# A10 Device 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 A10 authentication. Authentication to A10 devices is supported for vulnerability scanning, using Unix authentication records.

## A10 Device 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 "show version" to identify the series and build version.

### 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 A10 device 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 (A10 uses the Unix record for authentication) and choose A10 as the Target Type in the Unix record. 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 A10 targets, 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.

## A10 Device Setup – Scan User Account Privileges

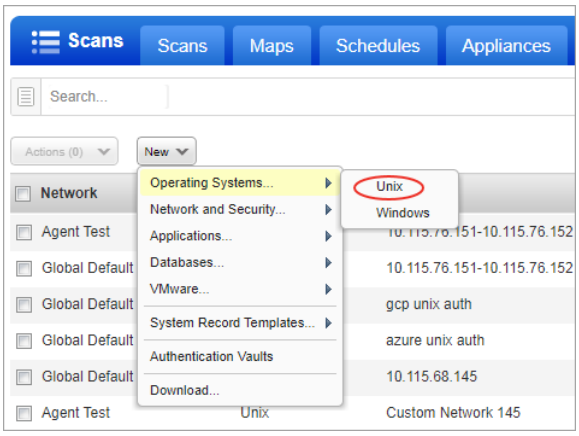
For the vulnerability scan to work properly and to be able to identify A10 devices and fetch the patch status of each system, the scan user account you provide for authentication must have privileges to access the command listed below.

- Show version

## Unix Authentication Record

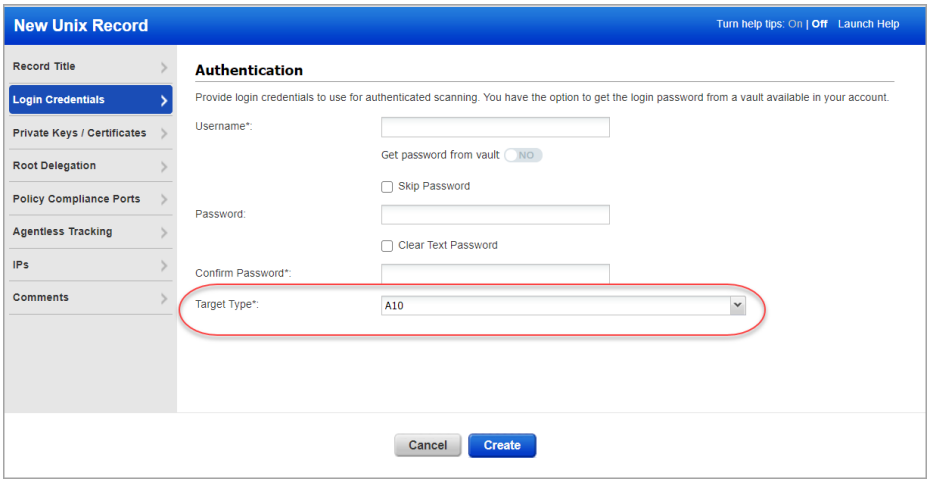
### How to add a Unix record

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.

On the **Login Credentials** tab, you'll need to pick **A10** from the **Target Type** menu to authenticate to these devices.



## Sample Reports

Here's a sample VM scan report showing the A10 operating system detected.

Summary of Vulnerabilities

| Vulnerabilities Total | 5 | Security Risk (Avg) | 4.0 |
|---|---|---|---|

by Severity

| Severity | Confirmed | Potential | Information Gathered | Total |
|---|---|---|---|---|
| 5 | 0 | 0 | 0 | 0 |
| 4 | 2 | 0 | 0 | 2 |
| 3 | 1 | 0 | 0 | 1 |
| 2 | 1 | 0 | 1 | 2 |
| 1 | 0 | 0 | 0 | 0 |
| Total | 4 | 0 | 1 | 5 |

5 Biggest Categories

| Category | Confirmed | Potential | Information Gathered | Total |
|---|---|---|---|---|
| Hardware | 4 | 0 | 0 | 4 |
| Information gathering | 0 | 0 | 1 | 1 |
| Total | 4 | 0 | 1 | 5 |

Scan Results page 1

Vulnerabilities by Severity



Operating Systems Detected



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

RESULTS:

| Operating System | Technique | ID |
|---|---|---|
| A10 Advanced Core OS 4.1.4-GR1-P2 | Unix login | |
| cpe:/o:a10:a10 advanced core os:4.1.4-gr1-p2::: | CPE | |

Last updated: September 25, 2020