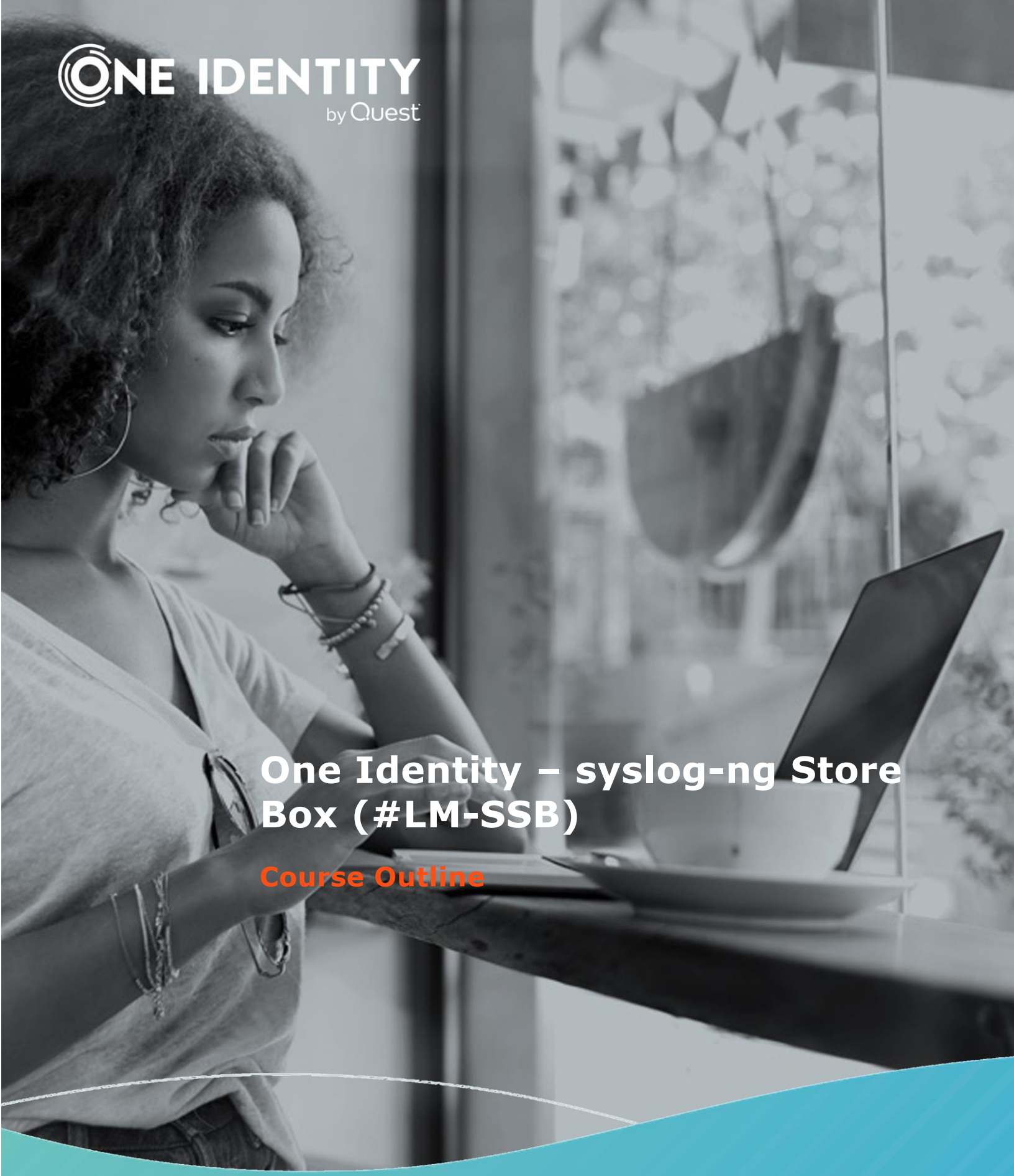

One Identity – syslog-ng Store Box (#LM-SSB)

Course Outline

Course Outline - syslog-ng Store Box (#LM-SSB)

Overview

The purpose of this course is to provide students with a general overview of the One Identity syslog-ng Store Box (SSB) feature-set, installation, configuration and customization of the solution framework as well an overview of the main business processes that are part of the solution framework. This course focuses on lab performance and was developed for people just interested how SSB can be installed configured. Also for those who wants to deploy SSB.

Course:	Log Management Foundations (#LM-FND)
Audience:	Customer, sales and Technical Sales
Language:	English
Duration:	4FIXME days (remote)
Prerequisite:	None

Topics

- Overview and introduction to syslog-ng Store Box (SSB)
- Configure and initialize by the Welcome Wizard
- Simple settings of SSB
- Access control on the box
- Backup, Cleanup and archive logspaces
- Filtering and Rewriting messages
- MRA: message rate alerting and Reports
- Forwarding message to external devices
- How HA works and when to use them
- Troubleshooting SSB and How to use the support system

Training Course Details

Please note: Agenda, Labs and Demos show all available parts for an existing Training module. Depending on the course, smaller parts of it might not be taught or performed. Typically, suitable Labs must be taught but Demos could be selected during a training.

Topics	Labs
Introduction and Overview of SSB **Training Module: SSB-INT** • What is SSB • Basic functions and benefits of the device	• -
Configuration and Welcome Wizard **Training Module: SSB-CWI** • Initialize your SSB • Getting familiar with the interface	• Initialize SSB
Simple Settings **Training Module: SSB-SST** • Basics of SSB • Sources • Logspaces • The search interface • Sharing logspaces	• Install and configure syslog-ng Agent for Windows • Search in logspace • Create multiple logspace • Create filtered logspace • Share a logspace

Access Control
Training Module: SSB-ACL
• Ways of access control in SSB
  ○ Web interface
  ○ Logspaces
  ○ Shares
  ○ Encryption
	• ACL on the web interface
	• Encrypt and decrypt logspaces
	• Encrypt the communication channel

Backup, Cleanup & Archive **Training Module: SSB-BCA** • Methods of backup and archive • Setup backup • Perform a full backup and restore	• Configure Microsoft Share • Setup system backup to the share • Setup logspace backup to the share
Filter and Rewrite messages and Parsers **Training Module: SSB-FRP** • Setup filters and parsers • Configure pattern-db	• Configure a filter • Setup K-V Parser • Setup sudo parsers • Setup pattern-db
Fetching from SQL **Training Module: SSB-FSD** • Configure SQL fetching	• Prepare database • Configure fetching
Alerting Monitoring and Reports **Training Module: SSB-AMR** • Configure alerting methods • Configure trap cases • Configure reports	• Setup SNMP • Setup log alerts • Setup content based alerts • Configure reports
Forwarding Messages **Training Module: SSB-FWD** • Sending messages to syslog servers • Storing messages in SQL databases • Storing messages on HDFS	• Configure syslog-destination • Configure SQL destination
Hight Availability **Training Module: SSB-HAB**	• -

Topics	Labs
• HA concept • Setup HA	
Troubleshoot SSB **Training Module: SSB-TRB** • Troubleshoot network • SSB log messages • System debug • Config export/import • Firmware upgrade • Tainted firmwares • Other debug tools	• -