IBM VIOS Authentication

Thank you for your interest in authenticated scanning! When you configure and use authentication, you get a more in-depth assessment of your hosts, the most accurate results and fewer false positives. This document provides tips and best practices for setting up IBM VIOS authentication. To detect hosts running IBM VIOS, and their respective vulnerabilities, Qualys recommends running an authenticated scan. Authentication to IBM VIOS devices is supported for vulnerability scanning only at this time, using Unix authentication records.

IBM VIOS Authentication for Vulnerability Scanning

Why use authentication?

With authentication, we can remotely log in to each target system with credentials that you provide, and because we're logged in we can do more thorough testing. This will give you better visibility into each system's security posture.

What privileges are needed for vulnerability scans?

The account you provide must be able to perform certain commands like 1) execute "uname" to detect the platform for packages, 2) read /etc/redhat-release and execute "rpm" (if the target is running Red Hat), and 3) read /etc/debian_version and execute "dpkg" (if the target is running Debian).

There are many more commands that must be performed. The *NIX Authenticated Scan Process and Commands article describes the types of commands run, and gives you an idea of the breadth and scope of the commands executed. It includes a list of commands that a Qualys service account might run during a scan. Not every command is run every time, and *nix distributions differ. This list is neither comprehensive nor actively maintained.

Are my credentials safe?

Yes, credentials are exclusively used for READ access to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the vulnerability scan.

What are the steps?

First, set up an IBM VIOS user account and privileges on target hosts (we'll help you with this below). Then, using Qualys, complete these steps: 1) Add a Unix authentication record to associate credentials with hosts (IBM VIOS uses the Unix record for authentication). 2) Launch a vulnerability scan. 3) Run the Authentication Report to view the detailed report for each scanned host. For vulnerability scans you must enable authentication in an option profile and then select the profile at scan time. Go to Scans > Option Profiles. Edit an option profile (or create a new one), go to the Scan section and select each type of authentication you want to use. For IBM VIOS, be sure to check the Unix/Cisco option since Unix authentication is used.

Can I have multiple records?

Yes. You can create multiple records with different IP addresses. Each IP address may be included in one Unix type record.

IBM VIOS Setup – Scan User Account Privileges

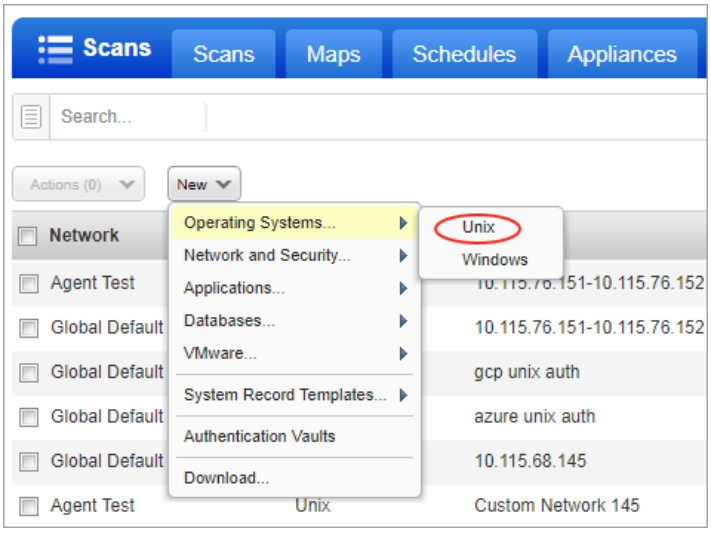
For the vulnerability scan to work properly and to be able to identify VIOS and fetch the patch status of each system, the scan user account you provide for authentication must have privileges to access the commands listed below.

- uname –V
- uname –a
- One of these commands must be successful:
  - instfix –ik <ifix-number>
  - print 'instfix -ik <ifix-number>' | oem_setup_env
- One of these commands must be successful:
  - emgr -lv3
  - print 'emgr -lv3' | oem_setup_env
- One of these commands must be successful:
  - emgr -l|grep -E '[[:blank:]](S|P|SP|QP)[[:blank:]].*[0-9]{2}/[0-9]{2}/[0-9]{2}'|awk '{print $3}'|head -n 30000
  - print 'emgr -l|grep -E "[[:blank:]](S|P|SP|QP)[[:blank:]].*[0-9]{2}/[0-9]{2}/[0-9]{2}"|awk "{print \$3}"|head -n 30000' | oem_setup_env

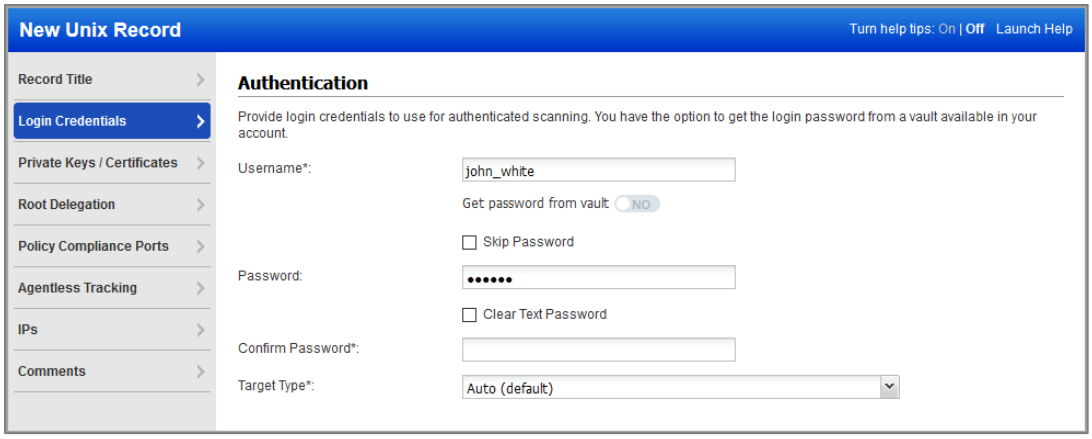
Unix Authentication Record

How to add a Unix record

Go to Scans > Authentication. Then select New > Operating Systems > Unix.



Enter the login credentials (user name, password) our service will use to log in to Unix hosts at scan time. Then walk through our wizard to select the options you want for private keys, root delegation, target IPs, and more. Our online help is always available to assist you.



Sample Reports

Here's a sample VM scan report showing the AIX VIOS operating system detected.

Here are sample results for QID 45017 (Operating System Detected):

RESULTS:

Operating System	Technique	ID
AIX 6.1 VIOS 2.2.6.30	Unix login	

Last updated: September 21, 2020