Tanium™ Provision User Guide

Version 1.2.45

May 17, 2022

The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://docs.tanium.com for the most current Tanium product documentation.

This documentation may provide access to or information about content, products (including hardware and software), and services provided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.

Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored into the ongoing delivery schedule of features and releases with our existing resources.

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, email Tanium Support at support@tanium.com, or email accessibility@tanium.com to make further inquiries.

Table of contents

Provision overview

> NOTE Provision is currently in limited availability and is subject to approval before it can be installed. For more information, Contact Tanium Support on page 32.

Provision provides bare-metal provisioning of Microsoft Windows to on-premises and Internet-connected devices. It also enables re-imaging outdated or broken devices.

OS bundles

An *OS bundle* includes all of the files and settings that an operating system deployment requires. You can create an OS bundle for each Windows version, or for unique configurations that you can use for location, hardware, or business processes.

For more information, see Configure an OS bundle on page 20.

Offline domain join

If you want newly-deployed Windows endpoints to join an Active Directory (AD) domain, you can use Tanium Provision to set up an offline domain join (ODJ) process. Provision uses ODJ functionality through a web service called TaniumODJ. The TaniumODJ service joins newly-deployed Windows endpoints to AD.

For more information, see Setting up offline domain join on page 24.

PXE endpoints

A *Preboot eXecution Environment (PXE) endpoint* is an endpoint that runs a service to provide required content for clients. The TaniumPXE service provides the PXE endpoint capabilities. You can boot devices from a PXE network or from USB media.

For more information, see Provisioning endpoints on page 26.

Getting started with Provision

Follow these steps to configure and use Provision.

Step 1: Install and configure Provision

See Installing Provision on page 14 and Configuring Provision on page 15.

Step 2: Prepare OS bundle content

See Preparing OS bundle content on page 18.

Step 3: (Optional) Set up offline domain join

See Setting up offline domain join on page 24.

Step 4: Provision endpoints

See Provisioning endpoints on page 26.

Provision requirements

Review the requirements before you install and use Provision.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Provision. Provision is licensed with the Tanium IT Operations Suite (Tanium™ Asset, Tanium™ Deploy, Tanium™ Discover, and Tanium™ Patch).
- **Tanium™ Core Platform servers**: 7.3.314.4250 or later
- **Tanium™ Client**: Any supported version of Tanium Client. For the Tanium Client versions supported for each OS, see Tanium Client Management User Guide: Client version and host system requirements.
  If you use a client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed client versions.

Computer group dependencies

When you first sign in to the Tanium Console after a fresh installation of Tanium Server 7.4.2 or later, the server automatically imports the computer groups that Provision requires: `All Computers`.

For earlier versions of the Tanium Server, or after upgrading from an earlier version, you must manually create the computer groups. See Tanium Console User Guide: Create a computer group.

Solution dependencies

Other Tanium solutions are required for Provision to function (required dependencies) or for specific Provision features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

Some Provision dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 9. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Provision requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Provision, the Tanium Server automatically imports all your licensed solutions at the same time. See Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Provision to import, you must manually import dependencies. See Tanium Console User Guide: Import, re-import, or update specific solutions.

Required dependencies

Provision has the following required dependencies at the specified minimum versions:

- Tanium Client Management 1.7 or later

Tanium™ Module Server

Provision is installed and runs as a service on the Module Server host computer. The impact on the Module Server is minimal and depends on usage.

For information about Module Server sizing in a Windows deployment, see Tanium Core Platform Deployment Guide for Windows: Host system sizing guidelines.

Endpoints

Supported Internet protocols

Provision supports only IPv4 addresses.

Supported operating systems

The following endpoint operating systems are supported with Provision.

Operating System	Version	Supported Services
Windows	Windows 10 and later	PXE service and ODJ service
	Windows Server 2016 and later	PXE service and ODJ service
macOS	Same as Tanium Client support. See Tanium Client Management User Guide: Client version and host system requirements.	PXE service
Linux	Same as Tanium Client support. See Tanium Client Management User Guide: Client version and host system requirements.	PXE service

Disk space requirements

Provision requires that the endpoint has at least twice the total size of all OS bundles for the PXE service.

Host and network security requirements

Specific ports and processes are needed to run Provision.

Ports

The following ports are required for Provision communication.

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17518	TCP	
PXE service	PXE service	67, 69, 4011	UDP	macOS and Linux endpoints
		17519	TCP	HTTP cache port - configurable in Provision Settings
		17530	TCP	HTTPS/TLS cache port - configurable in Provision Settings
ODJ service	ODJ service	8100	TCP	

Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.

Security exclusions

If security software is in use in the environment to monitor and block unknown host system processes, Tanium recommends that a security administrator create exclusions to allow the Tanium processes to run without interference. The configuration of these exclusions varies depending on AV software. For a list of all security exclusions to define across Tanium, see Tanium Core Platform Deployment Reference Guide: Host system security exclusions.

Provision security exclusions

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\provision-service\TaniumProvisionService.exe`
		Process	`<Module Server>\services\twsm-v1\twsm.exe`

Provision security exclusions (continued)

Target Device	Notes	Exclusion Type	Exclusion
Windows endpoints		Process	`<Tanium Client>\Python38\TPython.exe`
		Folder	`<Tanium Client>\Python38`
		Process	`<Tanium Client>\Tools\Provision\TaniumODJ.exe`
		Process	`<Tanium Client>\Tools\Provision\TaniumODJ_x86.exe`
		Process	`<Tanium Client>\Tools\Provision\TaniumPXE.exe`
		Folder	`<Tanium Client>\Tools\Provision`
Linux endpoints		Process	`<Tanium Client>/python38/python`
		Folder	`<Tanium Client>/python38`
		Folder	`<Tanium Client>/Tools/Provision`
macOS endpoints		Process	`<Tanium Client>/python38/python`
		Folder	`<Tanium Client>/python38`
		Folder	`<Tanium Client>/Tools/Provision`

User role requirements

The following tables list the role permissions required to use Provision. To review a summary of the predefined roles, see Set up Provision users on page 16.

For more information about role permissions and associated content sets, see Tanium Console User Guide: Managing RBAC.

Provision user role permissions

Permission	Provision Administrator[1]	Provision Read Only User	Provision Service Account[1,2]	Provision Endpoint Configuration Approver[2]
Provision SHOW: View the Provision workbench Read and write access to the Provision module	✓ SHOW READ WRITE	✓ SHOW READ	✓ SHOW READ WRITE	✓ SHOW

Provision user role permissions (continued)

Permission	Provision Administrator[1]	Provision Read Only User	Provision Service Account[1,2]	Provision Endpoint Configuration Approver[2]
Provision Endpoint Configuration Approve Provision items in Endpoint Configuration	✗	✗	✗	✓ APPROVER
Provision Service Account Access to perform service account administration	✗	✗	✓ EXECUTE	✗

[1] This role provides module permissions for Tanium Interact. You can view which Interact permissions are granted to this role in the Tanium Console. For more information, see Tanium Interact User Guide: User role requirements.

[2] This role provides module permissions for Tanium Endpoint Configuration. You can view which Endpoint Configuration permissions are granted to this role in the Tanium Console. For more information, see Tanium Endpoint Configuration User Guide: User role requirements.

Provided Provision administration and platform content permissions

Permission	Permission Type	Provision Administrator	Provision Read Only User	Provision Service Account	Provision Endpoint Configuration Approver
Action Group	Administration	✓ READ WRITE	✓ READ	✓ READ WRITE	✗
Action	Platform Content	✓ READ WRITE	✓ READ	✓ READ WRITE	✗
Action For Saved Question	Platform Content	✓ WRITE	✗	✓ WRITE	✗
Dashboard	Platform Content	✓ READ WRITE	✓ READ	✓ READ WRITE	✗

Provided Provision administration and platform content permissions (continued)

Permission	Permission Type	Provision Administrator	Provision Read Only User	Provision Service Account	Provision Endpoint Configuration Approver
Dashboard Group	Platform Content	READ WRITE	READ	READ WRITE	
Filter Group	Platform Content	READ WRITE	READ	READ WRITE	
Own Action	Platform Content	READ	READ	READ	
Package	Platform Content	READ WRITE	READ	READ WRITE	
Plugin	Platform Content	READ EXECUTE	READ EXECUTE	READ EXECUTE	READ EXECUTE
Saved Question	Platform Content	READ WRITE	READ	READ WRITE	
Sensor	Platform Content	READ WRITE	READ	READ WRITE	

You can view which content sets are granted to any role in the Tanium Console.

Installing Provision

Before you begin

- Contact Tanium Support on page 32 to request the Tanium Provision XML file to install Provision. For more information about how to install a solution with an XML file, see Tanium Console User Guide: Import content files.
- Read the release notes.
- Review the Provision requirements on page 8.
- Assign the correct roles to users for Provision. Review the User role requirements on page 11.
    - To import the Provision solution, you must be assigned the Administrator reserved role or a role that has the **Import Signed Content** permission.
    - To configure the Provision action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group** write permission.

Manage solution dependencies

When you start the Provision workbench for the first time, the Tanium Server checks whether all the Tanium modules and shared services (solutions) that are required for Provision are installed at the required versions. The Provision workbench cannot load unless all required dependencies are installed. If you selected **Tanium Recommended Installation** when you imported Provision, the Tanium Server automatically imported all your licensed solutions at the same time. Otherwise, if you manually imported Provision and did not import all its dependencies, the Tanium Console displays a banner that lists the dependencies and the required versions. See Solution dependencies.

Perform the following steps if a banner indicates any Provision dependencies are not installed:

1. Install the dependencies as described in Tanium Console User Guide: Import, re-import, or update specific solutions.
2. From the Main menu, go to **Modules > Provision** to open the Provision **Overview** page and verify that the Console no longer displays a banner to list missing dependencies.

Verify Provision version

After you import or upgrade Provision, verify that the correct version is installed:

1. Refresh your browser.
2. From the Main menu, go to **Modules > Provision** to open the Provision **Overview** page.
3. To display version information, click Info .

Configuring Provision

If you did not install Provision with the **Apply All Tanium recommended configurations** option, you must configure certain features.

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

Tanium Endpoint Configuration delivers configuration information and required tools for Tanium Solutions to endpoints. Endpoint Configuration consolidates the configuration actions that traditionally accompany additional Tanium functionality and eliminates the potential for timing errors that occur between when a solution configuration is made and the time that configuration reaches an endpoint. Managing configuration in this way greatly reduces the time to install, configure, and use Tanium functionality, and improves the flexibility to target specific configurations to groups of endpoints.

Endpoint Configuration is installed as a part of Tanium Client Management. For more information, see the Tanium Client Management User Guide: Installing Client Management.

Additionally you can use Endpoint Configuration to manage configuration approval. For example, configuration changes are not deployed to endpoints until a user with approval permission approves the configuration changes in Endpoint Configuration. For more information about the roles and permissions that are required to approve configuration changes for Provision, see User role requirements on page 11.

To use Endpoint Configuration to manage approvals, you must enable configuration approvals.

1. From the Main menu, go to **Administration > Shared Services > Endpoint Configuration** to open the Endpoint Configuration **Overview** page.
2. Click Settings and click the **Global** tab.
3. Select **Enable configuration approvals**, and click **Save**.

For more information about Endpoint Configuration, see Tanium Endpoint Configuration User Guide.

If you enabled configuration approvals, the following configuration changes must be approved in Endpoint Configuration before they deploy to PXE endpoints:

- Provision tools
- Provision contract
- Provision manifest

Configure Provision

Configure service account

The service account is a user that runs several background processes for Provision. This user requires the following roles and access:

- **Provision Service Account** role
- If you installed Tanium Client Management, Endpoint Configuration is installed, and by default, configuration changes initiated by the module service account (such as tool deployment) require approval. You can bypass approval for module-generated configuration changes by applying the **Endpoint Configuration Bypass Approval** permission to this role and adding the relevant content sets. For more information, see Tanium Endpoint Configuration User Guide: User role requirements.

For more information about Provision permissions, see User role requirements on page 11.

> NOTE If you imported Provision with default settings, the service account is set to the account that you used to perform the import. Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization.

1. On the Provision **Overview** page, click Settings and then click **Service Account** if needed.
2. Provide a user name and password, and then click **Save**.

Configure Provision action group

By default, the Provision action group is set to the `All Computers` computer group. You can update the action group if needed.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Click **Tanium Provision**.
3. Select the computer groups that you want to include in the action group and click **Save**.
   If you select multiple computer groups, choose an operator (AND or OR) to combine the groups.

Set up Provision users

You can use the following set of predefined user roles to set up Provision users.

To review specific permissions for each role, see User role requirements on page 11.

For more information about assigning user roles, see Tanium Core Platform User Guide: Manage role assignments for a user.

Provision Administrator

Assign the **Provision Administrator** role to users who manage the configuration and deployment of Provision functionality to endpoints.
This role can perform the following tasks:

- Configure Provision service settings.
- View and modify Provision configurations.

Provision Read Only User

Assign the **Provision Read Only User** role to users who need visibility into Provision data.
This role can view Provision service settings and configurations.

Provision Service Account

Assign the **Provision Service Account** role to the account that configures system settings for Provision.
This role can perform several background processes for Provision.

Provision Endpoint Configuration Approver

Assign the **Provision Endpoint Configuration Approver** role to a user who approves or rejects Provision configuration items in Tanium Endpoint Configuration.
This role can perform the following tasks: approve, reject, or dismiss changes that target endpoints where Provision is installed.

Configure PXE settings

1. On the Provision **Overview** page, click Settings and then click **Configuration** if needed.
2. (Windows endpoints) To automatically open the required firewall ports on Windows endpoints, select **Create Local Firewall Rule**.

   IMPORTANT For macOS or Linux endpoints, manually open UDP ports 67, 69, 4011, and the TCP port that is used for caching. The default port for HTTP caching is 17519 and the default port for HTTPS/TLS caching is 17530.
3. (Optional) If you want to enable reporting of DHCP requests and other helpful information for troubleshooting, select **Verbose Logging**.
4. (Optional) If you want to use Tanium Client instead of directly downloading files, select **Use Tanium Client to download content to Tanium PXE**.
5. (Optional) If you want to use a different port for HTTP caching, provide any unused TCP port number in the **HTTP Cache Port** field.
6. (Optional) If you want to use a different port for HTTPS/TLS caching, provide any unused TCP port number in the **HTTPS/TLS Cache Port** field.
7. Click **Save**.

Preparing OS bundle content

Deploying a Windows operating system using Tanium Provision requires some files from the Windows Assessment and Deployment Kit (ADK).

Before you begin

You must obtain the following content before you complete the Provision setup.

- **Windows ADK**: You can download the latest Windows 11 or Windows 10 ADK files from Microsoft Documentation: Download and install the Windows ADK to use with Tanium Provision. Both the Windows ADK and the WinPE add-on must be installed. For the ADK installation, the deployment tools and User State Migration Tool (USMT) components must be installed on any supported Windows endpoint, such as Windows 10, Windows 11, or Windows Server.
- **Windows image file**: You can use the `install.wim` file from the standard Windows media ISOs, or a custom WIM file captured after the OS was sysprepped using Microsoft Deployment Toolkit (MDT). For more information about how to acquire the WIM file from the Windows media, see Microsoft Documentation: Create a Windows 10 reference image.
- **Tanium Client installer package**: Create a client configuration for Windows using Tanium Client Management. For more information, see Tanium Client Management User Guide: Create a client configuration.
- **Drivers for the models of computers that you are deploying**: Each computer model needs different driver packages, which can include INF, catalog, driver, or other files. Copy these drivers and create separate ZIP files for each model, where the file name indicates the model with which the drivers use. For example, `drivers_SurfaceBook.zip`. For more information, see Microsoft Documentation: Components of a Driver Package.
- **Patches**: (Optional) You can specify one or more OS updates or patches to inject into the OS offline, before booting into the OS for the first time.

  Use Tanium Patch to install patches after the endpoint is provisioned to save deployment time in Provision.

Download provided files for Provision

Provision includes two ZIP files that are used to Generate the Windows ADK content on page 19 and Create custom content on page 20 for OS bundles.

1. From the Provision **Overview** page, click Settings and then click **File Downloads**.
2. (Optional) Click **scripts.zip** to download the optional custom content files.

   Download this file only if you need to make modifications to the included Provision scripts.
3. Click **utility.zip** to download the required scripts and related files.

Generate the Windows ADK content

1. Extract the contents of the previously downloaded `utility.zip` file to a folder, such as `C:\Users\Administrator\Documents`.
2. Open an elevated PowerShell command.
   a. Ensure that the execution of scripts is allowed by entering the following command:

   ```
   Set-ExecutionPolicy bypass
   ```

   b. Navigate to the folder that contains the `ADKPrep.ps1` script by entering the following command:

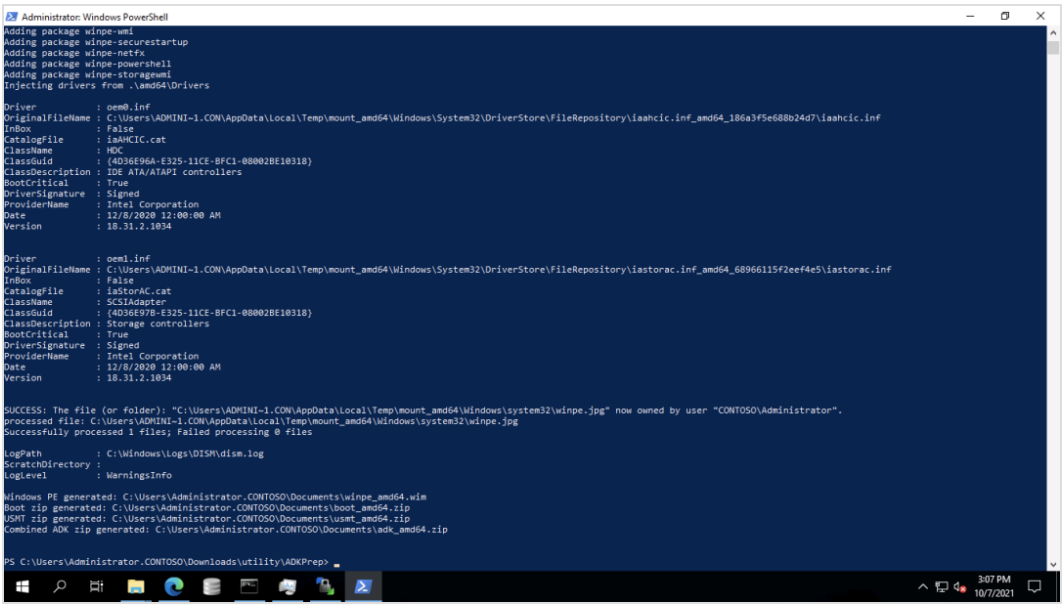
   ```
   cd C:\Users\Administrator\Documents\utility\ADKPrep
   ```

   c. (Optional) If any additional mass storage drivers are required for Windows PE, put them in an architecture-specific folder, such as `C:\Users\Administrator\Documents\utility\ADKPrep\amd64\Drivers`. These files are automatically injected into Windows PE as part of the `ADKPrep.ps1` script execution.

   d. Generate the ADK zip files for the architecture that you need by entering the following command:

   ```
   .\ADKPrep.ps1 -Architecture amd64
   ```

3. Ensure that no errors were generated.



4. Copy the generated `ADK_<architecture>.zip` files to a convenient location that is easy to remember, such as `C:\ProvisionFiles`.

TIP The `utility.zip` file also includes an `Unattend` folder with `unattend_<architecture>.xml` template files that are required to create an OS bundle. You can copy them to `C:\ProvisionFiles` to use in Configure an OS bundle on page 20.

Create custom content

You can create a ZIP file that contains at least a `Customer.ps1` PowerShell script file for any custom content that you want to include. The main Provision scripts download and extract the contents of the ZIP file (if specified in the OS bundle) into the `C:\_t` folder, and then automatically run the `Customer.ps1` PowerShell script, if found.

BEST PRACTICE Do not name your custom ZIP file `scripts.zip`. If your `Customer.ps1` script requires additional files, you can include those files in your custom ZIP file.

IMPORTANT Any files in this custom ZIP file can overwrite any of the standard scripts from Tanium Provision.

Configure an OS bundle

To specify the details of the OS that you want to deploy, create an OS bundle.

1. From the Provision menu, click **OS Bundles**, and then click **Create OS Bundle**.
2. In the **Details** section, provide a name, optional description, and select a **Bundle Architecture**.
3. In the **OS Image File** section, click **Browse for File** to select the `install.wim` file that you previously downloaded in Before you begin on page 18.

   TIP For the default image, select the **Image Index** of **3** for Windows 10 Enterprise.
4. In the **ADK Files** section, click **Browse for File** to select the `ADK_<architecture>.zip` file that you previously generated in Generate the Windows ADK content on page 19.
5. In the **Additional Files** section, add unattend, Tanium Client installation, and script files.
   a. For **Unattended XML File**, click **Browse for File** to select the appropriate `unattend_<architecture>.xml` file that you previously extracted from the `utility.zip` file.
   b. For **Tanium Client Installation Files**, click **Browse for File** to select the ZIP file that you previously downloaded from Tanium Client Management.
   c. (Optional) For **Script and Other Files**, click **Browse for File** to select the custom ZIP file that you previously created in Create custom content on page 20.

6. (Optional) In the **Drivers and Patches** section, add driver and patch files.

   a. For **Driver ZIPS**, click **Browse for File** to select each `drivers_<model>.zip` file that you previously created in Before you begin on page 18.

   > NOTE
   >
   > Driver files are downloaded and used only when they match the following regular expression: `drivers.zip|drivers_%Model%.zip|drivers_%ModelAlias%.zip|drivers_%Version%.zip`
   >
   > where *Model* is the computer model, *ModelAlias* is the first four characters of Lenovo model IDs, and *Version* is generally a descriptive model string, such as `Lenovo ThinkPad X1 Carbon gen 2`.
   >
   > Any spaces in the *Model* or *Version* strings are removed prior to checking against the regular expression.
   >
   > To get the *Model*, *ModelAlias*, and *Version* strings, you can run the following PowerShell commands:
   >
   > **Model**
   >
   > `(Get-ComputerInfo | Select-Object -ExpandProperty CsModel).Replace(" ","")`
   >
   > **ModelAlias**
   >
   > `(Get-ComputerInfo | Select-Object -ExpandProperty CsModel).Substring(0,4)`
   >
   > **Version**
   >
   > `(Get-WmiObject -Class Win32_ComputerSystemProduct| Select-Object -ExpandProperty Version).Replace(" ","")`

   b. For **Patches**, click **Browse for File** to select each .msu file name extension for the patches that you previously gathered in Before you begin on page 18.

7. (Optional) In the **Key Value Entries** section, click **Add Key Value Pair** to add the following key/value pairs.

Key	Description
AdminPassword	The password for the local Administrator account password. If a value is not specified, the password is randomized. NOTE: ***-%serialnumber%*** is automatically appended to the end of the password.
BitLocker	A value to enable BitLocker drive encryption during pre-provisioning, prior to the OS image being applied. If the value `XTS-AES-256` is specified, the encryption level is set to that value before initializing BitLocker encryption on the device. Any other value encrypts the drive using the default XTS-AES-128 encryption. If a value is not specified, BitLocker pre-provisioning is not performed and the drive is unencrypted.
BundleID	The bundle to be selected by default.
BundleTimeout	The number of seconds before the currently-selected bundle is automatically chosen.

Key	Description
ComputerName	The computer name is set to the value that you specify. ComputerName also supports variable substitution, such as `TAN-%RAND:10%` to generate a name with ten random digits, or more complex names like `A-%Manufacturer:3%-%SERIAL%` to generate a name where the first three characters of the manufacturer are inserted with the complete serial number. Do not use this format for virtual machines. If a value is not specified, the computer name is randomly generated.
DomainName	If an ODJService value is specified, specify the domain to join.
Migrate	For an OS refresh, specify `no` to skip the USMT capture/restore.
ODJService	The URL of the ODJ service, such as `https://myServer.myDomain.com:myPort/getblob`. If a value is not specified, domain join is not performed.
OU	If an ODJService value is specified, specify the OU where you want the device to be created, such as `OU=MyComputerOU,DC=myDomain,DC=com`.
Tags	A comma-delimited list of tags to be added to the Tanium Client during the deployment process. If a value is not specified, only an **OSD** tag is added.
Timezone	A Windows time zone string, such as `Eastern Standard Time` to be set on the endpoint.
WaitFor	A path or file to wait for that path or file to exist, such as `C:\Program Files\PuTTY`. Specify `CX` to wait for the Tanium Deploy and Tanium Patch CX files to be installed.

TIP

Specify JSON strings if you want to prompt for values during the deployment process. These JSON strings support simple text input, checkboxes, and dropdown lists.

Examples include:

```
{ "parameterType":
"com.tanium.components.parameters::TextInputParameter", "label":
"Computer Name", "helpString": "Specify the name to assign to the
computer." }
{ "parameterType":
"com.tanium.components.parameters::TextInputParameter", "label":
"Admin Password", "helpString": "Specify the password to be
assigned to the Windows local Administrator account." }
{ "parameterType":
"com.tanium.components.parameters::DropDownParameter", "label":
"Time Zone", "helpString": "Specify the time zone that should be
configured.", "values": ["Eastern Standard Time", "Pacific Standard
```

TIP

```
Time"] }
{ "parameterType":
"com.tanium.components.parameters::CheckBoxParameter", "label":
"Debug" }
```

8. Click **Save**.

NOTE

Depending on connection speeds, uploading this content could take some time. After the upload is complete, it can take several more minutes before the OS bundle is available to use.

Clone an OS bundle

To make a copy of an existing OS bundle, select an OS bundle and click Clone Selected  . `Clone:` is automatically prepended to the OS bundle name, but you can make any changes before you click **Save**.

Setting up offline domain join

If you want your Windows endpoints to join an AD domain, you can use Tanium Provision to set up an ODJ process instead of updating `unattend.xml` answer files with clear text passwords that contain the domain join credentials.

Before you begin

- Make sure that you create a firewall rule to allow inbound connections to the port that is specified in the `<Tanium Client>\Tools\Provision\settings.yml` file. The default port is 8100.
- The computer account for the TaniumODJ service must be granted rights to create computer accounts in any organizational unit that is provided to it, using AD Users and Computers.
- For endpoints that are imaged with Provision to successfully complete the ODJ process, you must configure the `ODJService` and `DomainName` variables in Configure an OS bundle on page 20. If the `ComputerName` value is blank, then the current computer name, which is typically randomly generated, is used. If the OU is not specified, then the default OU that is configured in AD is used.

Install the TaniumODJ service

To set up the ODJ process, you must deploy the **Tanium Provision - Offline Join Deployment** package to at least one computer.

1. In Interact, target the endpoint on which you want to install the TaniumODJ service.
2. Click **Deploy Action** and select the **Tanium Provision - Offline Join Deployment** package.
3. (Optional) Customize the port, duration, passcode, or max blobs settings.
4. In the **Targeting Criteria** section, click **Show Preview to Continue** and then click **Deploy Action**.

For example, if you deploy the ODJ service to an endpoint that is named `myServer.myDomain.com`, then the ODJ URL is `https://myServer.myDomain.com:myPort/getblob`.

(Optional) Add certificates and group policy templates

ODJ blobs can optionally contain additional certificates and group policy templates by adding parameters in the `settings.yml` file. In the following example, the **DirectAccess Client Settings** and **Default Domain Policy** group policy settings, the root certificates that are configured in AD, and the computer-specific certificate that was generated using the **orgComputer** AD Certificate Services template are included, with the service listening on port 8100:

```
PolicyNames:
 - DirectAccess Client Settings
 - Default Domain Policy
IncludeRootCerts: yes
CertTemplate: orgComputer
Port: 8100
```

Troubleshoot the ODJ process

Issue

If the computer account already exists for the specified computer name, the ODJ blob creation fails because the service does not specify to overwrite the existing computer object in AD.

Solution

Make sure that the computer account does not already exist.

This issue is less likely to occur because Provision appends a numeric suffix to the computer name if needed. For example, if you specify `myComputer` for the computer name, Provision tries **myComputer** first. If **myComputer** already exists, Provision tries **myComputer-1**, and continues to increase the suffix if that account already exists.

Provisioning endpoints

Deploy the Tanium PXE service

You can deploy the Tanium PXE service to one or more endpoints. These endpoints can be running Windows, Windows Server, macOS, or Linux.

1. From the Provision menu, click **PXE Endpoints**, and then click **Add PXE Endpoints**.
2. Search for the endpoint by IP address or computer name, select the endpoint, and click **Add PXE Endpoints**.

The required service and related files are deployed automatically using Tanium Endpoint Configuration.

This process can take several minutes. The **PXE Server Endpoints** page is updated when the process is complete.

After you create and deploy a PXE profile, you can boot endpoints on that network segment from a PXE network. The deployed Tanium PXE service detects the PXE boot request and responds with the required information.

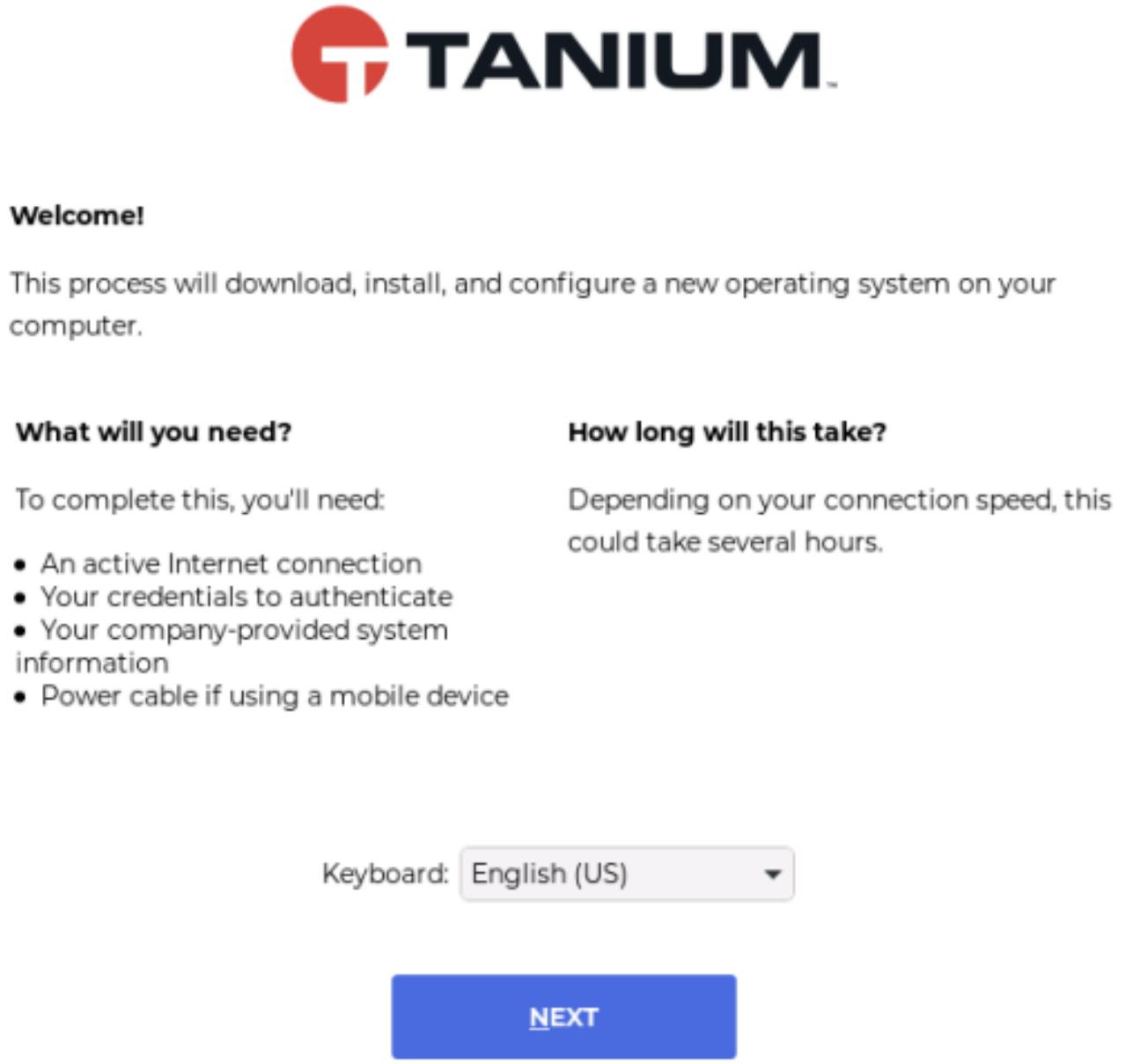
If you have more than one PXE server in the same local network, the first PXE server to respond to the PXE boot request might not be the expected Tanium PXE service. For more information, see Error: PXE boot does not boot to the Tanium PXE service on page 31.

Initiate PXE network boot

To initiate the PXE network boot process, select one or more keys during the device power-on sequence, which vary by manufacturer. For example, on a Lenovo device, you must select the **Enter** key and then **F12** to get to a boot menu where you can choose the PXE boot (IPv4) option.

After a PXE response is sent, a Grand Unified Bootloader (GRUB) loader screen displays for a few seconds before the Linux boot environment is downloaded and boots. After it initializes, the deployment wizard prompts you to begin the provisioning process.

Deployment wizard



Create bootable USB media for deployments

To create bootable USB media for Unified Extensible Firmware Interface (UEFI) devices, use the `USBKey.ps1` script that you previously extracted from the `utility.zip` file in Download provided files for Provision on page 18.

IMPORTANT Make sure that your USB media is at least 1 GB in size, but less than 32 GB.

1. Open an elevated command prompt.
2. Choose which option you want to run the `USBKey.ps1` script:
   - If you want to get the USB content from the Tanium PXE server at the specified IP address and write that content to the USB key at the specified drive, run the script with two parameters. For example:

     ```
     .\USBKey.ps1 -TPXEHost 10.1.2.3 -Destination D:
     ```

   - If you want to get the USB content from the Tanium PXE server at the specified IP address and write that content to the ISO at the specified drive, run the script with two parameters and specify the ISO file name. For example:

     ```
     .\USBKey.ps1 -TPXEHost 10.1.2.3 -Destination C:\Media.iso
     ```

   - If you want to get the USB content from the Tanium PXE server at the specified IP address, but configure the USB key to pull the content from an alternate IP address during the boot process, run the script with three parameters. For example:

     ```
     .\USBKey.ps1 -TPXEHost 10.1.2.3 -AnchorHost 10.1.5.1 -Destination D:
     ```

3. The script reformats and labels the USB key with a default label of PROVISION and then downloads the required boot files from the specified PXE server. After the script finishes, eject the USB device and use it to boot a physical device.

To boot the device from USB media, you must select one or more keys during the device power-on sequence, which varies by manufacturer. For example, on a Lenovo device, you must select the **Enter** key and then **F12** to get to a boot menu where you can choose the USB key.

Refresh an existing operating system

To refresh an existing operating system, including user state migration, you can target the corresponding Tanium package that is created when you created the OS bundle.

1. If needed, Configure an OS bundle on page 20.
2. From the main menu, go to **Administration > Content > Packages** and filter the list to search for `Tanium Provision`.
3. Select the package that corresponds to the OS bundle that you created and click **Deploy Action**.

   When you create an OS bundle, a corresponding Tanium package is created. The package is named **Tanium Provision - *<OS bundle name>* - *<time stamp>* [*<bundle architecture>*]**. For example, if you created an OS bundle named `Windows 10` for the x64 bundle architecture, the corresponding Tanium package is named **Tanium Provision - Windows 10 - yyyy-MM-dd'T'HH:mm:ss'Z' [Windows x64]**.

4. In the **Targeting Criteria** section, choose the targeting criteria: computer groups, manual list, or filter question.
5. Click **Show Preview To Continue**, review the list of targeted endpoints, and then click **Deploy Action**.

You can also use Interact to find an endpoint to deploy the corresponding Tanium package.

Monitor a deployment

You can monitor deployments with the **Tanium Provision - Deployment Progress** sensor.

Monitor in-progress deployments from the Tanium PXE server

To monitor in-progress deployments and deployments that completed in the last 48 hours, ask the following question in Interact:

```
Get Tanium Provision - Deployment Progress?maxAge=50 from all machines with
Tanium Provision - Deployment Progress:Source equals Tanium PXE
```

View historical deployment information from deployed clients

To see historical information on clients that were deployed by Provision, ask the following question in Interact:

```
Get Tanium Provision - Deployment Progress?maxAge=50 from all machines with
Tanium Provision - Deployment Progress:Source equals Client
```

Remove the PXE service from endpoints

1. From the Provision menu, click **PXE Endpoints**.
2. Select one or more endpoints and then click **Remove PXE Endpoints**.

Troubleshooting Provision

If Provision is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

The information is saved as a ZIP file that you can download with your browser.

1. From the Provision **Overview** page, click Help  .
2. Click **Download Support Bundle**.
   A `tanium-provision-support-<timestamp>.zip` file downloads to the local download directory.
3. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 32.

Tanium Provision maintains logging information in the `provision.log` file in the `\Program Files\Tanium\Tanium Module Server\services\provision-files\logs` directory.

Review endpoint logs

If you have issues during the endpoint provisioning process, you can review the following logs to troubleshoot possible causes.

Linux PXE and ODJ endpoints

```
/opt/Tanium/TaniumClient/Tools/Provision/logs
```

macOS PXE and ODJ endpoints

```
/Library/Tanium/TaniumClient/Tools/Provision/logs
```

Windows PXE and ODJ endpoints

```
<Tanium Client>\Tools\Provision\logs
```

Imaging logs

```
C:\_t\logs\Provision-OS.log
```

```
C:\Windows\temp\logs
```

The `C:\_t\logs` folder is created only if the imaging process did not complete successfully during provisioning. After successful OS imaging, the logs are copied to the `temp` folder and the `C:\_t` contents are deleted.

PXE Linux environment

`/tmp`

Error: PXE boot does not boot to the Tanium PXE service

Issue

When multiple PXE servers exist in the local network, the PXE boot request accepts the response from whichever PXE server responds first. If the PXE boot request does not boot to the Tanium PXE service, it is likely that a different PXE server responded before a Tanium PXE service did.

Solution

Check with your network team to determine if any PXE servers are configured in DHCP (scope options 66 and 67).

Error: Provisioning process incomplete

Issue

The provisioning process does not appear to be complete and **Other User** cannot sign in.

Solution

You must use non-OEM product keys, except on Enterprise editions and Windows Server operating systems.

Error: Provision-pe.ps1 cannot be found

Issue

The system is missing the storage drivers.

Solution

Update PE.

1. Download the Dell Windows PE driver pack CAB file from Dell Technologies: WinPE 10 driver pack.
2. Extract the contents of the file into a folder.
3. Copy the contents of `\winpe\x64\storage\HHN7T_A00-00\F6\NonVMD\f6flpy-x64` (Intel Rapid Storage Technology Driver) into the `C:\Users\Administrator\Documents\utility\ADKPrep\amd64\drivers` folder.

   The **HHN7T** part of the folder name could change if the driver is updated.

4. To create a new `adk_amd64.zip` file in the `/Documents` folder, run the `ADKPrep.ps1` script in an elevated command prompt.
5. From the Provision **OS Bundles** page, update any existing OS bundles to use the new `adk_amd64.zip` file.

   Wait for the status of the OS bundles to change from **Updating** to **Ready**.
6. When the Dell logo appears in the PXE endpoint, select the **F12** key and then select **ONBOARD NIC (IPV4)**.

Contact Tanium Support

To contact Tanium Support for help, sign in to https://support.tanium.com.