control Center or the CLI after the BoKS Server Agent for Unix/Linux software is installed and the setup performed. The Server Agent is automatically registered and included in the BoKS domain.
- Most steps of installing BoKS Server Agent for Unix/Linux on a pre-registered host are the same as installing on a normal, non pre-registered host. The main difference occurs when you come to the setup stage.

Installing pre-registered hosts as BoKS Server Agents for Unix/Linux includes:

- Install Preparations for Pre-registered Hosts
- Installing a Pre-registered Host

See also:

- The section "Pre-registered Host Basics" in the Administration Guide.
- The section "Pre-registered Host Key Features" in the Administration Guide.

Install Preparations for Pre-registered Hosts

Before you install BoKS Server Agent for Unix/Linux on a pre-registered host, there are some preparations you need to make. These are:

- The host must have been pre-registered in BoKS Manager for the appropriate BoKS domain using FoxT Control Center **or** the BoKS CLI or a pre-registration type must have been added which the host can be registered as.
- You will need the following information when you install BoKS Server Agent for Unix/Linux on the host:

- Either:

  The *host name*: This is specified when the host is pre-registered; your BoKS Administrator should be able to provide this.

  OR:

  The *host name* and *pre-registration type*: If the host name has not been pre-registered, you also need to provide a pre-registration type. This is a type specified in the BoKS database that enables hosts to be auto-registered without the host name being pre-registered in BoKS. Your BoKS Administrator should be able to provide this.

- The *pre-registration secret*: This is specified when the host is pre-registered or a pre-registration type is defined; your BoKS Administrator should be able to provide this.

  > **NOTE:** Be sure not to type the secret on the command line to the setup command, as this will allow it to be seen in a ps listing.
  > Either let the program prompt for it, or for automated install, keep it in the parameters file pointed out by the `-A FILE=`*path_to_parameterfile* parameter to the setup program.

- The *IP address* or *FQDN hostname* of the BoKS Master; your BoKS Administrator or appropriate network administrator should be able to provide this.

- Ensure that the pre-registered host is able to contact the BoKS Master.
- You can use server certificates or server certificate fingerprints to securely identify the BoKS Master server when you are setting up the Server Agent. If you choose to do this, you will need the server certificate or server certificate fingerprint for the BoKS Master in the appropriate domain when you install BoKS Server Agent for Unix/Linux on the pre-registered host. Your BoKS Administrator should be able to supply this.

> **NOTE:** Your organization may use a list of server certificates / server certificate fingerprints if you are using multiple BoKS domains.

See also:

- The section “Pre-Registering a Host” in the Administration Guide.
- The section “Host Certificate Fingerprints” in the Administration Guide.
- The section “CA Basics” in the Administration Guide.

Installing a Pre-registered Host

To install BoKS Server Agent for Unix/Linux on a pre-registered host:

1. Follow steps 1 - 13 in the procedure for installing on a normal, non pre-registered host.

   For details, see To install BoKS Server Agent for Unix/Linux:.

2. Open a terminal and run the setup program with the `-a` flag to begin setting up the pre-registered host as a BoKS Server Agent for Unix/Linux:

```
/opt/boksm/sbin/setup -a client
```

(for a default installation directory), or use the path to your `$BOKS_sbin` directory.

If you type the command using only the `-a` option, you will be prompted to enter your user name, the host name, where applicable the type, and the pre-registration secret for the host.

Alternatively, you can specify the parameters for registering the pre-registered host in a file and direct the setup program to that file using the `-A FILE=`*path_to_parameters_file*:

```
/opt/boksm/sbin/setup -a -A FILE=path to parameters file client
```

The following table displays all the auto-registration options that can be used with the `setup -a client` command:

setup client -a -A parameter	Mandatory?	Description
USER=*user*	Yes	The user to log the auto-registration option as.
HOST=*hostname*	Yes	The hostname for the pre-registered host.
SECRET=*secret*	Yes	The secret specified when the host was pre-registered Note: FoxT recommends the pre-registration secret is either entered at the prompt from the setup programs or entered in a parameters file pointed out using the FILE variable. Avoid entering the secret directly from the command line using the SECRET= parameter.
HOSTGROUPS	No	This parameter is only needed if the pre-registration entry has the flag `CLIENT_CHOOSE_HOSTGROUPS` set. If so, a (possibly empty) space separated list of Host Groups should be given. The Host Groups given must be in the list of allowed Host Groups for the pre-registration entry.
HOSTID=*hostid*	No	For pre-version 6.6.2 Server Agents that use DHCP, specify the HostID that will be used to identify the host instead of primary IP address. For 6.6.2 and later Server Agents, you can supply the HostID directly via the `-h` option for the `setup` program.
TYPE=*type*	No	The pre-registration type the host should be registered with.

FILE=*filename*	No	File to read options from. You can save the other parameters required for registering the pre-registered host in a file and only specify this option indicating the file where the other parameters can be read.
PORTNO=*port*	No	Port for secure communication between the pre-registered host and the BoKS Master. The default setting is port 6507. If a non-default port is to be used, the port number used by the boks_autoregisterd daemon on the Master must be changed by adding -p port in the boksinit.master file on the Master and restarting BoKS.
MASTER=*host_or_ip*	No	The name or IP address of the Master. If this is not provided, BoKS tries the IP addresses specified in the $BOKS_etc/bcastaddr file.
CACERT=*cacertfile*	No	A file containing the root CA certificate from the BoKS Master. The file may contain several certificates from the BoKS Master. It may contain several certificates (e.g. for Masters from different BoKS domains). For details of using certificate authentication with auto-registration, see "Pre-registered Host Authentication" in the BoKS Manager 7.2 Administration Guide.

FINGERPRINTS= *fingerprintfile*	No	A file containing SHA256 fingerprints of allowed server-side certificates, i.e. the fingerprint of the Master's host certificate must be included. For details of using fingerprint authentication with auto-registration, see "Pre-registered Host Authentication" in the BoKS Manager 7.2 Administration Guide.
TIMEOUT	No	Specifies the number of seconds to wait for a response from a BoKS server. Default is 120 seconds.

For further details, see the BoKS man page **boks_autoregister**.

Note: If the hostname you enter is not pre-registered in the BoKS database, the **setup** program prompts you to enter a pre-registration type instead, as long as there is at least one type registered. If no types are registered and the hostname has not been pre-registered, the installation will fail.

3. If you use SSH, enable BoKS SSH by finding the `BOKS_SSHD` variable in the **$BOKS_etc/ENV** file and changing its value from `off` to `on`. For other optional SSH configuration, see *Configuring SSH* in the chapter "System Configuration" in the *Administration Guide*.
4. If you use RSA SecurID tokens, configure this host for SecurID authentication as described in *Configuring Hosts for SecurID Authentication* in the chapter "Managing Authenticators" in the *Administration Guide*.
5. Restart the BoKS daemons by typing (assuming installation in the default directory **/opt/boksm/**):

```
# /opt/boksm/sbin/boksadm Boot -k
# /opt/boksm/sbin/boksadm Boot
```

6. Import the root account for the host into the database, using **Import users** in the host details page in FoxT Control Center. Fox Technologies recommends you use the local hostname as prefix for system accounts and particularly the root account. That is, create the root account as *hostname*:root, where *hostname* is the hostname of the host. See *About Importing Unix System Accounts* in the chapter "User Administration" in the *Administration Guide*. This is necessary in order to do administration while BoKS Protection is activated.
7. If this host uses a time zone different from the Master or the host's configured Replica, specify the time zone for the host using the CLI option `hostadm -z` or the host details page in FoxT Control Center.

See also:

- The section "Pre-registered Host Basics" in the Administration Guide.
- The section "Pre-Registering a Host" in the Administration Guide.

Listing BoKS Server Agents for Unix/Linux in the Domain

For Server Agents that are registered in the BoKS Manager domain, you can list different information in a number of ways:

- To list details for hosts, including the type, comment and IP address, use the menu **List >Hosts**.

  From the command line, you can list similar information using the program **lh** and **hostadm**.

- To list Host Groups and how many members they contain, use the menu **List > Host Groups**.

  From the command line, use the program **hgrpadm**.

- To list installed BoKS Manager versions, use **boks_upgrade** (see procedure below).
- To list BoKS environment variables for a single Server Agent, use **cadm**.
- To take a system snapshot of a single Server Agent, including the version, operating system, licensing information and copies of recent logs, use **boksinfo**.

To list Server Agents with BoKS version and operating system version:

1. Log in to the BoKS Master, become root and start a BoKS shell.
2. Run the following command, specifying the Host Groups that you want to list, or `ALL` for all Server Agents:

   ```
   BoKS# boks_upgrade info -h <hostgroup> [, <hostgroup>]
   ```

   where `<hostgroup>` is any hostname or Host Group name, or the word `ALL`.

   `ALL` lists all hosts, even those that have BoKS Manager or Server Agent for Unix/Linux installed but that are not Server Agents in the Master's domain.

Example output:

ae-aix Not a client

aqa-hp1 Not a client

aqa-sol3

Version: 6.6 Patch 2

Hotfixes:

Platform: SunOS sol11x86c 5.11 11.0 i86pc i386 i86pc

quentin Not a Unix BoKS host

See also:

- The man pages **boks_upgrade**, **lh, hostadm**, **hgrpadm**, **cadm**, **boksinfo**
- Installing Hotfixes, Patches and Upgrades using boks_upgrade (using **boks_upgrade**)

- The chapter *System Monitoring Tools* in the **Administration Guide**
- Deploying BoKS Server Agents for Unix/Linux (overview of topics)

Installing Hotfixes, Patches and Upgrades using boks_upgrade

> **NOTE:** The **boks_upgrade** script is only supported for BoKS installations done using the tar archive package. It is not supported for BoKS installations done using native packages, such as RPM.
> If you attempt to upgrade a native package installation using boks_upgrade, the operation will fail with an error message similar to the following:
> `/opt/boksm/lib/boks_upgrade_upgrade: line 129: grep:: command not found Failed to retrieve version from client. Please run "boks_upgrade setup" and retry upgrade.`

The script **boks_upgrade** automates the install hotfix, patch or upgrade routine for a number of specified Server Agents for Unix/Linux, for example, for all hosts in a given Host Group. You can also use it on a single Server Agent. **boks_upgrade** uses an SSH channel to make the install secure. **boks_upgrade** is safe because it does not run under the control of BoKS Manager: if the install should fail for any reason on a particular host, it leaves you with an open SSH connection to the host, over which you can take any required steps (such as manually backing out a patch where the patch installation aborted).

The **boks_upgrade** script automates the following procedures, which you can also use separately on their own:

- To **install a patch**: Installing a BoKS Manager Patch.
- To **uninstall a patch**: Backing Out a BoKS Manager Patch .
- To **install or uninstall a hotfix**, the procedure given in the hotfix Readme.
- To **upgrade**: Upgrading a Server Agent for Unix/Linux (using the program **upgrade_client**).

After the automatic install, depending on the environment, you may need to perform some configuration (for example, reconfiguring encryption levels or SSH).

The **boks_upgrade** script cannot uninstall BoKS Server Agent for Unix/Linux or back out an upgrade. See Uninstalling BoKS Server Agent for Unix/Linux.

See also:

- The man page **boks_upgrade**
- The man page for **cadm**, used to connect to BoKS Server Agents for Unix/Linux
- BoKS Server Agent for Unix/Linux Basics
- Upgrading BoKS Server Agents for Unix/Linux
- Installing OS Patches

Prerequisites

The same prerequisites apply for **boks_upgrade** as for a manual hotfix, patch or upgrade. These include:

- `/var/tmp` has at least 200 MB free space for temporary storage on each Server Agent to be updated.
- The BoKS installation must be done from a tar archive package, not a native package like RPM.
- **For upgrading** only, make sure the Master's or a Replica's IP address is in **$BOKS_etc/bcastaddr** on all Server Agents to be upgraded, so that the **install** program setup can reach the Master or a Replica. For other upgrade prerequisites, see the following:
- Prerequisites for Upgrading
- Server Agent Upgrade Basics
- Upgrading a Server Agent for Unix/Linux
- **For hotfix and patch prerequisites**, see the requirements stated in the Readme.

Using a boks_upgrade Configuration File

A number of variables used by the **boks_upgrade** program can be defined using an external configuration file. Program options that can be set using the configuration file include `-x` (SSH directory) and `-p` (package directory).

For more information on using a **boks_upgrade** configuration file, see the BoKS man page **boks_upgrade**.

To automatically update Server Agents for UNIX:

The **boks_upgrade** script provides many options and can be used for many purposes. The procedure below is typical but not exclusive. For other options, examples and full detail, including using a **boks_upgrade** configuration file, see the man page **boks_upgrade**.

The **boks_upgrade** script updates a list of Server Agents. As a precaution and to keep runs manageable, Fox Technologies suggests that you only update a portion of your network at one time, for example, one Host Group, while using this script.

CAUTION: After running **boks_upgrade**, be sure to shut down the special **boks_upgrade** SSH channel (as described below) so that all access is again under BoKS' control.

CAUTION: When patching or upgrading, all hotfixes are removed. You should be aware that a released patch or upgrade might not include a removed hotfix, and, in that case, should contact Fox Technologies.

1. Log in on the Master and become superuser.
2. Download from the Fox Technologies web site the package containing the upgrade, patch or hotfix for all platforms concerned.
3. Download from the Fox Technologies web site the latest special upgrade OpenSSH package for all platforms concerned. Note that this is not the BoKS OpenSSH included in BoKS.
4. Download from the Fox Technologies web site the **boks_uname** script for all platforms concerned and place it in the same directory as the upgrade OpenSSH package.This script can also be copied from the **prog** subdirectory of an upgrade or a patch package.
5. Make sure all logged-in users are notified that the Server Agents concerned are about to be updated.
6. Start a BoKS shell by typing:

```
# $BOKS_sbin/boksadm
```

For details, see *Launching the BoKS Manager CLI* in the chapter *BoKS Manager Administration* in the **Administration Guide**.

7. **Generate SSH keys** on the Master, if they do not already exist from a previous **boks_upgrade** session, using **boks_upgrade**'s **keygen** subcommand:

```
BoKS # boks_updgrade keygen
```

8. **Set up the special ssh daemon** on the Server Agents that are to be updated with the **setup** subcommand:

```
BoKS # boks_upgrade setup -h <hostlist> -x <sshdirectory>
```

where `<hostlist>` is one or more hosts or Host Groups separated by commas, for example, "GROUP1, GROUP2, host3" and `<sshdirectory>` is the directory that contains the upgrade OpenSSH package (downloaded from the Fox Technologies web site) and the **boks_uname** program (downloaded or copied from the prog subdirectory of a BoKS patch distribution).

9. **Check installed version level** with the **info** subcommand. This step is optional.

```
BoKS # boks_upgrade info -h <hostlist>
```

where `<hostlist>` is the collection of hosts being operated upon.

For each host, output includes installed version with patch level, installed hotfixes list, and platform.

10. **Run boks_upgrade** using the **hotfix, patch or upgrade** subcommand, the hosts and the distribution that you want to install. See the man page for details:

```
BoKS # boks_upgrade <update_type> -h <hostlist> -p <package_
directory> -s <version>
```

where:

`<update_type>` is one of **hotfix, patch or upgrade**

`<hostlist>` is one or more hosts or Host Groups separated by commas

`<package_directory>` is the directory containing the hotfix, patch or upgrade package and

`<version>` is the product version to install, for example "7.2". For a hotfix, `<version>` is the hotfix package name, for example "HFBM-0235".

Successful upgrade displays the following line for each host:

`<hostname>` **Upgrade OK** (or Hotfix OK or Patch OK, respectively)

Failed upgrade displays a similar message for each failed host.

11. **Check installed version level** with the **info** subcommand. This step is optional.

```
BoKS # boks_upgrade info -h <hostlist>
```

where `<hostlist>` is the collection of hosts being operated upon.

For each host, output includes installed version with patch level, installed hotfixes list, and platform.

12. **Shutdown the update daemons** and close the SSH channel using the **shutdown** subcommand. This step is optional but highly recommended; **shutdown** cleans up the system and most importantly, **closes the SSH channel** so that BoKS again controls all access to the host (assuming BoKS Protection is activated).

    ```
    BoKS # boks_upgrade shutdown -h <hostlist>
    ```

    where `<hostlist>` is again the collection of hosts being operated upon.

    For each host, the message “Stopped OK” is displayed

Emergency Access to a Server Agent

The upgrade OpenSSH daemon installed on Server Agents with the **boks_upgrade setup** subcommand is left active until the **shutdown** subcommand is used. This channel can be used to gain root access to the Server Agent from the Master if something goes wrong during the hotfix, patch or upgrade, and normal access is blocked by BoKS Manager.

To access the Server Agent from the Master via this SSH channel, use the command:

```
$BOKS_bin/ssh -F $BOKS_etc/upgrade/ssh_config <host> <command>
```

where `<host>` is the Server Agent hostname and `<command>` is the UNIX command to be executed on the Server Agent (for example, to kill BoKS, `$BOKS_sbin/Boot -k`).

Enabling Offline Login to a BoKS Server Agent

It is possible to allow a BoKS Server Agent user to log in and use a set of predefined access methods even if the BoKS Server Agent cannot communicate with a BoKS server.

An administrator can enable offline login to a BoKS Server Agent in two ways:

- During Server Agent setup after a BoKS installation. See To enable BoKS Server Agent offline login during installation.
- By editing the file **$BOKS_etc/ENV**. See the *BoKS Manager Administration Guide* for details on how to enable offline login by editing the **ENV** file, and also for more details concerning BoKS Server Agent offline login in general.

Note: Support for offline login is disabled by default.

To enable BoKS Server Agent offline login during installation

1. When the BoKS installation has finished, quit the setup program by typing `q` for quit.
2. At the command line, type for example:

```
# ./setup -o "telnet login rlogin" -O "login" client
```

where `-o` adds access methods to the `OFFLINE_SERVICES` variable, and `-O` to the `OFFLINE_SERVICES_ROOT` variable in the file **$BOKS_etc/ENV**.

Uninstalling BoKS Server Agent for Unix/Linux

To **uninstall BoKS Server Agent for Unix/Linux**, use the procedure Uninstalling BoKS Manager, paying attention to delete the host from the BoKS domain after uninstalling. See About Deleting, Changing Host Type or Domain and Uninstalling Server Agents.

CAUTION: Uninstalling a Server Agent removes all BoKS protection from the host. In addition, until you delete the host from the BoKS domain so that it is no longer a member of any Host Groups or part of any Access Rules, this unprotected host may even allow unintended access to protected Server Agents (for example, if this host is a member of a trusted Host Group, from which access is allowed to protected Server Agents).

- For a way (using Access Rules) to insure no access to BoKS-protected hosts in the domain via the uninstalled host during uninstallation, see the BoKS man page **uninstall**.

Note: If you uninstall BoKS from a host while there are **suexec** sessions with keystroke logging still running, the keystroke log files are not finalized and sent to the Master.

To **uninstall a hotfix or patch**, see Installing Hotfixes, Patches and Upgrades using boks_upgrade.

See also:

- BoKS Server Agent for Unix/Linux Basics
- The BoKS man page **uninstall**