SOLUTION OVERVIEW

tenable®

Tenable for Microsoft ActiveSync

Reduce Cyber Risk with Mobile Device Management

Microsoft

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 Microsoft ActiveSync 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 Microsoft ActiveSync provides a way for security teams to understand the cyber exposure of their mobile devices being managed by ActiveSync. Tenable collects mobile device hardware and software information by importing asset lists and asset data from Microsoft ActiveSync 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 Microsoft ActiveSync 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 5.11 or higher
- Microsoft ActiveSync

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**.

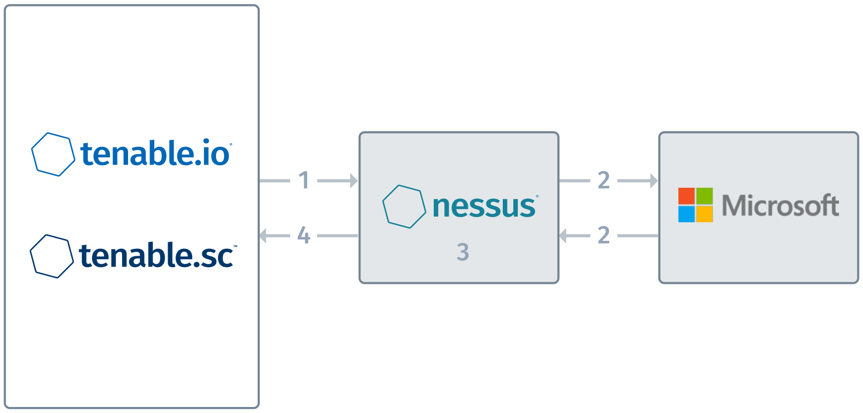
ABOUT MICROSOFT

At Microsoft, our mission is to empower every person and every organization on the planet to achieve more. Our mission is grounded in both the world in which we live and the future we strive to create. Today, we live in a mobile-first, cloud-first world, and the transformation we are driving across our businesses is designed to enable Microsoft and our customers to thrive in this world. We do business in 170 countries and are made up of 144,000 passionate employees dedicated to fulfilling our mission of helping you and your organization achieve more.

Learn more at: **www.microsoft.com**

How It Works

1. Tenable launches Mobile Device Management Scan process.
2. Nessus® connects to Microsoft ActiveSync and gathers all known information about Android and iOS devices.
3. Nessus® uses the data collected from Microsoft ActiveSync 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

For support please contact:

docs.tenable.com

For support please contact:
support.tenable.com