

# Quick Start Guide: Utilizing Nessus to Secure Microsoft Azure

## Introduction

Tenable Network Security is the first and only solution to offer security visibility, Azure cloud environment auditing, system hardening, and continuous monitoring so you can regain visibility, reduce attack surface, and detect malware across your Microsoft Azure deployments. This document describes how to deploy the following Tenable solutions to help ensure a secure and compliant Microsoft Azure cloud environment:

- [Auditing Microsoft Azure Cloud Environment](#)
- [Nessus BYOL \(Bring Your Own License\) Scanner](#)
- [Nessus Agent Scans of Microsoft Azure Cloud Instances](#)

With more than one million users, Nessus is the world's most widely-deployed vulnerability, configuration, and compliance assessment product. Nessus prevents attacks by identifying the vulnerabilities, configuration issues, and malware that hackers could use to penetrate your network. It is as important to run these assessments in Microsoft Azure as it is in any other IT environment.

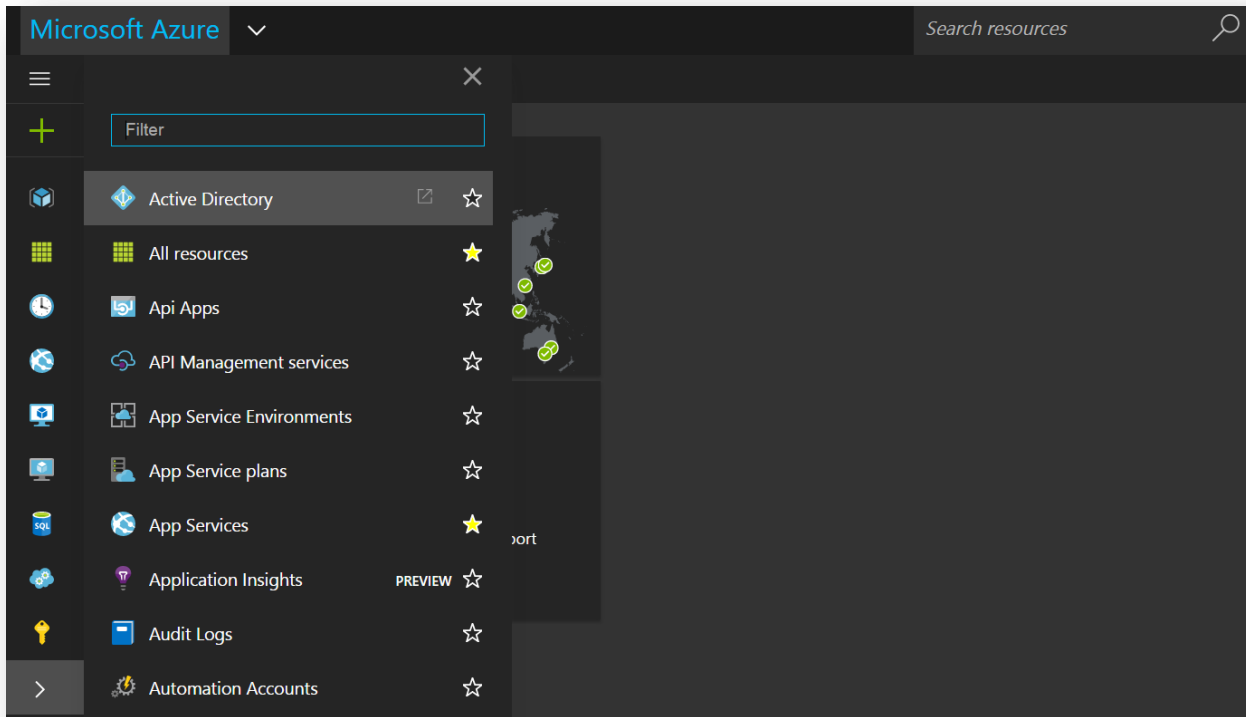
Please email any comments and suggestions to [support@tenable.com](mailto:support@tenable.com).

## Auditing the Microsoft Azure Cloud Environment

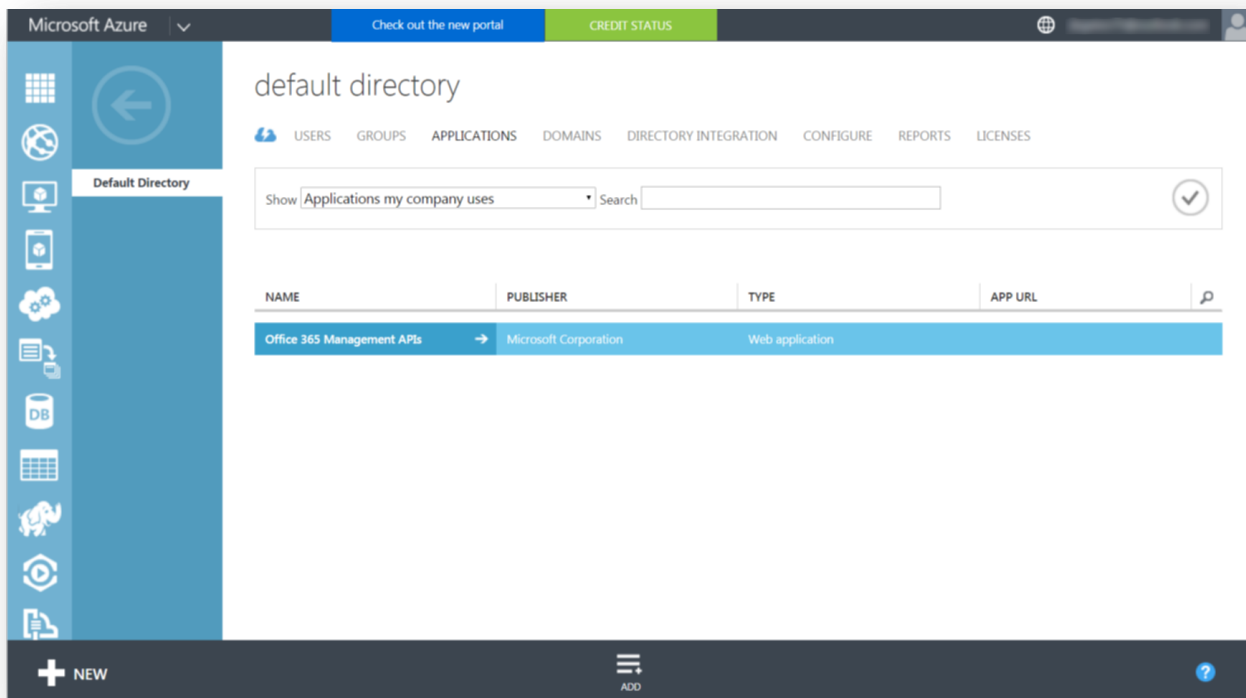
Tenable offers the ability to audit the Microsoft Azure Cloud environment to detect misconfigurations within the cloud environment and with account settings. Audits can be performed using Nessus Cloud, Nessus Manager, or a standalone Nessus scanner. No pre-authorization is needed from Microsoft to perform the audit, but a Microsoft Azure account is required.

In order to perform an audit of the Microsoft Azure cloud environment, Nessus will need a Microsoft Azure “**Client ID**”. To obtain a Client ID, navigate to Microsoft Azure (<https://manage.windowsazure.com>) and log in.

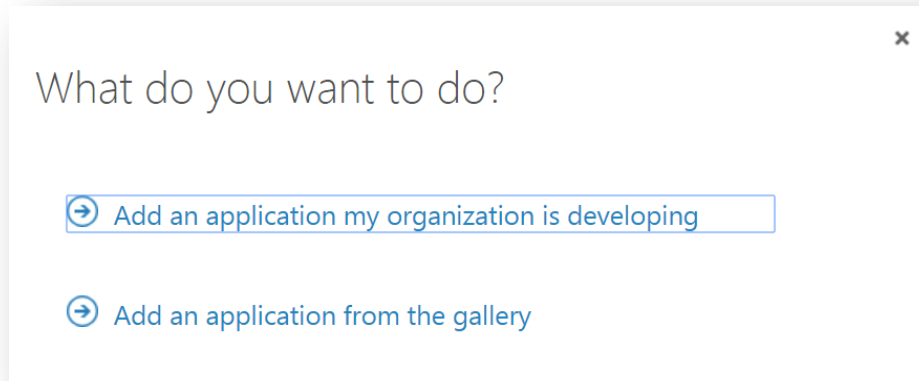
Once logged in, click the browse “>” button on the left-hand menu and select “Active Directory”.



Click on “Applications” and then click on “Add” located at the bottom center of the window.



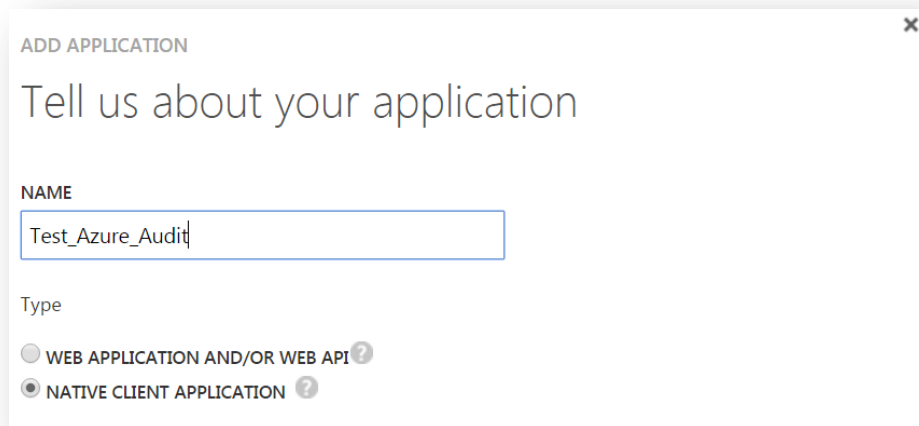
Click “Add an application my organization is developing”.



A dialog box titled "What do you want to do?" with a close button (X) in the top right corner. It contains two options, each preceded by a right-pointing arrow icon in a circle:

- Add an application my organization is developing
- Add an application from the gallery

Enter a name for the application, select “Native Client Application”, and click the right arrow to proceed.



A dialog box titled "ADD APPLICATION" with a close button (X) in the top right corner. The main heading is "Tell us about your application".

NAME

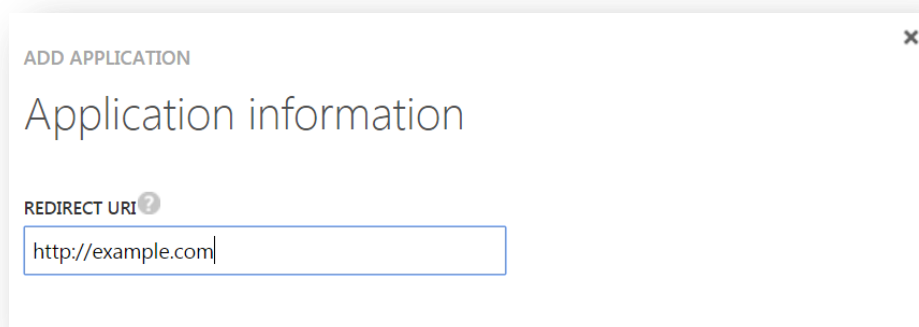
Test\_Azure\_Audit

Type

☐ WEB APPLICATION AND/OR WEB API ?

☒ NATIVE CLIENT APPLICATION ?

Enter a “Redirect URI” and click the checkmark to complete the setup.



A dialog box titled "ADD APPLICATION" with a close button (X) in the top right corner. The main heading is "Application information".

REDIRECT URI ?

http://example.com

Click **Configure** to display the Client ID. Copy the **Client ID**. This information will be used to complete the audit configuration with Nessus.

test\_azure\_audit

DASHBOARD CONFIGURE

properties

NAME  ?

CLIENT ID  ?

REDIRECT URIS  ?

On the bottom of that same window click **Add application**.

permissions to other applications

Windows Azure Active Directory Delegated Permissions: 1

**Add application**

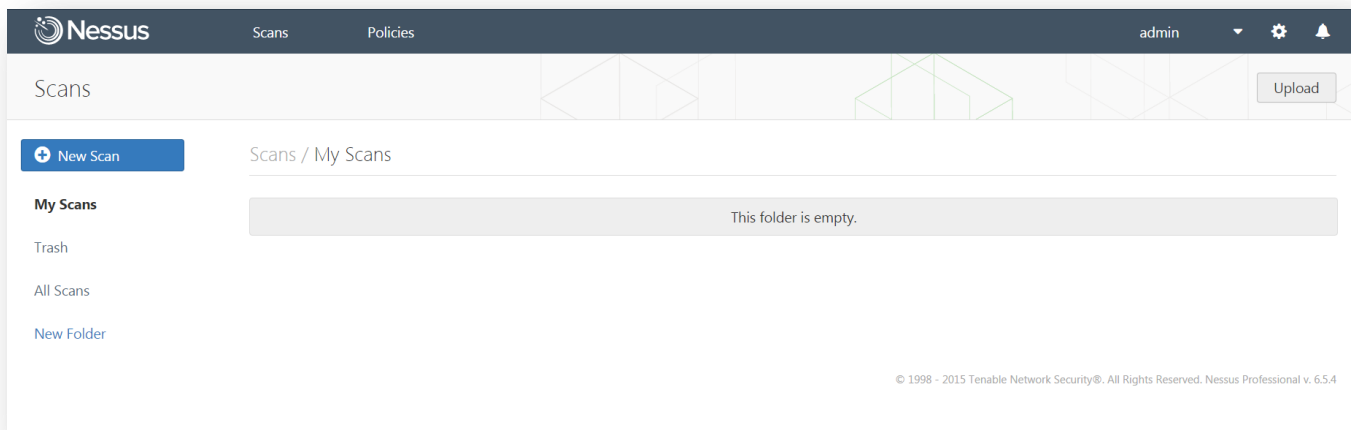
Click the “+” next to “**Windows Azure Service Management API**” to add the necessary permissions. When the permissions have been granted, the “+” will turn into a green checkmark. Click the green checkmark on the bottom right-hand side of the screen to complete the process.

## Permissions to other applications

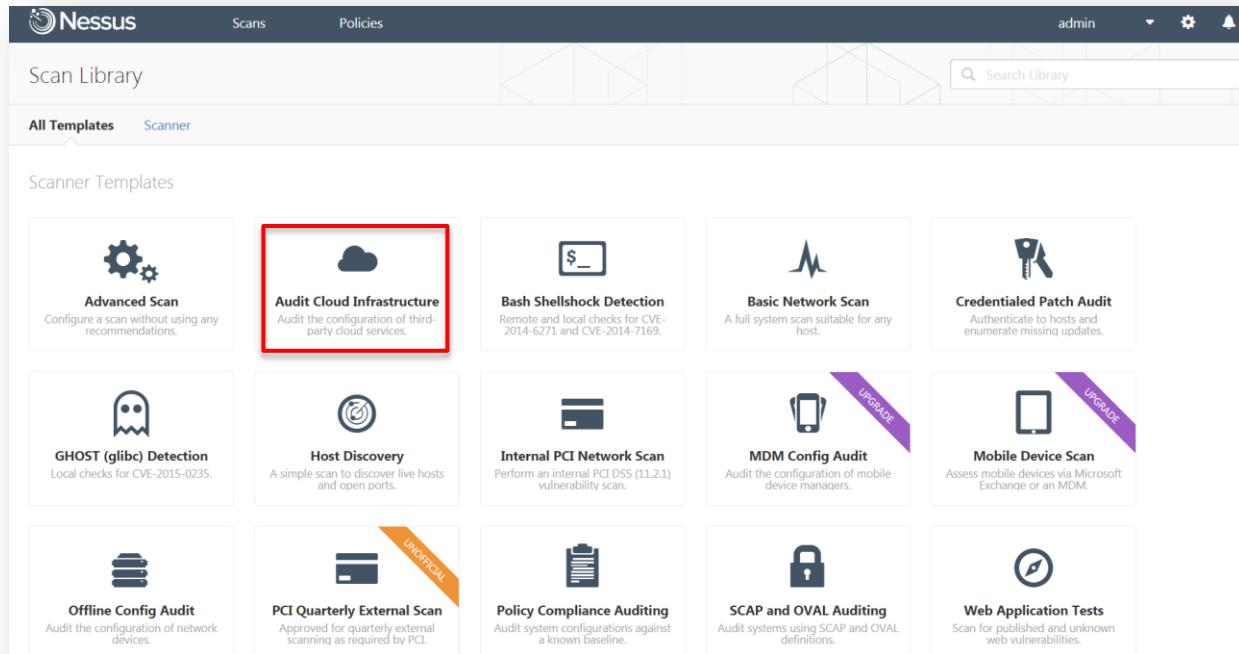
SHOW <span>Microsoft Apps</span> <span>✓</span>		
NAME	APPLICATION PERMISSIONS	DELEGATED...
Microsoft Graph	14	33
Office 365 Management APIs	3	3
Windows Azure Active Directory	✕ 4	8
Windows Azure Service Management API	✓ 0	1
		SELECTED
		<span>i</span> Windows Azure Service Manageme

You will be returned to the previous configuration screen. Click “**Save**” located near the bottom of the window to finalize the setup.

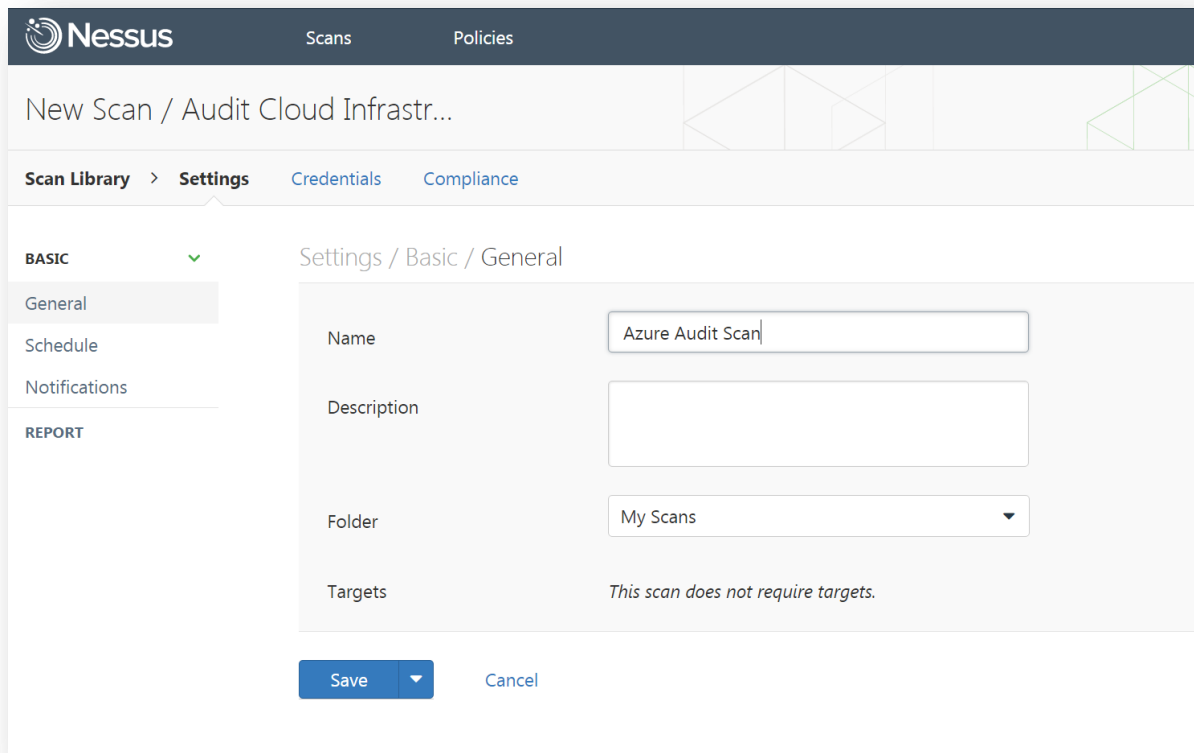
Log into Nessus and click “**New Scan**”.



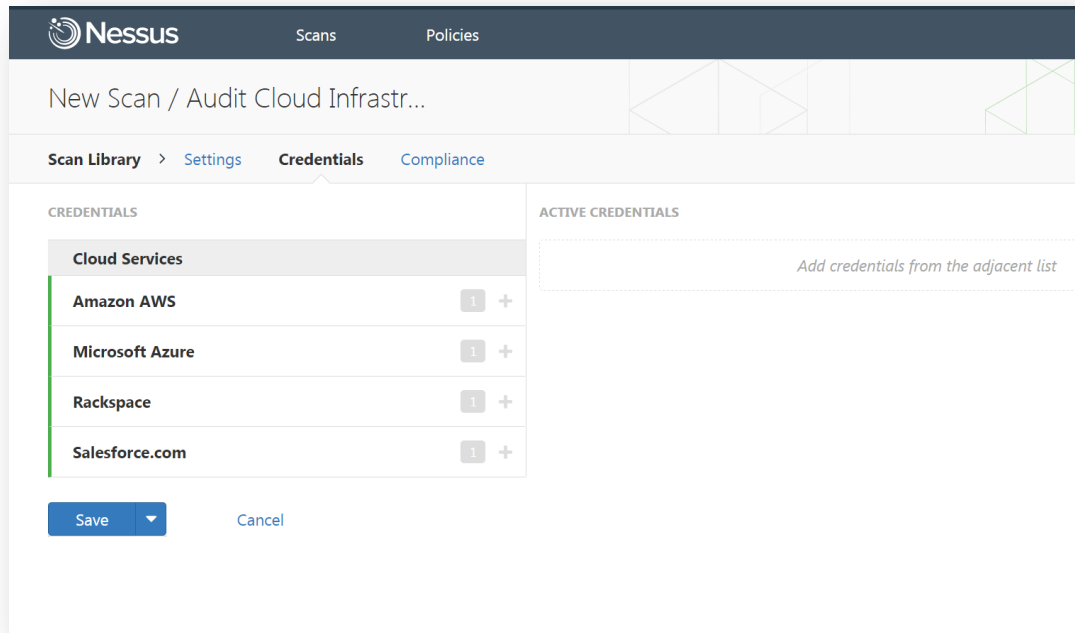
Select the “Audit Cloud Infrastructure” template.



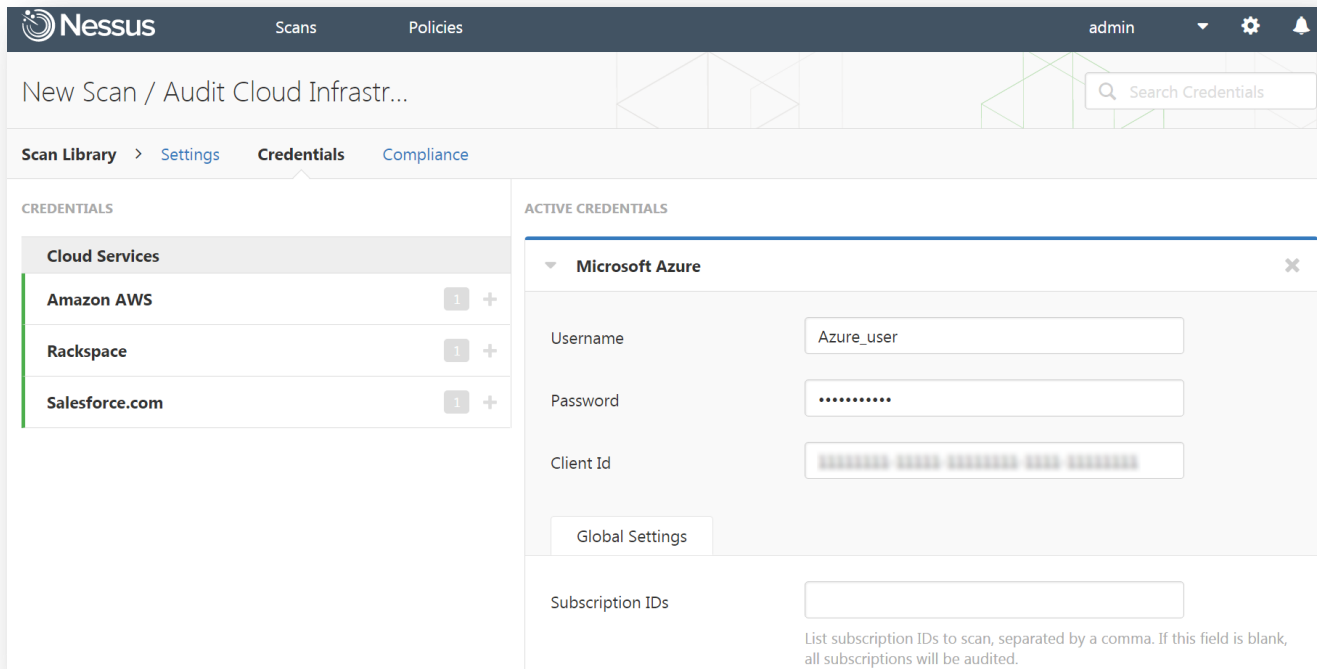
Enter a descriptive name for the scan and then click on “Credentials”.



Click the “+” next to **Microsoft Azure** to open the “Credentials” options.



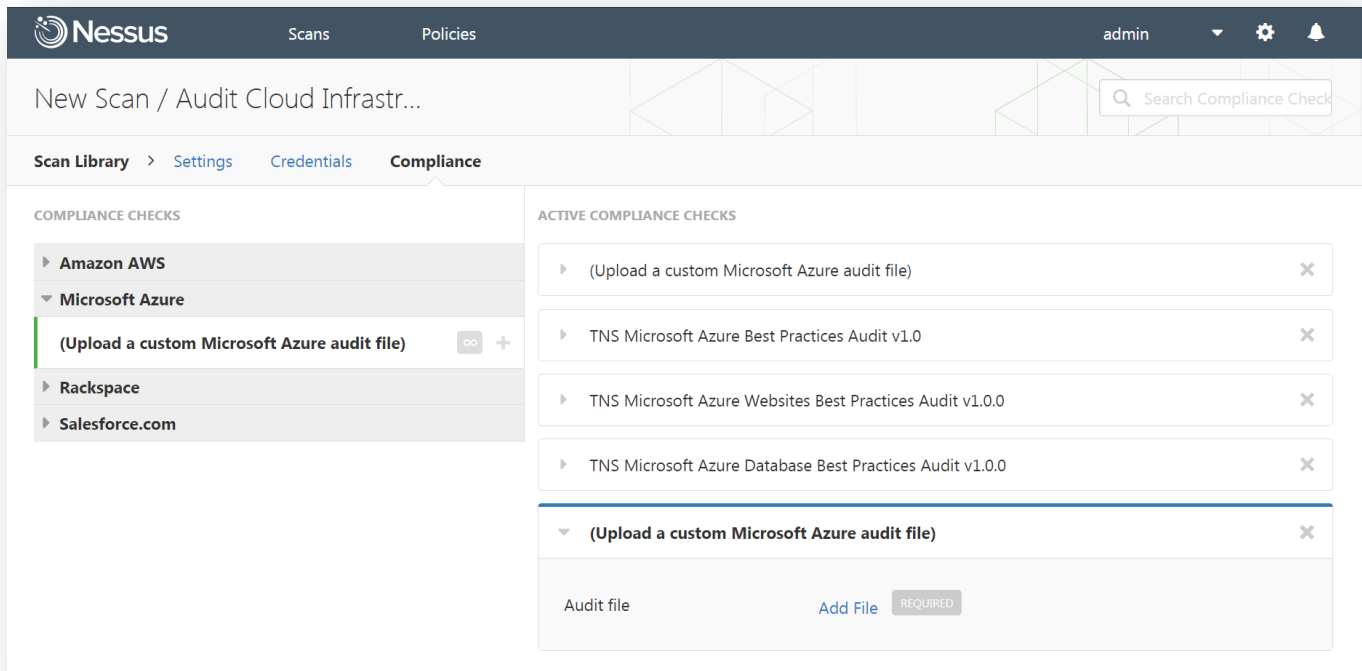
Enter your Microsoft Azure “Username” and “Password”, “Client ID”, and “Subscription IDs” into the appropriate boxes. Leave the “Subscription IDs” box blank if you want to audit all of your Azure subscriptions.



Click **“Compliance”** and expand the **“Microsoft Azure”** option. Tenable offers three pre-configured compliance checks and also provides the ability to upload a custom Azure audit file. Click the **“+”** next to each compliance check you want to add to the scan.

If you choose to add a custom audit file, click **“Add File”** and select the file to upload.

Once the compliance checks are added, click **“Save”** or click the drop-down arrow next to **“Save”** and select **“Launch”** to initiate the scan.



**Microsoft Azure Best Practices – Infrastructure:** This audit file implements a set of general best practices for Microsoft Azure infrastructure items including Principals, Virtual Networks, Certificates, and Virtual Machines.

**Microsoft Azure Best Practices – Websites:** This audit file implements a set of general best practices for Microsoft Azure Website items including Website Status, SSL Status, and recent Site modifications.

**Microsoft Azure Best Practices – Databases:** This audit file implements a set of general best practices for Microsoft Azure items including Database Configuration, Audit Events, and Recoverable Databases.

For additional information on configuring Nessus scans, please refer to the [Nessus documentation](#) on the Tenable website.

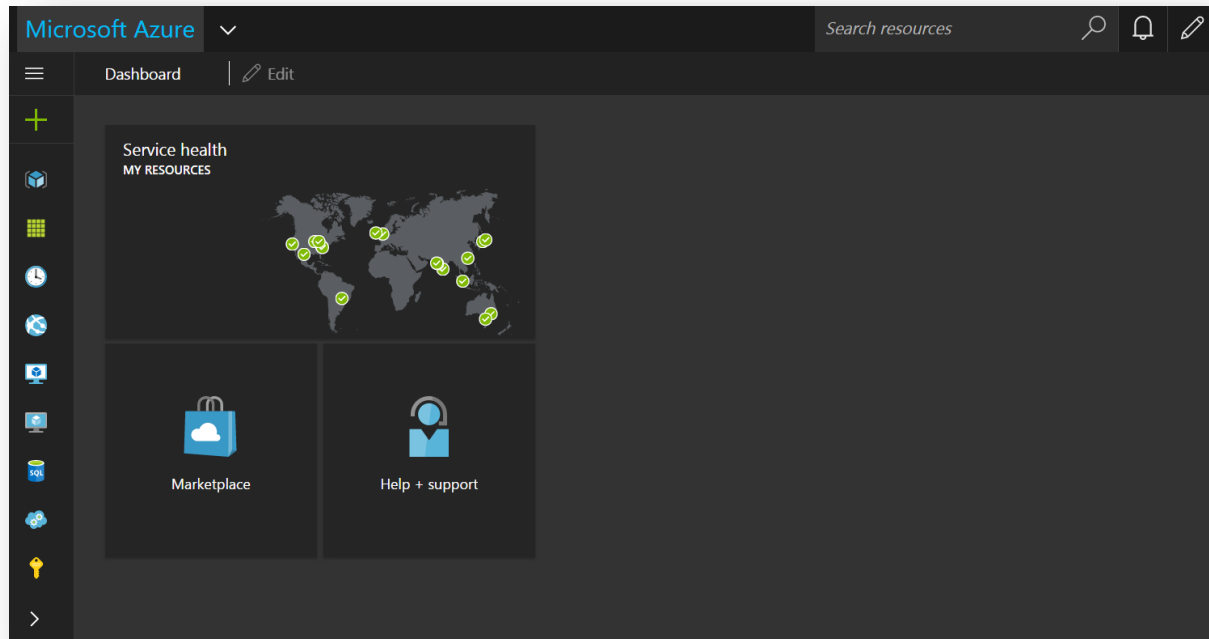
## Provisioning Nessus BYOL from the Microsoft Azure Marketplace

The Nessus BYOL is an instance of Nessus installed within Microsoft Azure that allows scanning of the Azure cloud environments and instances. Nessus BYOL capabilities include web application scanning and detection of vulnerabilities, compliance violations, misconfigurations, and malware.

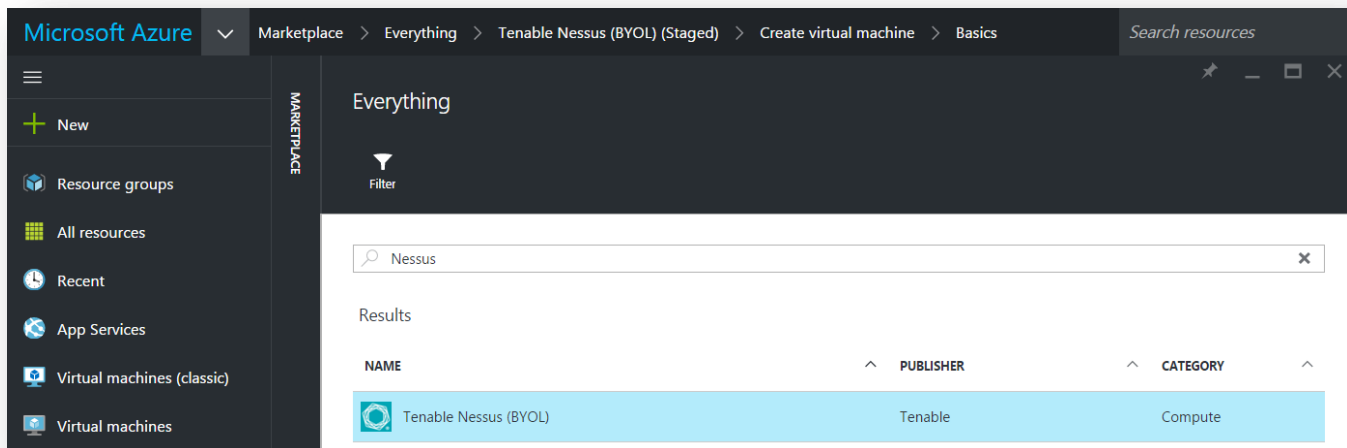
Customers interested in leveraging Nessus BYOL to secure their environments and instances must first purchase a Nessus license either directly from Tenable's [e-Commerce store](#) or from an [authorized reseller](#). The license will provide an Activation Code to apply when provisioning Nessus from your Microsoft Azure account.



To provision a Nessus BYOL instance, go to Microsoft Azure (<https://manage.windowsazure.com>) and log in.

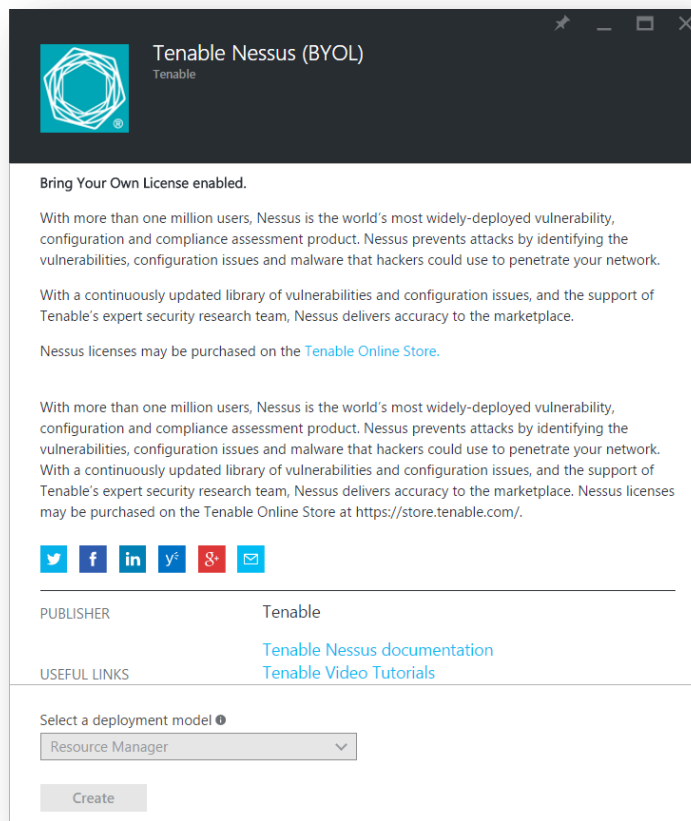


Click on “Marketplace” and search for “Nessus”.



Click “Tenable Nessus (BYOL)” to review the product page.

Choose an option under “**Select a deployment model**” and click “**Create**” to begin deployment of the Nessus BYOL virtual machine.



On the “**Basics**” screen, enter the following information and click “**OK**”.

**Table 1 – Nessus BYOL Scanner Basics**

Option	Description
Name	Descriptive name for the Nessus BYOL scanner
User name	User account name used to access the Nessus BYOL scanner
Authentication Type	Select “SSH public key”
SSH public key	Once generated, enter the SSH public key
Subscription	Select the subscription to which the virtual machine will be added
Resource group	Enter the name of a new Resource group or select an existing Resource group
Location	Select the geographical location for the virtual machine

Create virtual machine

Basics

1 Basics  
Configure basic settings

2 Size  
Choose virtual machine size

3 Settings  
Configure optional features

4 Summary  
Tenable Nessus (BYOL) (Staged)

5 Buy

Name

BYOL1

User name

Nessus\_user

Authentication type

Password

SSH public key

SSH public key

Subscription

Free Trial

Resource group

Nessus

Select existing

Location

East US

OK

Microsoft’s recommended sizes are displayed. To view all available sizes, click on “**View all**”.

Choose a desired virtual machine size by clicking on one of the displayed options and clicking “**Select**”.

Create virtual machine

Choose a size

1 Basics  
Done

2 Size  
Choose virtual machine size

3 Settings  
Configure optional features

4 Summary  
Tenable Nessus Professional B...

5 Buy

Prices presented below are estimated retail prices that include both Azure infrastructure and applicable third-party software costs. Prices do not reflect applicable discounts for your subscription and may include currency conversions.

★ Recommended | View all

A0 Standard	A1 Standard	A2 Standard
0.25 Cores	1 Core	2 Cores
0.75 GB	1.75 GB	3.5 GB
1 Data disks	2 Data disks	4 Data disks
1x500 Max IOPS	2x500 Max IOPS	4x500 Max IOPS
Load balancing	Load balancing	Load balancing
Auto scale	Auto scale	Auto scale
14.88	44.64	89.28

Select



On the “**Settings**” screen, enter the following information and click “**OK**”.

*Table 2 – Nessus BYOL Scanner Settings*

Option	Description
Disk type	Select Standard or Premium disk type
Storage account	Create or select a storage account type
Virtual network	Create or select a virtual network the Nessus BYOL will reside in
Subnet	Assign Nessus BYOL to a subnet in the virtual network
Public IP address	Option to create a public IP address so that the Nessus BYOL virtual machine is accessible outside the virtual network
Network security group	Enables firewall rules to control traffic to and from the Nessus BYOL virtual machine
Diagnostics	Enabling this option provides minute-by-minute metrics on the Nessus BYOL virtual machine
Availability set	Provides redundancy by grouping two or more virtual machines in an availability set

**Create virtual machine**

1 Basics Done ✓

2 Size Done ✓

3 Settings Configure optional features >

4 Summary Tenable Nessus Professional B... >

5 Buy >

**Settings**

**Storage**

Disk type ⓘ  
Standard Premium (SSD)

\* Storage account ⓘ  
(new) nessus7477 >

**Network**

\* Virtual network ⓘ  
(new) Nessus >

\* Subnet ⓘ  
default (10.0.0.0/24) >

\* Public IP address ⓘ  
(new) BYOL1 >

\* Network security group ⓘ  
(new) BYOL1 >

**Monitoring**

Diagnostics ⓘ  
Disabled Enabled

\* Diagnostics storage account ⓘ  
(new) nessus7477 >

**Availability**

\* Availability set ⓘ  
None >

OK

You are now presented with a summary of your selections. Click “OK” to continue; you will be given the option to “Purchase” the Nessus BYOL virtual machine you have configured.

**Purchase**

---

**Offer details**

Tenable Nessus (BYOL) by Tenable <a href="#">Terms of use and privacy policy</a>	0.0000 USD/hr *
Standard A0 by Microsoft <a href="#">Terms of use and privacy policy</a>	0.0200 USD/hr + <a href="#">Pricing for other VM sizes</a>

**\* Marketplace Offering:** May not be purchased using Microsoft subscription credits or monetary commitment funds and does not participate in discounts. These purchases are billed separately.

**+ Azure Resource:** May be purchased using Microsoft subscription credits or monetary commitment funds and participates in discounts. Prices presented are retail prices and may not reflect discounts associated with your subscription.

**Terms of use**

By clicking "Purchase", I (a) agree to the legal terms and privacy statement(s) associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s), and (c) agree that Microsoft may share my contact information and transaction details with the seller(s) of the offering(s). Microsoft does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

**Purchase**

If you are deploying the instance into an Azure Virtual Network, you must ensure you can reach TCP port 8834 on an IP address associated with the instance. This will be needed to complete the configuration process, as well as for the use of the product.

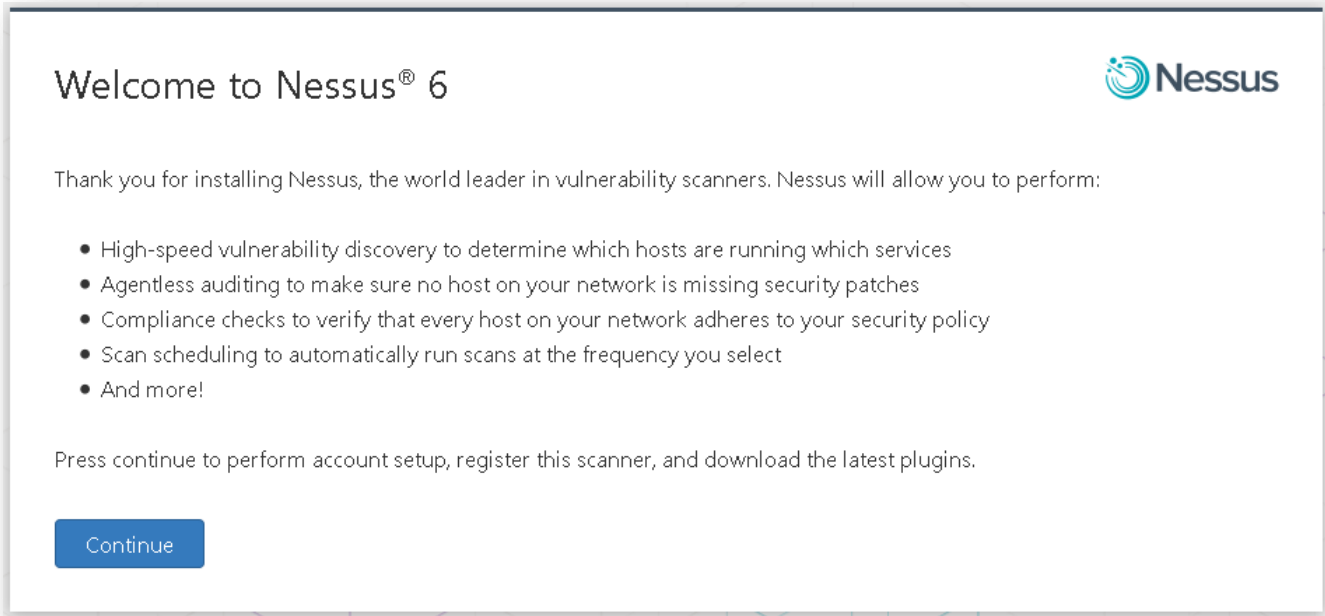
Configure the instance and/or the Azure Virtual Network so that Nessus can communicate with Tenable servers; this is required for registration and plugin updates. If for some reason this is not possible, please refer to the [Nessus documentation](#) regarding off-line updates.

Generally, you will connect to the public IP address (or external hostname) associated with an instance. If you are connecting to Nessus over a VPN to an Azure Virtual Network, it may be the private IP address. The IP addresses associated with the instance can be found under the virtual machine "Settings".

After the instance has initialized, open a browser and connect to the instance to complete the configuration. For example:

`https://<IP address or hostname>:8834`

The following welcome screen will be displayed:



To complete the configuration, please refer to the [Nessus documentation](#) on the Tenable website.



Prior to scanning, you must request permission to conduct vulnerability and penetration testing on instances in the Microsoft Azure cloud environment. Please visit the following page to review the approval process and to submit a testing request: <https://security-forms.azure.com/penetration-testing/terms>.

## Nessus Agent Scans of Microsoft Azure Cloud Instances

Tenable's Nessus Agents provide the ability to perform local scans on instances within the Microsoft Azure cloud environment. Nessus agent scans, which are configured, managed, and updated through Nessus Cloud or Nessus Manager, help identify vulnerabilities, compliance violations, misconfigurations, and malware.

Nessus Agents are downloaded from the [Tenable Support Portal](#), installed on an instance running in the Microsoft Azure cloud environment, and then linked to Nessus Cloud or Nessus Manager.



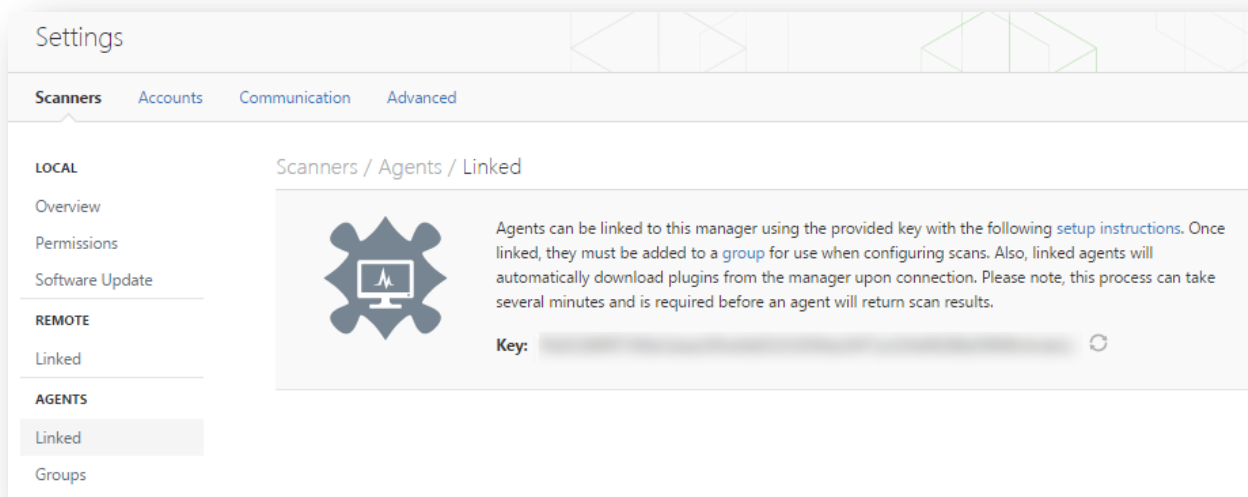
Agents can be installed on your target(s) manually, via Group Policy, SCCM, or other third-party software deployment applications.

Nessus Agents are linked to a Nessus Cloud or Nessus Manager in the same manner as linking to a secondary scanner. Prior to installing Nessus Agents, you must acquire the Agent Key from within Nessus Cloud or Nessus Manager.

To acquire the Agent Key, log into Nessus Cloud or Nessus Manager and go to **"Settings"**.

Select **"Agents"** under the **"Scanners"** section, and then select **"Linked"**.

A key will be generated that is used as a shared secret for the Nessus Agents to link to the scanner.



For more information on installing and configuring Nessus Agents refer to the [Nessus documentation](#) on the Tenable website.

## 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](https://tenable.com).