Scanning Check Point Gaia with Tenable Nessus

Last Revised: Tuesday, October 12, 2021

Table of Contents

Scanning Check Point Gaia with Tenable Nessus

Configuring a vulnerability scan for a network device can be challenging. This whitepaper explains how to scan Check Point Gaia devices with Tenable Nessus. Nessus is the endpoint sensor for Tenable.io cloud-based vulnerability management and Tenable.sc on-prem vulnerability management solutions.

SSH is the primary entry point for Nessus credentialed vulnerability scans of Gaia devices. Users accessing a Gaia device over SSH interact with the host using the shell that is configured for that user. Nessus credentialed scans are only supported for users configured with the Gaia Clish, bash, or Bourne (sh) shells.

Gaia versions R80.30 and higher are the primary focus of this whitepaper. The basic information presented below work for versions as far back as the R77 series, but screenshots may be inaccurate and specific features may not be available for versions older than R80.30.

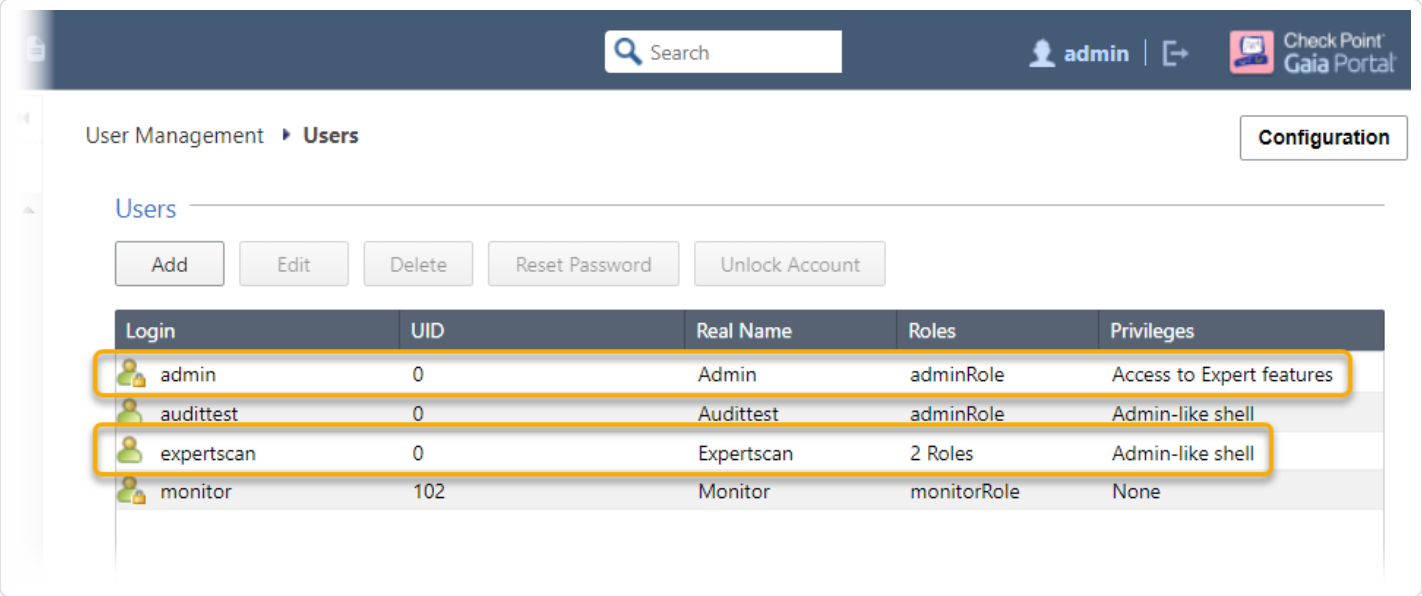
This whitepaper applies to Check Point Gaia versions R80.30 and later. The information presented in the whitepaper works for R77 and later; however, the screenshots are inaccurate and specific features aren't available for versions prior to R80.30.

Background on Gaia Clish

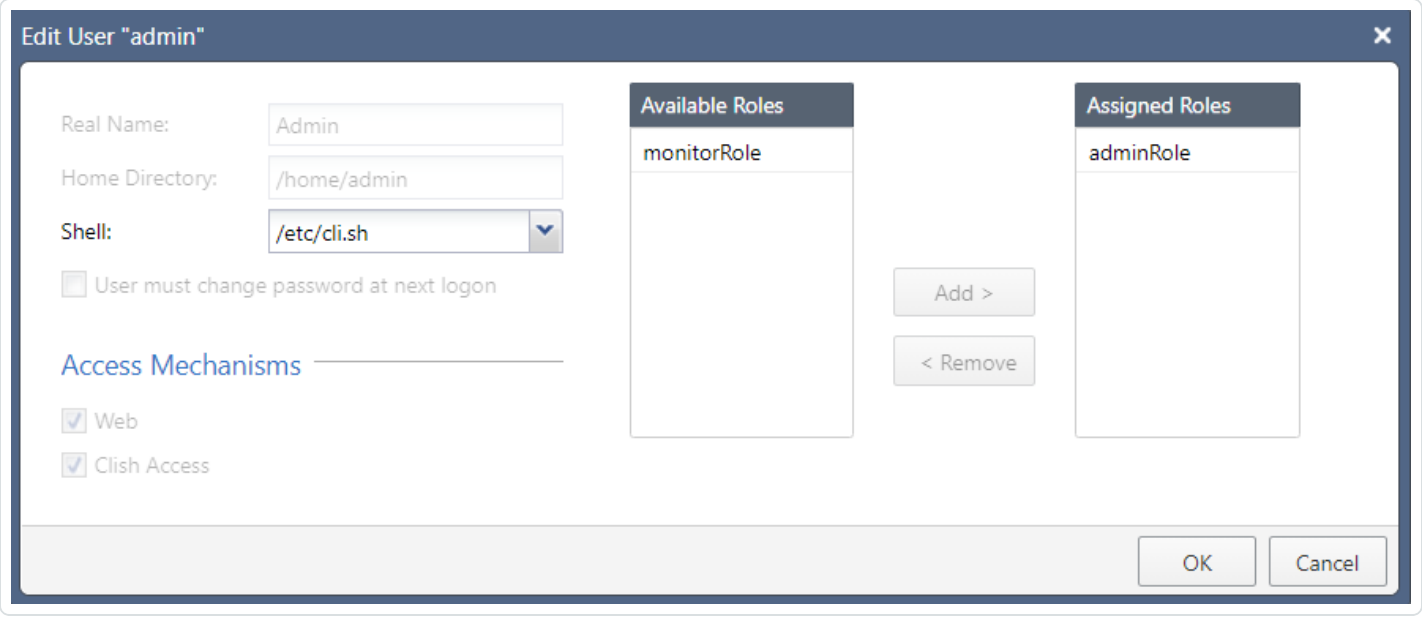
The default Gaia shell is called Clish. Gaia Clish restricts access to Linux system functions using role-based access control. Gaia Clish does not give access to low-level system functions. From the Clish shell, a user can access Linux system functions with the *expert* command. Another way to access Linux is to provision a user that is configured with a Linux shell. From the Linux shell, users with authorization can enter the Clish shell with the *clish* command.

Configuring Users on Check Point Gaia

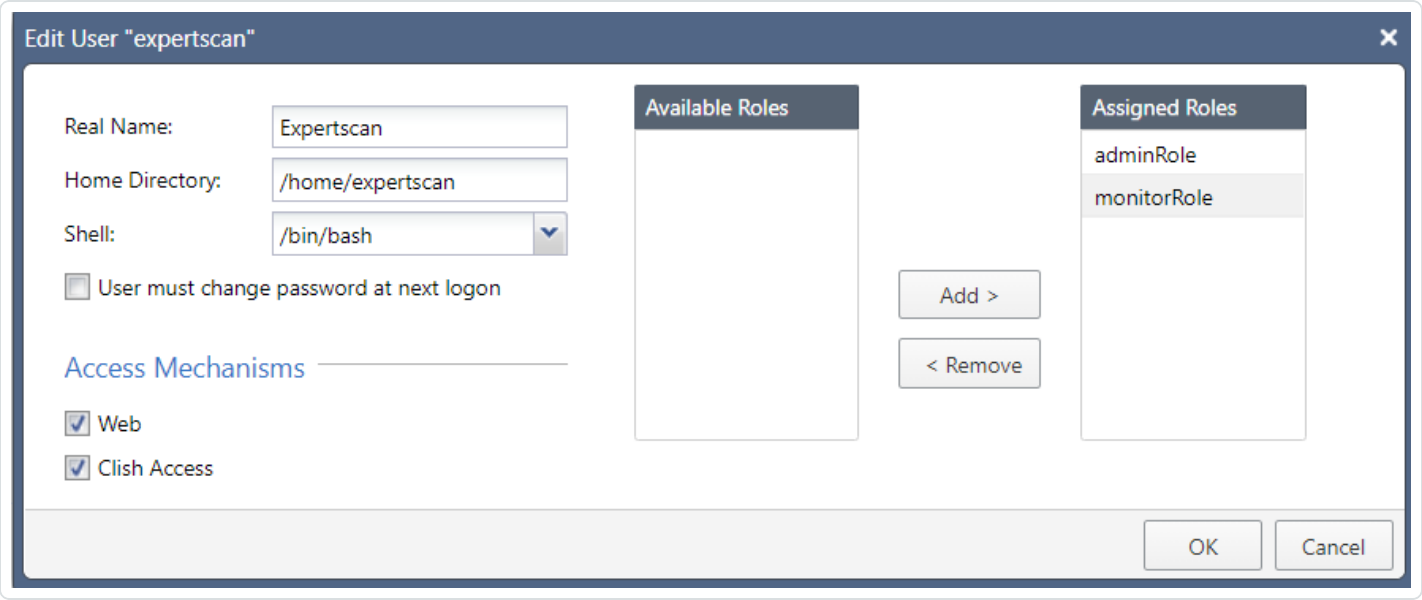
The following screenshots capture examples of the Gaia Clish and Expert mode users as configured on Check Point Gaia. In this example, the Gaia Clish user is named `admin`, and the Expert mode user is named `expertscan`. Nessus will use both of these accounts to run scans on the Gaia device.



This is an example configuration for a Gaia Clish shell user:



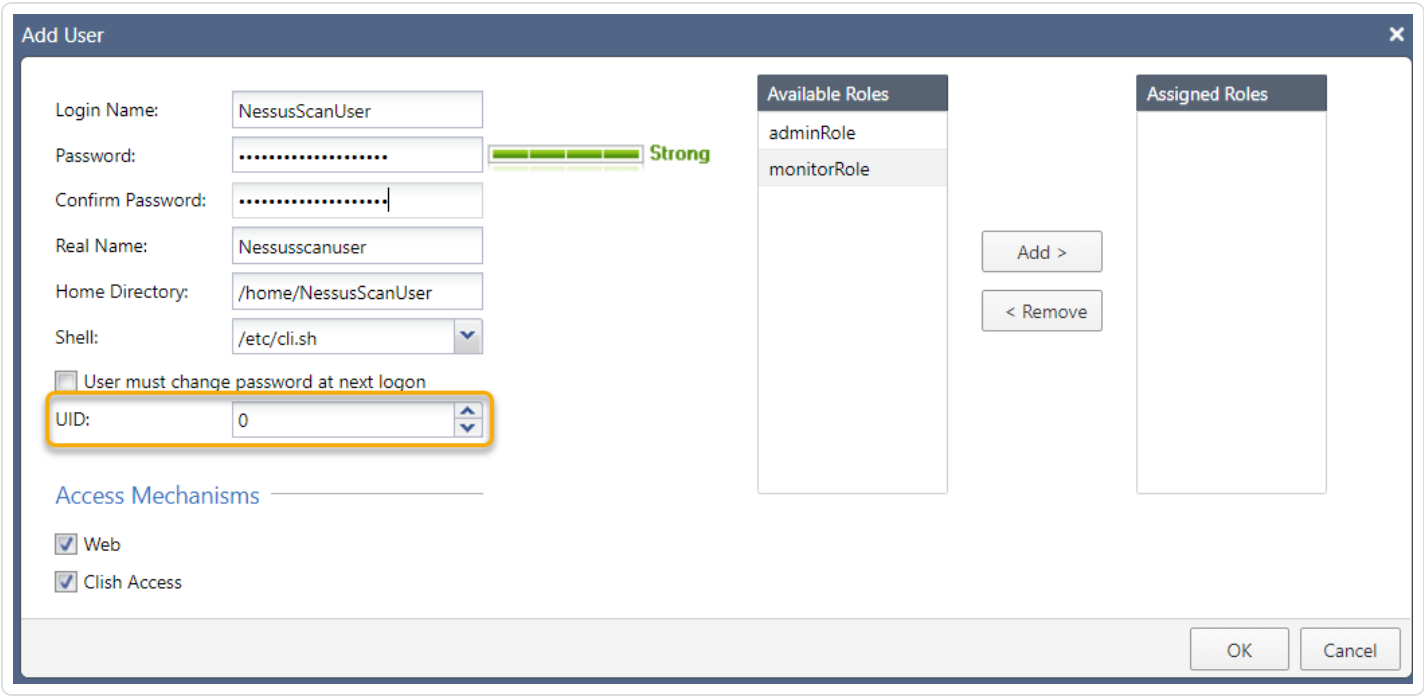
This is an example configuration for an Expert mode user:



Users configured with the Gaia Clish shell escalate privileges using the *expert* command in order to run Linux-based commands. Expert mode users enter the Gaia Clish shell using the *Gaia Clish* command. Nessus scans over SSH operate in the same fashion.

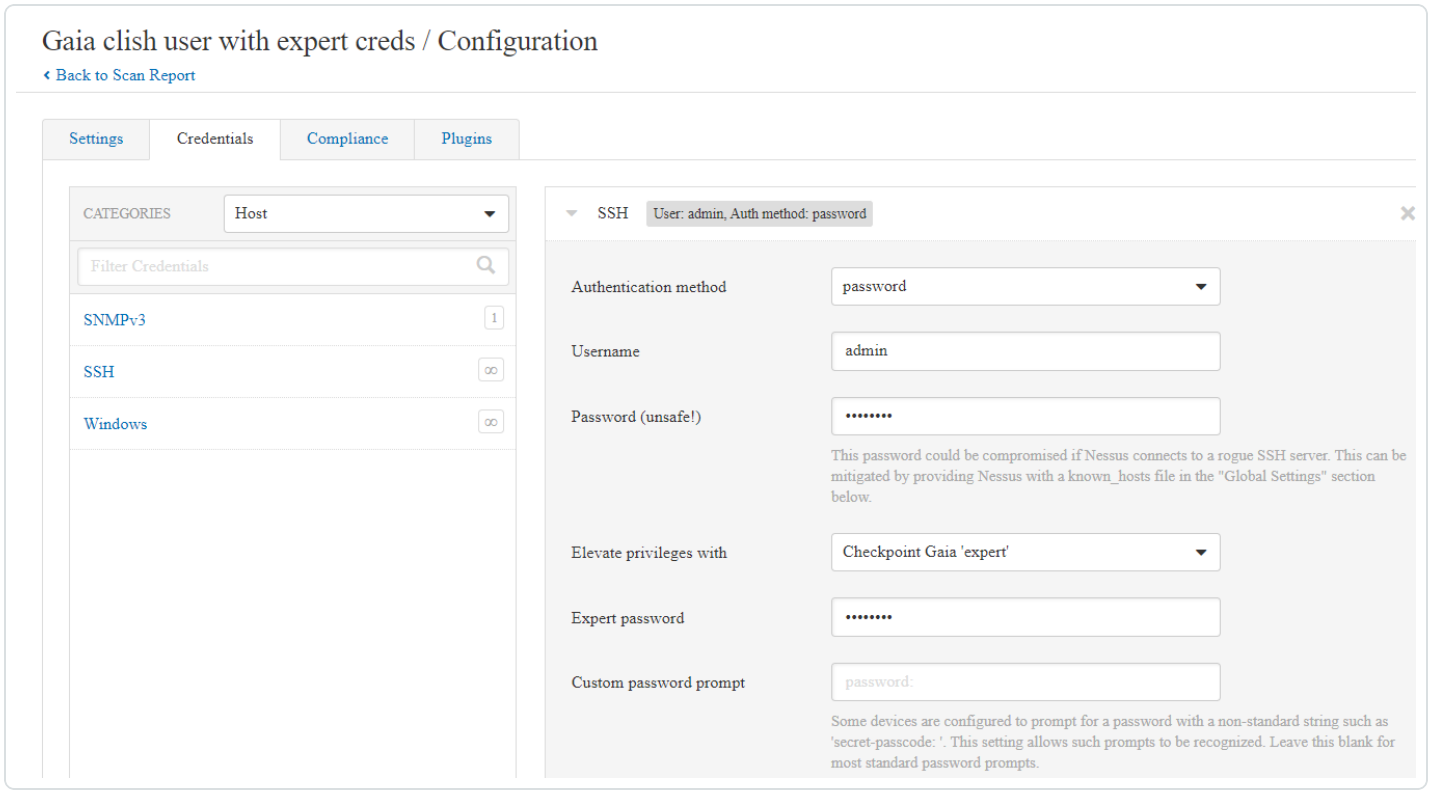
In either mode, Nessus will attempt to switch to the other mode to run certain commands. If the scan user is configured with the Gaia Clish shell, the Nessus scan credential will have to include an escalation password to allow the scanner to switch to Expert mode. Likewise, a scan user configured with an Expert mode shell will have to have **Gaia Clish Access** selected to allow Nessus to run Gaia Clish-based commands. All users created for Nessus scanning should have **Gaia Clish Access** selected.

Finally, Nessus only supports expert privilege escalation of Gaia Clish shell users to Expert mode. It is possible to create an Expert mode user with lower privileges by mapping its identity to an existing Linux identity on the device. However, a scan with that user will likely be incomplete because normal Linux escalation methods, such as *su* or *sudo*, are not currently supported for the Gaia OS. So, when creating an Expert mode user for scanning by Nessus, **UID 0** should be assigned to that user.



Configuration Notes on the Nessus Scanner

Nessus can be configured with the **Check Point Gaia *expert*** escalation method to escalate from the Gaia Clish shell to Expert mode. Here is an example Nessus credential for a Gaia Clish shell user with Expert mode escalation:



Summary

- Nessus only supports Gaia with SSH users configured with **Gaia Clish**, **bash**, or **Bourne (sh)**.
- Nessus scans can escalate from Gaia Clish to Expert mode using the **Check Point Gaia *expert*** escalation type.
- Users should be given Gaia Clish access.
- Expert mode users should be assigned **UID 0**.

Notes

- If a Nessus scan cannot run both Expert mode and Gaia Clish commands, the results will be incomplete.
- Scanning with a Gaia Clish shell user is likely to produce slower scans because of the way Nessus performs device discovery over SSH.