

BoKS® Manager is the server software used in the FoxT Enterprise Access Controls Management solutions BoKS Access Control for Servers, BoKS Access Control for Applications and BoKS Access Control for Desktops. BoKS Client for UNIX is the client component that protects a server in the BoKS Access Control for Servers solution. This information applies to BoKS Manager 6.5.2 and BoKS Client for UNIX 6.5.2.

Supported Platforms

Vendor	Platform	Master	Replica	Client	Availability
HP	HP HP-UX 11.0, 11i v1, 11i v2, 11i v3 for PA-RISC and Intel Itanium	✓	✓	✓	Now
	HP Tru64 5.1 (a) and (b)			✓	Now
	HP HP-UX 10.20			✓	On request
IBM	IBM AIX 6.1 (32 & 64 bit)	✓	✓	✓	Now
	IBM AIX 5.1, 5.2 and 5.3 (32 & 64 bit) [‡] [◇]	✓	✓	✓	Now
	IBM AIX 4.3.2 (32 bit), IBM AIX 4.3.3 (32 & 64 bit)			✓	On request
Red Hat	Red Hat Enterprise Linux 5.0 on x86 and x64	✓	✓	✓	Now
	Red Hat Enterprise Linux AS/ES/WS 4.0 on x86 and x64	✓	✓	✓	Now
	Red Hat Enterprise Linux AS/ES/WS 3.0 on x86 and x64	✓	✓	✓	Now
	Red Hat Enterprise Linux 2.1, AS, WS and 7.2			✓	Now
	Red Hat Linux 6.2			✓	On request
Microsoft	Microsoft Windows Server 2003, SP2 or later (32 bit)			✓	Now
NCR	NCR UNIX 3.0.3			✓	On request
Nokia	Nokia Firewall IPSO4			✓	On request
SCO	SCO UnixWare 7.1.1-7.1.4			✓	On request
Silicon Graphics	Silicon Graphics Irix 6.5.x			✓	On request
Sun	Sun Solaris 10 on SPARC, x86 and x64	✓	✓	✓	Now
	Sun Solaris 9 on SPARC and x86, 8 on SPARC	✓	✓	✓	Now
	Sun Solaris 2.5.1, 2.6, 7			✓	On request
SUSE from Novell	SUSE Linux Enterprise Server 10 on x86 and x64	✓	✓	✓	Now
	SUSE Linux Enterprise Server 9 on x86 and x64	✓	✓	✓	Now
	SUSE Linux 8.0			✓	On request
VMware	VMWare ESX 3.0, 3.5 [†]			✓	Now
	VMWare ESX 2.5 ^Δ			✓	Now

[‡] AIX 5.1 requires Maintenance Level 3 or higher, AIX 5.3 requires Maintenance Level 1 or higher

[◇] AIX 5.3 package includes support for IBM VIO Server (Client installation only)

[†] VMware 3.0 & 3.5 support included in the BoKS Manager package for Red Hat Enterprise Linux AS/ES/WS 3.0

^Δ VMware 2.5 support included in the BoKS Manager package for Red Hat Enterprise Linux 2.1, AS, WS and 7.2



Disk Space

Type	Disk Space
Master	At least 300 MB
Replica	At least 280 MB
Client for UNIX	At least 170 MB

Note that these are minimum recommendations.

Requirements depend on platform, domain size, number of hosts and users, etc.

Encryption Strength

Type	BoKS Manager
Line Encryption	RC5 128 bit
Key Exchange	RSA 512 or 1024 bit*
CA Certificate Key Length	512, 1024 or 2048 bit*
Virtual Card Key Length	512 or 1024 bit*

* Configurable

System Resources

Installation Type	Shared Memory	Semaphores
Master	16 MB (minimum)*	2
Replica	16 MB (minimum)*	2
BoKS Client for UNIX host	n/a	-

The required shared memory size, configurable in BoKS Manager, depends on the size of the security database. These are minimum starting values. Note that BoKS Manager and BoKS Client for UNIX do not touch the kernel.

** At least 24 MB for hosts with servc enhancements enabled.*

Integration

Compatible versions of products that can be used with BoKS Manager 6.5.2

Product	Compatible Versions
RSA Authentication Manager (previously called ACE/Server)	5.0 and later
Secure Computing PremierAccess/SafeWord Plus Server	All versions that support the EASSP 20x protocol
BoKS Desktop	5.7 and later
BoKS SSH Client for Windows	6.5 and later
BoKS Agents using SSL	All when used with BoKS Desktop 5.7 or later
BoKS Agent for SNC (Access Control for SAP R/3)	5.6 and 5.7

Ports

Default ports are 6500-6508, and 2478 with protocols TCP, UDP, SSL, and HTTP. Ports are configurable.

Requirements for Remote Administration

BoKS Manager can be managed in any browser that supports http 1.0 or later, HTML 4 and SSL with 128-bit encryption strength.

Authentication for login to the administration interface can be configured globally or per administrator to require any one of the following:

- RSA Authentication Manager (ACE/Server) and RSA SecurID tokens
- BoKS Desktop
- Third-party CA certificate or BoKS certificate installed on the browser.
- Password

An authenticated, authorized administrator has access to the full GUI. A sub-administrator's access to menu operations can be restricted to specific menus, hosts, user accounts, etc.