White Paper

Security

Security for SBM-Powered Solutions in an On-Demand Environment

MICRO FOCUS

Who Should Read This Paper?

This white paper describes security aspects of Solutions Business Manager (SBM) in an on-demand environment. The intended audience for this white paper includes:

- Technical decision makers who are considering SBM as their Business Process Management platform.
- IT Analysts and IT Managers who are interested in understanding the security aspects of SBM and its solutions.

Overview

SBM is a leading Business Process Management Suite (BMPS) designed to orchestrate and automate processes and provide transparency across an organization including software development life cycle (SDLC), IT operations, and the broader business. SBM is available in a variety of offerings, including:

- SBM On-Premise
- SBM Platform-as-a-Service (PaaS)
- SBM Hosted
- SSM On-Demand (legacy offering for existing customers only)

About the SBM PaaS Environment

The SBM PaaS environment consists of servers running on AWS, accessible only through SSL connections on AWS Application Load Balancers with no file system access. Application access is controlled via SBM user credentials using SSO. SBM PaaS user IDs are defined and administered in Application Administrator. Authentication can utilize internal passwords or SAML2.

Users and administrators access SBM via the HTTPS protocol. This includes the Web portal (SBM Work Center, Request Center, Application Repository, and Application Administrator) and SBM Composer access, and Web Services/REST calls.

The SBM servers run on Windows Server EC2 instances and are not accessible from the public internet other than assigned ports. Port 443 is used for Work Center, Request Center, and Application Administrator, while port 8443 is used for Application Repository and SBM Composer access. Attempts to use non-SSL ports 80 and 8085 results in redirection to the SSL ports. The Windows Servers are kept up to date with Microsoft Security patches on a regular basis.

The database server used for SBM PaaS is also part of the private AWS network, and is not accessible from the public internet without the optional VPN service.

For details on AWS security and compliance, see **https://aws.amazon.com/security/**.

Differences Between SBM PaaS and SBM On-Premises

The SBM PaaS environment consists of servers running on AWS, accessible only through SSL connections on AWS Application Load Balancers with no file system access. Application access is controlled via SBM user credentials using SSO. SBM PaaS user IDs are defined and administered in Application Administrator. Authentication can utilize internal passwords or SAML2.

The SBM PaaS offering provides all of the same features and capabilities of the on-premise verison, with the following exceptions:

- SBM Configurator (available with SBM Hosted option)
- SBM System Administrator
- Various SBM ModScript functions not available for security purposes. (e.g. file system access)
- SBM AppScript, which is disabled in the PaaS environment

Access and Security

All of the APIs and integrations in the on-premise offering are available in SBM PaaS. These include:

- SBM Application Engine Web Services API (e.g. sbmappservices72 and sbmadminservices72)
- SBM ModScript (limited)
- SBM JSON API
- SBM JavaScript Library
- SBM Application Engine C++ API

General Data Protection Regulation (GDPR) and SBM PaaS

The methods we use for storing your data in an SBM PaaS environment are GDPR compliant. To learn more about GDPR, visit this site.

Other Questions?

For further information or questions, please contact your Micro Focus account manager.

Learn More At
www.microfocus.com/sbm

Contact us at:
www.microfocus.com