# Nessus Agents

February 17, 2015

# Table of Contents

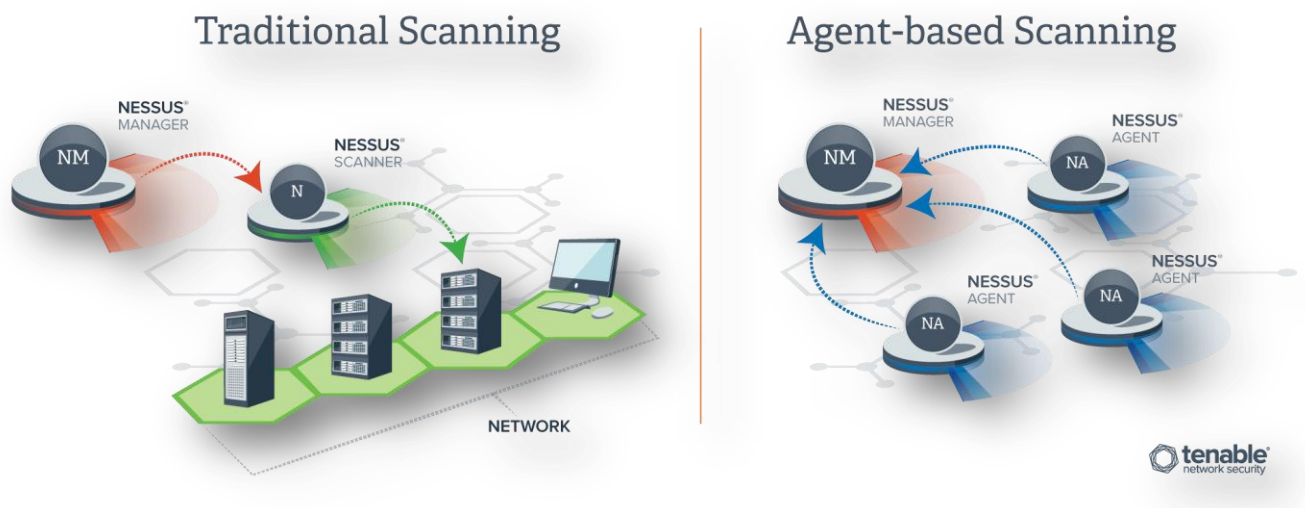
Introduction ........ 3
What Are Nessus Agents? ........ 3
Scanning ........ 4
Results ........ 6
Conclusion ........ 6
About Tenable Network Security ........ 6

## Introduction

Today's changing threat landscape requires organizations to constantly change how they detect threats against the network. As part of Nessus 6.3, Tenable has released Nessus Agents, a host-based tool designed to help organizations solve some of the problems encountered with traditional, network-based vulnerability assessments.

Network-based vulnerability assessments have a few core challenges. First, to provide the most detailed and complete results, they require credentials in order to access resources on target hosts. In some organizations, this requirement can cause considerable issues, especially in situations where the IT department believes that there is too much risk in providing credentials to the security team. Additionally, some organizations may not feel comfortable allowing a single username and password combination to connect across the entire environment. Those credentials need to follow the organization's password policy, and more than one set of credentials may be required to scan all systems on the network, even on a single platform.

Second, network-based vulnerability assessment tools shine when they are scanning a mostly static network. However, increasingly mobile workforces have decreased the effectiveness of traditional scanning. Geographically distributed sales teams, remote workers, and traveling executives can easily create gaps in asset availability during a vulnerability assessment. While traditional network scans have to originate from a scanner that reaches out to the hosts being scanned, using Nessus Agents, hosts can run the scan while they're not on the network, and then call back in to Nessus Manager once they obtain their results.

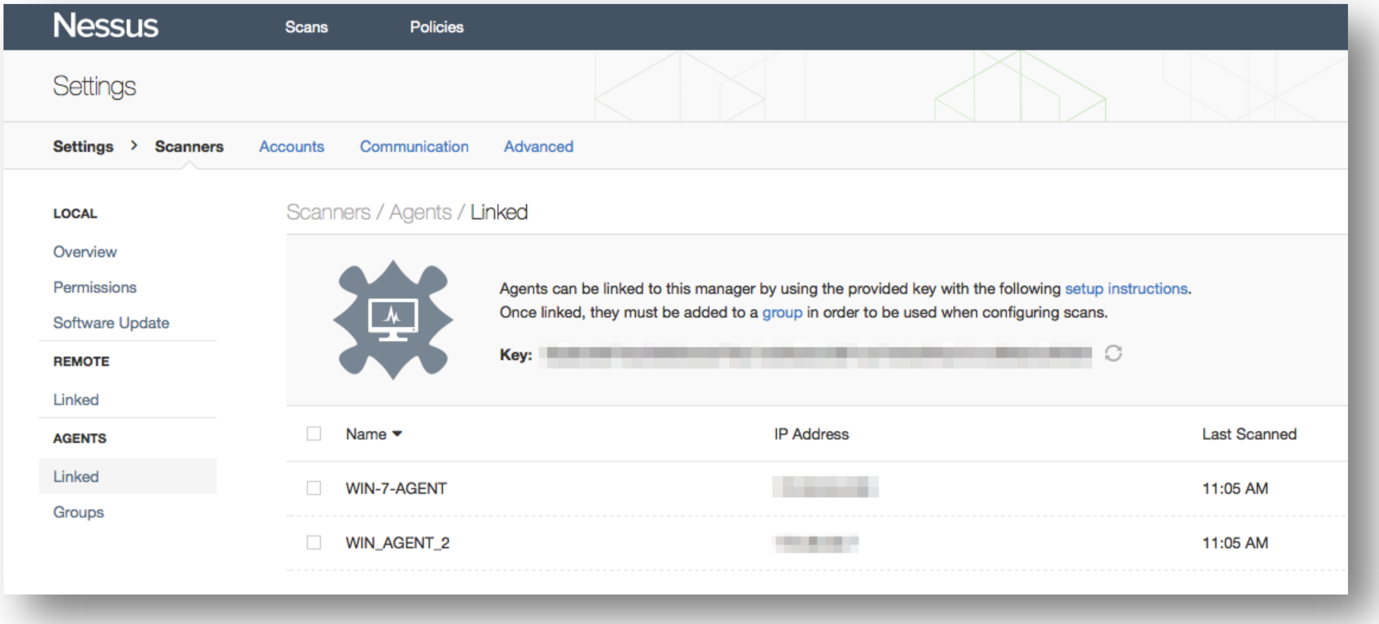


## What Are Nessus Agents?

Nessus Agents are lightweight programs that are installed locally on a host. Agents collect vulnerability, compliance, and system data and report that information back to a Nessus Manager system. Nessus Agents currently support 32 and 64-bit editions of the following operating systems:

- Windows 7
- Windows Server 2008 and Server 2008 R2
- Windows Server 2012 and Server 2012 R2
- Windows 8

Agents run under the local SYSTEM account in Windows, and require sufficient privileges to install software under that account on setup. Nessus Agents are packaged as .msi files for installation on Windows platforms, and after installation, a scriptable command can be used to register the agent with an instance of Nessus Manager. Once agents are connected, they are managed and updated via Nessus Manager.



Nessus Scans Policies

Settings

Settings > Scanners Accounts Communication Advanced

LOCAL
- Overview
- Permissions
- Software Update

REMOTE
- Linked

AGENTS
- Linked
- Groups

Scanners / Agents / Linked

Agents can be linked to this manager by using the provided key with the following setup instructions.
Once linked, they must be added to a group in order to be used when configuring scans.

Key: [redacted]

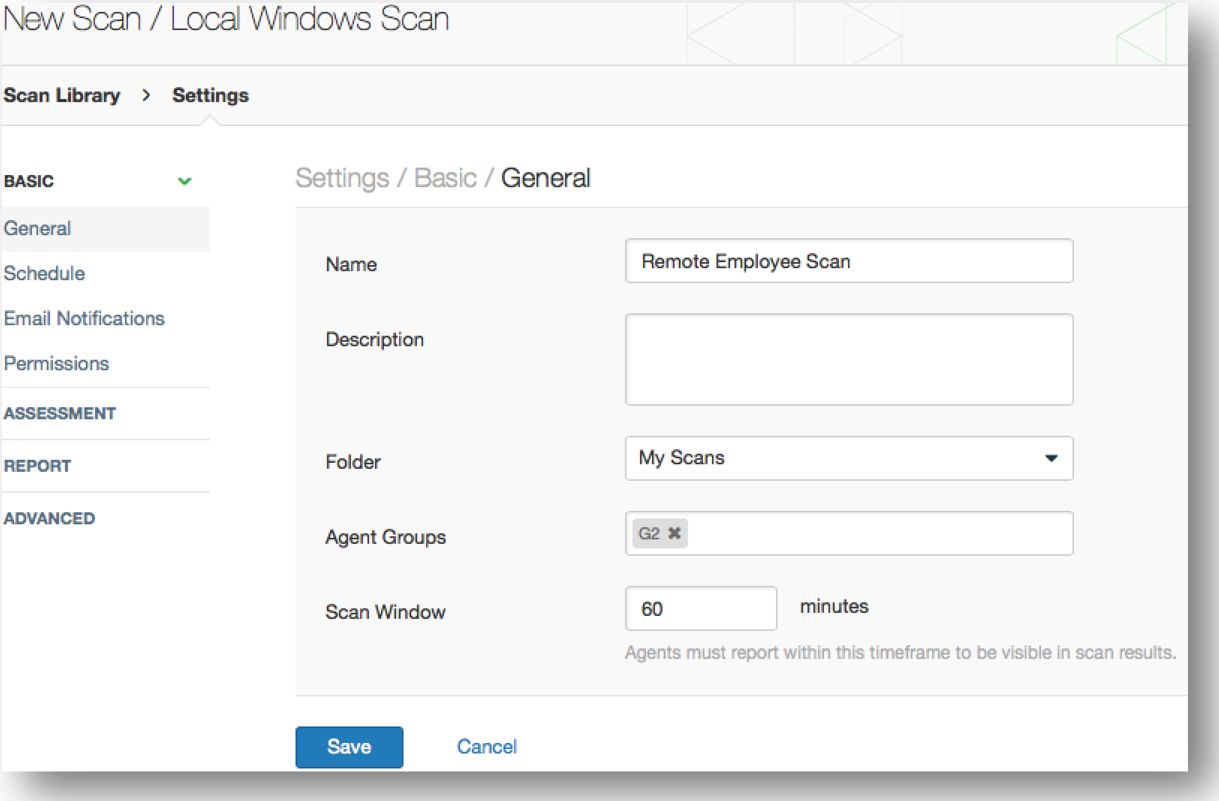
| □ | Name ▾ | IP Address | Last Scanned |
|---|---|---|---|
| □ | WIN-7-AGENT | [redacted] | 11:05 AM |
| □ | WIN_AGENT_2 | [redacted] | 11:05 AM |

By default, Nessus Agents communicate back to the Nessus Manager in the same way that standard Nessus scanners do: over TCP port 8834. That communication is encrypted with AES-256 encryption, depending on configuration at the time of installation.

Because Nessus Agents are packaged as .msi files, they can be deployed using software management systems such as Microsoft's System Center Configuration Manager (SCCM). Additionally, the configuration of Nessus Agents can be scripted, which allows administrators to easily deploy agents across multiple systems with minimal effort. All of this can be done without needing to create additional administrator or service accounts on the network. Nessus Agents also auto-update from the Manager once they are installed, so deployment only needs to be done once.

## Scanning

Starting an agent-based assessment will look very familiar to existing Nessus users, with a few slight differences. To get started, users will need to select a template from the new "Agents" section of the Scan Library. Instead of selecting a scanner or manually entering targets, users will be provided with an option to select groups of agents to serve as targets for the assessment. Users will then need to specify how long a scan is to run; this is the window of time in which targeted agents can check in and upload their results for a particular assessment.



New Scan / Local Windows Scan

Settings / Basic / General

Name: Remote Employee Scan

Description:

Folder: My Scans

Agent Groups: G2

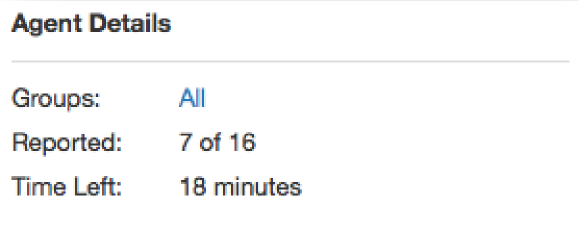
Scan Window: 60 minutes

Agents must report within this timeframe to be visible in scan results.

There are three types of agent scans: Local Windows, Compliance, and Advanced, which is a combination of the other two scan types. Additionally, there are a series of local configuration checks that can be run on the local host. Because each agent runs its local scan independent from other scanners, assessments complete and report their results back quickly.

| Scan Type | Capabilities |
|---|---|
| **Local Windows Scan** | Local patch checking and local information gathering, such as users, status of antivirus software, software starting up via the registry, USB device history, and more. |
| **Windows Compliance Audit** | Checks hosts against administrator-specified compliance and system hardening and configuration policies. |
| **Advanced Agent Scan** | A fully customizable agent scan that allows administrators to turn off specific plugins, check for malware and other harmful software, and more. |

When a scan is initiated, the Nessus Manager sends instructions to each Nessus Agent to run a configured scan. Once the scan has been initiated on the Manager, each agent in the defined scan group is given a certain amount of time to check back in to the Manager with their results. If an agent is offline or cannot connect back to the Manager within the defined window, it is treated the same way that an offline host would be in a traditional network scan, and doesn't appear in the results. A



Agent Details

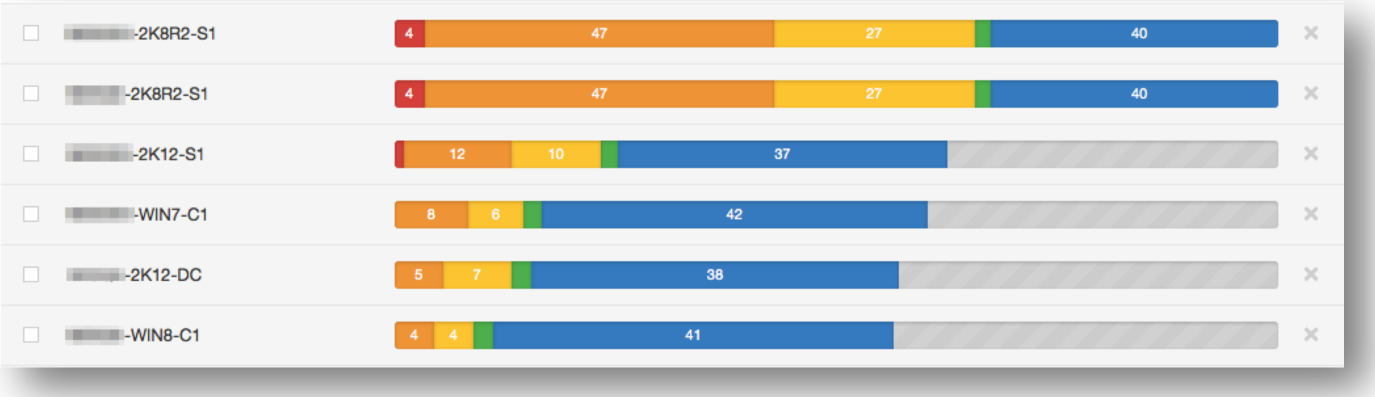
| | |
|---|---|
| Groups: | All |
| Reported: | 7 of 16 |
| Time Left: | 18 minutes |

scan will show as still running while it waits for any agents that have not checked back in with their results.

When creating scans, administrators can now choose between either traditional scans using full Nessus scanners or agent-based scans using Nessus Agents. Each type of scan serves a different role. Traditional, credentialed scans are well suited to assessing servers and static desktops, while agents can be used on laptops and other systems that may need special consideration. For organizations that are comprised completely of remote workers, a fully agent-based deployment enhances the assessment capabilities from previous versions of Nessus. Because agents are easily added to existing Nessus Manager deployments, organizations that simply wish to augment their existing assessment infrastructure with the flexibility that agents provide can do so.

## Results

Scan results from Nessus Agents will look familiar to users who have previous experience with Nessus. Results are organized by the hostname of the device on which the agent is installed, and display the number of detected vulnerabilities. Results management, for the most part, remains similar to that of traditional Nessus usage, where reports can be generated and sent to administrators or analysts for action.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ☐ | [redacted]-2K8R2-S1 | 4 | 47 | 27 | | 40 | × |
| ☐ | [redacted]-2K8R2-S1 | 4 | 47 | 27 | | 40 | × |
| ☐ | [redacted]-2K12-S1 | | 12 | 10 | | 37 | × |
| ☐ | [redacted]-WIN7-C1 | | 8 | 6 | | 42 | × |
| ☐ | [redacted]-2K12-DC | | 5 | 7 | | 38 | × |
| ☐ | [redacted]-WIN8-C1 | | 4 | 4 | | 41 | × |

However, by using Nessus Agents on individual laptops or workstations, additional reporting options are available for organizations.

## Conclusion

Tenable's new Nessus Agents feature gives organizations increased flexibility and options when deploying Nessus. Lightweight Nessus Agents can provide visibility into parts of an organization's network that would have previously been difficult or impossible to scan using traditional methods. Also, because agents are installed similarly to other Windows applications, there is no need for the creation of additional user accounts or managing system account passwords. Systems that were previously off-limits due to internal policies regarding credential management, assets that might have been unavailable previously, and other types of remote and mobile systems are now more easily accessible thanks to Nessus Agents.

## About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.