



Tenable for BlackBerry® UEM

Reduce Cyber Risk with Mobile Device Management

Business Challenge

Security teams are constantly challenged with the ability to monitor their changing fleet of mobile devices and associated vulnerabilities for the organization. Without integrating the Tenable plugin with BlackBerry® Unified Endpoint Manager (UEM), scanning and gaining additional vulnerability data becomes increasingly complex and if devices are unaccounted for or fail to have the correct policies, personal and enterprise data is at major risk.

Solution

The Tenable® plugin for BlackBerry® UEM provides a way for security teams to understand the cyber exposure of their mobile devices being managed by BlackBerry® UEM. Tenable collects mobile device hardware and software information by importing asset lists and asset data from BlackBerry® UEM and runs its plugins against the collected data to determine vulnerabilities. Comprehensive reports are then generated for security teams to better understand their Cyber Exposure and risk and help ensure compliance across their mobile environment.

Value

The Tenable plugin for BlackBerry® UEM provides the ability to:

- Gather all known information for your organizations iOS and Android devices
- Receive vulnerability information for your organizations mobile devices
- Report on vulnerability findings within Tenable for your organizations mobile devices



Technology Components

- Tenable.io/Tenable.sc 5.12 or higher
- BlackBerry® UEM

ABOUT TENABLE

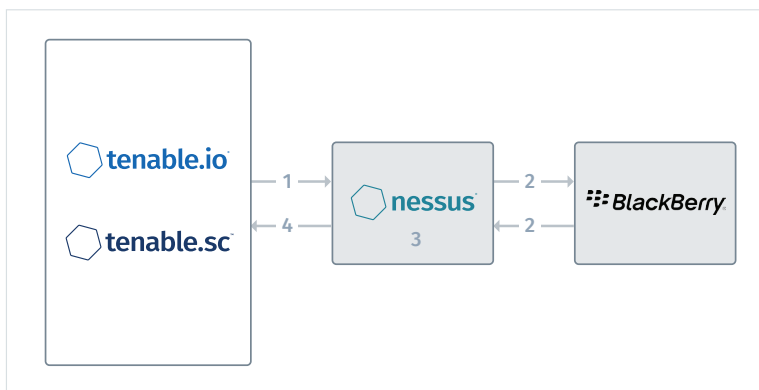
Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

ABOUT BLACKBERRY

The Internet of Things represents the next great wave in business transformation. BlackBerry is leading the way with a single platform for securing, managing and optimizing how intelligent endpoints are deployed in the enterprise, enabling our customers to stay ahead of the technology curve that will reshape every industry. Learn more at blackberry.com

How It Works

1. Tenable launches Mobile Device Management Scan process.
2. Nessus® connects to BlackBerry® UEM and gathers all known information about Android and iOS devices.
3. Nessus® uses the data collected from BlackBerry® UEM to discover vulnerabilities.
4. Findings are returned to and reported within Tenable.



More Information

Tenable Installation Links:

<https://www.tenable.com/products/tenable-io>

<https://www.tenable.com/products/tenable-sc>

Configuration Documentation:

docs.tenable.com

For support please contact: support@tenable.com

COPYRIGHT 2020 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, TENABLE.OT, LUMIN, INDEGY, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.