Acronis

Acronis Snap Deploy 6

User Guide

Table of contents

Copyright statement

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

Introducing Acronis Snap Deploy 6

Overview

What is Acronis Snap Deploy 6

Acronis Snap Deploy 6 is a flexible, efficient software solution for deployment of a fully configured operating system (with or without application software and any other data) to multiple machines. Because the product uses disk imaging technology, it is ideal for rapid bare-metal installations and flexible centralized provisioning.

Who needs Acronis Snap Deploy 6

Acronis Snap Deploy 6 is primarily designed to be used by:

- Small and medium-size businesses:
  - IT service providers
  - Hardware retailers
- IT departments of larger corporations
- Schools and universities
- R&D and software testing labs

The enterprise features of Acronis Snap Deploy 6 (scheduled deployment, support for Preinstallation Environment, command-line interface, and scripting, to name a few) can help automate the tasks of the IT department in large enterprise environments.

Acronis Snap Deploy 6 infrastructure

Components of the Acronis infrastructure are installed on Windows machines. Managing the Acronis infrastructure is performed by using Management Console.

A reference image, called the master image, can be taken in Windows, in the Acronis environment, or in Windows Preinstallation Environment (WinPE) that contains components of Acronis Snap Deploy 6.

Deployment is performed in the Acronis environment or in WinPE that contains components of Acronis Snap Deploy 6. In either environment, Acronis Snap Deploy 6 provides the graphical user interface (GUI). In addition, command-line mode and scripting are supported in WinPE.

A dedicated bootable utility enables fully-functional deployment with GUI on a stand-alone machine (a machine that is isolated from the network or is included in a network without Acronis Snap Deploy 6 infrastructure).

What's new in Update 1

- Deployment via "Session ID".
- Multiple deployment sessions per deploy server.
- Deployment from TIBX format.
- Support for Windows 11 and Windows Server 2022.

What's new in Acronis Snap Deploy 6

- Architectural improvements: 64-bit and compatibility with Acronis Cyber Protect/Acronis Cyber Protect Cloud
- Windows activation key in individual deployment settings
- Preserve original machine name after deployment
- Correct licensing assignment for machines deployed through docking station, which share the same MAC
- VLAN tags support in bootable media
- Deploy from VHDX format
- UX enhancements: Sort by machine name, IP, MAC address, Last deployment finish time
- Deployment over Wi-Fi networks

What you can do with Acronis Snap Deploy 6

This section describes typical usage scenarios for Acronis Snap Deploy 6.

Taking an image of the master system

First, you create the desired system configuration and save the image of the system hard disk to a network folder, detachable media (such as a USB hard drive) or removable media (such as a DVD). An image, also called a master image, is a file that contains the system in a packaged form.

Scenarios

Scenario 1

Each department in your organization, such as accounting, sales, and technical support, uses a fixed set of applications for daily work.

You create a library of master images. For example, you create one image for each department. You then deploy these images to new hardware without having to manually configure the operating system and applications.

Scenario 2

You might need to deploy the standard configuration, which is included in the image library, to various hardware.

Acronis Universal Deploy configures Windows or Linux so that the system is able to boot on dissimilar hardware.

Deployment to specific machines (immediate, manual, and scheduled deployment)

You can perform deployment to a specific list of machines with known physical addresses (called MAC addresses). The deployment can run immediately after you set it up, on a schedule, or when you start it manually.

These ways of deployment are also known as manual deployment and scheduled deployment.

When the deployment is about to start, the software will turn on the target machines with predefined MAC addresses by using the BIOS Wake-on-LAN (WOL) functionality.

Machines in another subnet can be woken up through a component called Wake-on-LAN Proxy, which is delivered with Acronis Snap Deploy 6. The machines typically boot into the PXE server that is installed in the same subnet.

Machines that do not support Wake-on-LAN can be booted into the bootable environment manually before the deployment starts. Such machines will also be deployed, provided that they are listed for deployment.

Machines that are always turned on before the deployment starts can be configured to reboot automatically into the bootable environment. This feature is called online deployment.

Scenarios

Scenario 1. An organization receives a shipment of machines from a manufacturer along with the list of their MAC addresses. The IT department has to deploy the operating system to the new hardware.

Scenario 2. An Internet cafe, school or university lab has 100 machines with known MAC addresses. The nightly deployment of the initial standard image on these machines is needed.

Deployment to any ready machines (event-driven deployment)

You can set up deployment to start when a specific number of any machines become ready. Unlike deployment to specific machines, this way of deployment does not require knowing the MAC addresses of the machines.

The software counts how many machines have connected to the deployment server and starts deployment when the number of machines you specified (for example, 10) is connected.

This way of deployment is also called event-driven deployment or deployment upon an event.

You can specify a time-out period. After the time-out, deployment will start on the machines that are ready despite the fact that the predefined number is not reached.

Scenario

Your organization receives 100 machines from a manufacturer. You want to deploy the operating system and programs to all these machines at once.

1. You set up a deployment operation that waits until any 100 machines are ready.
2. You boot each machine into the Acronis environment, by using either Acronis bootable media or Acronis PXE (Preboot Execution Environment) Server.
3. Acronis Snap Deploy 6 uses multicasting to perform the deployment to all machines at once.

Stand-alone deployment

The administrator might need to perform deployment to a machine that is isolated from a network or is included in a network without an Acronis Snap Deploy 6 infrastructure (such as the deployment server or the license server). A dedicated bootable utility enables a fully-functional deployment with the graphical user interface on a stand-alone machine.

The master image for deployment can be located in a network folder or on a removable drive (such as a DVD) on the machine you are performing deployment to. The image cannot be located on the local hard disk of the machine, because deployment usually involves overwriting the contents of the disk.

Deployment with individual deployment settings

You can set up individual deployment settings for a machine. These settings will override the general settings of the deployment operation (the deployment template).

Scenarios

Scenario 1

You want to perform deployment to several machines. For each machine, you want to assign a specific name, rather than an automatically-generated name.

1. You enter the MAC addresses of the machines so that they all appear in the list of machines.
2. You select each machine in the list and specify an individual setting: the machine name.
3. You set up a deployment operation. Other deployment settings will be the same for all machines.

Scenario 2

You want to perform deployment to a big number of machines. For one of those machines, however, you need to perform deployment to the second hard disk, rather than to the first hard disk.

1. You enter the MAC addresses of all machines so that all machines appear in the list of machines.
2. You specify an individual setting for the corresponding machine: to deploy to the second hard disk.
3. You set up a deployment operation to perform deployment to the first hard disk. Deployment to that specific machine will be performed to the second hard disk.

User-initiated deployment (custom deployment)

Acronis Snap Deploy 6 can be configured in such a way that users will be able to deploy and re-deploy their machines with one click on the boot menu.

This way of deployment is also called custom deployment.

Scenarios

Scenario 1

Software testers have to deploy clean operating systems or preconfigured systems on test machines.

A test team leader creates a custom bootable media or a PXE package that provides a fixed set of choices on the target side. A test team member reboots a test machine and selects what to deploy from the boot menu with one click. The deployment starts immediately. The choices can be various operating systems, various editions of the same operating system, the same operating system with various settings or various applications, to name a few. The deployment proceeds independently on each machine.

Scenario 2

In a university or school lab, switching between exercises requires reconfiguring the machine entirely. Students can switch or restart exercises without the teacher's assistance. If a student messes up the machine (for example, deletes a file or changes configuration), the student can choose a self-restore option from the boot menu.

Deployment of a disk volume and MBR

You do not necessarily have to deploy the entire disk. Provided that the master and the target disks have a similar partitioning scheme, you can image and deploy only the system volume or only the data, depending on your needs.

When deploying a system volume, Acronis Snap Deploy 6 will automatically repair the bootability of the deployed system.

Command-line mode and scripting under WinPE

Acronis Snap Deploy 6 provides a command-line utility that can be added to a bootable media based on Windows Preinstallation Environment (WinPE). The administrator can create such media on a physical drive or place it to the PXE server.

Having booted a machine into Windows Preinstallation Environment, the administrator can perform imaging or deployment in the command-line mode or execute scripts.

Scenarios

Scenario 1

The administrator needs to deploy a different image to each machine on the network.

The administrator writes a deployment script that can read the target machine's MAC address (for example, 01-02-03-04-05-06) and pull an image whose name matches the MAC address (for example, image-01-02-03-04-05-06.tib) The image can be located in any convenient location, such as a network share.

The administrator then runs the script on any number of target machines to deploy the corresponding image to each of them.

Scenario 2

The administrator needs to start imaging or deployment automatically each time a machine boots from the PXE server.

The administrator creates an imaging or deployment script, adds the script to the PE and includes the script in the **startnet.cmd** file. On booting into the PE, the operation will be performed automatically.

Scenario 3

The administrator needs to automatically execute pre-deployment operations (disk partitioning, for example) on the machines on the network.

The administrator creates a script that performs pre-deployment operations, adds the script along with deployment script to the PE and includes both scripts in the **startnet.cmd** file. On booting into the PE, both operations will be performed automatically.

Features of Acronis Snap Deploy 6

List of machines

Acronis Snap Deploy 6 provides the **Machines** view. This view contains a list of all machines that you added for deployment or that have ever been deployed.

In this view, you can:

- View and edit the list of machines.
- Check which machines are ready for deployment.
- Examine the current state of the deployment operation, and the result of the last deployment.
- Add machines for subsequent deployment by specifying the machines' MAC addresses.
- Specify individual deployment settings.

- Set up deployment for one or more machines.
- Organize machines into groups.

List of deployment tasks

Centralized deployment is performed by a deployment task. Acronis Snap Deploy 6 provides a list of deployment tasks in the **Deployment tasks** view.

In this view, you can:

- View and edit the list of tasks, including scheduled tasks and tasks that perform deployment when a specified number of machines are ready.
- Edit tasks; for example, to change the list of machines to perform deployment to.
- Start any task manually; for example, to perform deployment outside the normal schedule.
- Examine the current state of the task and the result of the last run of the task.

Per-deployment licensing

In addition to per-machine licensing, Acronis Snap Deploy 6 supports per-deployment licensing.

A deployment license enables you a single successful deployment to a particular machine. A machine license enables you an unlimited number of deployments to a particular machine.

For more details, see "Licensing policy".

Scenario

You provision machines to end users by deploying the operating system with the necessary software to a machine and then shipping the machine to the end user. Because you are planning to perform deployment to each machine only once, you want a cheaper license for the machine.

You buy a number of deployment licenses based on the number of machines that you want to provision. A deployment license becomes used only if the deployment to the corresponding machine has been successful.

Support for the VHD and VHDX format

In addition to using its own format for an image, Acronis Snap Deploy 6 can perform deployment from Virtual Hard Disk files: VHD files created in Windows 7 and Windows Server 2008, and VHDX files created in Windows 8 or later. Such files can store the contents of one or more disks.

Scenario

You saved the disks of one of your machines to a VHD or VHDX file by using the Windows Backup program. Now you want to deploy that machine to other machines.

When setting up the deployment, you specify the VHD or VHDX file as you would specify an image file created by Acronis Snap Deploy 6. When performing the deployment, the software can change the settings for the machines being deployed.

Graphical user interface in WinPE

A bootable media based on Windows Preinstallation Environment (WinPE) now provides a graphical user interface (GUI) similar to that in an Acronis bootable media.

By using the GUI, you can take a master image and perform deployment.

You may want to use a WinPE-based media if the Acronis media cannot recognize a specific device, such as an exotic storage device.

A WinPE-based bootable media also provides a command-line utility for performing imaging and deployment.

E-mail notifications about deployment

When using the command-line mode, you can set up e-mail notifications about the result of each deployment operation.

Scenario

In Scenario 1 or Scenario 2 described in "Command-line mode and scripting under WinPE", the administrator also wants to receive e-mail notifications about deployment.

The administrator includes in the deployment script a command that sets up the parameters of the e-mail notifications, such as the administrator's e-mail address and the parameters of the mail server.

An e-mail notification is sent after each deployment command. Each notification contains the MAC address and IP address of the corresponding machine and whether the deployment has been successful.

Compatibility with images created by other Acronis products

As a master image, Acronis Snap Deploy 6 can use a disk-level backup created by the following products:

- Acronis True Image
- Acronis Backup & Recovery 10
- Acronis Backup & Recovery 11
- Acronis Backup 11.5
- Acronis Backup 11.7

Support for multiple network adapters

A machine license is bound to the machine's network adapter (also known as network interface card, NIC).

If the machine has more than one network adapter, Acronis Snap Deploy 6 ensures that only one license is assigned to the machine. No extra license will be consumed if you add or remove a network adapter.

To make sure that only one license is assigned to the machine, do not remove all network adapters at once.

When using the Wake-on-LAN functionality for the machine, the software sends a special packet, called the magic packet, to all network adapters of the machine.

Multicast TTL and network bandwidth throttling

Deployment configuration has a parameter that specifies time to live (TTL) for multicast packets. By using this setting, you can limit the distribution of multicast packets via gateways.

By setting the permitted bandwidth, you can limit the network usage during deployment.

Encrypted communication

Components of Acronis Snap Deploy 6 communicate to each other by using the Secure Sockets Layer (SSL) cryptographic protocol. Encryption starts on the first (earliest) stage of the connection attempt, so all data transferred in the next steps (including data required for client authentication) is encrypted.

After the components of Acronis Snap Deploy 6 are installed, encrypted communication between the components is enabled automatically.

The contents of the master image are transferred unencrypted.

Password protection

Master images taken with Acronis Snap Deploy 6 can be protected with a password to prevent unauthorized deployment.

Acronis Snap Deploy 6 also supports password-protected backups created by Acronis True Image, Acronis Backup & Recovery 10, Acronis Backup & Recovery 11, Acronis Backup 11.5, or Acronis Backup 11.7.

To prevent Acronis bootable components from unauthorized execution, the bootable components in the Acronis boot menu can also be protected with a password. The user will be asked for the password when selecting a bootable component. No password is required to start the operating system on the machine.

Online deployment

You can configure Acronis Snap Deploy 6 to automatically make turned-on target machines (running Windows) ready for deployment every time the deployment starts. Thereby, manual rebooting of the target machines into the bootable environment is not required.

Supported operating systems for imaging and deployment

Acronis Snap Deploy 6 provides full-featured imaging and deployment of the operating systems listed in the table that follows.

For most operating systems, you can change settings such as the network name that the machines will have after the deployment.

Deploying an operating system requires a license. Depending on the type of an operating system, you need a server license or a workstation license. For details about licensing, see "Licensing policy".

Operating system	Imaging and deployment	Changing settings	License type
Windows Server 2022	Yes	Yes	Server
Windows Server 2019 - any edition, including IoT, LTSC (formerly LTSB)	Yes	Yes	Server
Windows Server 2016 (any edition)	Yes	Yes	Server
Windows Server 2012 Foundation	Yes	Yes	Server
Windows Server 2012 R2 Foundation	Yes	Yes	Server
Windows Server 2012 Essentials	Yes	Yes	Server
Windows Server 2012 R2 Essentials	Yes	Yes	Server
Windows Server 2012 Standard	Yes	Yes	Server
Windows Server 2012 R2 Standard	Yes	Yes	Server
Windows Server 2012 Datacenter	Yes	Yes	Server
Windows Server 2012 R2 Datacenter	Yes	Yes	Server
Windows Server 2008 R2 (No Service Pack or Service Pack 1)	Yes	Yes	Server
Windows Server 2008 (x86, x64) (No Service Pack, Service Pack 1, or Service Pack 2)	Yes	Yes	Server
Windows Server 2003 (x86, x64) (No Service Pack, Service Pack 1, or Service Pack 2)	Yes	Yes	Server
Windows Server 2003 R2 (x86, x64) (No Service Pack, Service Pack 1, or Service Pack 2)	Yes	Yes	Server
Windows Small Business Server 2011 (No Service Pack)	Yes	Yes	Server

Windows Small Business Server 2008	Yes	Yes	Server
Windows Small Business Server 2003 (No Service Pack, Service Pack 1, or Service Pack 2)	Yes	Yes	Server
Windows Storage Server 2003 R2 (No Service Pack, Service Pack 1, or Service Pack 2)	Yes	Yes	Server
Windows Server 2003 x64 Edition (No Service Pack, Service Pack 1, or Service Pack 2)	Yes	Yes	Server
Windows 11 Home	Yes	Yes	Workstation
Windows 11 Pro	Yes	Yes	Workstation
Windows 11 Enterprise	Yes	Yes	Workstation
Windows 10 Home (x86, x64)	Yes	Yes	Workstation
Windows 10 Pro (x86, x64)	Yes	Yes	Workstation
Windows 10 Enterprise (x86, x64)	Yes	Yes	Workstation
Windows 10 Education (x86, x64)	Yes	Yes	Workstation
Windows 8 (x86, x64)	Yes	Yes	Workstation
Windows 8.1 (x86, x64) (including Update 1)	Yes	Yes	Workstation
Windows 8 Pro (x86, x64)	Yes	Yes	Workstation
Windows 8.1 Pro (x86, x64) (including Update 1)	Yes	Yes	Workstation
Windows 8 Enterprise (x86, x64)	Yes	Yes	Workstation
Windows 8.1 Enterprise (x86, x64) (including Update 1)	Yes	Yes	Workstation
Windows 7 Home Basic (x86, x64) (No Service Pack or Service Pack 1)	Yes	Yes	Workstation
Windows 7 Home Premium (x86, x64) (No Service Pack or Service Pack 1)	Yes	Yes	Workstation
Windows 7 Professional (x86, x64) (No Service Pack or Service Pack 1)	Yes	Yes	Workstation
Windows 7 Ultimate (x86, x64) (No Service Pack or Service Pack 1)	Yes	Yes	Workstation
Windows Vista Home Basic (x86, x64) (No Service Pack, Service Pack 1, or Service Pack 2)	Yes	Yes	Workstation
Windows Vista Home Premium (x86, x64) (No Service Pack, Service Pack 1, or Service Pack 2)	Yes	Yes	Workstation

Windows Vista Business (x86, x64) (No Service Pack, Service Pack 1, or Service Pack 2)	*Yes*	*Yes*	*Workstation*
Windows Vista Ultimate (x86, x64) (No Service Pack, Service Pack 1, or Service Pack 2)	*Yes*	*Yes*	*Workstation*
Windows XP Home (Any Service Pack or no Service Pack)	*Yes*	*Yes*	*Workstation*
Windows XP Professional (No Service Pack, Service Pack 1, Service Pack 2, or Service Pack 3)	*Yes*	*Yes*	*Workstation*
Windows XP Professional x64 Edition (No Service Pack, Service Pack 1, or Service Pack 2)	*Yes*	*Yes*	*Workstation*
Windows 2000 Server (Any Service Pack or no Service Pack)	*Yes*	*No*	*Server*
Windows 2000 Advanced Server (Any Service Pack or no Service Pack)	*Yes*	*No*	*Server*
Windows 2000 Professional (Any Service Pack or no Service Pack)	*Yes*	*No*	*Workstation*
Windows NT/4.0 Server	*Yes*	*No*	*Server*
Windows 98/Me	*Yes*	*No*	*Workstation*
Linux (kernel 2.4.9 and later)	*Yes*	*No*	*Workstation*

Acronis Snap Deploy 6 enables imaging and deployment of any PC-based operating system. However, for certain operating systems, some operations or options will not be available. For example, Windows 98/NT/ME, NT/4.0 Server, Windows 2000, and Linux (kernel 2.4.9 and later) can be deployed only as is; on-the-fly settings adjustment is not performed.

Deploying an unrecognized operating system or a disk without an operating system requires a *workstation* license.

Acronis Universal Deploy is not applicable to the Windows 2000, Windows 98/NT/ME, and Windows NT/4.0 Server operating systems.

Licensing policy

Acronis Snap Deploy 6 licensing is based on the number of machines (servers or workstations) that you deploy. For example, to deploy a system on 100 machines, you need 100 licenses.

Subscription licenses

Subscription licenses are always machine license types, with support for both Server and Workstation editions.

The subscription period start date is encoded in the serial number (key) provided along with the purchase, and it matches the date when the serial number is generated by Acronis.

Since the serial numbers may be pre-generated, Acronis provides a period of up to 30 days of additional usage with each subscription key to compensate for this potential gap between the dates. In this way, we ensure that the product can be used for no less than the defined subscription period.

Example scenario

You purchase a 1-year subscription license from a partner on the 10th of January.

A few days later (on the 12th of January, for the purpose of this example), you get a newly-generated license key.

When you register your license key in Acronis Account (https://account.acronis.com) and/or you add the license in Acronis Snap Deploy license management interface, the subscription period starts from the key generation date, and it will last for the period defined in the license (1 year, for this example) plus 30 days.

Your subscription, therefore, would start on the 12th of January and would last until the 12th of February of the following year (1 year + 30 days).

Machine licenses and deployment licenses

In terms of the number of allowed deployments, a license can be one of two types:

- **A machine license** enables an **unlimited number of deployments** to a particular machine. You may want to use this type of license if you perform deployment to the same machine on a regular basis.
- **A deployment license** enables a **single successful deployment** to a machine. You may want to use this type of license if you perform deployment to the same machine once or infrequently. If deployment under a deployment license fails, you can perform another deployment under the same license.

You can obtain a license key that corresponds to a number of deployment licenses.

When setting up a deployment operation, you can choose whether a deployment license can be automatically used instead of a machine license, or conversely.

Server licenses and workstation licenses

In terms of the operating system you can deploy, a license can be one of two types:

- **A server license** enables deploying a server operating system.
- **A workstation license** enables deploying a workstation operating system. A workstation license is needed to deploy a disk or volume that does not contain an operating system, if the target machine has not been assigned a machine license before.

Linux is considered as a workstation operating system. See also the complete list of supported server and workstation operating systems.

If Acronis Snap Deploy 6 fails to identify the type of operating system, the operating system is considered as a workstation operating system.

When setting up a deployment operation, you can choose whether a server license can be automatically used instead of a workstation license for deploying a workstation operating system.

Trial version of Acronis Snap Deploy 6

The Acronis Snap Deploy 6 trial version has all the functionality of the full version.

To use the trial version, you need to obtain a trial license. You can obtain a server or workstation trial license.

A trial license enables you an unlimited number of deployments on up to five machines for 30 days.

To upgrade from the trial to full version you do not need to re-download the software. Simply buy the full licenses and import them to the license server. Acronis Snap Deploy 6 will start using a full license as soon as the corresponding trial license expires.

Upgrading to Acronis Snap Deploy 6

To upgrade from Acronis Snap Deploy 5 to Acronis Snap Deploy 6, upgrade both the licenses and the software components.

Upgrading licenses

To upgrade the licenses of Acronis Snap Deploy 5, obtain the necessary number of upgrade licenses and import them to the license server.

You should obtain one upgrade license for Acronis Snap Deploy 6 per each license for Acronis Snap Deploy 5 that you have. After you import the upgrade licenses to the license server, you will be able to perform deployment to any machine by using Acronis Snap Deploy 6.

It does not matter whether the ASD5 license is itself an upgrade license for an even earlier version.

The following table illustrates how the various combinations of licenses will be upgraded. Use this table to calculate the number of upgrade licenses that you need.

You have	You obtain and import	You now can
Acronis Snap Deploy 5 full license *Available*	Acronis Snap Deploy 6 upgrade license	Perform deployment to any target machine
Acronis Snap Deploy 5 full license	Acronis Snap Deploy 6 upgrade license	Perform deployment to Machine1

Assigned to Machine1		
Acronis Snap Deploy 5 upgrade license License(s) for an earlier version *Available*	Acronis Snap Deploy 6 upgrade license	Perform deployment to any target machine
Acronis Snap Deploy 5 upgrade license License(s) for an earlier version *Assigned to Machine1*	Acronis Snap Deploy 6 upgrade license	Perform deployment to Machine1
No license	Acronis Snap Deploy 6 full license	Perform deployment to any target machine

Upgrading components

Upgrade from Acronis Snap Deploy 5 is not possible with the default 64-bit installer of Acronis Snap Deploy 6. Uninstall Acronis Snap Deploy 5 first. For more details, refer to https://kb.acronis.com/content/68468.

Technical Support

Maintenance and Support Program

If you need assistance with your Acronis product, please go to https://www.acronis.com/support/

Product Updates

You can download the latest updates for all your registered Acronis software products from our website at any time after logging into your **Account** (https://account.acronis.com/) and registering the product. See **Registering Acronis Products at the Website** (https://kb.acronis.com/content/4834) and **Acronis Website User Guide** (https://kb.acronis.com/content/8128).

Understanding Acronis Snap Deploy 6

This section describes the components of the Acronis Snap Deploy 6 infrastructure and their interaction.

Terminology

The following table lists the common terms and descriptions used in this document.

Master system	The system to be deployed.
Master image (Image)	A file that contains the master system in a packaged form. The file has the .tib extension.
Online imaging	Taking a master image while the master system is in a production state (the operating system is running on the master machine).
Offline imaging	Taking an image while the master machine is booted into the Acronis environment or Windows Preinstallation Environment.
Deployment	Transferring the operating system, applications, and data from the master image file to a physical hard disk (see "Target disk"). In most cases, deployment is performed by multicasting the master image through the network.
Stand-alone deployment	Deployment to a machine isolated from a network or included in a network without Acronis Snap Deploy 6 infrastructure. Stand-alone deployment is performed locally by using a bootable component of Acronis Snap Deploy 6.
Target disk	The physical disk to be deployed to (an internal hard disk of the target machine).
Target machine (Target)	The hardware to perform deployment to.
Deployment template (Template)	Configuration parameters of the deployment operation: • Path to the master image • The operation mode, such as whether to use multicast or unicast and how to handle the target disk free space • Settings to be applied to the deployed systems, such as machine names and user accounts • Operations to be performed on the deployed systems, such as transferring files, running applications, shutting down, or restarting Once you save a deployment template, you can use it in the future.
Administrator	The person who has rights to manage the Acronis Snap Deploy 6 infrastructure.
User-initiated deployment mode	The mode when deployment can be initiated on the side of the target machine.

User	The person on the side of the target machine who starts the user-initiated deployment. This term relates to the user-initiated deployment mode only.

Components

Acronis Snap Deploy 6 includes the following components:

Components for Windows

These are components that are installed on machines running Windows and provide Acronis Snap Deploy 6 infrastructure.

- **Management Console** is an administrative tool for remote access to Acronis servers and Management Agent.

  When disconnected from the Acronis components, the console allows only for the installation of product components on remote machines and for the creation of bootable media.
- **OS Deploy Server** (the deployment server) is a component that performs centralized hardware-independent deployment through the network with the help of agents.
- **Management Agent** takes an image of a machine running Windows or enables OS Deploy Server to start deployment on this machine while the operating system is running.
- **Acronis PXE Server** allows booting machines over the network into Agent, Master Image Creator, or Windows Preinstallation Environment. The machines must support PXE. Using Acronis PXE Server considerably reduces the time required for booting multiple machines as compared to using bootable media. It also eliminates the need to have a technician onsite to install the bootable media into the system that must be booted.
- **Acronis Wake-on-LAN Proxy** is a component that enables OS Deploy Server to wake up the target machines located in another subnet.
- **License Server** is a component that tracks licenses of Acronis products.

Bootable components

These are components that are available in the Acronis environment or Windows Preinstallation Environment. A machine must boot into the corresponding component when you need to perform imaging or deployment.

- **Agent** is a bootable component that performs deployment to a target machine under the control of OS Deploy Server.

  There are two ways to load an agent on target machines: locally from bootable media or remotely by using Acronis PXE Server.
- **Master Image Creator** is a bootable, locally controlled component that creates an image of the master system.

  There are two ways to load Master Image Creator on a master machine: directly from bootable media or remotely by using Acronis PXE Server.

- **Standalone Utility** is a bootable component that enables fully-functional deployment with a GUI on a stand-alone machine (a machine isolated from the network or included in a network without Acronis Snap Deploy 6 infrastructure).
- **Acronis System Report** is a bootable component that collects information about the machine and saves this information to a locally-attached USB drive.

    There are two ways to load Acronis System Report: directly from an Acronis bootable media or remotely by using Acronis PXE Server.

Support for file systems and storage media

Supported file systems

Acronis Snap Deploy 6 provides full-featured imaging and deployment of the following file systems:

- FAT16
- FAT32
- NTFS
- Ext2
- Ext3
- Ext4
- ReiserFS
- Reiser4
- Linux SWAP
- XFS
- JFS

Acronis Snap Deploy 6 can perform imaging and deployment of corrupted or unsupported file systems by using a sector-by-sector approach. This approach usually leads to a bigger size of the master image and makes the imaging or deployment process longer. A volume with an unsupported file system cannot be resized during deployment.

Note

Deployment of images (backups) created by Acronis Cyber Protect or Acronis Cyber Protect Cloud via Agent for Linux for systems with LVM is not supported.

Supported media

Master Image Creator and **Management Agent** can save an image:

- In a network folder.
- On an internal hard disk of the master machine.
- On USB and FireWire (IEEE-1394) storage devices (hard drives, flash drives) attached to the master machine.

- On DVD+R/RW, DVD-R/RW, CD-R/RW, or recordable Blu-ray Discs (BD-R, BD-RE) loaded in the media drive of the master machine.

A sizeable image can be split between multiple media automatically.

OS Deploy Server can deploy images located:

- In network folders.
- On an internal hard disk of the deployment server.
- On USB and FireWire (IEEE-1394) storage devices (hard drives, flash drives) attached to the deployment server.
- On DVD+R/RW, DVD-R/RW, CD-R/RW, or recordable Blu-ray Discs (BD-R, BD-RE) loaded in the media drive of the deployment server.

The best practice is keeping images on the deployment server's hard disk. This minimizes network traffic during deployment.

The image created on removable media has to fit into one media disk. To deploy an image spread over two or more CDs, DVDs or other media, copy all parts of the image to the same folder on the deployment server or to a network folder.

Standalone Utility can deploy images located:

- In network folders.
- On USB and FireWire (IEEE-1394) storage devices (hard drives, flash drives) attached to the managed machine.
- On DVD+R/RW, DVD-R/RW, CD-R/RW, or recordable Blu-ray Discs (BD-R, BD-RE) loaded in the media drive of the managed machine.

Supported types of disks and firmware interfaces

Acronis Snap Deploy 6 can image and deploy **basic disks** that use the master boot record (MBR) or GUID Partition Table (GPT) partitioning scheme. Deployment to uninitialized disks is also supported.

Dynamic volumes (in Windows), MD devices and logical volumes (in Linux) are not supported for imaging and deployment.

Note
To perform imaging and deployment of disks and volumes that are not supported by Acronis Snap Deploy 6, use the Acronis Backup products.

Both **basic input/output system (BIOS)** and **Unified Extensible Firmware Interface (UEFI)** firmware interfaces are supported for master and target machines.

Usage

This section gives a general idea of using the product and does not contain the detailed instructions on how to perform operations. Nevertheless, advanced users are welcome to use this section as a

step-by-step quick start guide. The details can be found in the further sections.

Offline imaging

Offline imaging means that the master system is stopped and the master machine boots into the Acronis environment or into Windows Preinstallation Environment (WinPE).

To perform offline imaging

1. Configure the master system.
2. Install Management Console.
3. Do one of the following:
   - Create a bootable media (either an Acronis media or a WinPE-based media) with Master Image Creator.

   OR
   - Install Acronis PXE Server, connect the console to the PXE server and upload Master Image Creator.
4. Depending on your choice in the previous step, boot the machine into Master Image Creator from the bootable media or from the PXE server.
5. On the master machine, follow the instructions of the Master Image Creator wizard to configure and launch the imaging operation. The image can be saved in a network folder, on detachable media (such as a USB drive), or removable media (such as a DVD). To access the network from the bootable environment, you must have a DHCP server or configure the network settings of the master machine manually.

Offline imaging

Online imaging

Online imaging means that the master system is imaged live (without restarting the machine or suspending operations). Online imaging can be performed remotely whenever you need. The disadvantage is that you have to install imaging software that is included in the master image. This is not always rational.

To perform online imaging

1. Configure the master system.
2. Install Management Console.
3. Install Management Agent on the master system either locally by using the setup program, or remotely by using Management Console.

   After Management Agent is installed, you can image the master system online (without restarting the machine) at any time.
4. Connect the console to the master system, click **Create image -> Next -> A master image**. Follow the instructions of the Master Image Creator wizard to configure and launch the imaging operation. The image can be saved in a network folder, on detachable media (such as an USB drive) or on removable media (such as a DVD).

Online imaging

Deployment

This section illustrates the Acronis components functionality by the example of deployment that you start manually. For details about the ways of deployment, see "Deploying a master image".

This procedure presumes that you have installed Management Console and created a master image.

To perform deployment

1. Install License Server.
2. Import licenses to the license server.
3. Install OS Deploy Server.
4. Do one of the following:
   - Create bootable media (either Acronis media or WinPE-based media) with Agent.

   OR
   - Install Acronis PXE Server, connect the console to the PXE server, and then upload Agent.
5. Depending on your choice in the previous step, boot the target machines into Agent from the bootable media or from the PXE server.

   You must have a DHCP server or configure the network settings of the target machines manually to enable the target machines to connect to OS Deploy Server.
6. Connect the console to OS Deploy Server. Go to the **Machines** view.
7. Make sure that the target machines are displayed in the list and have the **Ready** state. This means that the machines are connected and ready for deployment.
8. Select the machines, click **Deploy image** on the toolbar, and then follow the Create Deployment Task Wizard instructions to configure and launch the deployment operation. When prompted about when you want to run the deployment, select **Now**.
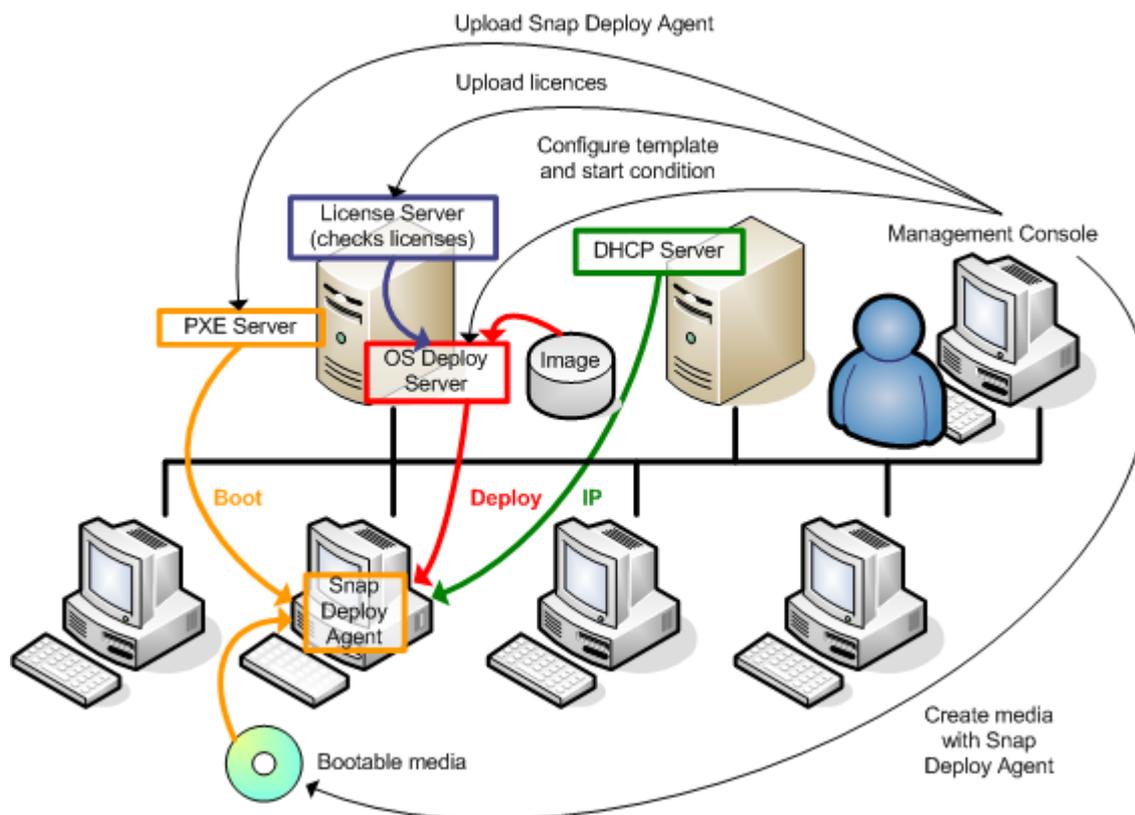
Deployment that starts manually

What is Acronis Universal Deploy

Acronis Universal Deploy is the Acronis proprietary technology that helps deploy and boot up a Windows or a Linux operating system on dissimilar hardware. Acronis Universal Deploy saves you from configuring a new master system for each make of hardware you need to perform deployment to.

If you plan to deploy an operating system to multiple machines that are identical to each other but differ from the master machine hardware, deploy the master image to one of the identical machines by using Acronis Universal Deploy. This will adjust the operating system to the dissimilar hardware. Then, create a master image of the adjusted system and deploy that image to the identical machines.

Acronis Universal Deploy purpose

An image of a system can be deployed easily on the hardware where it was created or to identical hardware. However, if you change a motherboard or use another processor version, the deployed system could be unbootable. An attempt to transfer the system to a new, much more powerful machine will usually produce the same result. This is because the new hardware is usually incompatible with the most critical drivers included in the image.

Using Microsoft System Preparation Tool (Sysprep) does not solve this problem, because Sysprep permits adding drivers only for Plug and Play devices (such as sound cards, network adapters, and video cards). As for the system Hardware Abstraction Layer (HAL) and mass-storage device drivers, they must be identical on the source and the target machines; see Microsoft Knowledge Base, article 302577.

Acronis Universal Deploy technology provides an efficient solution for hardware-independent system deployment by adding the crucial Hardware Abstraction Layer (HAL) and mass-storage device drivers.

Acronis Universal Deploy in Windows

Automatic HAL and mass-storage drivers selection

Acronis Universal Deploy searches the Windows default driver storage folders (in the master image being deployed) for HAL and mass-storage device drivers and installs drivers that better fit the target hardware. You can specify a custom driver repository (a network folder or a CD) which will also be used for driver searches.

Note
The Windows default driver storage folder is determined by the **DevicePath** value in the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** registry key. This storage folder is usually WINDOWS\inf.

Manual selection of mass-storage device driver

If the target hardware has a specific mass-storage controller (such as a SCSI, RAID, or Fibre Channel adapter) for the hard disk, you can install the appropriate driver manually, bypassing the automatic driver search-and-install procedure.

Installing drivers for Plug and Play devices

Acronis Universal Deploy relies on built-in Plug and Play discovery and configuration process to handle hardware differences in devices that are not critical for the deployed system startup, such as video, audio and USB. Windows takes control over this process during the logon phase, and if some of the new hardware is not detected, you will have a chance to install drivers for it later manually.

Acronis Universal Deploy in Linux

Acronis Universal Deploy can be applied to Linux operating systems with a kernel version of 2.6.8 or later.

When Acronis Universal Deploy is applied to a Linux operating system, it updates a temporary file system known as the initial RAM disk (initrd). This ensures that the operating system can boot on the new hardware.

Acronis Universal Deploy adds modules for the new hardware (including device drivers) to the initial RAM disk. As a rule, it finds the necessary modules in the **/lib/modules** directory of the operating system you are deploying. If Acronis Universal Deploy cannot find a module it needs, it logs the module's file name.

Acronis Universal Deploy may modify the configuration of the GRUB boot loader. This may be required, for example, to ensure the system bootability when the new machine has a different volume layout than the original machine.

Acronis Universal Deploy never modifies the Linux kernel.

Reverting to the original initial RAM disk

You can revert to the original initial RAM disk if necessary.

The initial RAM disk is stored on the machine in a file. Before updating the initial RAM disk for the first time, Acronis Universal Deploy saves a copy of it to the same directory. The name of the copy is the name of the file, followed by the **_acronis_backup.img** suffix. This copy will not be overwritten if you run Acronis Universal Deploy more than once (for example, after you have added missing drivers).

To revert to the original initial RAM disk, do any of the following:

- Rename the copy accordingly. For example, run a command similar to the following:

```
mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
```

- Specify the copy in the **initrd** line of the GRUB boot loader configuration.

Acronis Universal Deploy and Microsoft Sysprep

Acronis Universal Deploy is not a system preparation tool. You can apply it to any system image created by Acronis products, but you cannot apply it to images of systems prepared with Microsoft System Preparation Tool (Sysprep).

How to

How to image a machine without installing additional software to it?

Perform offline imaging.

How to image a machine without restarting it?

Perform online imaging.

How to prepare deployment tools?

Create bootable media with Agent. The machines will boot from these media.

How to deploy an image to a list of specific machines?

Use the **The machines listed below** option in the Create Deployment Task wizard. Specify the list of machines to perform deployment to.

How to deploy an image to a number of any machines?

Use the **Any machines ready for deployment** option in the Create Deployment Task wizard. Specify the number of machines to wait for.

How to deploy an image in the absence of a network connection?

Use Standalone Utility.

How to enable users to start deployment on their own?

Set up user-initiated deployment.

How to view the status of mass deployment?

Open the **Deployment tasks** view.

How to view the list of machines?

Open the **Machines** view.

How to add or remove licenses for deployment?

Open the **Licenses** view.

Getting started with Acronis Snap Deploy 6

This section describes how to install Acronis Snap Deploy 6 and perform a simple deployment.

By following the procedures in this section, you will:

A. Install and start Acronis Snap Deploy 6.
B. Create a master image of a machine.
C. Deploy the master image to the same or a different machine.

Step 1. Installing Acronis Snap Deploy 6

In this step, you will install Acronis Snap Deploy 6 in a typical configuration. For the complete description of installation methods and procedures, see the installation section.

Before installation, make sure that:

• You have a machine running a modern version of Windows, such as Windows 10 Pro. For the list of operating systems where you can install Acronis Snap Deploy 6, see "Supported operating systems".

• You have the setup program. You can download the setup program from the Acronis product download Web page.

• You have one or more license keys for Acronis Snap Deploy 6. You can buy full license keys or obtain trial ones by going to the Acronis Snap Deploy 6 Web page. The type of license ("for Server" or "for Workstation") determines the type of operating system that you can deploy.

On the machine where you want to install Acronis Snap Deploy 6, do the following:

1. Log on as an administrator and start the setup program.
2. Click **Install Acronis Snap Deploy 6** .
3. Accept the terms of the license agreement, and then click **Next**.
4. Click **Typical**.
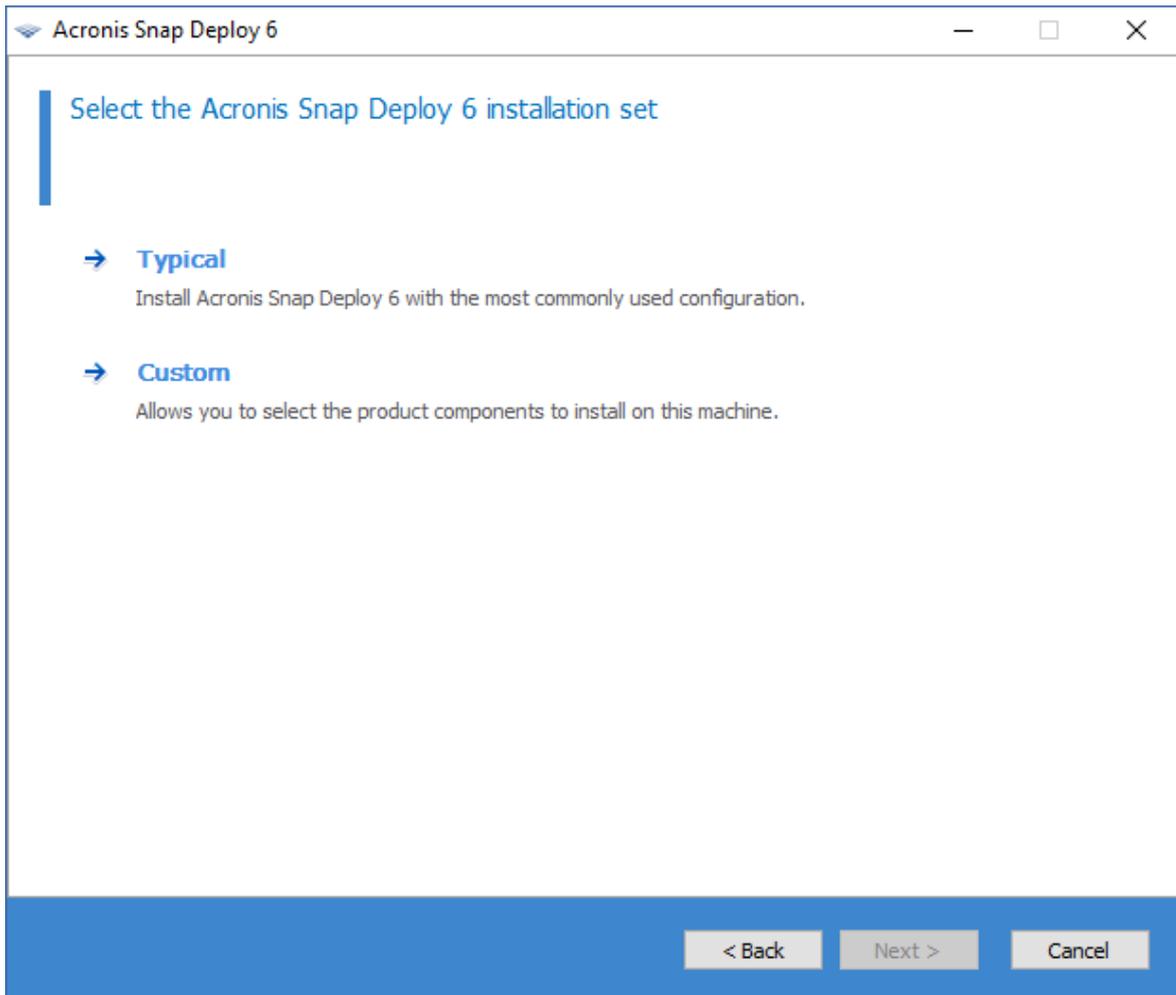
5. Click **Add license**, and then specify the license keys. You can type the license keys manually or import them from a text file.
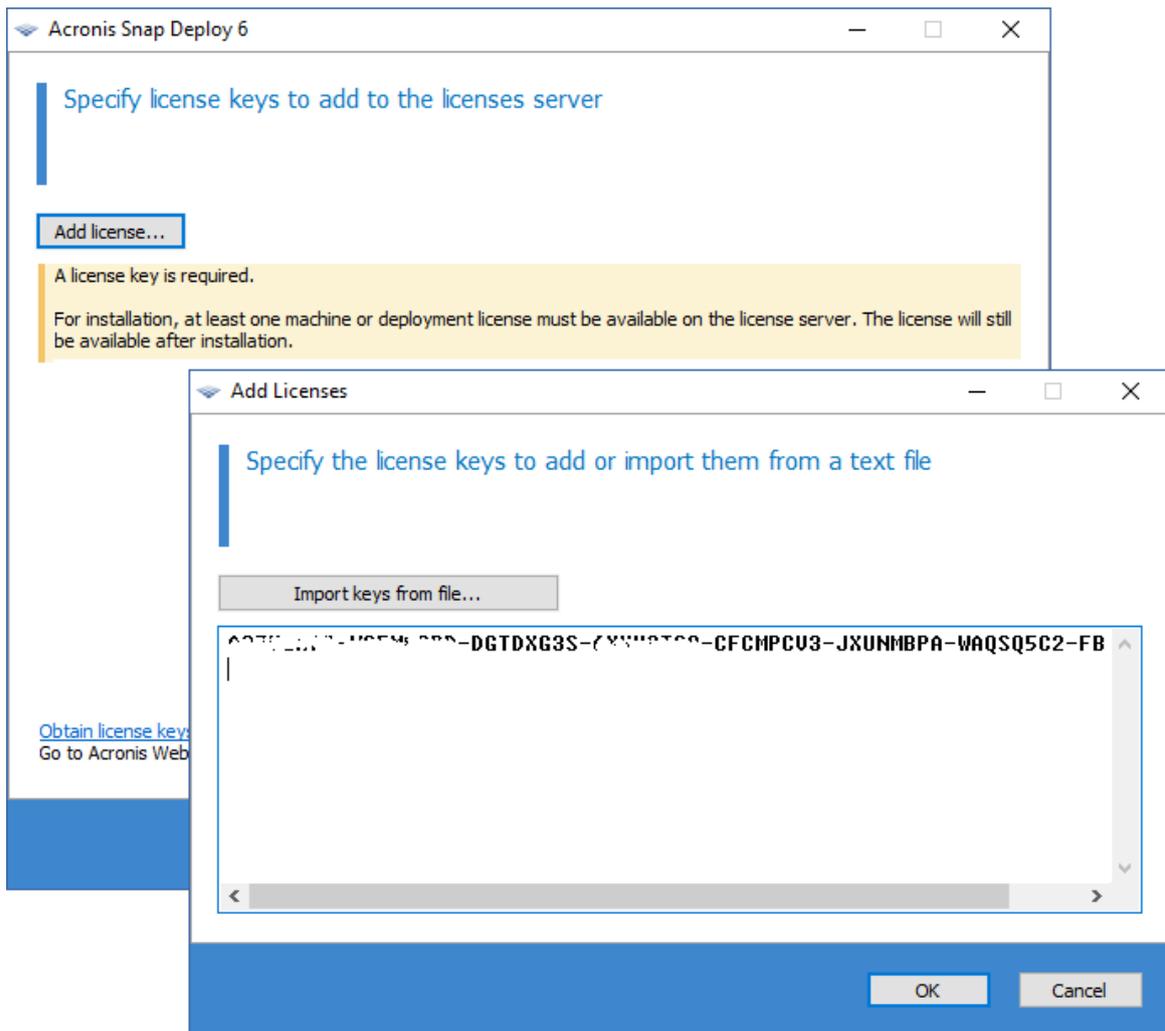
6. Specify whether the machine will participate in the Customer Experience Program (CEP).
7. Click **Install**.

Step 2. Starting Acronis Snap Deploy 6

On the machine where you installed Acronis Snap Deploy 6:

- On the desktop, click **Acronis Snap Deploy 6** .

When Acronis Snap Deploy 6 starts, the welcome screen appears.
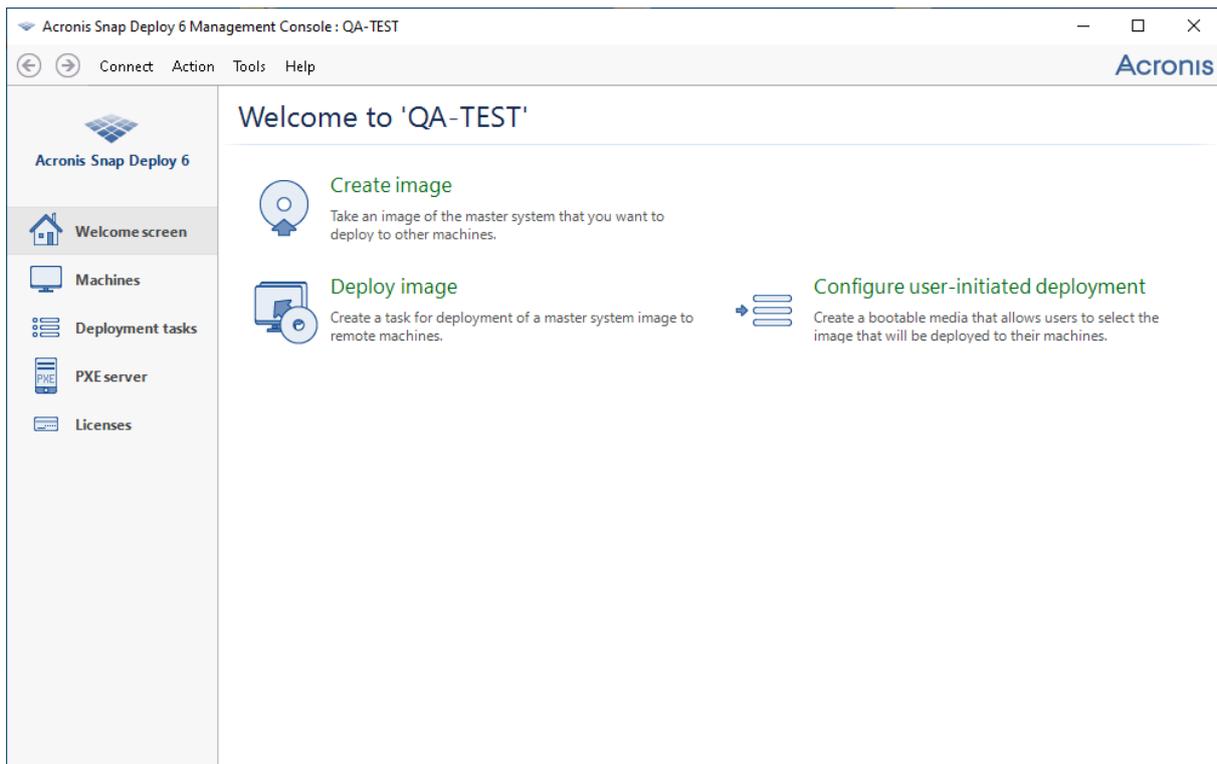
Step 3. Creating a bootable media

In this step, you will create a bootable media that enables creating master images and performing deployment.

On the machine where you installed and started Acronis Snap Deploy 6, do the following:

1. On the **Tools** menu, click **Create bootable media**.
2. In the list of components, select **Agent** and **Master Image Creator**.
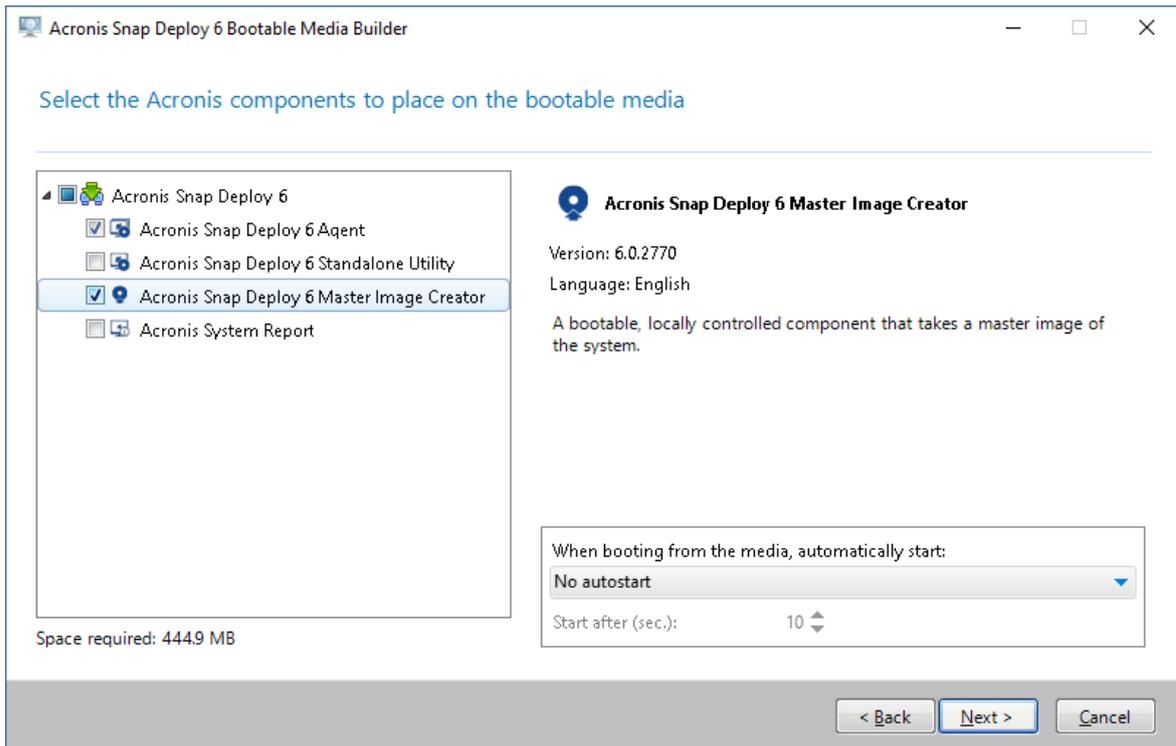
3. In **Network settings**, in **Server name/IP**, specify the name of the machine where you installed Acronis Snap Deploy 6.

4. Choose to create the media on a CD or DVD. Insert a blank CD-R/RW or DVD-R/RW.

   Tip. If no CD-RW, DVD-RW, or a similar optical disc drive is present on the machine, you can choose to create an ISO file that you can later burn to an optical disc on another machine. You can also create the media on a USB drive. For details, see "Creating a bootable media".

5. Click **Create**.

Step 4. Creating a master image

In this step, you will create an image of a machine and save the image to a USB hard disk.

Choose a machine whose image you want to create. No license is required for imaging the machine. However, a server or a workstation license will be used for deploying the machine, depending on whether the machine is running a server operating system (such as Windows 2008 Server or Linux) or a workstation operating system (such as Windows 7). For the list of server and workstation operating systems, see "Supported operating systems for imaging and deployment".

On the machine whose image you want to create, do the following:

1. Make sure that the CD or DVD drive has a higher boot priority than the hard disk drive. You may need to open the BIOS setup utility of the machine and adjust the boot priority setting, similarly to what is shown in the following picture.
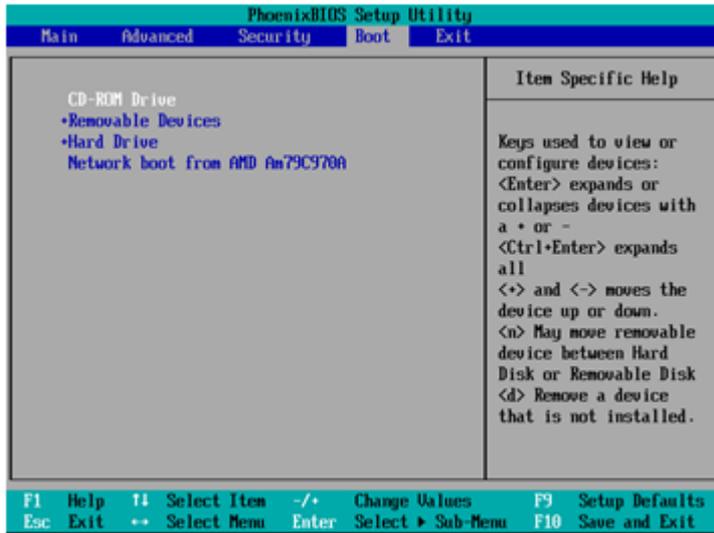
2. Attach the USB hard disk drive to the machine.

   Tip. Alternatively, you will be able to save the image to a network folder, as described later in this procedure.

3. Boot the machine from the bootable media you created.

4. On the boot menu, click **Master Image Creator**.
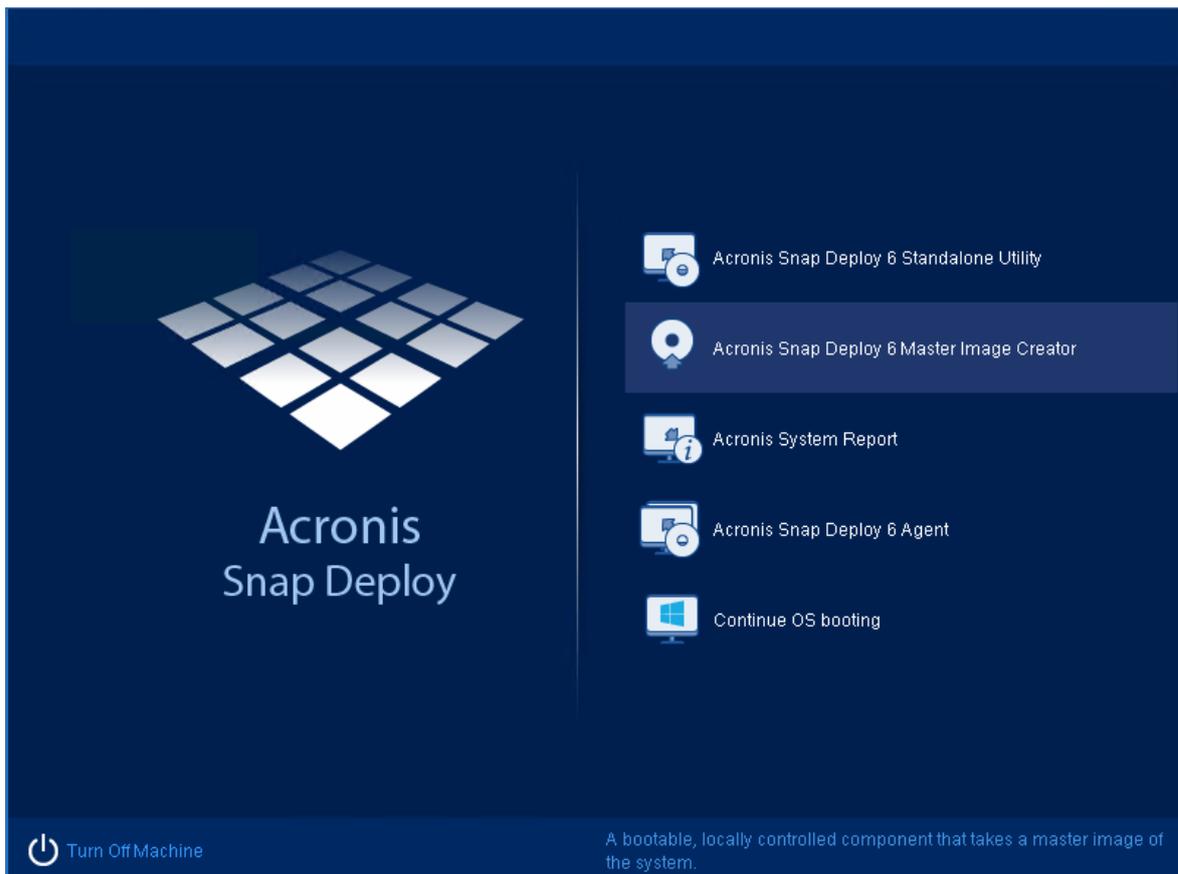
5. In the pop-up window, click **Cancel** or wait until that window closes.

6. Select the volumes that you want to include in the master image. You can leave the default selection, which normally includes the volumes that contain the operating system.
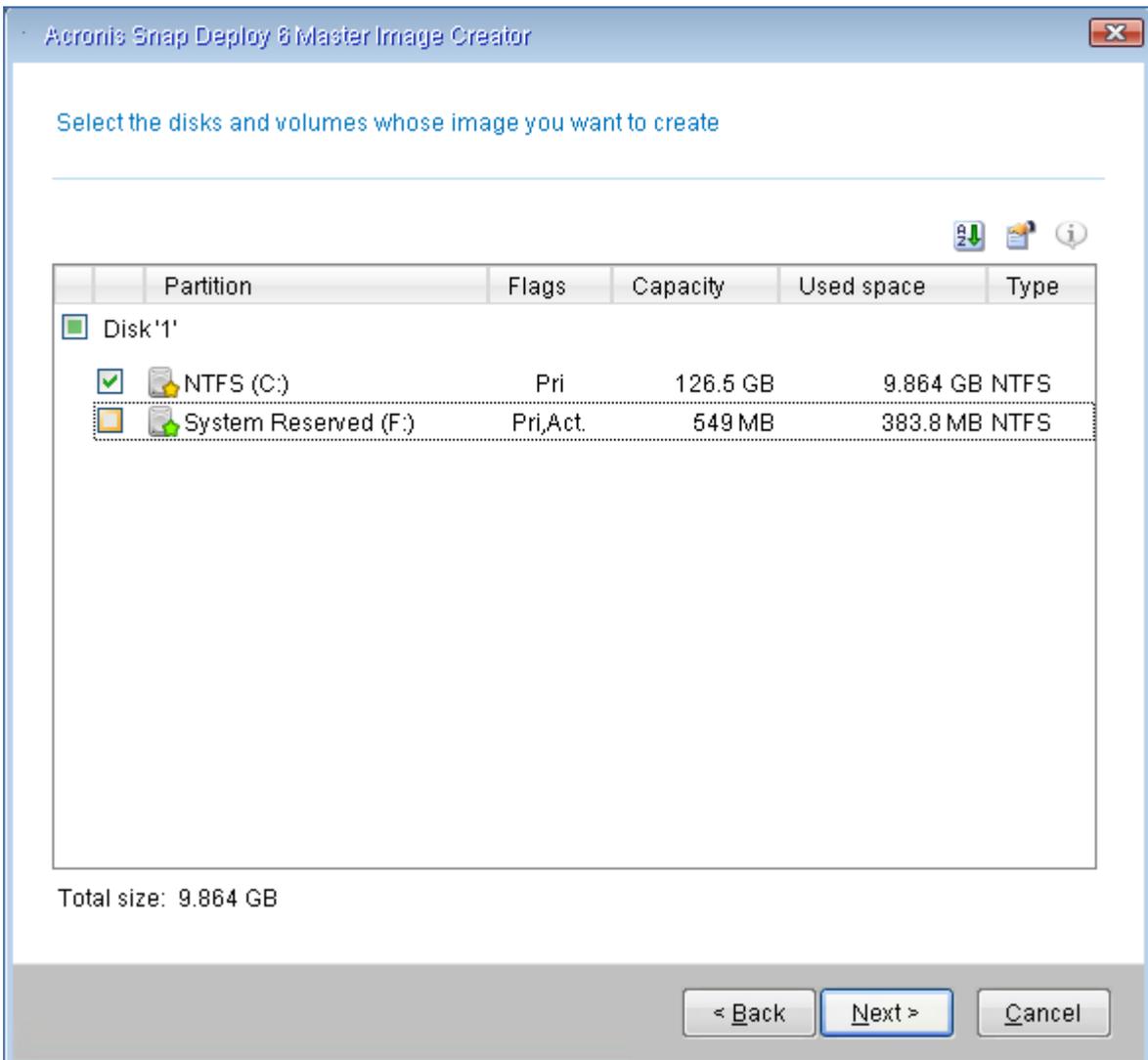
7. Specify a folder on the USB hard disk where you want to save the image.

   Alternatively, specify a network folder, and the user name and password to access that folder.

8. Keep clicking **Next** until the summary screen appears. Click **Create** in that screen.

Acronis Snap Deploy 6 starts creating the image.
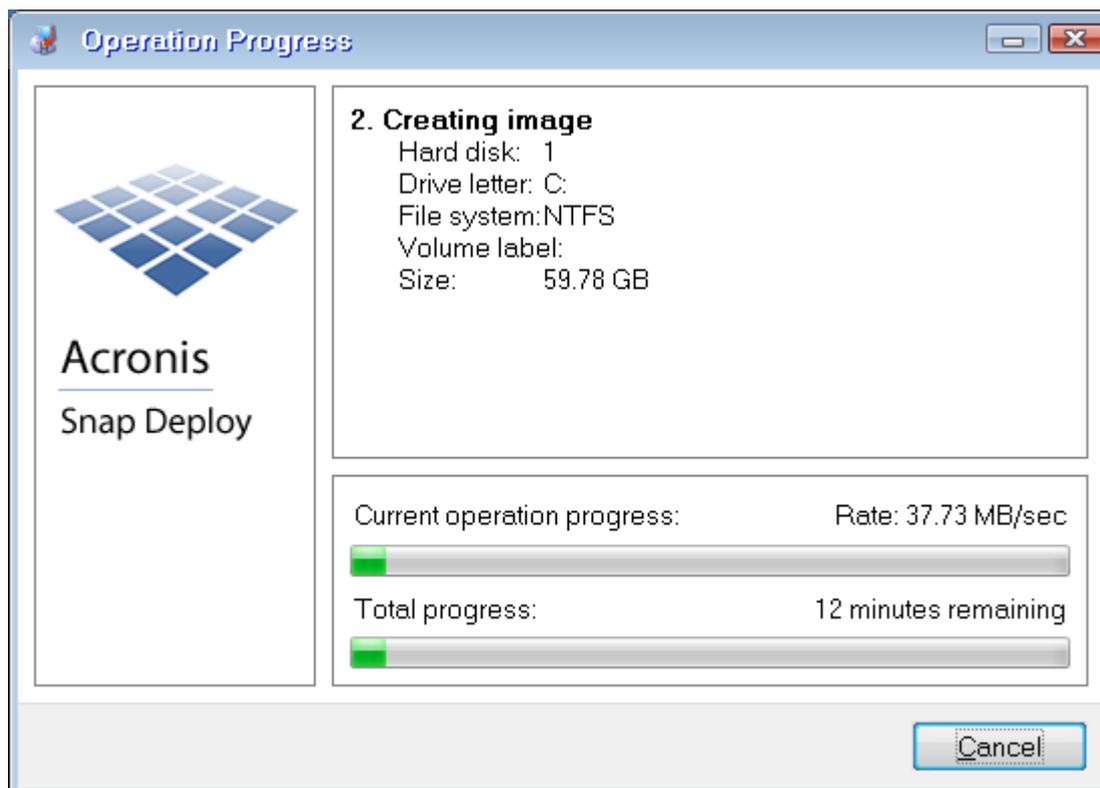
After the image is created, the machine will restart.

Step 5. Performing deployment

In this step, you will deploy the created master image to a single machine (the target machine).

Note

For getting started, we recommend performing deployment **to the same machine** from which you created the image, or to **a machine with identical hardware.** This way, no extra steps, such as using the Universal Deploy option, are required.

Preparing the target machine

On the target machine, do the following:

1. Make sure that the CD or DVD drive has a higher boot priority than the hard disk drive. You may need to open the BIOS setup utility of the machine and adjust the boot priority setting.
2. Boot the machine from the bootable media you created.
3. On the boot menu, click **Agent**.
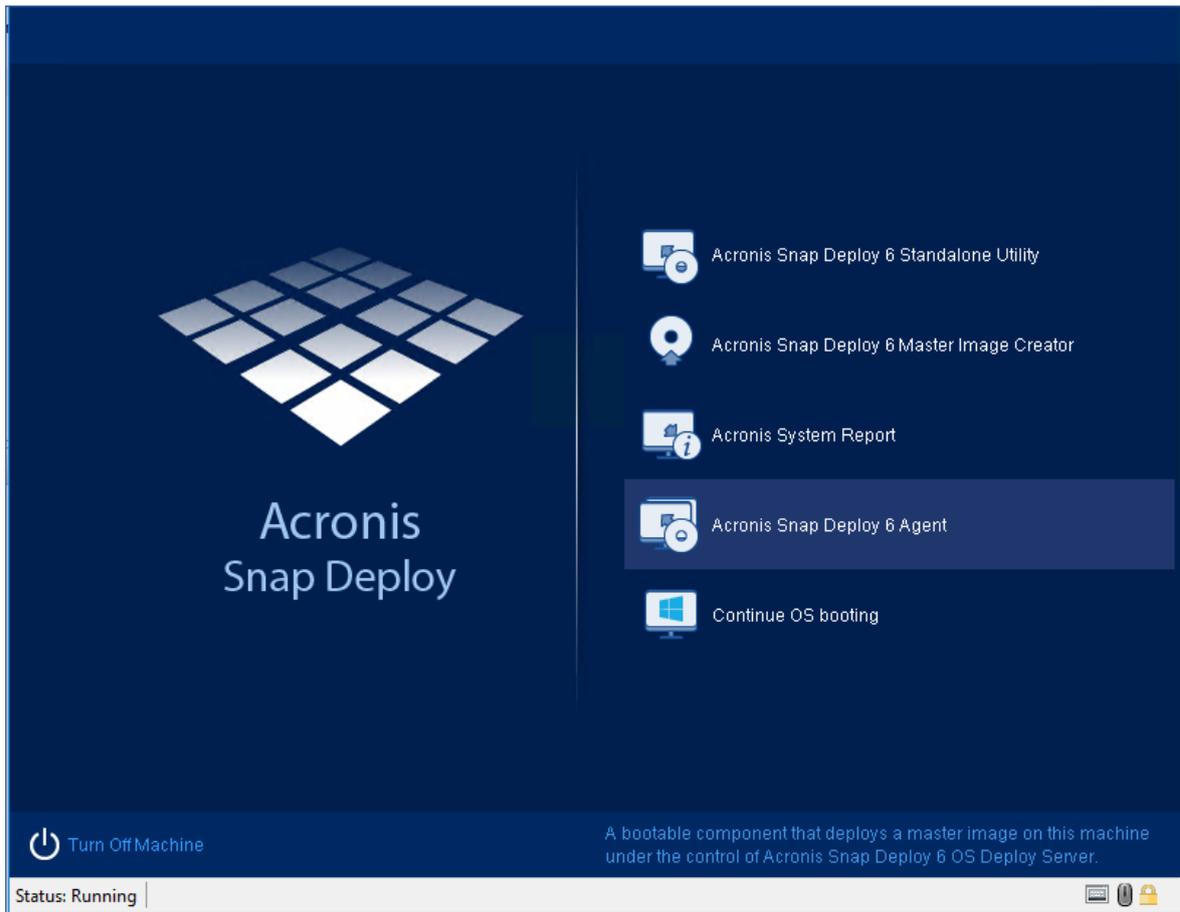
4. In the pop-up window, click **Cancel** or wait until that window closes.

5. Make sure that the machine is ready for deployment. The window should look similar to the following picture.
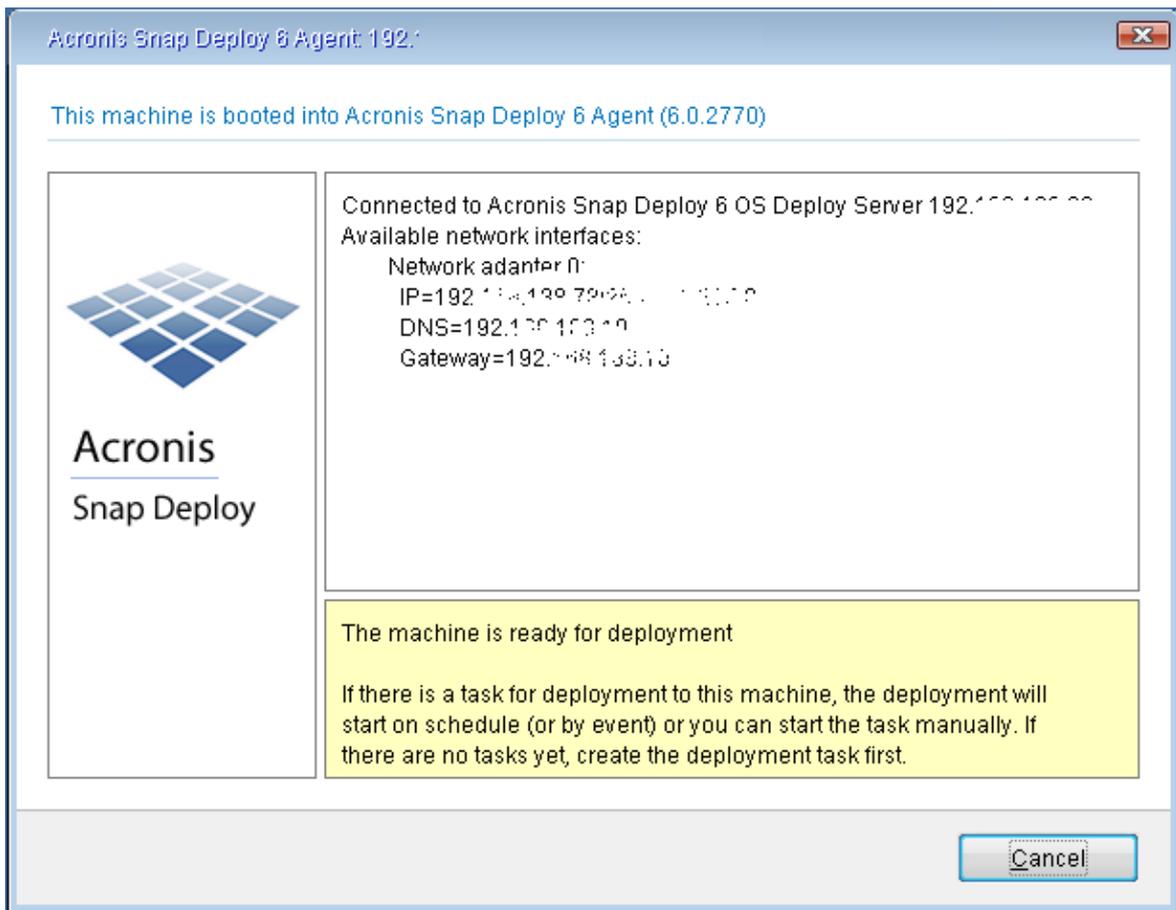
**Details.** The target machine becomes ready for deployment when it connects to OS Deploy Server. This server is part of Acronis Snap Deploy 6. If the machine does not connect to the server, you may need to adjust network settings, as described in "Booting the target machines".

After the target machine is ready, you can deploy the master image to it.

Deploying the master image

On the machine where you installed Acronis Snap Deploy 6, do the following:

1. Attach the USB hard disk drive with the master image to the machine. Optionally, copy the image to the local hard disk of the machine.
2. Click the **Machines** view. Make sure that the target machine you prepared is shown in the list and has the **Ready** state.
3. Right-click the target machine, and then click **Deploy image**.
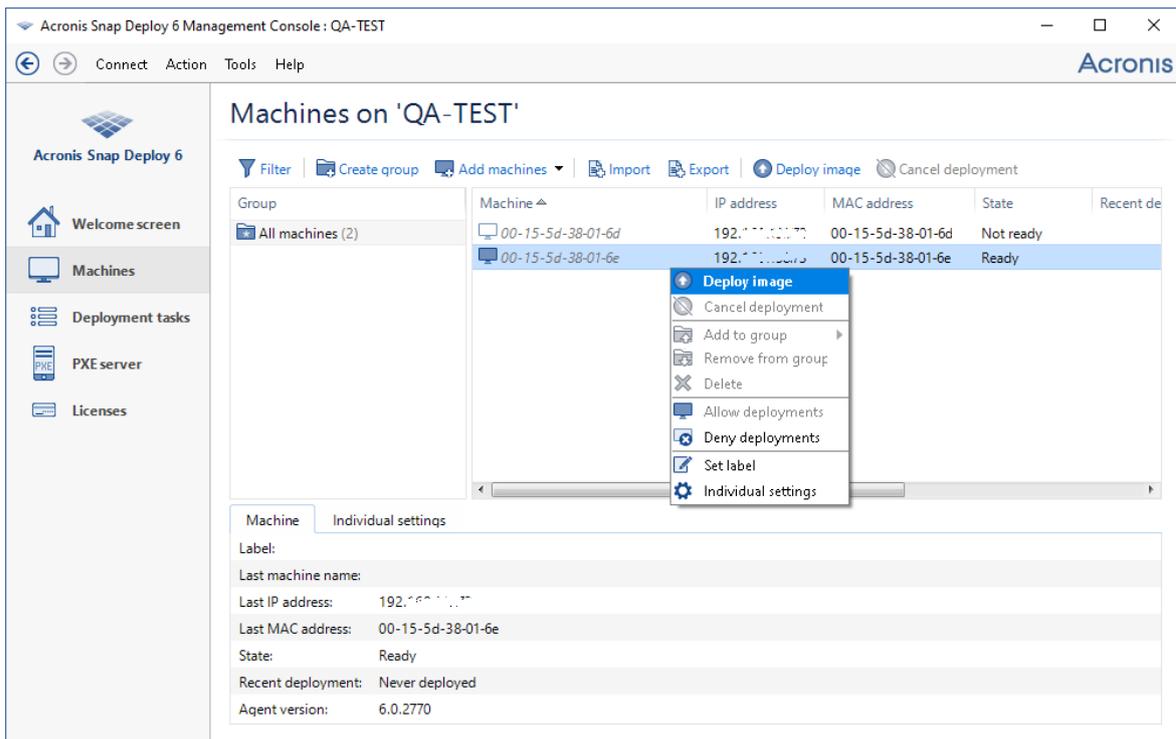
4. Keep clicking **Next** until the template selection window appears. Click **Create new** in that window.

5. Click **Create a new template**, and then click **Next**.

6. Select the master image (the .tib file) that you created, and then click **Next**.

7. In the deployment settings window, click **Next**.

   Note. If you imaged a machine running a workstation operating system (such as Windows 7) but you only have server licenses (such as Acronis Snap Deploy 6 for Server – Trial License), you may want to allow the software to use this type of license to deploy the machine. To do so, click **Licensing** in the deployment settings window, and then click **Use a server license automatically**.
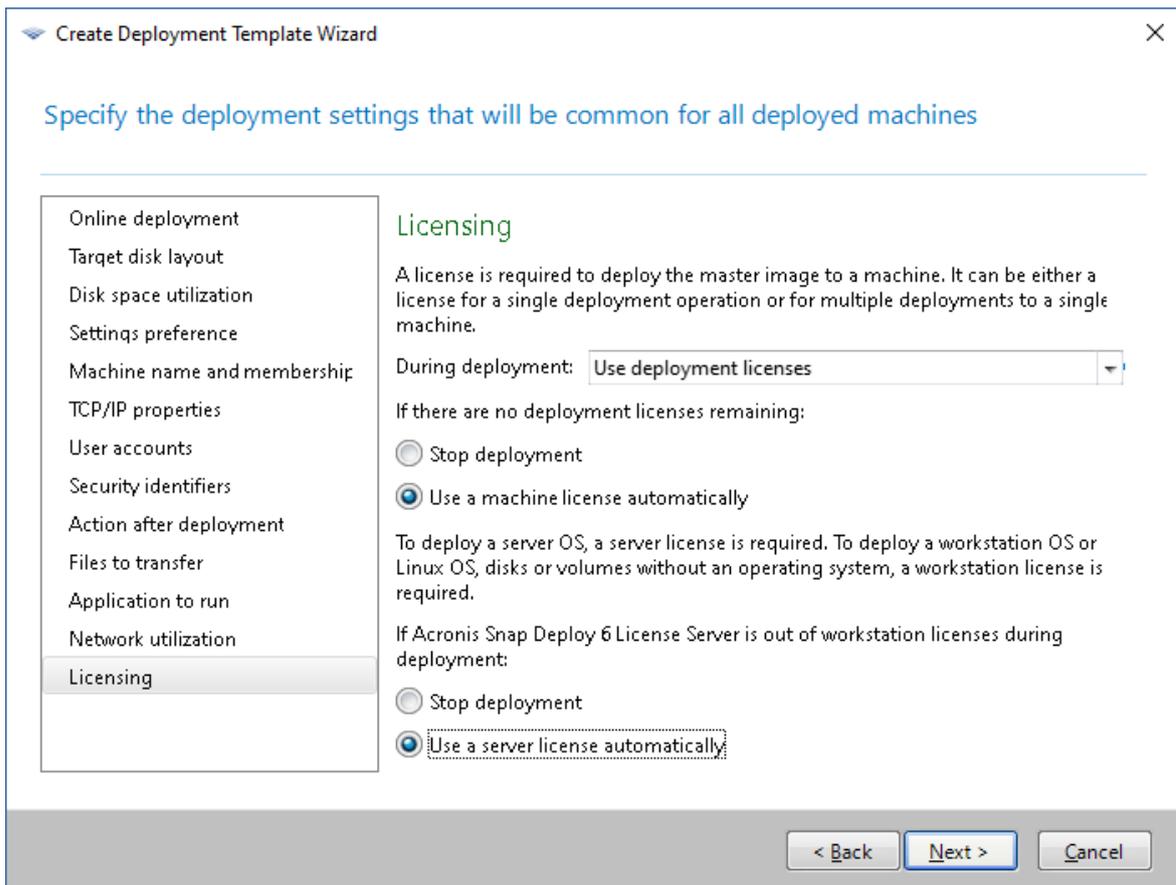
Alternatively, you can add a workstation license before starting the deployment, by opening the **Licenses** view and clicking **Add license** on the toolbar.

8. Keep clicking **Next** until the summary window appears. Click **Save** in that window.

   Details. You have created a deployment template. It determines how to perform deployment. You can reuse this template in other deployment tasks.

9. Select the deployment template you created, and then click **Next**.
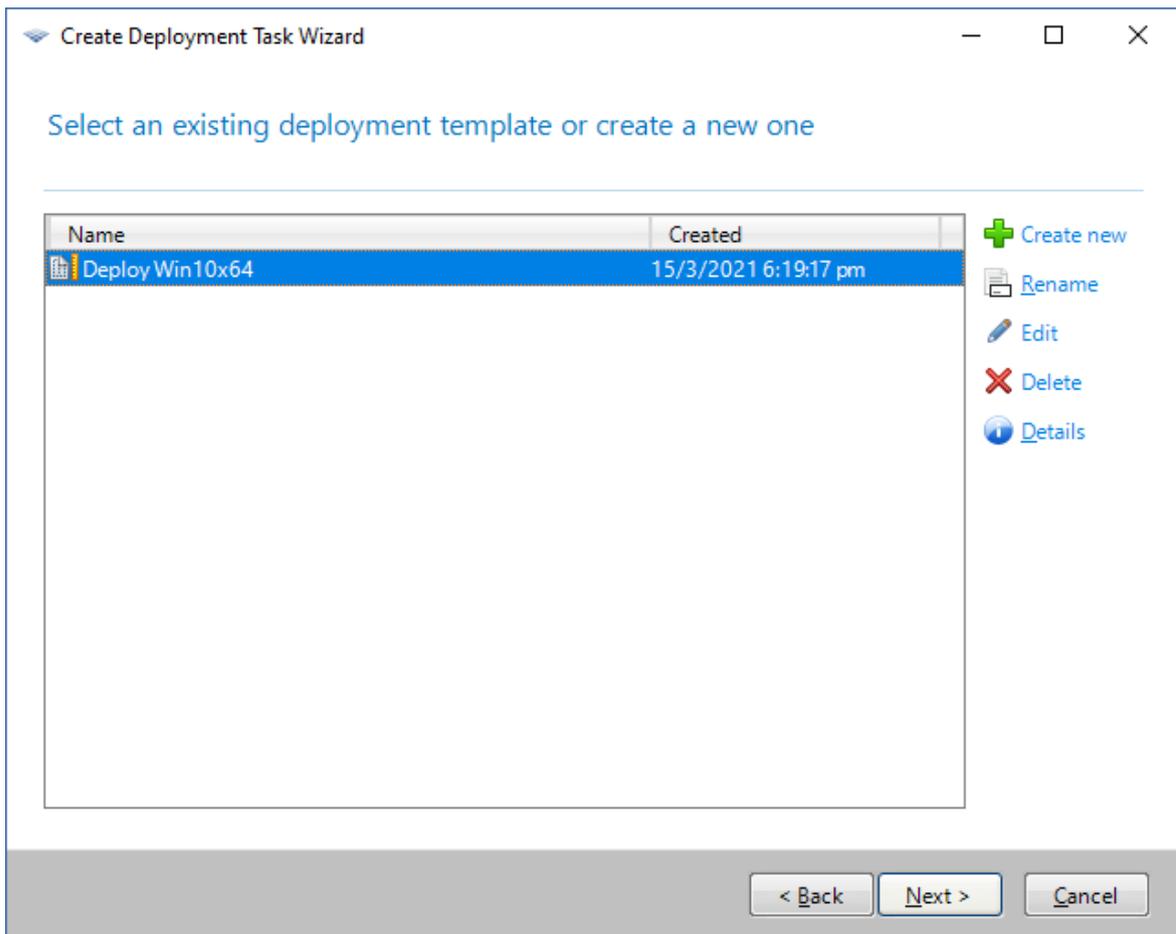
10. When asked about when to run the deployment, select **Now** and type the user name and password that you use to log on to Windows.
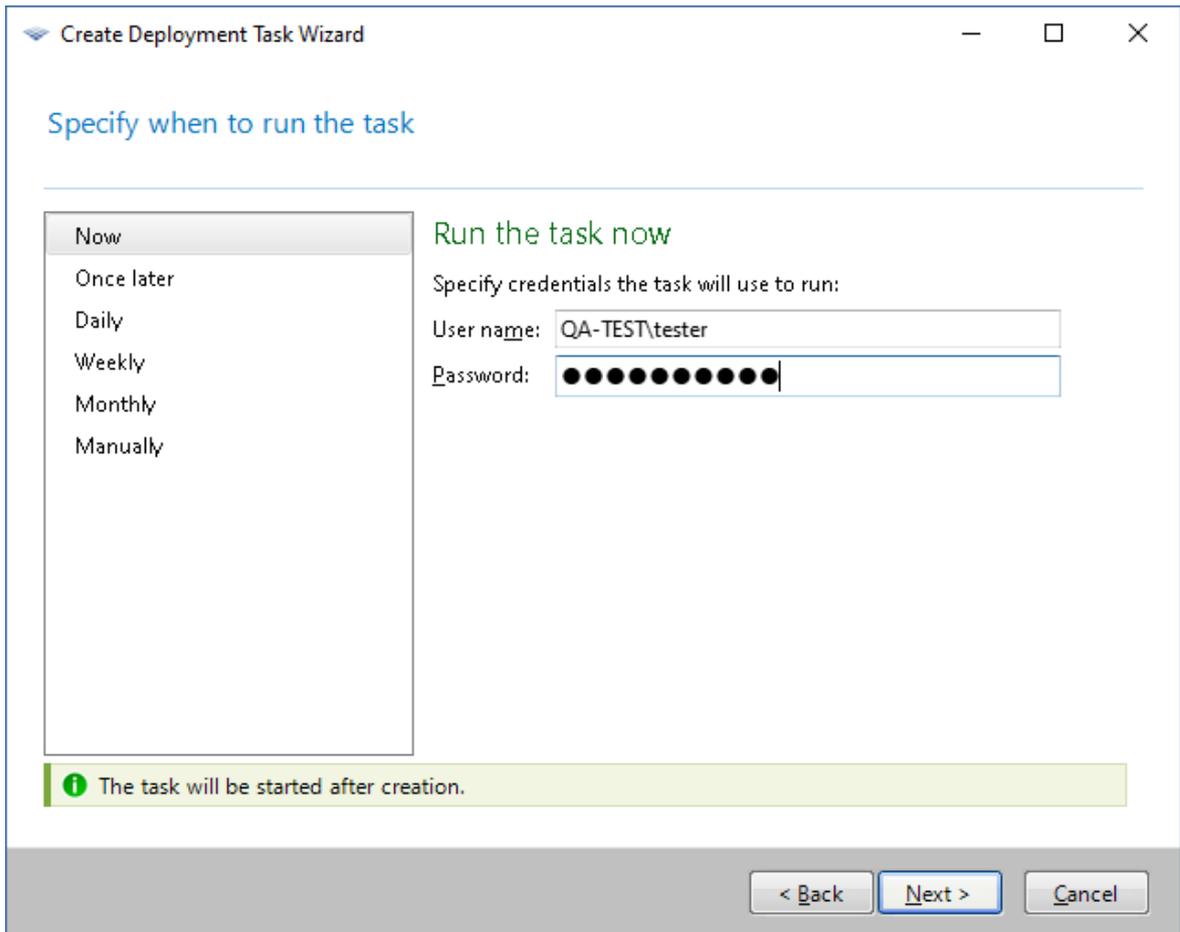
11. Keep clicking **Next** until the summary window appears. Click **Create** in that window.

You can view the progress of the deployment both on the machine where you installed Acronis Snap Deploy 6 and on the target machine.

© Acronis International GmbH, 2003-2023
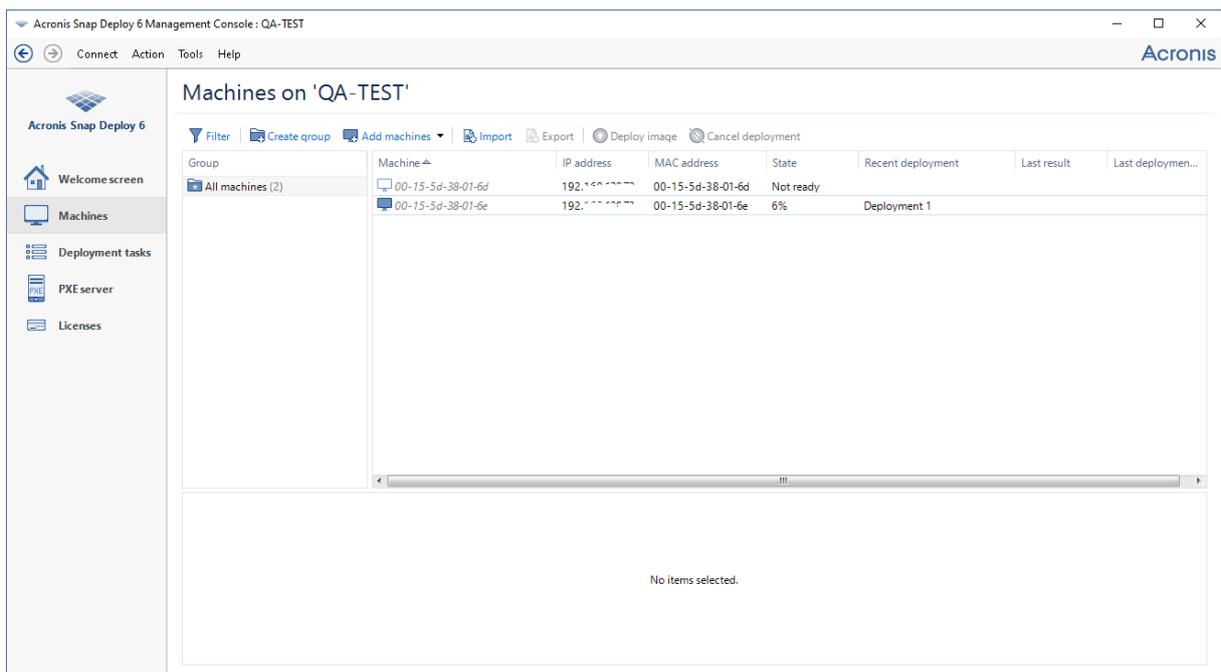
Viewing the deployment progress on the machine with Acronis Snap Deploy 6
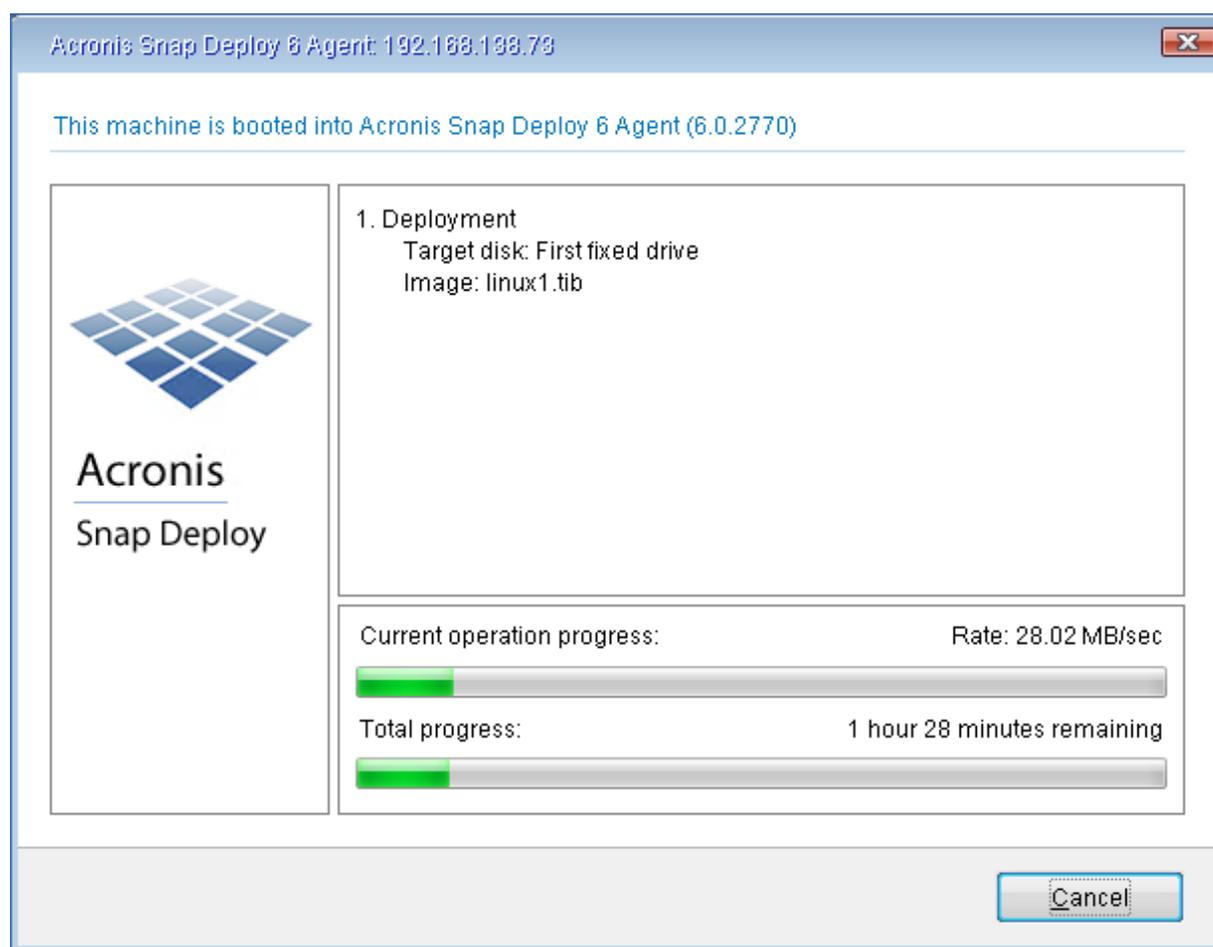
Viewing the deployment progress on the target machine

What you can do next

In the navigation pane, you can open the corresponding views to navigate across the software.

- **To run the deployment again,** open the **Deployment tasks** view, select the task you created, and then click **Run** on the toolbar.

  For details about the **Deployment tasks** view, see "Managing deployment tasks".

- **To add more machines,** open the **Machines** view and then click **Add machines**. You can add machines by their physical addresses, known as MAC addresses.

  Another way to add a machine to this view is to boot the machine so that it becomes ready for deployment, as described in "Preparing the target machine" earlier in this section. You can then turn off or restart the machine without performing deployment. The machine remains in the view.

  For details about the **Machines** view, see "Managing the list of machines".

- **To add more licenses for deployment,** open the **Licenses** view and then click **Add license** on the toolbar. Clicking **Obtain license** opens the Acronis Snap Deploy 6 Purchasing Web page.

For details about managing licenses, see "Using License Server". For information about license types, see "Licensing policy".

- **To set up network booting of machines** (instead of booting them from a media), open the **PXE server** view, click **Upload components to PXE**, and then follow the steps similar to those described in "Creating a bootable media" earlier in this section.

  For details about setting up the network booting, see "Configuring Acronis PXE Server".

Installation of Acronis Snap Deploy 6

Supported operating systems

This section lists the operating systems where components of Acronis Snap Deploy 6 can be installed.

It does not matter which Service Pack (if any) is installed in the operating system.

Any components for Windows can be installed in the following operating systems:

- Windows Server 2022 - any edition
- Windows Server 2019 - any edition, including IoT, LTSC (formerly LTSB)
- Windows Server 2016 - any edition
- Windows Server 2012 Foundation
- Windows Server 2012 R2 Foundation
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials
- Windows Server 2012 Standard
- Windows Server 2012 R2 Standard
- Windows Server 2012 Datacenter
- Windows Server 2012 R2 Datacenter
- Windows Server 2008 R2
- Windows Server 2008 (x86, x64)
- Windows Server 2003 (x86, x64)
- Windows Server 2003 R2 (x86, x64)
- Windows Small Business Server 2011
- Windows Small Business Server 2008
- Windows Small Business Server 2003
- Windows Server 2003 x64 Edition
- Windows 11 Pro
- Windows 11 Enterprise
- Windows 10 Pro (x86, x64)
- Windows 10 Enterprise (x86, x64)
- Windows 8 Pro (x86, x64)
- Windows 8.1 Pro (x86, x64)
- Windows 8 Enterprise (x86, x64)
- Windows 8.1 Enterprise (x86, x64)
- Windows 7 Professional (x86, x64)
- Windows 7 Ultimate (x86, x64)
- Windows Vista Business (x86, x64)

- Windows Vista Ultimate (x86, x64)
- Windows XP Professional
- Windows XP Professional x64 Edition

For local management only, **Management Console** and **Management Agent** can be installed on a machine running any of the following operating systems:

- Windows 11 Home
- Windows 10 Home
- Windows 10 Educational
- Windows 8
- Windows 8.1
- Windows 7 Home Basic, Windows 7 Home Premium
- Windows Vista Home Basic, Windows Vista Home Premium
- Windows XP Home

System requirements

Components for Windows

Component	Disk space required during installation or update	Disk space occupied by the component(s)	Additional
Complete installation	1554 MB	777 MB	
Management Console	1326 MB	663 MB	CD-R/RW, DVD-R/RW, or BD-R/RE for creating bootable media 1024x768 screen resolution Mouse (required)
OS Deploy Server	66 MB	33 MB	
Management Agent	66 MB	33 MB	
PXE Server	38 MB	19 MB	
Wake-on-LAN Proxy	18 MB	9 MB	
License Server	40 MB	20 MB	

Minimum memory requirements for a component are the same as for the Windows operating system where it is installed.

Network interface card is a common requirement for all the components.

Bootable media

Media type	Memory	ISO image size
Based on Windows PE 3/4	512/1024 MB	163 MB
Linux-based	256 MB	545 MB

Ports and IP addresses used by Acronis Snap Deploy 6

The Acronis Remote Agent service that acts as a main cross-components interaction service between the Acronis PXE Server, the OS Deploy Server, the Management Agent, and the Management Console, uses the following ports and IP addresses for remote operations:

- UDP port: 9876
- TCP port: 9876. If this port is busy, the deployment server and the management console select a port at random.
- TCP port: 5357. This port is used for multicast communications.
- IPv4 multicast address: 239.255.219.45

The Acronis OS Deploy Server uses the following ports:

- TCP ports: 23789, 9881. These ports are used for communication with the Deployment Agent.
- TCP ports: Some ports are used for inter-process communication. These ports are selected at random.

The Management Console uses the following ports:

- TCP ports: Some ports are used to communicate with the Acronis Remote Agent. These ports are selected at random.

The Acronis PXE Server uses the following ports and IP addresses:

- UDP ports: 67, 68, and 4011
- TCP port: 2000. This port is used to communicate with the Acronis Remote Agent.
- Broadcast address: 255.255.255.255

For a remote installation, Snap Deploy 6 uses TCP port 25001.

The Acronis File Server (part of the Acronis OS Deploy Server) uses the following ports:

- UDP port: 69
- TCP port: 24001. This port is used to communicate directly with the Acronis PXE server. The port is selected at random.

The Acronis Snap Deploy Agent running in bootable media environment uses the following ports:

- TCP ports: 2 ports are used to communicate with the OS Deploy Server. These ports are selected at random.

If you are using a firewall, you may need to set the appropriate access options.

Typical installation

With typical installation, all components of Acronis Snap Deploy 6 that are needed for deployment and offline imaging will be installed on the same machine.

Acronis Snap Deploy 6 will be installed with the following functionality:

- Performing deployment through the network
- Booting of the target machines over the network
- Managing the deployments by using the management console
- Creating a bootable media for deployment
- Creating a bootable media for taking a master image
- Storing and managing licenses of Acronis Snap Deploy 6

The following components will be installed on the machine:

- OS Deploy Server
- License Server
- Management Console
- Acronis PXE Server

To install Management Agent or Acronis Wake-on-LAN Proxy, and for more flexible installation, use custom installation.

To install Acronis Snap Deploy 6 (typical installation)

1. Log on as an administrator and start the setup program.
2. Click **Install Acronis Snap Deploy 6** .
3. Accept the terms of the license agreement, and then click **Next**.
4. Click **Typical**.
5. Click **Add license**, and then type the license keys for Acronis Snap Deploy 6 or import them from a file. You must provide at least one license key (either a machine license or a deployment license).

   Note
   The licenses will not be used until you start deployment.

6. Specify whether the machine will participate in the Customer Experience Program (CEP).
   You will be able to change this setting at a later time by starting Acronis Snap Deploy 6 and clicking **Help -> Customer Experience Program (CEP)**.
7. Click **Install**.

Custom installation

With custom installation, you can select which components of Acronis Snap Deploy 6 to install. You can also specify additional parameters. For example, you can change the default folder for installation.

You may want to use custom installation in the following cases:

- Installing Management Agent to take a master image of a machine without restarting it or to enable online deployment on the machine.
- Installing Acronis Wake-on-LAN Proxy to wake up machines that are located in another subnet.
- Installing different components on different machines, such as installing OS Deploy Server on one machine and Acronis PXE Server on another. For examples, see "Common installation configurations".

Installation procedure

Preparation

To be able to install OS Deploy Server, you need to have at least one machine license or deployment license on License Server. The license can be trial or full.

- If you are installing both License Server and OS Deploy Server on the same machine, you will be able to provide the license keys during installation.
- If License Server is installed on a different machine, load the license keys to that license server before installing the deployment server.

The license key just needs to be available on the license server. It will not become used until you start deployment.

Installation of other components does not require licenses.

To install Acronis Snap Deploy 6 (custom installation)

1. Log on as an administrator and start the setup program.
2. Click **Install Acronis Snap Deploy 6** .
3. Accept the terms of the license agreement, and then click **Next**.
4. Click **Custom**.
5. In the list of components, select the components that you want to install. For details about installing the components, see "Installation of components".
6. If you selected License Server for installation, provide the license keys of Acronis Snap Deploy 6.
7. If you selected OS Deploy Server without selecting License Server, specify the name or IP address of the machine where the license server is installed.
8. Specify the folder where the components will be installed.
9. If prompted, specify the following:

- Whether to install the components for all users on the machine (recommended) or only for the current user
- Whether the machine will participate in the Customer Experience Program (CEP). You will be able to change this setting at a later time by starting Acronis Snap Deploy 6 and clicking **Help - > Customer Experience Program (CEP)**.

10. Click **Install**.

Common installation configurations

Acronis Snap Deploy 6 components can be installed in various configurations, to distribute various components and features among the machines on the network.

a. The minimal configuration that enables only **offline imaging** and **stand-alone deployment** consists of:
- Management Console

b. The minimal configuration that enables **offline imaging, stand-alone deployment, and deployment through the network with OS Deploy Server** consists of the following components:
- Management Console
- License Server
- OS Deploy Server

On the target machines, no Acronis components are required.

c. The configuration that adds the **network boot of the target machines** to the functionality described in (b):
- Management Console
- License Server
- OS Deploy Server
- Acronis PXE Server

The components can be installed all on the same machine, or on different machines. On the target machines, no Acronis components are required.

This is the recommended elementary configuration that enables most of the Acronis Snap Deploy 6 functionality. This is the configuration for typical installation.

If physical access to the powerful server is limited, you can install the console on a separate machine. Another common configuration is:

Workstation:
- Management Console

Server:
- License Server
- OS Deploy Server
- Acronis PXE Server

Generally, you can install all Acronis servers on separate machines. In this case, you will have to connect the management console to each server separately to manage the server. With all servers on one machine, only one console connection is needed.

Note
If the target machines do not support PXE, you can install Management Agent on them and turn on the machines before starting the deployment.

---

d. To add to any configuration (a)–(c) the **online imaging ability** and **the ability to validate images integrity**, install **Management Agent**.

Online imaging means that the master system is imaged live (without restarting the machine or suspending operations). You can perform online imaging remotely, by connecting the console to the management agent installed on the master machine. The management agent will be included in the master image and deployed to all target machines.

However, having excess software in the master image is not always rational.

We recommend that you create a master image by using the bootable component called Master Image Creator. Nevertheless, having at least one management agent on the network (not necessarily on the master machine) makes sense. You will be able to validate (check) the integrity of your images by using the management agent.

e. To add to OS Deploy Server an **ability to perform deployment in another subnet** (across a network switch) in configuration (b) or (c), install **Acronis Wake-on-LAN Proxy** on any server in the subnet where the target machines are. No additional actions are required.

Acronis Wake-on-LAN Proxy has to be installed only if:

- You are going to perform deployment to a specific list of machines.

AND

- All or some of the target machines are in a subnet other than OS Deploy Server.

Installation of components

The setup program of Acronis Snap Deploy 6 includes the following components and component features:

- **OS Deploy Server**
- **License Server**, which includes:
  - License Server
  - The License Server Management Tool command-line utility
- **Management Console**, which includes:
  - Management Console
  - Media builders for creating an Acronis bootable media and a WinPE-based bootable media
- **PXE Server**
- **Management Agent**
- **Wake-on-LAN Proxy**
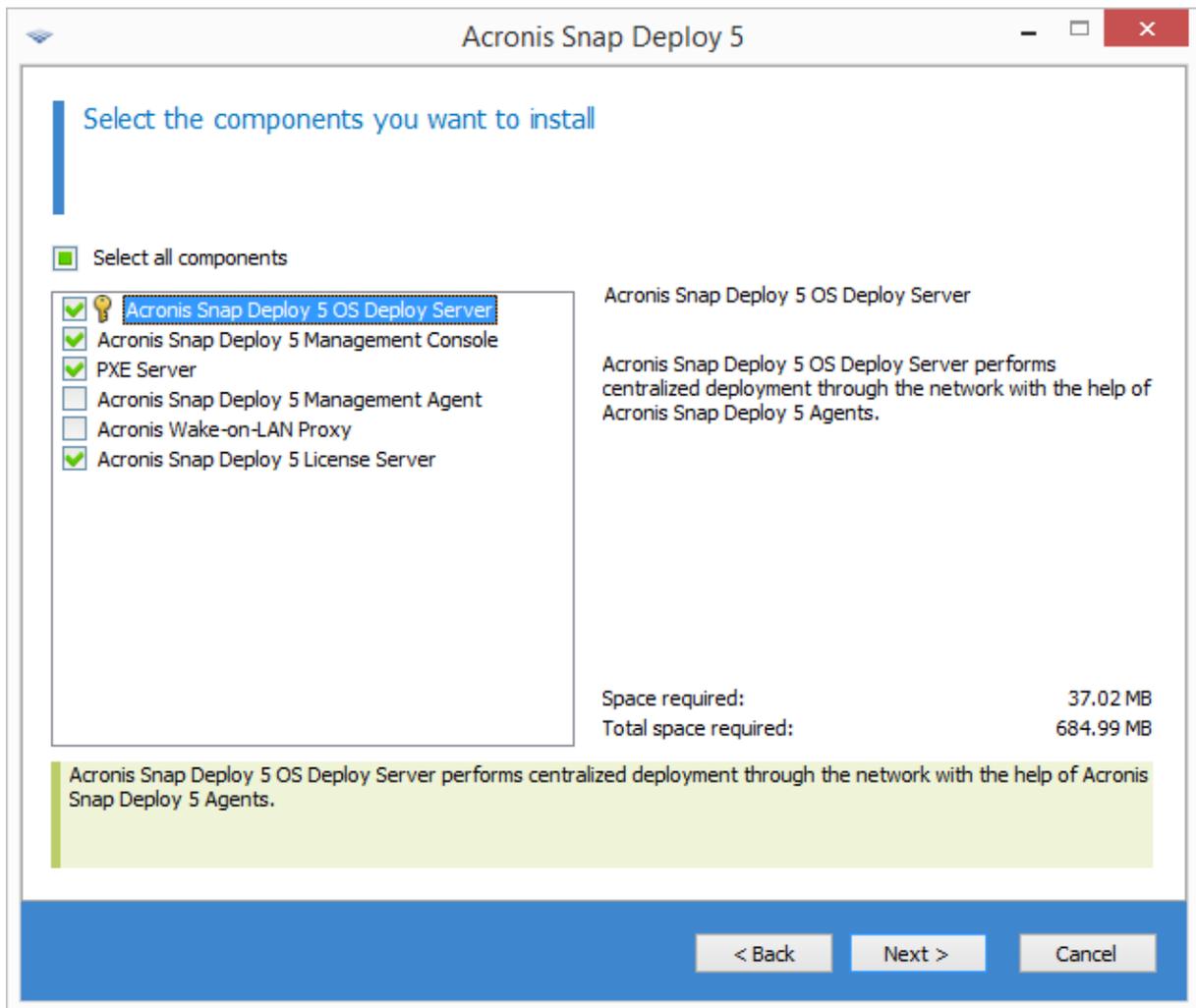
The list of components

Installation of Management Console

Management Console is an administrative tool for local and remote access to Acronis servers and Management Agent. Install Management Console on any machine from which you prefer to operate.

Installation of Management Console also includes the media builders for creating an Acronis bootable media and a bootable media based on Windows Preinstallation Environment (WinPE).

Once Management Console is installed, you can install other components remotely.

Installation of License Server

License Server is a component that tracks licenses of Acronis products. Install License Server on a machine accessible to OS Deploy Server. Consider installing both products on the same machine.

Installation of License Server also includes License Server Management Tool. This is a command-line utility for controlling the license server. Alternatively, you can control the license server by using Management Console.

> **Note**
> If you have already installed a license server that came with another Acronis product, you will still need to install License Server. You can install both license servers on the same machine. The machine will then act as a common license server for all Acronis products.

After installation, License Server launches automatically as a Windows service.

When installing License Server, you can add the license keys to it. You can add license keys at a later time, either by using the management console or in the command-line mode.

Installation of OS Deploy Server

OS Deploy Server is a component that performs centralized deployment through the network with the help of bootable components called agents.

Before installing OS Deploy Server, you need to install License Server and import license keys to it. You can install both servers on the same machine.

If License Server is not installed on the machine where you are installing OS Deploy Server, the setup program will ask you to specify a license server. Browse to the server, or enter its name or IP address.

> **Note**
> We recommend specifying the license server by its machine name. If you specify the license server by its IP address, OS Deploy Server will not be able to find the license server if this address changes.
>
> There is one exception to this recommendation: if your license server machine has non-English characters in its host name, you need to specify license server by IP address. Currently Unicode is not supported in Acronis Snap Deploy 6 communication between components, so OS Deploy Server will not be able to resolve the license server name properly if it contains non-English characters (i.e. if it contains Unicode symbols).

Installation of the deployment server does not decrease the number of licenses. The software just checks the availability of the licenses and stores the specified parameters of License Server to be able to access the license server at the time of deployment.

> **Important**
> If you are planning to use more than one deployment server, make sure that each particular machine is deployed only by one of them. Otherwise, each deployment server may use a separate license for the machine.

Installation of Acronis PXE Server

Acronis PXE Server allows network booting of the target machines for performing deployment.

Using Acronis PXE Server considerably reduces the time required for booting the machines as compared to using bootable media. It also eliminates the need to have a technician onsite to install

the bootable media into the system that must be booted. This allows for unattended scheduled deployment.

Using Acronis PXE Server makes sense if there is a Dynamic Host Control Protocol (DHCP) server in your network, so that the machines can automatically obtain IP addresses at boot. Without a DHCP server, you cannot boot machines from PXE.

We recommend that you have only one PXE server within a subnet to ensure predictability of the booting machines' behavior.

Acronis PXE Server starts running as a service immediately after installation. It will automatically launch at each system restart. You can stop and start this service in the same way as other services.

Installation of Acronis Wake-on-LAN Proxy

Acronis Wake-on-LAN Proxy enables OS Deploy Server to wake up the target machines located in another subnet.

You need to install Acronis Wake-on-LAN Proxy only if:

- You are going to perform deployment to specific machines (deployment to any ready machines does not involve waking up the machines by the deployment server)

AND

- All or some of the target machines are in a subnet other than OS Deploy Server.

Install Acronis Wake-on-LAN Proxy on any server in the same subnet as the target machines. No additional actions are required.

Acronis Wake-on-LAN Proxy runs as a service immediately after installation. Later on it will automatically launch at each system restart. You can stop and start this service in the same way as other services.

Installation of Management Agent

Installation of **Management Agent** adds the ability for online imaging, the ability to validate integrity of the master images, and enables OS Deploy Server to start deployment on the machine while it is online.

Online imaging means that the master system is imaged live (without restarting the machine or suspending operations). You can perform online imaging remotely by connecting the console to the management agent installed on the master machine. The management agent will be included in the master image and deployed on all target machines.

However, having excess software in the master image is not always rational.

We recommend that you create a master image by using the bootable component called Master Image Creator. Nevertheless, having at least one management agent on the network (not necessarily on the master machine) makes sense. You will be able to validate (check) the integrity of your images by using the management agent.

When installing the management agent on target machines in the environment with several deployment servers, do the following:

1. Turn off all of the deployment servers.
2. On each target machine, do the following:
    a. Install the management agent.
    b. Add the **ManagementAgent** key to the following registry key: **HKEY_LOCAL_ MACHINE\SOFTWARE\Acronis\SnapDeploy**
    c. Add the **Server** string value.
    d. In the **Server** string value, specify the IP address of the desired deployment server.
3. Turn on the deployment servers.

Other ways of installation

Installing components remotely

By using Management Console, you can install the following components of Acronis Snap Deploy 6 remotely:

- Management Agent
- Acronis Wake-on-LAN Proxy
- License Server
- OS Deploy Server

Preparation

Before proceeding with remote installation, prepare the remote machines as follows:

- **Simple file sharing.** For a successful installation on a remote machine running any version of Windows XP, the option **Control panel > Folder options > View > Use simple file sharing** must be *disabled* on that machine.
- **User Account Control.** For a successful installation on a remote machine running Windows Vista or later, User Account Control (UAC) must be *disabled*. To access this option, go to **Control panel > User Accounts > Change User Account Control Settings**.
- **File and Printer Sharing** must be *enabled* on the remote machine. To access this option:
    - On a machine running Windows XP with Service Pack 2 or Windows 2003 Server: go to **Control panel > Windows Firewall > Exceptions > File and Printer Sharing**.
    - On a machine running Windows Vista, Windows Server 2008, or Windows 7: go to **Control panel > Windows Firewall > Network and Sharing Center > Change advanced sharing settings**.
- **Ports.**Acronis Snap Deploy 6 uses TCP ports 445 and 25001 for remote installation. Make sure that these ports are added to exceptions in the firewall settings on the remote machines. TCP port 445 is added to exceptions automatically by Windows Firewall when you enable File and Printer Sharing.

To add a port to exceptions:

- In Windows XP, Windows 2003 Server, and Windows Vista: go to **Control panel > Windows Firewall > Exceptions > Add Port**
- In Windows 7: go to **Control panel > Windows Firewall > Advanced settings > Inbound Rules > New Rule > Port**

Note

If the remote machines are members of an Active Directory domain and use no firewall other than Windows Firewall, you can add TCP port 25001 to exceptions by using Group Policy. On a domain controller, create a Group Policy object, then go to **Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile > Windows Firewall: Define port exceptions** (or: **Define inbound port exceptions**), and then add the following port exception:

25001:tcp:*:enabled:Acronis remote install

You can exclude both ports from exceptions after the remote installation is complete.

Installation procedure

To install a component of Acronis Snap Deploy 6 remotely

1. Start Management Console.
2. On the **Tools** menu, click **Install components remotely**.
3. Select the location from which the installation packages of the components will be taken.
   The selection **The registered components** corresponds to the default folder:
   %ProgramFiles%\Common Files\Acronis\SnapDeploy\RemoteInstall
4. Select the component that you want to install.
5. If you are installing OS Deploy Server, specify the name or IP address of the machine with License Server. That license server must contain at least one available license.
6. In **Machine**, specify the name or IP address of the machine where you want to install the component. To open the list of machines on your network, click **Browse**.
7. To allow restarting the remote machine if it is required for installation, select the **Restart the machine automatically when required** check box. If you clear this check box, you may need to restart the remote machine later for the component to start working.
8. In **User name** and **Password**, specify the user name and password of an administrator on the remote machine.
9. Click **Install**.

Updating a component

To update a component on a remote machine, perform the same procedure.

Extracting the components of Acronis Snap Deploy 6

When you install Management Console, all installation files (.msi files) of Acronis Snap Deploy 6 components are placed in the **%ProgramFiles%\Common Files\Acronis\SnapDeploy\RemoteInstall** folder. As a result, you will be able to install a component remotely by using the management console; or install, modify, or repair a component by using the `msiexec` program.

To extract one or more components

1. Run the Acronis Snap Deploy 6 setup program.
2. Click **Extract installation files**.
3. Select the check boxes for the components whose installation files you want to extract.
4. Select a location for the installation files, and then click **Extract**.

Upgrading Acronis Snap Deploy 6

This section describes how to upgrade Acronis Snap Deploy 6.

Upgrading from a previous product version

Prerequisites

Before proceeding with the upgrade from a previous version of Acronis Snap Deploy, make sure that you have one or more license keys for Acronis Snap Deploy 6. These can be either standard license keys or upgrade license keys.

An upgrade license key enables you to continue using a license key for the previous version ("old" license key). The old license key cannot be reassigned to a different machine.

You need at least one license key for Acronis Snap Deploy 6 (no matter which type) to be able to upgrade Acronis OS Deploy Server. This license key will remain available.

To upgrade from Acronis Snap Deploy 5

Upgrade from Acronis Snap Deploy 5 is not possible with the default 64-bit installer of Acronis Snap Deploy 6. Uninstall Acronis Snap Deploy 5 first. For more details, refer to https://kb.acronis.com/content/68468.

Upgrading from older versions

Components of versions of Acronis Snap Deploy earlier than 5 are incompatible with Acronis Snap Deploy 6. To perform the upgrade:

1. Prepare a list of license keys that includes the license keys for the older version, and standard or upgrade license keys for Acronis Snap Deploy 6.
2. Uninstall all components of the older version.

3. Install Acronis Snap Deploy 6. For example, you can perform a typical installation. When prompted, specify all license keys from your list.

Upgrading from the trial to full product version

To upgrade from the trial to a full version of the software, buy the full licenses and import the license keys to License Server.

To upgrade to the full product version

1. Start Management Console.
2. Click **Licenses**. If prompted, specify the machine where the license server is installed.
3. Click **Add license**, and then provide the full license keys.

Acronis Snap Deploy 6 will start using the full licenses as soon as the trial ones expire.

Uninstalling Acronis Snap Deploy 6

To uninstall Acronis Snap Deploy 6, you should use the setup program.

To uninstall some or all components of Acronis Snap Deploy 6

1. Start the setup program of Acronis Snap Deploy 6.
2. Click **Install Acronis Snap Deploy 6** .
3. Do one of the following:
    - To uninstall all components, click **Remove**.
    - To uninstall individual components, click **Modify**, and then clear the check boxes for the components that you want to uninstall.
4. Proceed with the uninstallation.

Data remaining after uninstallation

Uninstalling License Server does not delete license keys. If you later reinstall the license server, all license keys automatically appear on the new license server. Used licenses remain used.

Uninstalling OS Deploy Server does not delete the deployment tasks, deployment templates, the list of machines, and individual deployment settings. If you later reinstall the deployment server, this data will be available to the new deployment server.

Using Management Console

Connecting to a machine

Connect to a local machine

When started, Management Console connects to the local machine if there is a manageable component of Acronis Snap Deploy 6 (such as OS Deploy Server) on this machine. You can manage any Acronis server or Management Agent installed on the same machine without any additional actions.
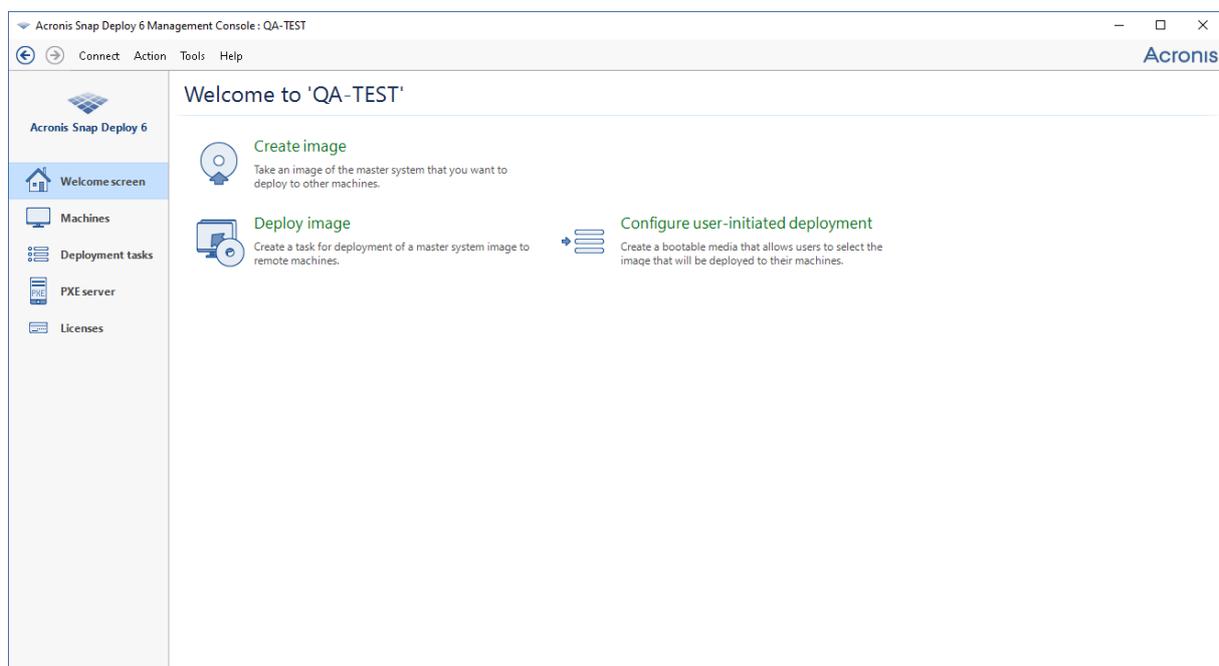
The welcome screen of the management console

Connect to another machine

Management Console can connect over the network to a machine where one or more of the following components are installed:

- OS Deploy Server
- License Server
- Acronis PXE Server
- Management Agent

Once connected, you can manage the Acronis server or perform operations by using Management Agent.

To connect to an Acronis component, you need the administrator's privileges on the remote machine.

To connect to a component

1. On the **Connect** menu, click **Connect**.
2. In **Machine**, specify the name or IP address of the machine where the component is installed. To open the list of machines on your network, click **Browse**.
3. In **User name** and **Password**, specify the user name and password of an administrator on that machine.
4. To save the password for the user name, select the **Save password** check box.

Alternatively, you can connect to the corresponding component when you open the **Machines**, **Deployment tasks**, **PXE server**, or **Licenses** view. In the welcome screen, you will be asked to connect to OS Deploy Server if this component is not installed on the local machine.
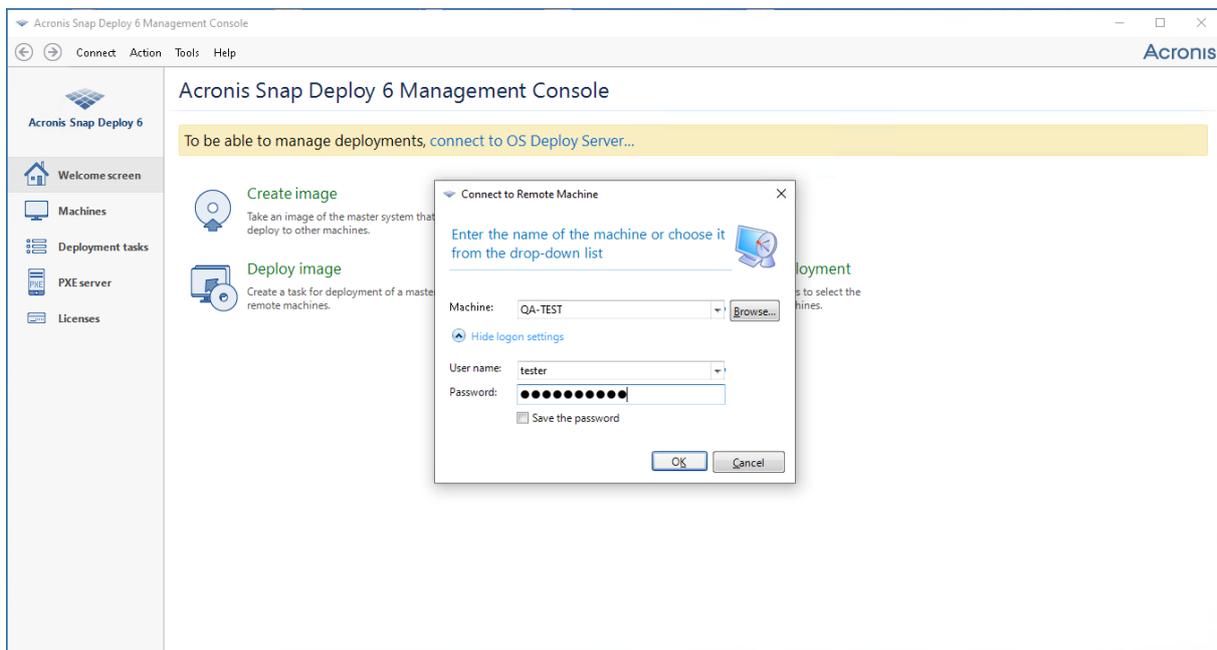
Connecting to a component on a remote machine

Connection to a component is needed to perform the following operations:

- *Managing deployment:* connect to OS Deploy Server.
- *Creating a master image of a machine without restarting it:* connect to Management Agent.
- *Validating a master image:* connect to Management Agent.
- *Managing licenses:* connect to License Server.
- *Configuring Acronis PXE Server:* connect to Acronis PXE Server.

No connection is needed to perform the following operations:

- *Creating an Acronis bootable media or a WinPE-based bootable media*
- *Installing Acronis components remotely*

Browsing logs

OS Deploy Server and Acronis PXE Server store the log of the operations they have performed.

The view the log of OS Deploy Server

1. Connect the management console to the machine with OS Deploy Server.
2. Do either of the following:
    - In the left pane, click **Deployment tasks**, and then click **Log** on the toolbar.
    - On the **Help** menu, click **View log**.
3. In the left pane, select a log. In the right pane, examine the events recorded in the log.

The left pane shows up to 50 log entries. If there are more log entries, you can browse the list by using the buttons with the left and right arrows.

To delete a log entry, select it and click the **Delete the selected log entry** button.

If any step was terminated by an error, the corresponding log entry will be marked by a red circle with a white "X" inside.

The right window shows the list of events contained in the selected log entry. The three buttons to the right control message filters: the white "X" in the red circle filters error messages, the exclamation sign in a yellow triangle filters warnings, and the "i" in a circle filters information messages.

To select columns to display (such as the date and time of an event), right-click the table header, and then select the columns.

To sort the events by a particular column, click the desired column name. To reverse the sort order, click the column again.

You can also change column width by dragging the borders.

To view the log of Acronis PXE Server

1. Connect the management console to the machine with Acronis PXE Server.
2. In the left pane, click **PXE server**.
3. Examine the log entries in the lower part of the view.

Checking for software updates

Each time you start the management console, Acronis Snap Deploy 6 checks whether a new version of the software is available on the Acronis Web site. If so, the software provides a link for downloading the setup program of the new version.

To check for updates manually, start the management console and then click **Help -> Check for update**. In that window, you also can disable the automatic checks for updates.

Using License Server

This section contains general information necessary for understanding License Server and covers operations with licenses.

Understanding License Server

License Server is a mechanism that tracks licenses of Acronis products. Acronis Snap Deploy 6 licensing is based on the number of machines (servers or workstations) that you deploy. For example, to deploy a system to 100 machines, you need 100 licenses.

License Server tracks the licenses using a MAC address, which is unique for each network interface card (NIC). Although a MAC address is usually hardwired to the NIC, some operating systems offer a way to change it. It is important to note that attempting to change the MAC address on a system may impede the License Server operation and prevent you from other deployments to the same machine.

When installing OS Deploy Server, you need to specify a license server. After the license server is found, the software checks for available licenses on the server and stores its network address to be able to access the license server later, when deployment is launched.

When starting a deployment, OS Deploy Server checks for available licenses on the license server. If an appropriate license is available for a machine, the deployment operation will run on the machine. The number of available licenses will decrease by the number of systems being deployed.

If deployment under a deployment license has failed, that license becomes available again. A machine license remains used by the machine regardless of the result of deployment.

License Server can import multiple license keys from .txt or .eml files, saving you from the time-consuming procedure of typing each number.

When upgraded, recovered or reinstalled, the license server keeps all the imported licenses intact. However, it is recommended that you copy the files with license keys to removable media, or create a hard copy of those files and keep it in a safe place. This ensures that you have license data available in case of hardware failure.

Adding licenses by using Management Console

You can add the licenses when you are installing License Server. After the license server is installed, you can add licenses by using Management Console, as follows.

To add one or more license keys to the license server

1. Run Management Console.
2. Click **Licenses**. If the license server is installed on a different machine, click **Connect to License Server**, and then type the name or IP address of that machine.
3. Click **Add License**.

4. In the **Add Licenses** window, type the license key or the path to a .txt or .eml file containing the license keys; or, you can browse to the file.

5. Click **Add**. License Server performs the operation and reports the number of newly-added licenses.
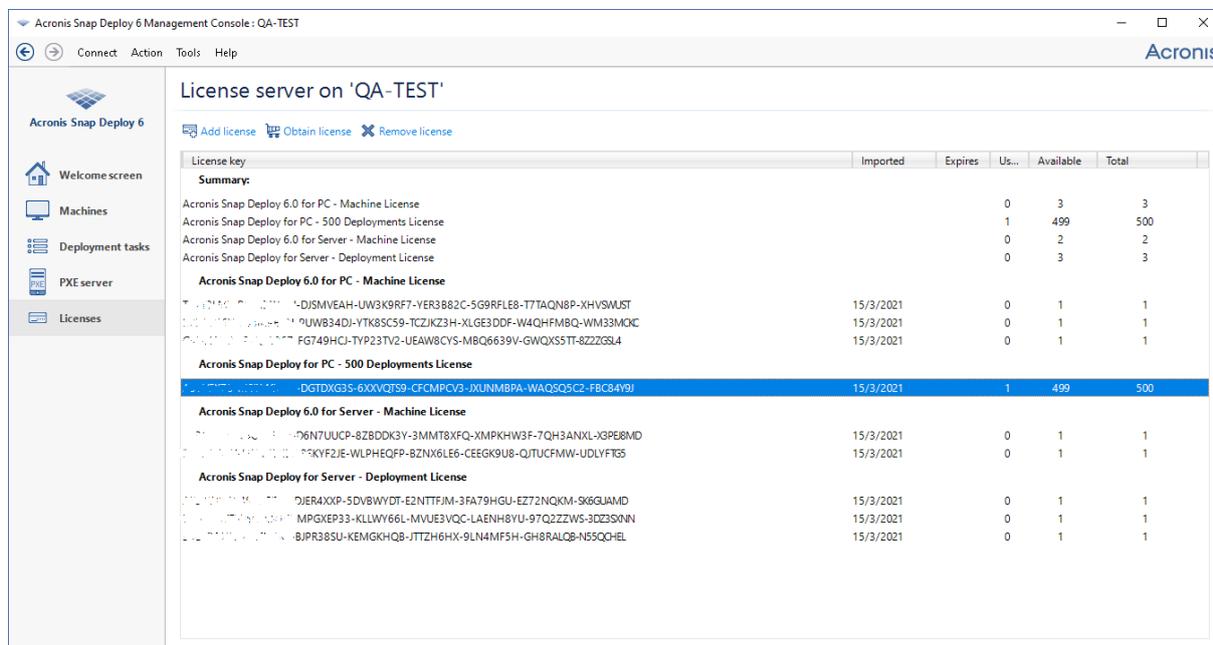
The license server has 10 license keys of various types. The license corresponding to the highlighted license key has already been used for deployment.

Viewing information about licenses

To view information about licenses

1. Run Management Console.

2. Click **Licenses**. If the license server is installed on a different machine, click **Connect to License Server**, and then type the name or IP address of that machine.

   This will display all license keys available on License Server. One license key can correspond to multiple licenses.
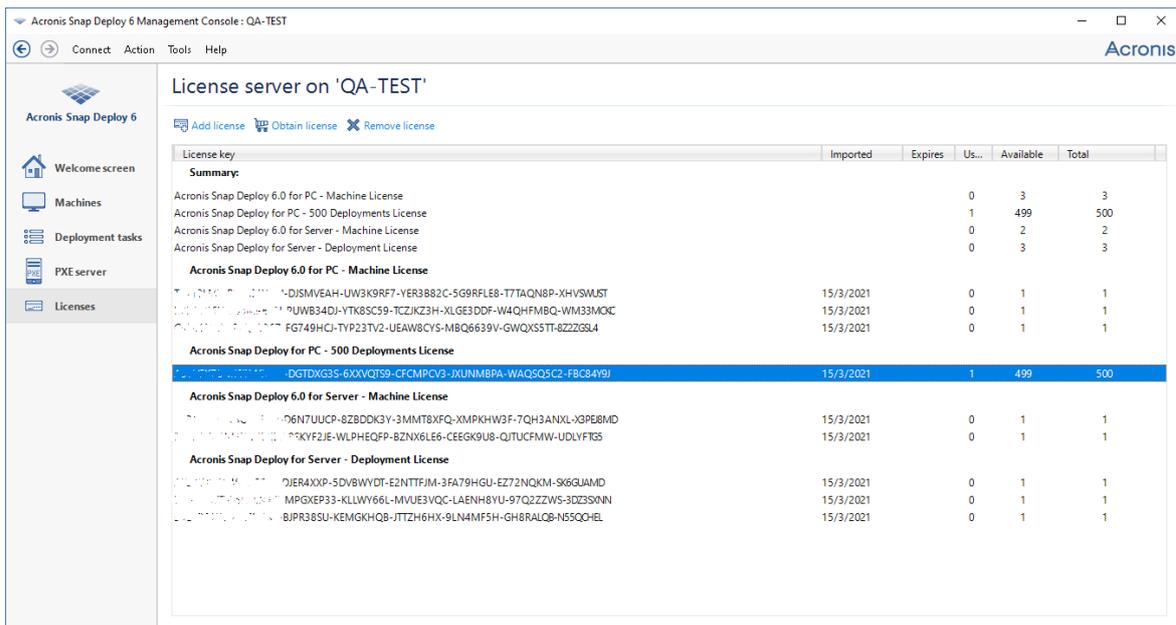
The license server contains 10 server licenses and five workstation licenses

3. Right-click the column headings bar to choose the details to display: license key, import date, expiration date (for trial licenses), the total number of licenses assigned to each license key, how many of them are available (that is, free), and how many are used. For example, if one license corresponds to one license key, Total=1, Available=1, Used=0 (if the license is free) or Available=0, Used=1 (if the license has been allocated).

Removing licenses

To completely remove a license from License Server, select the corresponding license key from the list, and then click **Remove license** on the toolbar.

The following licenses cannot be removed:

- Used licenses
- Trial licenses

When a trial license expires, Acronis Snap Deploy 6 will use an available full license of the corresponding type.

Adding licenses in the command-line mode

As an alternative to the graphical user interface, you can add licenses in the command-line mode, by using License Server Management Tool.

To add licenses in the command-line mode

1. Run **cmd.exe** to open the Command Prompt window.
2. Go to the folder where License Server is installed. By default, the folder name is: **%Program Files%\Acronis\SnapDeploy\LicenseServerConsole**

3. Run the following command:

    `LicenseServerCmdLine--import-file<server name><file name>`

    In this command:

    - `<server name>` is the name of the machine where License Server is installed.
    - `<file name>` is the name of the .txt or .eml file with the license keys.

For the complete syntax of License Server Management Tool, see "Using License Server Management Tool".

Example

The following command adds the license keys from the file **C:\Licenses.txt** to the license server **mymachine**:

```
licenseservercmdline --import-file mymachine c:\Licenses.txt
```


Using License Server Management Tool

License Server Management Tool is a command-line utility for controlling License Server. The tool is the `LicenseServerCmdLine.exe` file located in the installation folder. By default, the folder name is `%ProgramFiles(x86)%\Acronis\License Server\` in 64-bit Windows systems, or `%ProgramFiles%\Acronis\License Server\` in 32-bit Windows.

The management tool uses the following syntax:

`LicenseServerCmdLine<command><option1><option2> ...`

The management tool supports the following commands and parameters:

`--list`

> Displays the list of license servers found on the local network.

`--status<server name or IP address>`

> Displays the status of the specified license server, which is the number of total and available licenses for each Acronis product.

`--import<server name><license key>`

Adds a new license key. You can specify multiple license keys by separating them with a space.

`--import-file<server name><file name>`

Imports license keys from a .txt or an .eml file.

`--help`

Shows usage information.

Deployment tools

Before deployment, each target machine must boot into a dedicated bootable component of Acronis Snap Deploy 6. An example of such component is Agent.

The machine can boot into the component in either of these ways:

- From a physical media (such as a DVD or a USB drive) that contains the component. Such media is called a bootable media.
- Over the network, by using Acronis PXE Server with the component uploaded to it.

This section describes how to create a bootable media or configure the PXE server.

Bootable components

Acronis Snap Deploy 6 has a number of bootable components that can perform operations on any PC-compatible hardware, including bare metal and machines with unsupported file systems.

- **Agent** boots on a target machine to enable deployment performed by OS Deploy Server.
- **Master Image Creator** boots on a master machine and creates an image of the system.
- **Standalone Utility** boots on a target machine and performs deployment on its own.
- **Command-Line Utility** provides a command-line interface for performing imaging and deployment, and for sending e-mail notifications about deployment.
- **Acronis System Report** boots on a machine, collects information about the machine, and saves this information to a removable USB drive (such as a USB flash drive). For details, see "Collecting system information".

Creating a bootable media

You can create two types of bootable media:

- **Acronis bootable media** (recommended in most cases) is based on a Linux kernel and contains bootable components of Acronis Snap Deploy 6. To create this type of media, use the **Bootable Media Builder** wizard.
- **WinPE-based bootable media** is based on Windows Preinstallation Environment (WinPE) and contains bootable components of Acronis Snap Deploy 6. To create this type of media, use the **PE Builder** wizard.

Both types of media provide similar graphical user interface but differ in the set of bootable components they contain. Generally, you can use an Acronis media. You may want to use a WinPE-based media if the machine's hardware, such as network adapters, is not properly recognized from the Acronis media, or if you need to use the command-line interface.

You can create a bootable media on a physical media, such as a DVD or a USB drive. Acronis PXE Server with uploaded bootable components can also be thought of as a kind of bootable media. That is why you can create a bootable media or upload bootable components to the PXE server by using the same wizards. Alternatively, you can configure the PXE server directly.

Acronis bootable media

Acronis bootable media is a physical media (CD, DVD, USB flash drive, or other media supported by the machine's BIOS as a boot device) that contains bootable components of Acronis Snap Deploy 6.

Acronis bootable media supports both BIOS and UEFI architecture.

You can create an Acronis bootable media containing one or more of the following bootable components:

- **Agent**
- **Master Image Creator**
- **Standalone Utility**
- **Acronis System Report**

To create a bootable media

1. Start the management console.
2. On the **Tools** menu, click **Create bootable media**.
3. [Optional] Specify the parameters of the Linux kernel. Separate multiple parameters with spaces.

   For example, to be able to select a display mode for a bootable component each time the media starts, type: **vga=ask**

   For a list of parameters, see Kernel parameters.
4. Select the bootable components that will be placed on the media.

   For example, if you select Agent and Master Image Creator, you will be able to use such bootable media to perform deployment by using OS Deploy Server, and to create a master image.
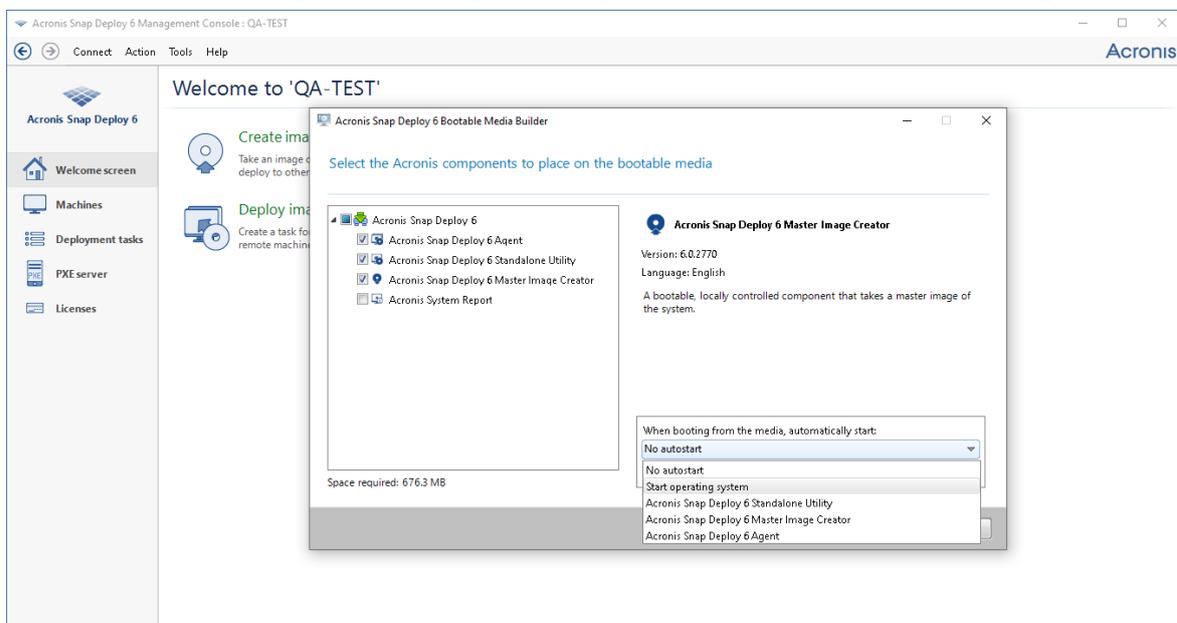
Selecting bootable components

5. Under **When booting from the media, automatically start**, select the component that will start automatically after a time-out you specify. Such component is also referred to as the

default boot menu item. The possible choices are the following:

- One of the components on the media: The component will start after the time-out.
- **No autostart**: The Acronis loader will display the boot menu and wait for someone to select whether to boot the operating system or one of the Acronis components.
- **Start operating system**: The operating system, if present on the booting machine's hard disk, will start after the time-out. This option is designed to make the target machine boot into the deployed operating system after deployment. The main usage scenario is as follows.
  - You use this wizard to configure the PXE server for deployment on a schedule. You set up the agent to start automatically. After the deployment is completed, the target machine reboots into the agent again and might be deployed by another deployment operation. How to avoid this situation?

    To ensure that the target machine boots into the deployed operating system *after the deployment*, choose the **Start operating system** option in this step of the wizard. To ensure that the target machine boots into the agent *before the deployment*, tune the PXE server to work with your deployment server when setting up the deployment.

    Note
    When booting from media, automatically start option does not apply when Acronis bootable media loads in the UEFI mode.

    ---

6. Under **Start automatically after**, specify the time-out interval in seconds. For example, if you choose to automatically start the agent, and set this parameter to **10**, the agent will launch 10 seconds after the boot menu is displayed.

7. If you are placing the agent on the media, specify whether the agent will connect to a particular OS Deploy Server. This setting allows you to have multiple deployment servers that perform different functions on the same network.

   To specify a deployment server, type its name or IP address in **Server name/IP**.

   Note
   Acronis bootable media uses NetBIOS networking protocol to resolve OS Deploy Server in a network. NetBIOS protocol uses ANSI characters for host names. So, machines that have non-English characters in their names cannot be accessed from Acronis bootable media. If the name of the OS Deploy Server machine contains non-English characters, use the machine's IP address to specify it in the network.

   The deployment server (along with the network settings for the agent) can also be specified onsite (on the target machine's side) when booting the agent. To be able to configure the agent onsite, set up a reasonable delay before the default network settings will be applied. For details, see "Booting the target machines".

   If not configured in either way, the deployment server will be found automatically. The agent will start the search after the number of seconds you specify in **Timeout (sec)**.
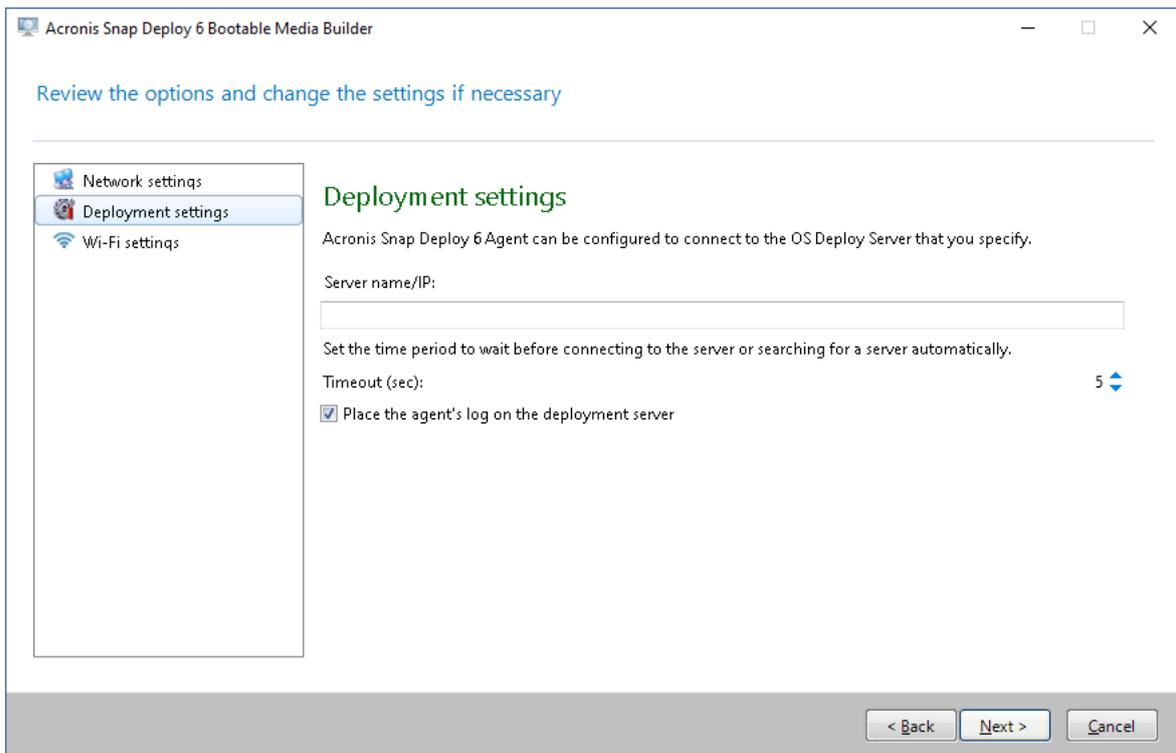
Settings for the agent

The option to save the agent's log to the deployment server is designed primarily for troubleshooting. The log will be available on the deployment server in the following folder:

%AllUsersProfile%\Application Data\Acronis\DeployServer\AgentsLogs

8. Select the type of bootable media to create. You can:
   - Create a CD, a DVD, or other media such as a USB flash drive if the hardware BIOS allows for booting from such media.
   - Create an ISO image of a bootable disc to burn it later onto a blank disc or writing it to a USB flash drive.
   - Upload the selected components to Acronis PXE server. The previously uploaded components will be deleted from the PXE server before uploading the newly selected ones.

   Note
   Standalone Utility can be placed on a physical media only. This component is not designed to boot from a PXE server.

   If you have chosen to create a physical media, insert a blank disc (so the software can determine its capacity) or attach a USB flash drive.

   If you have chosen to create an ISO image of a bootable disc, specify the name of the ISO file and the folder in which to place it.

   If you have chosen to upload the components to a PXE server, specify the name of the machine with the PXE server and provide the user name and password of an administrator on that machine.

9. [Optional] Protect the components being uploaded to the PXE server with a password to prevent the components from unauthorized execution. The password prompt will come up when selecting a bootable component. No password is required to start the operating system on the machine.
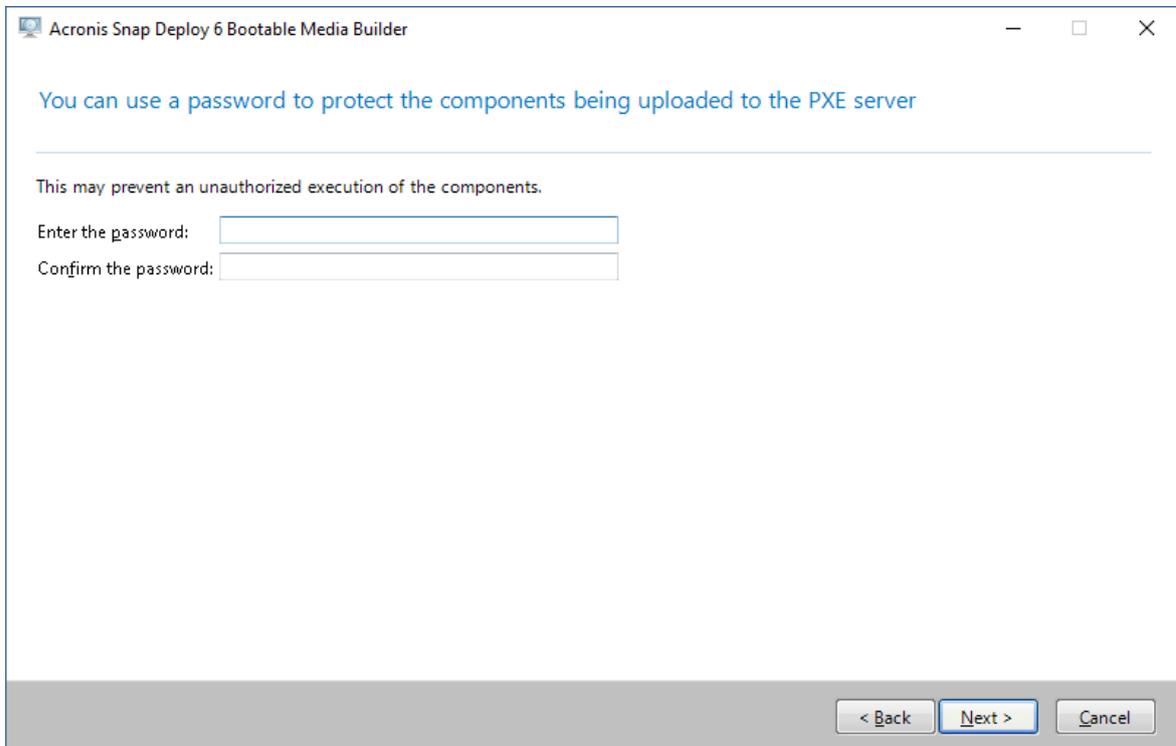
Protecting the bootable components with a password

10. Click **Create**. After you create the disc, mark it and keep it in a safe place.

Note

Components on an Acronis bootable media are based on a Linux kernel and are equipped with the Linux system and device drivers. Acronis regularly supplements the driver set with drivers for new devices. However, there may be a chance of drivers being incompatible with your hardware, so a bootable component cannot start, stops responding or cannot access the necessary device. In this case, consider creating a WinPE-based bootable media instead.

Kernel parameters

This window lets you specify one or more parameters of the Linux kernel. They will be automatically applied when the bootable media starts.

These parameters are typically used when experiencing problems while working with the bootable media. Normally, you can leave this field empty.

You can also specify any of these parameters by pressing F11 while in the boot menu.

Parameters

When specifying multiple parameters, separate them with spaces.

acpi=off

Disables Advanced Configuration and Power Interface (ACPI). You may want to use this parameter when experiencing problems with a particular hardware configuration.

noapic

Disables Advanced Programmable Interrupt Controller (APIC). You may want to use this parameter when experiencing problems with a particular hardware configuration.

vga=ask

Prompts for the video mode to be used by the bootable media's graphical user interface. Without the **vga** parameter, the video mode is detected automatically.

vga=_mode_number_

Specifies the video mode to be used by the bootable media's graphical user interface. The mode number is given by _mode_number_ in the hexadecimal format—for example: **vga=0x318**

Screen resolution and the number of colors corresponding to a mode number may be different on different machines. We recommend using the **vga=ask** parameter first to choose a value for _mode_number_.

quiet

Disables displaying of startup messages when the Linux kernel is loading, and starts the management console after the kernel is loaded.

This parameter is implicitly specified when creating the bootable media, but you can remove this parameter while in the boot menu.

Without this parameter, all startup messages will be displayed, followed by a command prompt. To start the management console from the command prompt, run the command: **/bin/product**

nousb

Disables loading of the USB (Universal Serial Bus) subsystem.

nousb2

Disables USB 2.0 support. USB 1.1 devices still work with this parameter. This parameter allows you to use some USB drives in the USB 1.1 mode if they do not work in the USB 2.0 mode.

nodma

Disables direct memory access (DMA) for all IDE hard disk drives. Prevents the kernel from freezing on some hardware.

nofw

Disables the FireWire (IEEE1394) interface support.

nopcmcia

Disables detection of PCMCIA hardware.

nomouse

Disables mouse support.

*module_name***=off**

Disables the module whose name is given by *module_name*. For example, to disable the use of the SATA module, specify: **sata_sis=off**

pci=bios

Forces the use of PCI BIOS instead of accessing the hardware device directly. You may want to use this parameter if the machine has a non-standard PCI host bridge.

pci=nobios

Disables the use of PCI BIOS; only direct hardware access methods will be allowed. You may want to use this parameter when the bootable media fails to start, which may be caused by the BIOS.

pci=biosirq

Uses PCI BIOS calls to get the interrupt routing table. You may want to use this parameter if the kernel is unable to allocate interrupt requests (IRQs) or discover secondary PCI buses on the motherboard.

These calls might not work properly on some machines. But this may be the only way to get the interrupt routing table.

WinPE-based bootable media

Windows Preinstallation Environment (WinPE) is a minimal Windows system. WinPE is commonly used by original equipment manufacturers (OEMs) and corporations for deployment, test, diagnostic and system repair purposes.

Similarly to creating an Acronis bootable media, you can create a bootable media that is based on WinPE and includes bootable components of Acronis Snap Deploy 6.

You may want to use a WinPE-based media instead of an Acronis bootable media for the following purposes:

- Performing imaging or deployment to machines with hardware that is not properly recognized by the Acronis bootable media (which is based on a Linux kernel)
- Performing deployment in the command-line mode; for example, to deploy different master images to different target machines
- Sending e-mail notifications about deployment

Note
WinPE-based bootable media of versions earlier than 4.0 do not support UEFI booting.

Components included in the bootable media

Each WinPE-based bootable media contains the following bootable components:

- **Agent**
- **Master Image Creator**
- **Command-Line Utility**
- **Standalone Utility**

PE Builder

PE Builder is a dedicated tool for creating a WinPE-based bootable media. The tool is installed with Management Console.

PE Builder creates the bootable media by adding components of Acronis Snap Deploy 6 to a source file called a PE image.

Note

The term "image" in "PE image" is unrelated to the notion of "master image."

A PE image is normally a .wim file. PE Builder can create a PE image automatically or use a PE image you provide.

Note

PE Builder also creates the **<AcronisMedia>.sdi** file, along with the PE image. This file must be in the same location as the PE image if you plan to use the image for online deployment.

PE Builder supports WinPE distributions that are based on any the following kernels:

- Windows Vista (PE 2.0)
- Windows Vista SP1 and Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) with or without the supplement for Windows 7 SP1 (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE for Windows 10.0)

PE Builder supports both 32-bit and 64-bit WinPE distributions. The 32-bit WinPE distributions can also work on 64-bit hardware. However, you need a 64-bit distribution to boot a machine that uses Unified Extensible Firmware Interface (UEFI).

Note

PE images based on WinPE 4 and later require approximately 1 GB of RAM to work.

Preparation: WinPE 2.x and 3.x

To be able to create or modify PE 2 or 3 images, install Management Console on a machine where Windows Automated Installation Kit (AIK) is installed. If you do not have a machine with the AIK, prepare it as follows.

To prepare a machine with the AIK

1. Download and install the AIK.

   AIK for Windows Vista (PE 2.0):

   https://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en

   AIK for Windows Vista SP1 and Windows Server 2008 (PE 2.1):

   https://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=en

   AIK for Windows 7 (PE 3.0):

   https://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en

   AIK Supplement for Windows 7 SP1 (PE 3.1):

   https://www.microsoft.com/download/en/details.aspx?id=5188

   You can find system requirements for installation by following the above links.
2. [Optional] Burn the AIK to DVD or copy to a flash drive.
3. Install the Microsoft .NET Framework from this kit (NETFXx86 or NETFXx64, depending on your hardware).
4. Install Microsoft Core XML (MSXML) 5.0 or 6.0 Parser from this kit.
5. Install the AIK from this kit.
6. Install Management Console on the same machine.

It is recommended that you familiarize yourself with the help documentation supplied with the AIK. To access the documentation, select **Microsoft Windows AIK -> Documentation** from the start menu.

Preparation: WinPE 4.0 and later

To be able to create or modify PE 4 or later images, install Management Console on a machine where Windows Assessment and Deployment Kit (ADK) is installed. If you do not have a machine with the ADK, prepare it as follows.

To prepare a machine with the ADK

1. Download and install the ADK.

   ADK for Windows 8 (PE 4.0): https://www.microsoft.com/en-us/download/details.aspx?id=30652

   ADK for Windows 8.1 (PE 5.0): https://www.microsoft.com/en-US/download/details.aspx?id=39982

ADK for Windows 10, version 1903 (PE for Windows 10.0): https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install

You can find system requirements for installation by following the above links.

2. Install Management Console on the same machine.

Adding Acronis Snap Deploy 6 components to WinPE

To add the bootable components to WinPE ISO:

1. Start Management Console.
2. On the **Tools** menu, click **Create PE image**.
3. Do one of the following:
    - If you do not have a PE image to base the media on, click **Create WinPE automatically**.
    - If you want to base the bootable media on a specific PE image, click **Use WinPE files located in the folder I specify**, and then specify the folder with the WIM file of the image.
4. In **Network settings**, specify whether the agent will connect to a particular OS Deploy Server.
5. In **Autostart**, specify whether to start the agent automatically after a time-out.
6. Select how you want to create the bootable media.
    - If you want to create a physical media, select **ISO image**. The software will create an ISO file that you can later burn to a DVD or write to a USB drive.
    - If you want to upload the bootable components to Acronis PXE server, select **Acronis PXE Server**.

      Note
      Standalone Utility can be placed on a physical media only. This component is not designed to boot from a PXE server.

    - If you want to create a PE image (a WIM file) to later upload it to the PXE server, select **WIM image**. You may want to select this setting if you are planning to use Preinstallation Environment for unattended deployment to specific machines. If so, make sure that you have selected to start the agent automatically (see the previous step).

      Note
      The setting **WIM image** enables you to create a PE image for any future purpose, such as for adding other tools in addition to Acronis components.

7. Do one of the following:
    - If you have chosen to create an ISO or a WIM file, specify the full path to the resulting file, including the file name.
    - If you have chosen to upload the components to Acronis PXE Server, specify the machine with the PXE server and provide the user name and password of an administrator on it.
8. [Optional] Specify the Windows drivers to be added to Windows PE.

Once you boot a machine into Windows PE, the drivers can help you access the device where the image is located. Add 32-bit drivers if you use a 32-bit WinPE distribution or 64-bit drivers if you use a 64-bit WinPE distribution.

Also, you will be able to point to the added drivers when configuring Universal Deploy. For using Universal Deploy, add 32-bit or 64-bit drivers depending on whether you are planning to deploy a 32-bit or a 64-bit Windows operating system.

To add the drivers:

- Click **Add** and specify the path to the necessary *.inf file for a corresponding SCSI, RAID, SATA controller, network adapter, or other device.

- Repeat this procedure for each driver you want to be included in the resulting WinPE bootable media.

9. Check your settings in the summary screen, and then click **Create**.

10. If you have chosen to create an ISO file, burn the file to a DVD by using a third-party tool, or write the file to a USB drive.

Uploading a PE image to Acronis PXE Server

You can upload a PE image created by using PE Builder to Acronis PXE Server.

To upload a PE image

1. Start Management Console.
2. Click **PXE server**. If prompted, specify the machine where Acronis PXE Server is installed.
3. Click **Upload PE image**.
4. Specify the path to the WIM file that you want to upload.
5. Check your settings in the summary screen, and then click **Create**.

Configuring a mutlicast range on the OS Deploy Server

You can run multiple multicast deployment tasks in parallel on the same OS Deploy Server. When multiple OS Deploy Servers are running in the network, they might use the same multicast address which will cause conflicts among deployment tasks that run simultaneously. To ensure that multiple deployment tasks can be executed in parallel without networking conflicts, you can define different ranges of IPv4 multicast addresses on each OS Deploy Server in the network.

Note
If you start multiple deployment tasks in parallel on the same OS Deploy Server, each deployment task will use an individual multicast address selected randomly from the defined range.

To assign a range of multicast addresses that an OS Deploy Server can use

1. Start the Management Console.
2. Connect the management console to the OS Deploy Server.
3. In the **Action** menu, click **Manage server settings**.

4. In the **Server settings** dialog, enter the minimum and maximum address of the range that the server can use for deployment tasks.
The minimum and maximum addresses are included in the range.

5. Click **OK**.
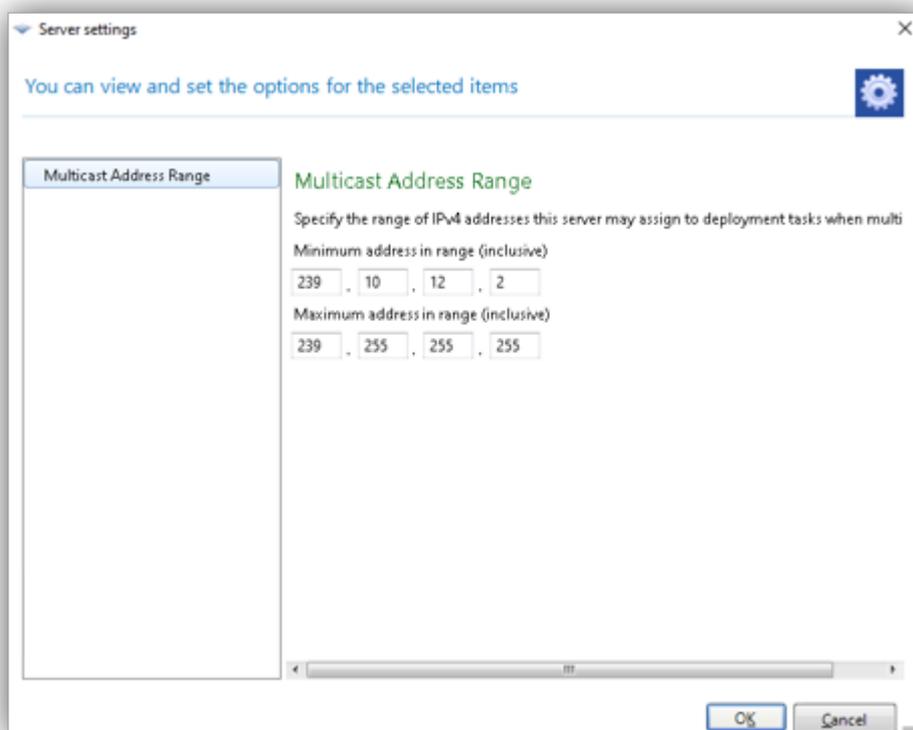
Configuring Acronis PXE Server

You can configure Acronis PXE server:

- When creating an Acronis bootable media or a WinPE-based bootable media.
- When creating a bootable media for user-initiated deployment.

Alternatively, you can use direct server configuration, as follows.

To perform a direct configuration of the PXE server

1. Start Management Console.

2. In the navigation pane, click **PXE server**.

3. If the PXE server is installed on a different machine, click **Connect to the PXE server**, and then specify the name or IP address of that machine. In logon settings, specify the user name and password of an administrator on that machine.

When connected to the PXE server, you can perform the following operations by clicking the corresponding buttons on the toolbar:

- **Upload components**: Upload bootable components, such as Agent, in the same way as when creating an Acronis bootable media. The previously uploaded components will be deleted from the PXE server before uploading the newly selected ones.
- **Upload PE image to PXE**: Upload the Preinstallation Environment (PE) image (a .wim file) that was previously created with PE builder. For details, see "Uploading a PE image to Acronis PXE Server".
- **Remove**: Remove a component or PE image from the PXE server.
- **Disable PXE Server**: Disable the PXE server. The service does not stop, but no longer responds to incoming requests.
- **Enable PXE Server**: Enable the previously disabled PXE server.
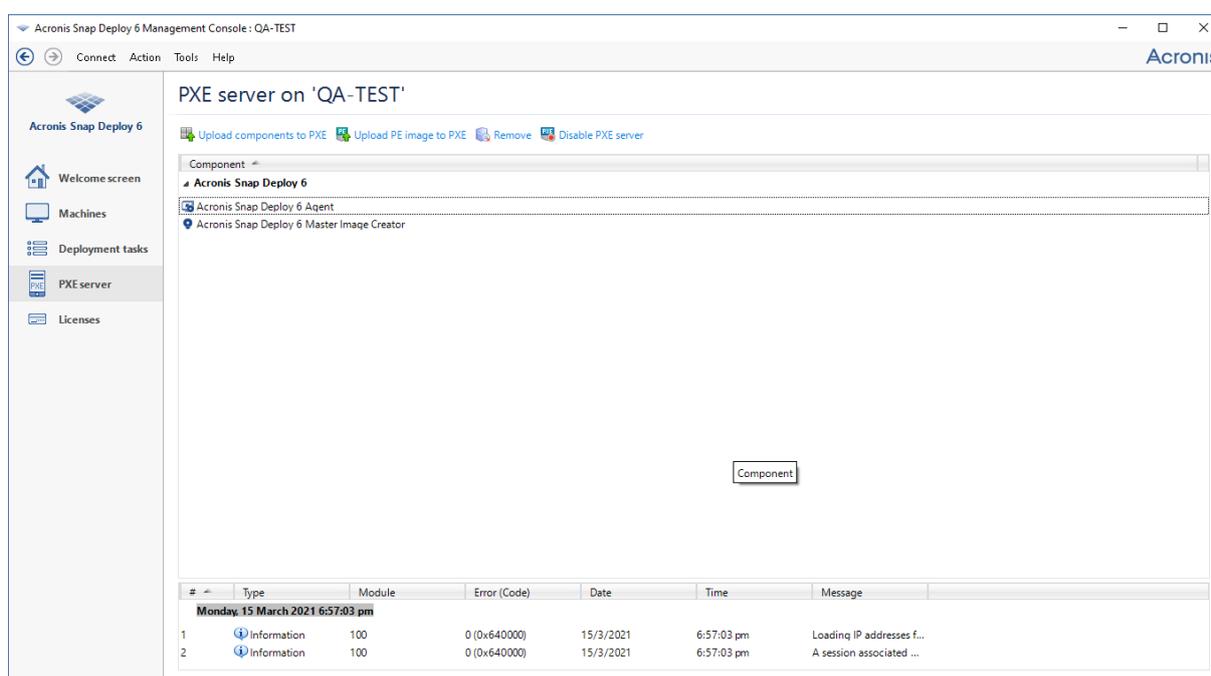
Two bootable components of Acronis Snap Deploy 6 are uploaded to the PXE server.

Creating a master image

To be able to deploy a system, you need to create the desired system configuration and then to save an image of the system's hard disk or volume to a network folder, detachable media (such as a USB drive) or removable media (such as a DVD).

This section describes how to create a master image by using Acronis Snap Deploy 6.

In addition, Acronis Snap Deploy 6 can use any of the following files as a master image:

- Backups created by the following Acronis products, including password-protected archives:
  - (TIB format) Acronis True Image, Acronis Backup & Recovery 10, Acronis Backup & Recovery 11, Acronis Backup 11.5, Acronis Backup 11.7
  - (TIBX format) Acronis Cyber Protect 15, Acronis Cyber Protect Cloud

  Note
  Deployment can be performed only from the most recent backup from the archive, so if it contains a set of full and incremental backups, the deployment will always use the latest incremental backup.

- Virtual Hard Disk files (VHD and VHDX format).

Preparation of the master operating system

In the Acronis environment and Windows Preinstallation Environment (any case except the command-line mode), Acronis Snap Deploy 6 automatically configures each of the deployed systems by using the deployment settings you specify.

Alternatively, you can prepare a master operating system by using the Microsoft System Preparation Tool (Sysprep) before creating the image of the system. Acronis Snap Deploy 6 does not configure the deployed systems in this case.

The Sysprep tool is designed for corporate system administrators, original equipment manufacturers (OEMs), and others who need to deploy and automatically configure operating systems on multiple machines.

After an operating system that was prepared with Sysprep is deployed to machines, Sysprep configures settings that are normally unique to each machine. In particular, Sysprep does the following:

- Generates a unique security identifier (SID) for the new machines
- Initiates Windows mini-setup for Plug and Play devices
- Applies the machine name, domain or workgroup membership, and other settings specified in the Sysprep.inf answer file

You can either download Sysprep from the Microsoft Web site, or extract it from the deploy.cab file, which is located on the installation disk of Windows NT, Windows 2000, Windows XP, and Windows

Server 2003. In Windows Vista, Windows 2008, and Windows 7, the Sysprep tool is located in the folder Windows\System32.

> **Important**
> If you are planning to use Sysprep, we strongly recommend that you read articles about Sysprep and disk duplication in the Microsoft Knowledge Base.

Online vs. offline imaging

You can create the master image in either of these ways:

- In Windows, by using Management Agent installed on the master machine. This type of imaging is called *online imaging*.
- By using a bootable media (either Acronis media or WinPE-based media) with Master Image Creator, or by using the command-line utility in a WinPE-based bootable media. This type of imaging is called *offline imaging*.

This section describes imaging with Management Agent and Master Image Creator. For information about imaging in the command-line mode, see "Command-line mode and scripting under WinPE".

Performing online imaging

Online imaging means that the master system is imaged live (without restarting the machine or suspending operations). Online imaging can be performed remotely whenever you need. The disadvantage is that you have to install imaging software that is included in the master image. This is not always rational.

To perform online imaging

1. Install Management Console.
2. Configure the master system.
3. Install Management Agent on the master system either locally by using the setup program, or remotely by using Management Console. Once Management Agent is installed, you can image the master system online (without a restart) at any time.
4. Start the Management Console.
5. Connect to the master machine.
6. Click **Create image -> Next -> A master image**.

   > **Note**
   > The alternative selection, **A bootable media**, enables you to create a bootable media for offline imaging.

7. Follow the steps of the Master Image Creator wizard.

Performing offline imaging

Offline imaging means that the master system is stopped and the master machine boots into the Acronis environment or into Windows Preinstallation Environment.

To perform offline imaging

1. Install Management Console.
2. Do one of the following:

    -   Create a bootable media that contains Master Image Creator.

    OR

    -   Install Acronis PXE Server, connect the console to the PXE server, and upload Master Image Creator. Make sure that network booting is enabled on the master machine.

    Note

   While creating the bootable media or uploading Master Image Creator to the PXE server, you can configure the image creator to start automatically after a time-out.

    ---

3. Configure the master system.
4. Depending on your choice in step 2, boot the master machine into Master Image Creator from the bootable media or from the PXE server.

   The boot menu appears on the master machine.
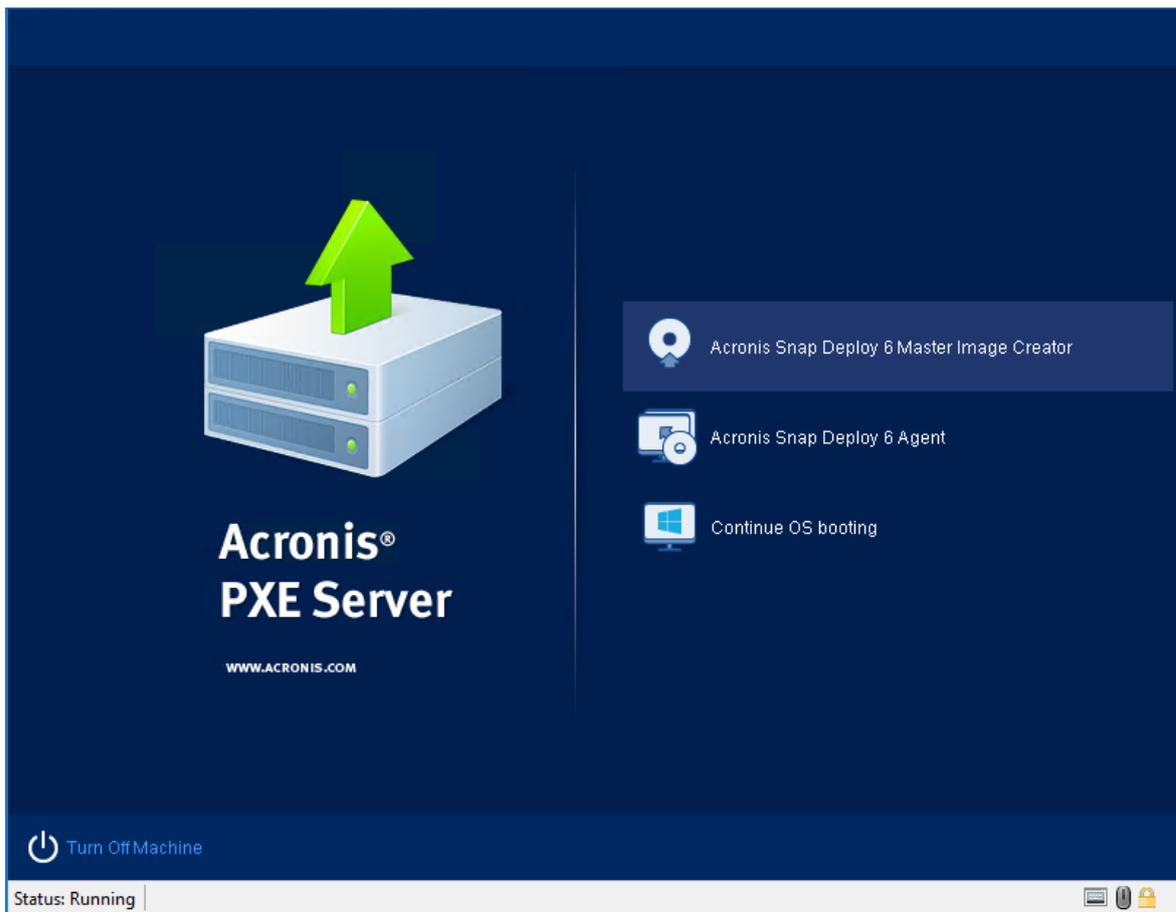
The boot menu on the master machine

If the boot menu does not appear and the machine has Secure Boot enabled, we recommend temporarily disabling Secure Boot on this machine as a workaround.

5. In the boot menu, click **Master Image Creator**.

6. The master image creator establishes a network connection to be able to save the image in a network folder. A dialog box appears asking whether you want to configure the network connection that will be used by the image creator.

   By default, Master Image Creator uses DHCP auto configuration. Ignore the prompt (click **Cancel**) if there is a DHCP server on the network or the image has to be placed on a local hard disk or a removable media.
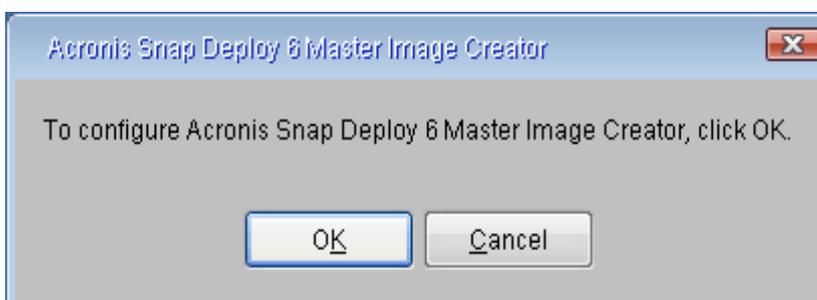
Prompt for configuring the master image creator

The master image creator can be preconfigured to apply the default network settings automatically after a time-out.

The manual configuration is needed if automatic configuration is not possible (no DHCP server on the network) or does not succeed. To configure the network connections manually, click **OK** in the prompt window.
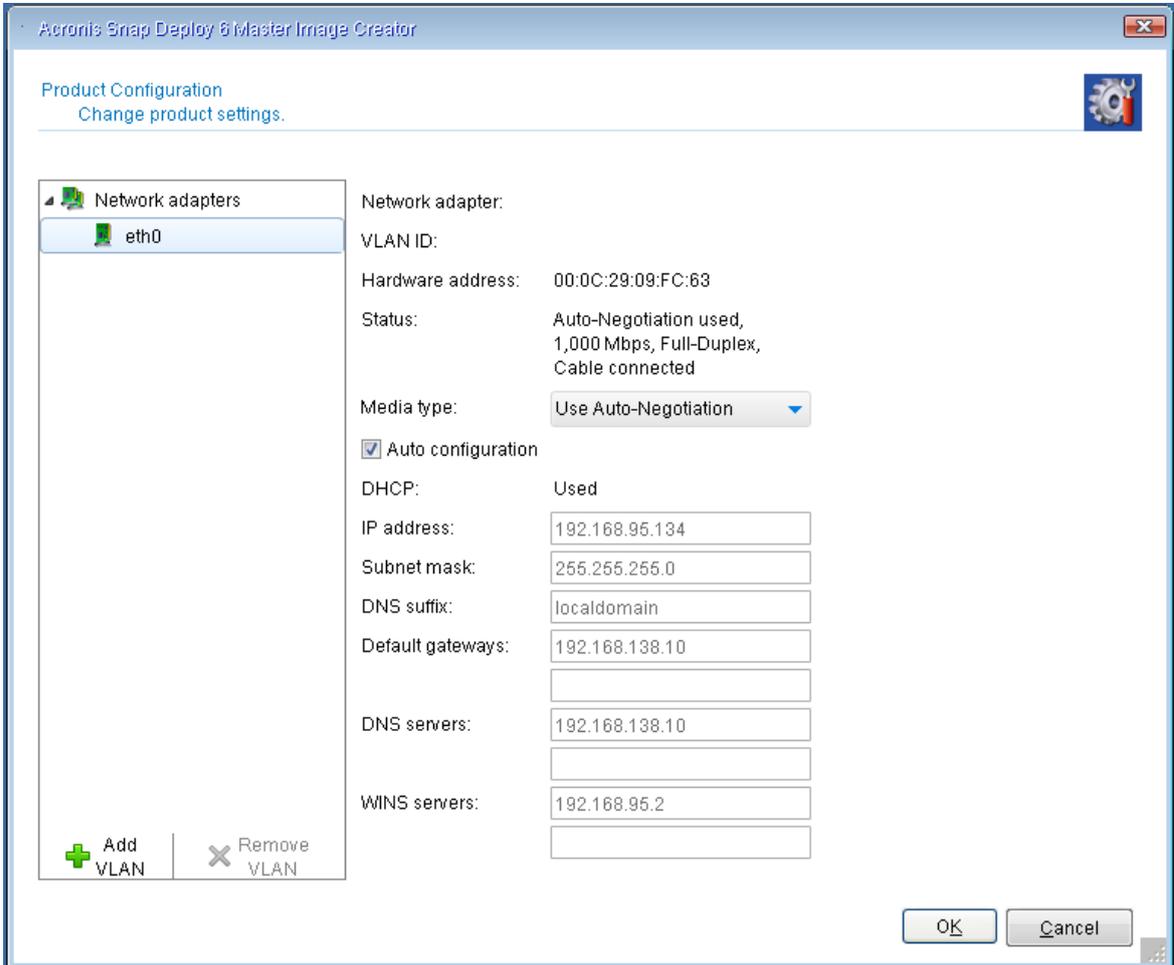
Master Image Creator configuration: network settings

The **Product configuration** window allows you to configure network settings for each network interface card (NIC) of the machine.

Changes made during a session will be lost after the machine reboots.

Adding VLANs

In the **Product configuration** window, you can add virtual local area networks (VLANs). Use this functionality if you need access to a backup location that is included in a specific VLAN.

VLANs are mainly used to divide a local area network into segments. A NIC that is connected to an access port of the switch always has access to the VLAN specified in the port configuration. A NIC connected to a trunk port of the switch can access the VLANs allowed in the port configuration only if you specify the VLANs in the network settings.

Set the preferable values and click **OK**.

> **Note**
> The VLAN settings configured on the Windows machine where you run the Media Builder are included in the created Linux-based media automatically, so you do not need to create them manually after booting from this media.

Master Image Creator configuration: Wi-Fi settings

You can configure Linux-based media to connect to a Wi-Fi network after booting. Thus, on machines with no Ethernet connection, the media can connect to an OS Deploy Server via Wi-Fi and start the deployment from there.

Configuring the Wi-Fi settings

In the **Product configuration** window, click **Wi-Fi settings** and select one of the available Wi-Fi networks. A dialog will prompt you to enter the password. Enter the password and click **Join**.

The Wi-Fi connection details will be included in the Linux-based media during media creation, so after booting, the machine will connect to the specified WI-Fi network automatically.

When the Master Image Creator starts, it displays the Master Image Creator welcome window.

7. In this window, click **Next**, and then follow the steps of the Master Image Creator wizard.

Steps of the Master Image Creator wizard

This section describes the steps of the Master Image Creator wizard in the order that they appear.

Use the **Next** and **Back** buttons to go between steps.

Disks or volumes to image

Select the disks or volumes that you want to include in the master image.

You can select any set of disks and volumes. The master boot record (MBR) will be also included in the image.

> **Important**
> An operating system includes a loader: a small program that loads the main part of the operating system. The loader and the rest of the operating system may reside on different volumes. For example, Windows 7 and Windows Server 2008 R2 place the loader on a hidden volume called **System Reserved**. If your operating system and its loader reside on different volumes, always include both volumes in the image. A volume with the loader is usually marked as the active volume and is shown with the **Act.** flag in the list. The volumes must also be deployed together; otherwise, there is a high risk that the operating system will not start.

> **Note**
> Also, machines with UEFI architecture have a special ESP partition (EFI System partition). If you are deploying a UEFI machine image to another UEFI machine, you should deploy ESP partition as well. Otherwise, the target machine will be non-bootable after deployment. When deploying a UEFI machine image to a BIOS machine, it is not necessary to deploy the ESP partition.
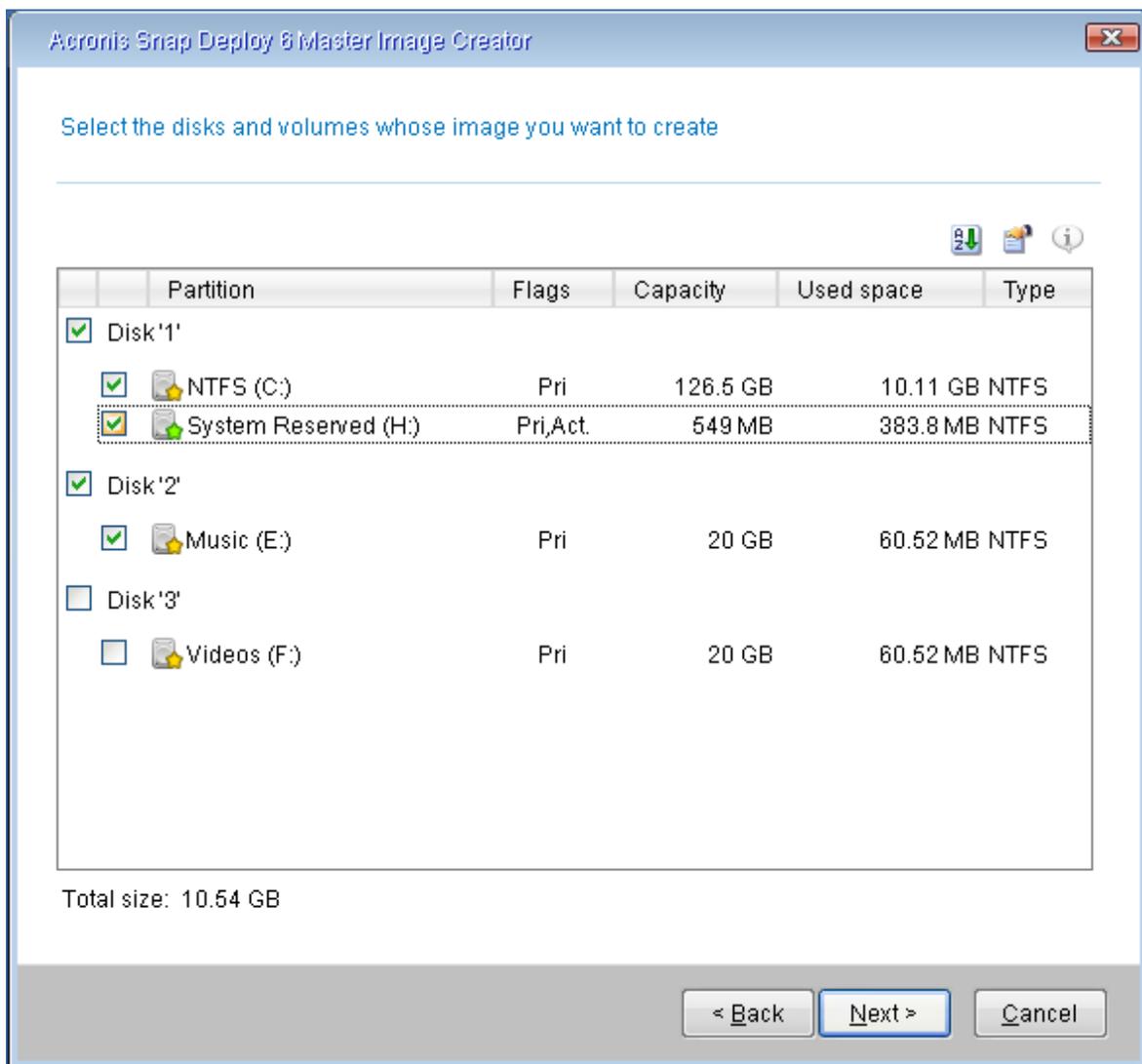
Selecting disks and volumes to image

Image name and location

Master Image Creator can save an image in any of the following locations:

- In a network folder
- On an internal hard disk of the master machine
- On a USB or FireWire (IEEE-1394) storage device (such as a flash drive) that is attached to the master machine
- On a DVD+R/RW, DVD-R/RW, CD-R/RW, or recordable Blue-ray Disc (BD-R, BD-RE) that is loaded in the media drive of the master machine

A sizeable image can be split between multiple media automatically.

Select the image location in the device tree. In **File name**, type the file name of the image. To generate a file name that is unique in the selected location, click **Generate a name for the file**.
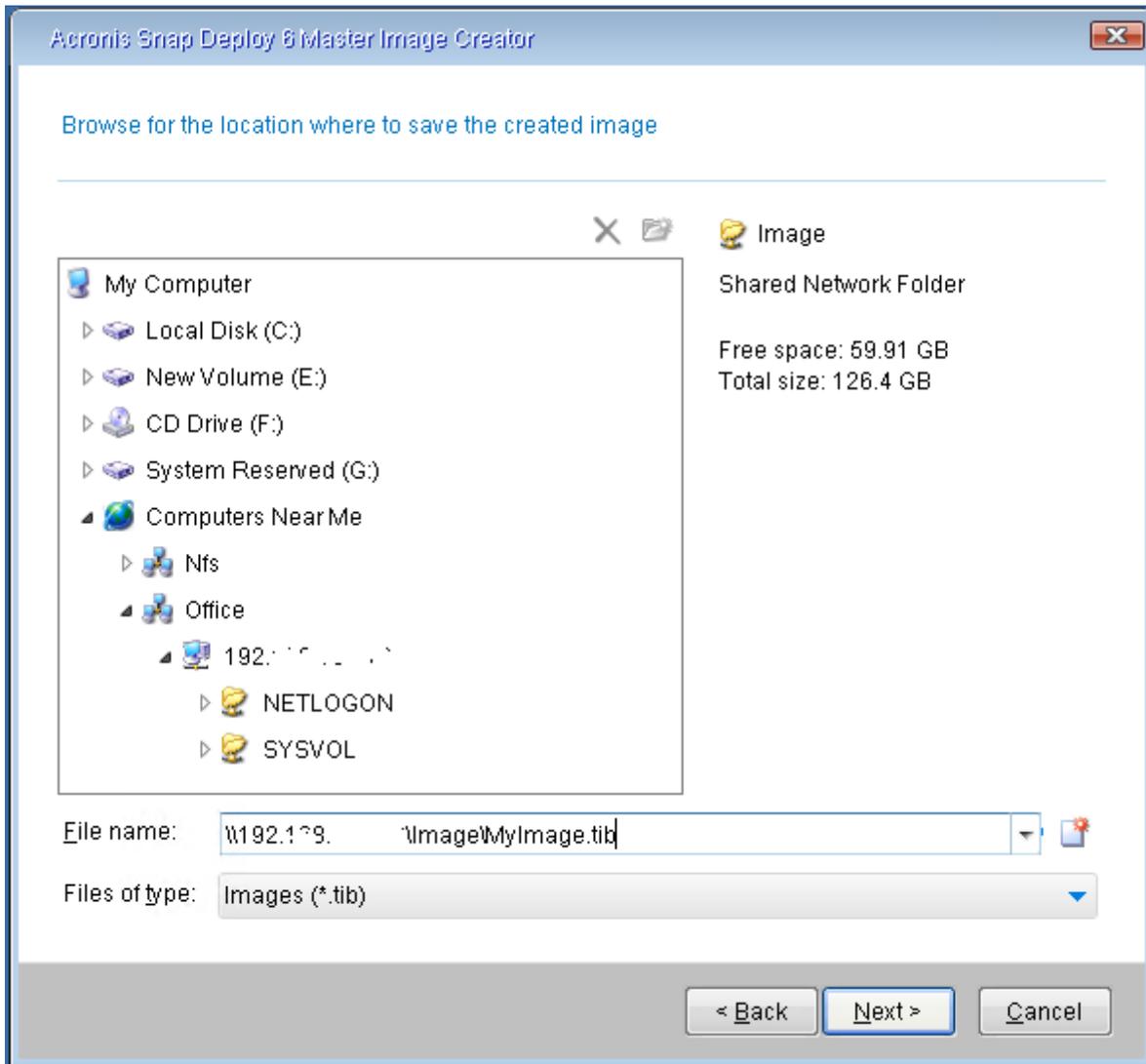
Note
Acronis bootable media uses NetBIOS networking protocol to resolve OS Deploy Server in a network. NetBIOS protocol uses ANSI characters for host names. So, machines that have non-English characters in their names cannot be accessed from Acronis bootable media. If the name of the OS Deploy Server machine contains non-English characters, use the machine's IP address to specify it in the network.

Options of imaging

Common Options

You can set the following options for both online and offline imaging.

Protection

Protection defines whether to protect the master image with a password or not. You may want to use this option to prevent unauthorized deployment.

By default, there is no password set.

To specify a password, type it in the **Enter the password** field and, again, in the **Confirm the password** field.

Important

Setting a password does not encrypt the contents of the master image.

Compression

Compression defines the compression level for the image.

The default is **Normal**. This is recommended in most cases.

Note

A higher compression level will lead to a smaller master image size, but creating the image will take longer.

Splitting

Splitting defines how to split a large master image into two or more files that, together, make up the entire master image.

The options are:

- **Automatic**. (Default)

  When creating the image on a hard disk, if the selected disk has enough space and its file system allows the estimated file size, the Master Image Creator will create a single master image file.

  If the storage disk has enough space, but its file system does not allow the estimated file size, the image will automatically be split into two or more files. This might be the case when the master image is created on FAT16 and FAT32 file systems that have a 4-GB file size limit.

  If free space on the disk runs out while creating an image, the operation will stop with an error.

  When creating an image on a CD-R/RW, DVD-R/RW, DVD+R/RW, or recordable Blu-ray Disc (BD-R, BD-RE), the Master Image Creator will ask you to insert a new disc when the previous one is full.

- **Fixed size. Please, specify the size:**

  Type the desired file size or select it from the list. The master image will be split into multiple files of the specified size. This is useful when creating an image that you plan to burn to multiple discs later on. You can enter the file size in bytes (**B**), kilobytes (**KB**), megabytes (**MB**), gigabytes (**GB**), or terabytes (**TB**).

Note

Creating images directly on CD-R/RW, DVD-R/RW, DVD+R/RW, or recordable Blu-ray Discs usually takes more time than it would on a hard disk.

Error handling

Error handling configures how to handle errors should they occur during imaging.

- **Ignore bad sectors**

  When this option is disabled (the default), the software will display a pop-up window each time it encounters a bad sector and ask for a user decision as to whether to continue or stop imaging.

- **Do not show messages and dialogs while processing (silent mode)**

  If this option is enabled, the software will automatically handle situations requiring user interaction (except handling bad sectors, which is defined by the **Ignore bad sectors** option). If an operation cannot continue without user interaction, it will fail. Details of the operation, including errors, if any, can be found in the operation log.

Additional settings

- **Validate backup archive upon its creation completion**

  If enabled, the program will check the integrity of the image upon creation.

  You can perform this check after imaging.

- **Sector-by-sector mode**

  If this option is disabled, only the sectors containing useful system and user data are imaged (for the supported file systems). When imaging a volume with an unrecognized or unsupported file system, or a disk that contains such volume, the software automatically switches to the sector-by-sector mode.

  If this option is enabled, the master image will contain all sectors of the selected disks or volumes, including unallocated space and those sectors that are free of data. During the deployment, these disks or volumes will be copied to the target machine 'as is', without volume resizing. This approach usually leads to a bigger master image, and makes the imaging or deployment process longer.

- **Reboot the machine automatically after the master image creation is finished**

  If the option is enabled, the machine will restart after the master image creation process is completed.

  For example, if the machine boots from a hard disk drive by default and you select this check box, the machine will be restarted and the operating system will start as soon as the bootable agent has finished creating the image.

- **Ask for first media**

    This defines whether to display the **Insert First Media** prompt when creating master image on a removable media.

    If the option is enabled, creating master image on removable media may not be possible if the user is away, because the program will wait for someone to click **OK** in the prompt box.

    Therefore, you should leave the options disabled when creating a master image to a removable media. Then, if the removable media is available (for example, a DVD is inserted), the task can run unattended.

Online Imaging Options

In additional, there are two options which are only available for online imaging.

Process priority

Process priority defines the priority of the image creation process.

The priority of any process running in the operating system determines the amount of CPU usage and system resources allocated to that process. Decreasing the image creation priority will free more resources for other programs. Increasing the image creation priority will speed up the master image creation by taking resources from the other running processes. The effect will depend on the total CPU usage and other factors.

The default is **Low**.

WinPE-based media

Defines whether to place a WinPE-based bootable media created by using PE Builder on the master image. If you plan to perform deployment to online machines with hardware that is not properly recognized by the Acronis bootable media (which is based on a Linux kernel), these machines can be booted into the media included in the master image. This speeds up the deployment and reduces the network load because the media is not transmitted to the machines over the network.

Comments and summary

We recommend providing a comment for easy identification of the master image.

After you click **Next**, the summary of the imaging procedure appears. Check the settings and then click **Proceed**.

The imaging operation starts and its progress is displayed.
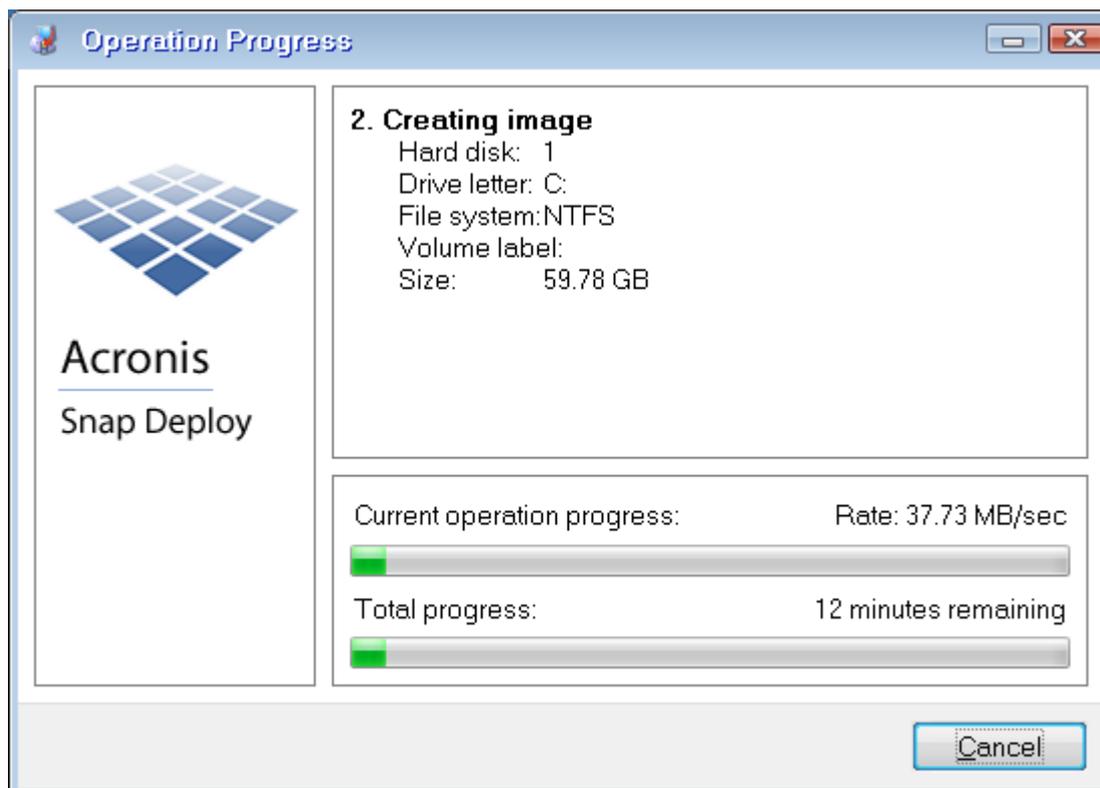
Acronis Snap Deploy 6 is taking the master image

© Acronis International GmbH, 2003-2023

Validating a master image

You can ensure that the master image is not damaged by validating it.

To validate a master image

1. Start Management Console.
2. Connect the management console to a machine where Management Agent is installed.
3. On the **Action** menu, click **Validate image**.
4. Select the master image that you want to validate.
5. Click **Validate** in the summary window.

The validation operation starts. You can stop the operation if need be, by clicking **Cancel**.

After the validation is complete, the software shows the result.

Deploying a master image

This section describes how to deploy a master image to one or more machines.

Warning!
Deployment to a machine involves deleting some or all data that is currently stored on that machine. Make sure that you are performing deployment to the correct machines and to the correct disks on those machines.

Files supported as master images

Acronis Snap Deploy 6 can perform deployment from any of the following files:

- A master image created by Acronis Snap Deploy 6 or an earlier version.
- A disk-level backup created by Acronis True Image, Acronis Backup & Recovery 10, Acronis Backup & Recovery 11, Acronis Backup 11.5, or Acronis Backup 11.7, Acronis Cyber Backup 12.5, or Acronis Cyber Protect 15, including both **.tib** and **.tibx** formats.
- A Virtual Hard Disk (VHD or VHDX) file.

Support for backups created by the Acronis products

Some backups (known as incremental and differential backups) depend on other backups. To ensure that Acronis Snap Deploy 6 finds all of the backups it needs, we recommend leaving the backup in the location where it was created by your Acronis product.

If the backup is split into two or more parts, make sure that all these parts are in the same folder. To specify such a backup, specify any one of these parts.

Support for VHD files

These files store disks and volumes of a machine. Such a file can be created by the following programs:

- Microsoft Virtual PC 2007 SP 1.0, Windows Virtual PC, and Microsoft Virtual Server
- Windows built-in backup utilities (starting with Windows 7)
- Acronis True Image Home 2010 and later

If the VHD file is split into two or more parts, make sure that all these parts are in the same folder. To specify the VHD file, select any one of these parts.

Licenses for deployment

OS Deploy Server performs deployment to a machine by using an available machine license or deployment license. Once used by one machine, the license cannot be reused by another machine.

A machine license becomes used when the first deployment to the machine starts. The license remains used regardless of the result of deployment.

Normally, a deployment license becomes used if the deployment has been successful. If the deployment has failed, OS Deploy Server can use the license for another deployment to the same machine or to a different machine.

In some cases, a deployment license becomes used even if the deployment has failed. OS Deploy Server will use the license for the next deployment to the same machine.

Deployment templates

A deployment template is a set of configuration parameters of the deployment operation. These parameters include:

- A path to the master image.
- The operation mode (multicast or unicast, how to handle the target disk free space, and so on).
- Settings to be applied to the deployed systems (for example, machine names and user accounts).
- Operations to be performed on the deployed systems (transfer files, run applications, shut down, restart).

All deployment templates are saved on OS Deploy Server. You can use a saved template in the future.

When setting up a deployment operation (deployment task), you must specify a deployment template. You can simply select a saved template and set up the condition for starting deployment. Alternatively, you can create a new template.

Templates also enable user-initiated deployment. In this mode, users can perform one-click deployment to their machines without the administrator's assistance. To set up this mode, the administrator must create one or more deployment templates.

To view or edit the list of saved templates, open the **Templates** window.

Creating a deployment template

You can create a deployment template when you create a deployment task or set up user-initiated deployment.

Alternatively, you can create a deployment template in the **Templates** window.

This section describes how to use the Create Deployment Template Wizard.

Master image selection

In this step, specify the following:

- The master image
- The user name and password for the network folder if the image is on the network. The best practice is to map the network folder as a local drive (on the desktop, right-click **Computer** or **My Computer**, and then click **Map Network Drive**)

In addition to images created by Acronis Snap Deploy 6, you can perform deployment from disk-level backups created by other Acronis products and from Virtual Hard Disk (VHD) files. For details, see "Files supported as master images".

Image location

OS Deploy Server can deploy an image located:

- In a network folder.
- On the internal hard disk of the deployment server.
- On a USB or FireWire (IEEE-1394) storage device (such as a flash drive) attached to the deployment server.
- On DVD+R/RW, DVD-R/RW, CD-R/RW, or recordable Blu-ray Discs (BD-R, BD-RE) loaded in the media drive of the deployment server.

The best practice is keeping images on the deployment server's hard disk. This minimizes network traffic during deployment.

The image created on removable media has to fit into one media disk. To deploy an image spread over several CDs, DVDs or other media, copy all parts of the image to the same folder on the deployment server or to a network folder.

**Standalone Utility** can deploy images located:

- In a network folder.
- On a USB or FireWire (IEEE-1394) storage device (such as a flash drive) attached to the managed machine.
- On DVD+R/RW, DVD-R/RW, CD-R/RW, or recordable Blu-ray Discs (BD-R, BD-RE) loaded in the managed machine's media drive.
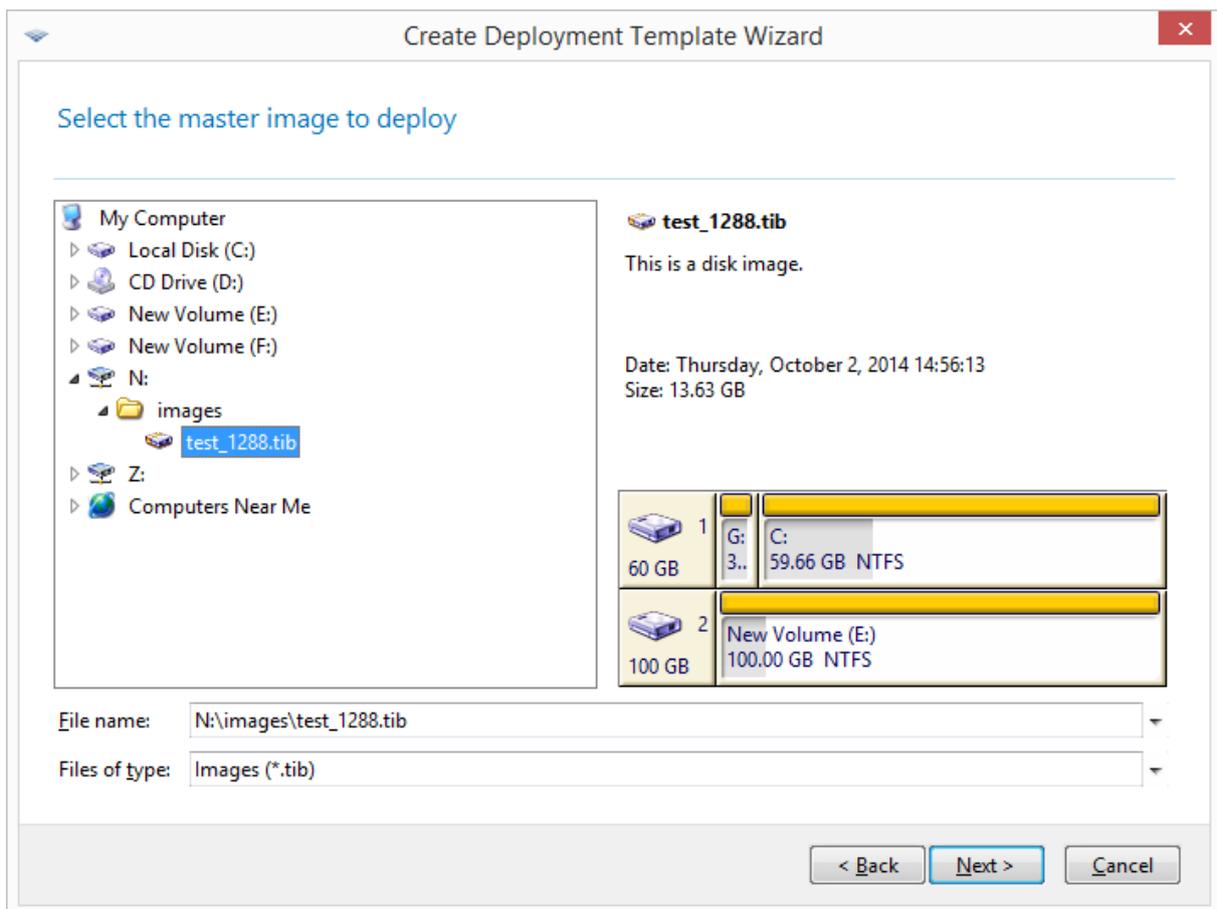
Selecting a master image

Disk and volume selection

If the image contains more than one disk, specify the disk that you want to deploy, and then click **Next**. You can select only one disk.
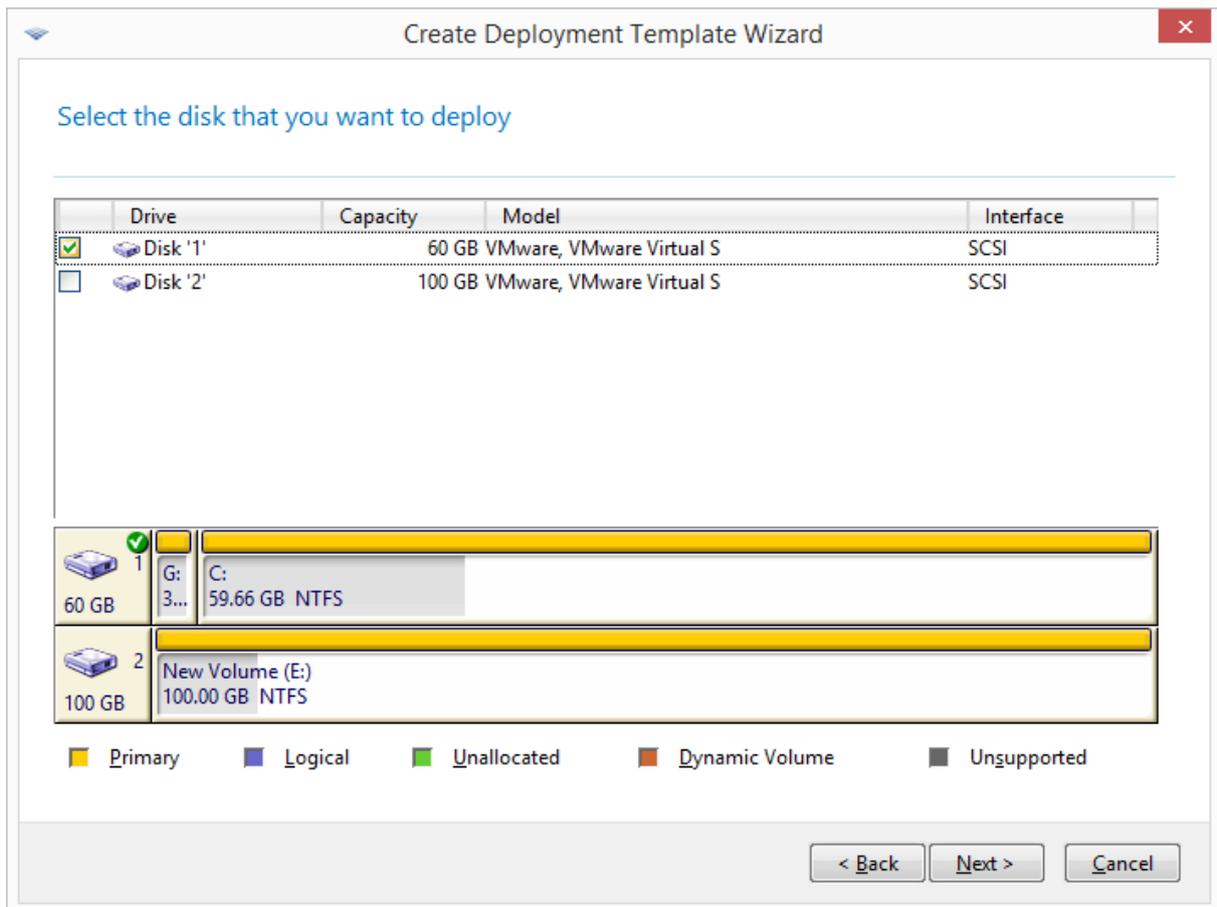
Selecting a disk from the master image

If the disk you selected contains more than one volume, specify the volumes that you want to deploy. You can select one or more volumes.
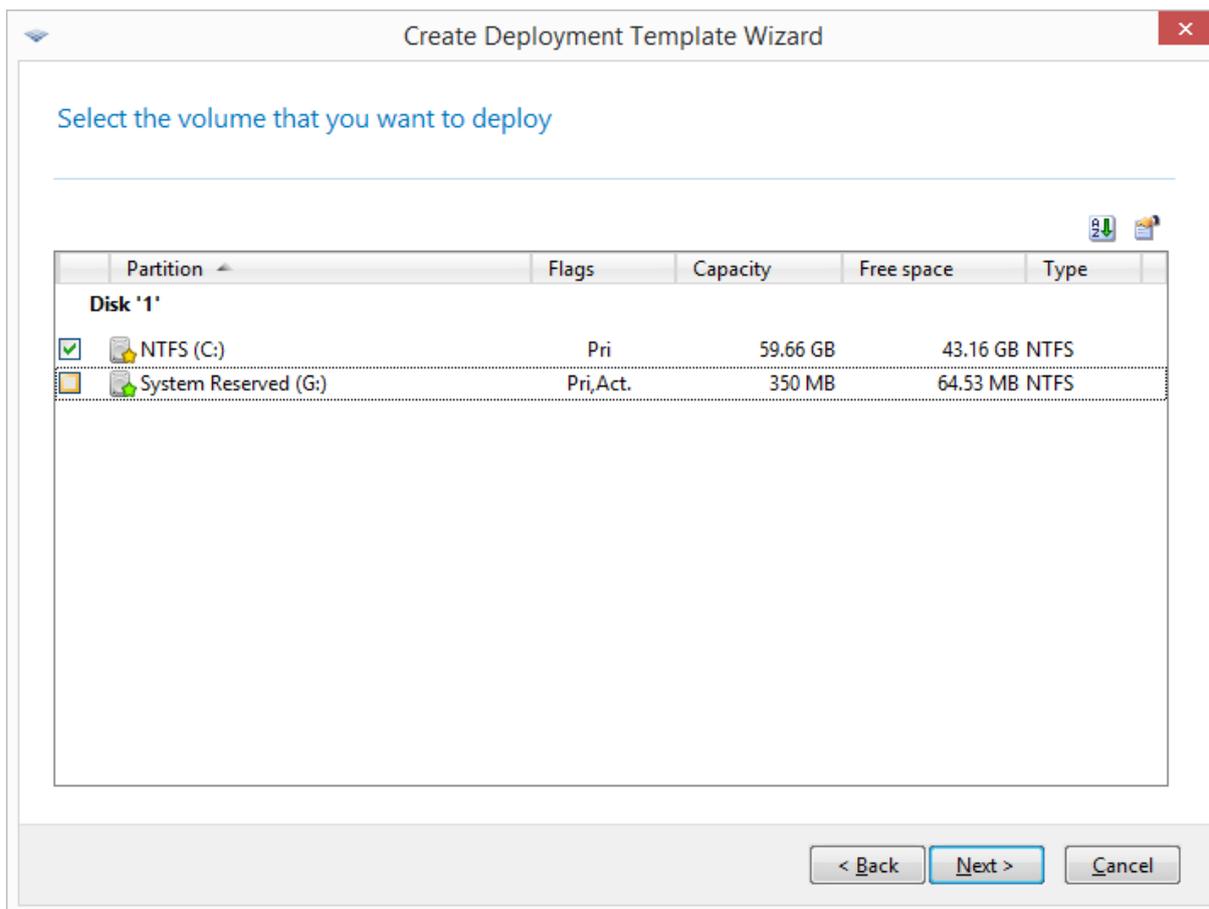
Selecting disk volumes to deploy

The further steps will depend on how many volumes you select.

- If you deploy **only one volume,** it is assumed that the target disk has volumes, so **you can select the target volume, to deploy over it.** Other volumes will remain untouched in this case. Alternatively, you can choose to delete all volumes that currently exist on the target disk.

- Deploying **more than one volume** will **delete all volumes on the target disk.** Only the newly deployed volumes will exist on the disk after deployment.

The master boot record (MBR) is always deployed from the image regardless of your choice.

Important

An operating system includes a loader: a small program that loads the main part of the operating system. The loader and the rest of the operating system may reside on different volumes. For example, Windows 7 and Windows Server 2008 R2 place the loader on a hidden volume called **System Reserved**. If your operating system and its loader reside on different volumes, always include both volumes in the image. A volume with the loader is usually marked as the active volume and is shown with the **Act.** flag in the list. The volumes must also be deployed together; otherwise, there is a high risk that the operating system will not start.

Deployment settings

In this step, specify the deployment settings.

The default values for these settings are taken from the default settings.

Most settings are related to configuring the operating system of the target machine. Such settings are unavailable if the volumes you selected do not contain an operating system for which changing settings is supported. You always can specify general settings such as the disk to perform the deployment to.

These settings can be overridden by individual settings for a machine.

Online deployment

This setting determines how to deploy the master image to the target machines that have the **Online** state in the **Machines** view.

Reboot into

      Specify into what bootable media the target machines will reboot to connect to the deployment server and become ready for deployment.

      The preset is: **Acronis media**

Acronis media

Select this option if you deploy the master image to BIOS-based or 64-bit UEFI-based machines.

WinPE-based media

Select this option if you deploy the master image to 32-bit UEFI-based machines or to the machines with hardware that is not properly recognized by the Acronis media (which is based on a Linux kernel).

Select **Use the media from the master image** if you specified the media in the **WinPE-based media** setting when creating the master image. Otherwise, specify a local or a network path to the media that was created by using PE Builder.

Install agent

If selected and Management Agent is not installed in the system that the master image contains, the management agent will be installed on a target machine after the master image is deployed to it.

Having the management agent installed on a machine enables the online deployment on this machine.

Target disk layout

This setting determines the target disk for deployment, and what space on the target disk will be available for deploying the master image.

The preset is: **Default disk**

The selection **Default disk** means that the image will be deployed to the hard disk whose number in the BIOS is 1. (Note for advanced users: for such disk, the hexadecimal value known as the physical drive number is 0x80.)

You can specify a different disk by clicking **Disk number in BIOS** and then typing or selecting the disk number.
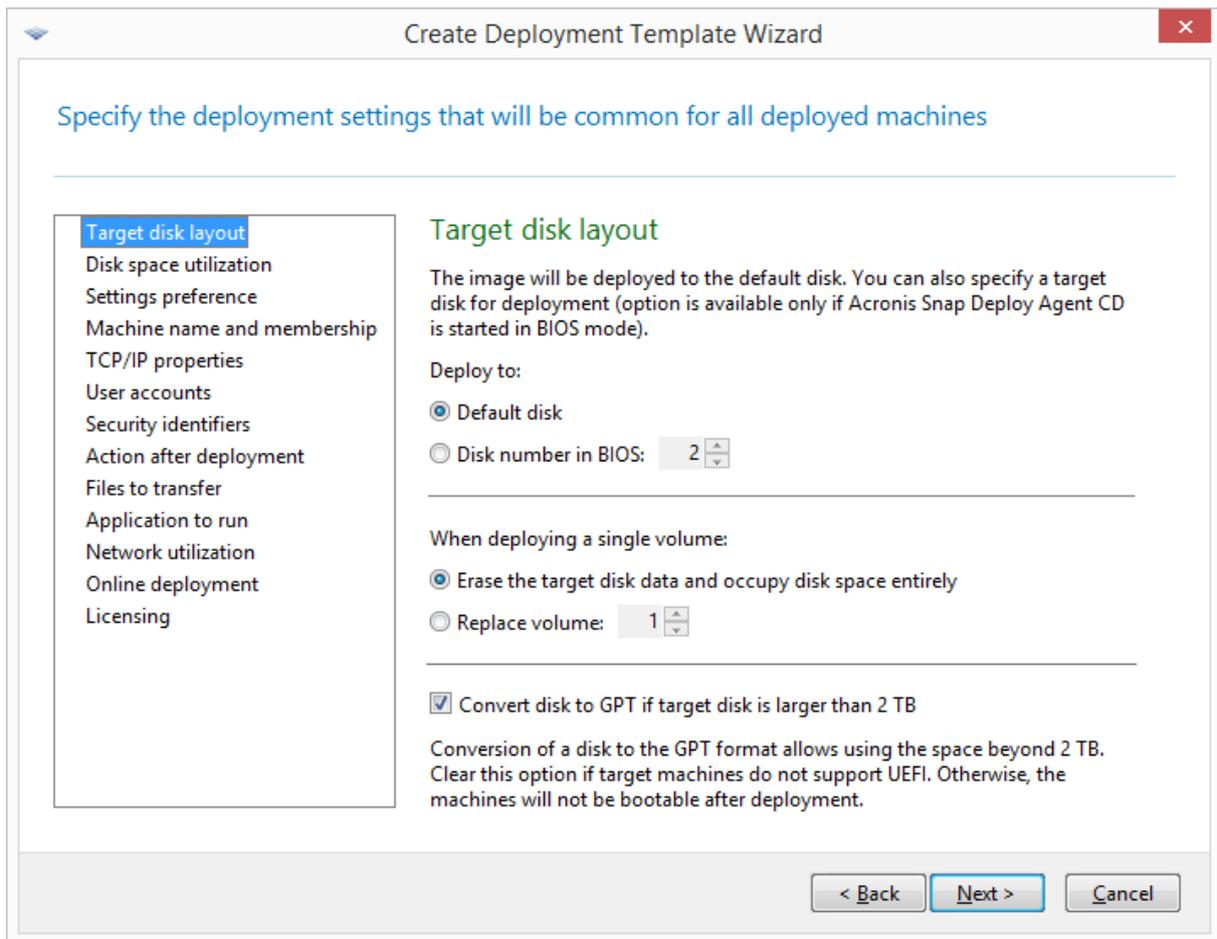
Selecting the target disk and volume

If you selected a single volume for deployment, specify how to place that volume on the target disk:

- **Replace all volumes**: All existing volumes on the target disk will be deleted, and the entire disk space (including the currently unallocated space) will be available for the volume you are deploying.
- **Replace volume**: Only the volume with the selected number will be deleted. If the target disk contains only one volume, the entire disk space (including the currently unallocated space) will be available for the volume you are deploying. Otherwise, only the space that was occupied by the selected volume will be available for the volume you are deploying; currently unallocated space will remain unallocated.

Note

The active volume of the target disk will remain active. Even if you deploy an active volume side by side with an already present active volume, the newly deployed volume will not become active. Therefore, you need to deploy an active volume to an active volume if you want to boot from the deployed volume.

To deploy a single volume to unallocated space or bare metal, first create a target volume of a desired size by using a third-party partitioning tool, such as Microsoft Disk Management or Acronis Disk Director.

In either case, the size of the deployed volume will depend on the setting in **Disk space utilization**.

The **When deploying a single volume** setting is not effective when you deploy multiple volumes. In this case, all existing volumes on the target disk are always deleted, and the entire disk space is available for the volumes.

Converting the target disk to GPT

This setting determines whether a target disk larger than 2 TB should be converted to GPT.

This setting is available only when the operating system stored in the image allows changing the boot mode from BIOS to UEFI. These are the following:

- 64-bit versions of all Windows operating systems starting with Windows Vista SP1
- 64-bit versions of all Windows Server operating systems starting with Windows Server 2008 SP1

The preset is: **Convert disk to GPT if target disk is larger than 2 TB**

MBR disks have a size limitation of 2 TB. If an image of an MBR disk is deployed to a target disk that is larger than 2 TB, only 2 TB of the disk capacity will be used. To get around this issue, Acronis Snap Deploy 6 can automatically change the target disk partitioning style to GPT. However, in order to boot from a GPT disk, the target machine must support the UEFI boot loader. If the target machine does not support UEFI, clear this check box.

Disk space utilization

This setting determines whether to change the size of the volumes you are deploying according to the available space on the target disk. The available space depends on the size of the target disk and on whether you selected to replace all volumes or only a particular volume (see the **Target disk layout** setting).

The preset is: **Resize volumes to fit target disk**

The settings are the following:

- **Resize volumes to fit target disk**: The software will proportionally extend or reduce each of the deployed volumes according to the available space on the target disk.
  The following examples assume that you have a 300-GB target disk that already contains two volumes: the first volume is 50 GB in size, and the second volume is 250 GB in size.
  - *Example 1.* You are deploying a single 100-GB volume. In **Target disk layout**, you selected to replace all volumes on the target disk. In this case, the size of the deployed volume will be 300 GB.
    Example 2. You are deploying a single 100-GB volume. In **Target disk layout**, you selected to replace the second (250-GB) volume on the target disk. In this case, the size of the deployed volume will be 250 GB. The first volume on the target disk will remain intact.
    Example 3. You are deploying two 50-GB volumes. Because you are deploying more than one volume, all volumes on the target disk will be deleted; see "Target disk layout". Each of the deployed volumes will be 150 GB in size.

Example 4. You are deploying a 10-GB volume and a 20-GB volume. All volumes on the target disk will be deleted. The deployed volumes will be 100 GB and 200 GB in size, respectively.

Example 5. You are deploying a 1000-GB volume and a 2000-GB volume, both of which contain little data. All volumes on the target disk will be deleted. The deployed volumes will be 100 GB and 200 GB in size, respectively. If either volume contains too much data to be reduced to the respective size, the deployment will fail.

- **As in the master image**: Each deployed volume will have the same size as in the master image. Any excess available space on the target disk will become unallocated. If the target disk does not contain enough available space for placing the volumes, the deployment will fail.

Settings preference

The **Settings preference** setting determines whether individual deployment settings of a machine can override the deployment settings in the template.

When the **Settings preference** setting is enabled and you set up an individual setting for a machine, deployment to that machine will be performed with the individual setting, ignoring the corresponding setting in the template.

When the **Settings preference** setting is disabled, deployment to all machines will be performed with the settings in the template, ignoring any individual settings.

Machine name and membership

This setting determines the machine names, also known as NetBIOS names, of the target machines; it also determines the name of the workgroup or the Active Directory domain to which the target machines will be added after the deployment.

The preset is: The same name and membership as those of the machine in the master image
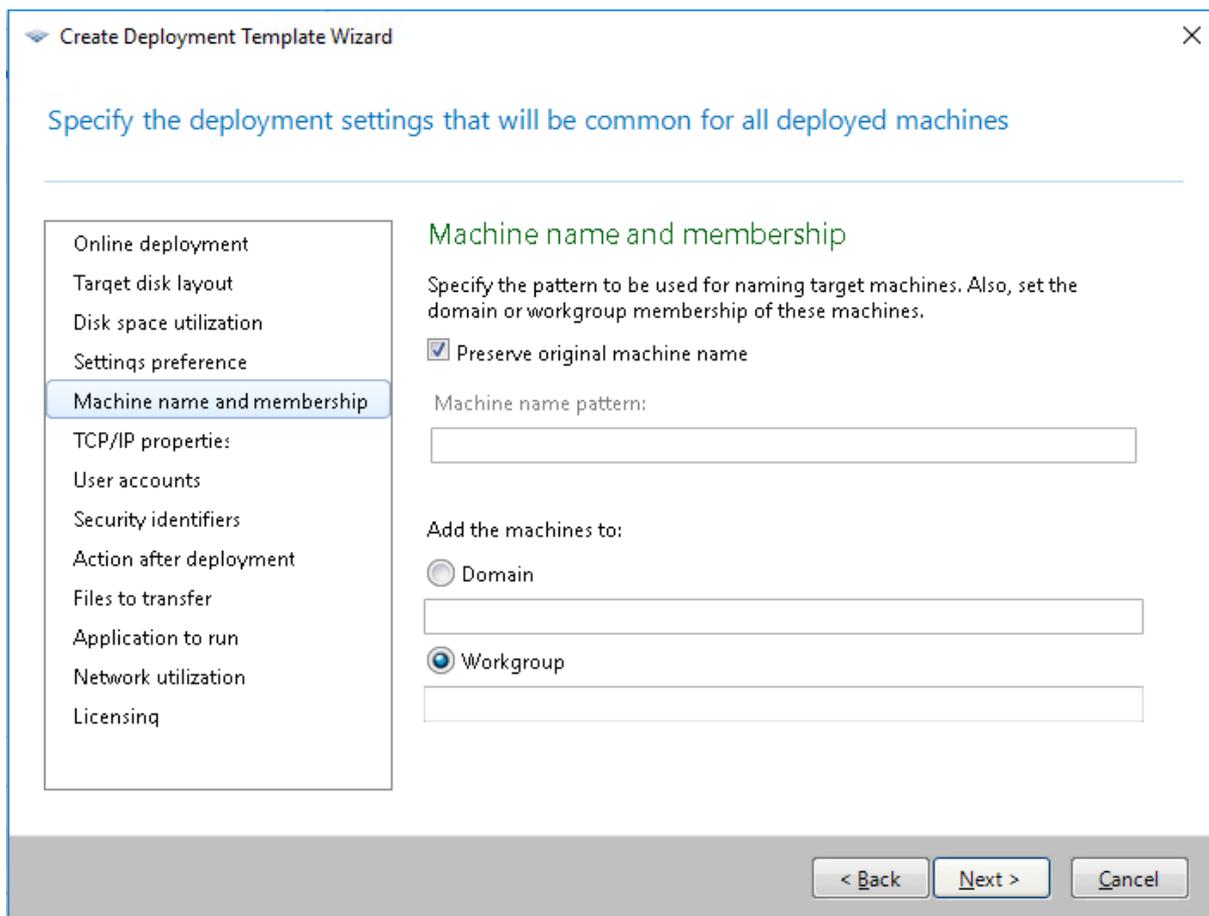
If **Preserve original machine name** is selected, the Management Agent installed inside the machine reads the current machine name defined in Windows, and applies it to this machine after the deployment of the new image.

Note
This option applies only for online deployments. For offline machines, the master image name will be used if there is no naming pattern defined.

If **Preserve original machine name** is not selected or when the deployed machines are offline, all deployed machines will have the same name as the machine in the master image. Alternatively, you can specify a name pattern for the machines.

Specify whether the machine will be a member of a workgroup or an Active Directory domain. If you have selected the domain membership, specify the user name and password of a domain administrator.

Name patterns

A name pattern determines the names that the target machines will have after the deployment.

To specify a single name for all target machines, type that name in **Machine name pattern**. For example, type: **DeployedMachine**

To generate different names for the target machines, include either of the following wildcards or their combination.

{*start***}**

Generates consecutive numbers starting with *start*. Each machine name will have its unique number.

For example, the pattern **{1}** generates the names **1**, **2**, **3**, and so on up to the number of target machines. Similarly, the pattern **{5}** generates the names **5**, **6**, **7**, and so on.

It makes sense to use only one such wildcard in the pattern.

{*start***,***count***}**

Generates *count* consecutive numbers starting with *start*.

For example, the pattern **{1,5}** generates the names **1**, **2**, **3**, **4**, and **5**. Similarly, the pattern **{8,5}** generates the names **8**, **9**, **10**, **11**, and **12**.

Make sure that the value of *count* is big enough. If the number of target machines exceeds *count*, deployment to the remaining machines will fail.

You can use two or more of these wildcards. See examples later in this section.

In the wildcards, the value of *start* must be 0 or greater. The value of *count* must be 1 or greater.

You can use the wildcards alone or accompany them with text, as in the following examples.

Examples

Machine{1}

This pattern generates the names **Machine1**, **Machine2**, ..., **Machine** *N*, where *N* is the number of target machines.

Name{1,3}

This pattern generates the names **Name1**, **Name2**, and **Name3**.

{1,3}{1,4}

This pattern generates the names **11**, **12**, **13**, **14**; **21**, **22**, **23**, **24**; **31**, **32**, **33**, and **34**

{1,9}{0,10}

This pattern generates 90 names: **10**, **11**, **12**, ..., **19**; **20**, **21**, **22**, ..., **29**; ...; **90**, **91**, **92**, ..., **99**

Machine{2,3}{5,4}

This pattern generates the names **Machine25**, **Machine26**, **Machine27**, **Machine28**, **Machine35**, **Machine36**, **Machine37**, **Machine38**, **Machine45**, **Machine46**, **Machine47**, **Machine48**

Name{0}{0,10}

This pattern generates the names **Name00**, **Name01**, ..., **Name09**, **Name10**, **Name11**, **Name12**, ..., **Name100**, **Name101**, and so on. Each machine will have a unique name.

Considerations when using name patterns

Patterns are most effective when you need to easily create different names for the target machines, no matter which machine gets which name. If you need to specify a particular name for a particular machine, you may want to use an individual deployment setting for that machine instead.

There is no order in which the names from the pattern are assigned to the machines. The same machine may be assigned a different name the next time you perform deployment.

TCP/IP properties

This setting determines the network settings for the target machines, such as the Internet Protocol (IP) addresses.

The preset is: The network settings of the master system

You have the options to:

- Use the network settings of the master system.
- Set up the target machines to obtain IP addresses automatically from a DHCP server.
- Specify a range of static IP addresses, a subnet mask, and a default gateway for the target machines. You may want to use this option if your network does not have the DHCP capability. Each machine will be assigned an IP address from the range. Make sure that the range is big enough. If there are more target machines than IP addresses in the range, deployment to the remaining machines will fail.
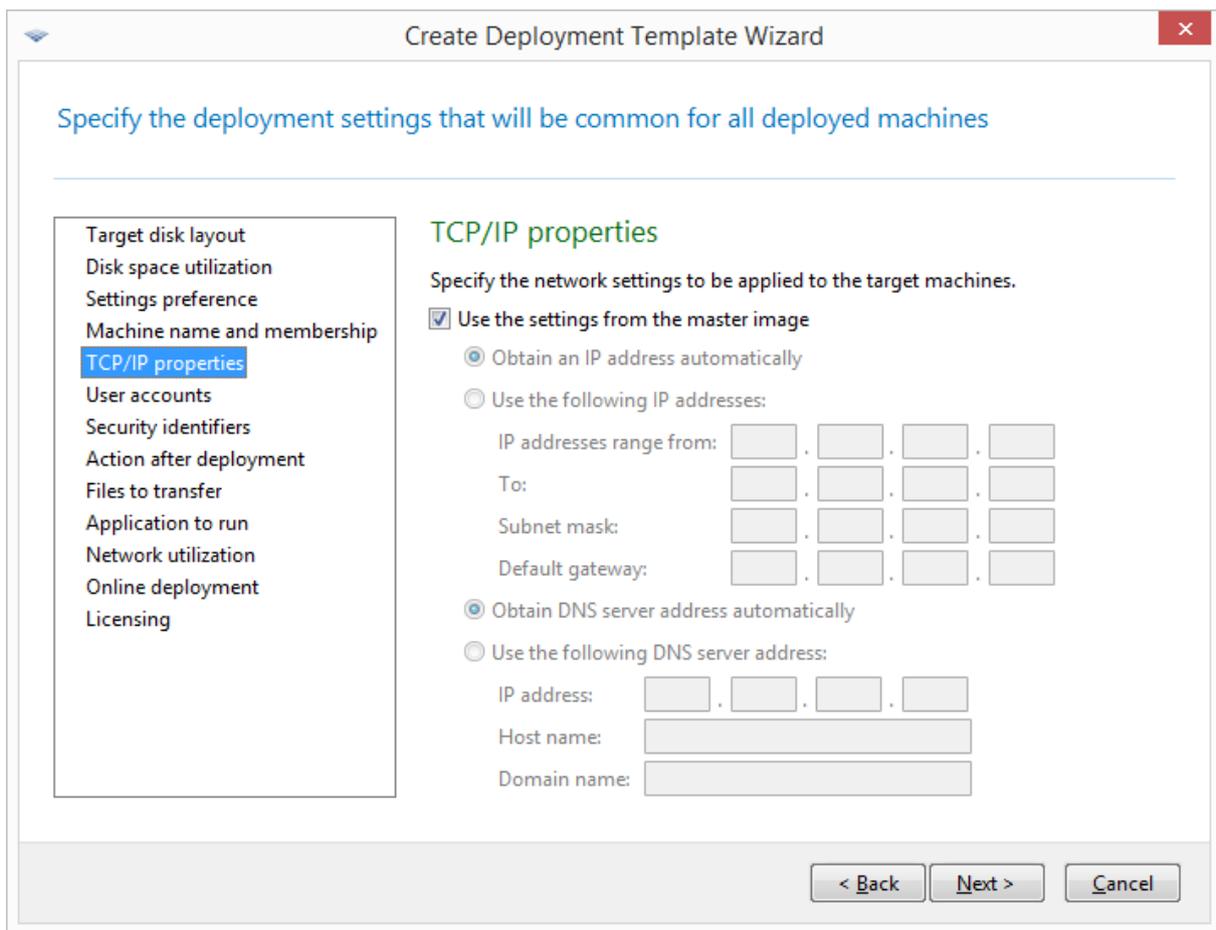
TCP/IP properties

If you have not selected to preserve the network settings of the master system settings, you can specify the DNS server. You can specify the IP address of the DNS server, such as 192.168.0.1; or the network name of the DNS server in **Host name** and **Domain name**, such as **dns** and **example.com** respectively if your DNS server is dns.example.com.

You will be able to change the network settings later when you start the operating system on the deployed machine.

User accounts

This setting determines the local user accounts that will be created on the target machines in addition to the accounts that exist in the master system.

Each user account can be added to the **Administrators**, **Power Users**, or **Users** group. Here you have an opportunity to add a unified administrator's account to all the systems, if needed. The **Remove** and **Remove all** buttons are provided to remove the accounts you specified.

The password complexity has to meet the password policy set for the master machine. To view or edit the password policy on the master machine:

1. Click **Start -> Control Panel -> Administrative Tools -> Local Security Policy**.
2. Under **Account Policies**, click **Password Policy**.

Security identifiers

This setting determines whether Acronis Snap Deploy 6 will generate unique security identifiers (SIDs) for the target machines.

The preset is: Generate a unique SID for each target machine

Note

Generating unique SIDs is not supported for machines running Windows 10 and Windows 11.

Generating unique SIDs should normally be enabled. We recommend not to change the SID only if you are deploying the image to the same machine from which the image was created.

You can keep the SID unchanged if there is no machine with the same SID in the same workgroup or domain. Such is the case when the master machine is no longer on the network.
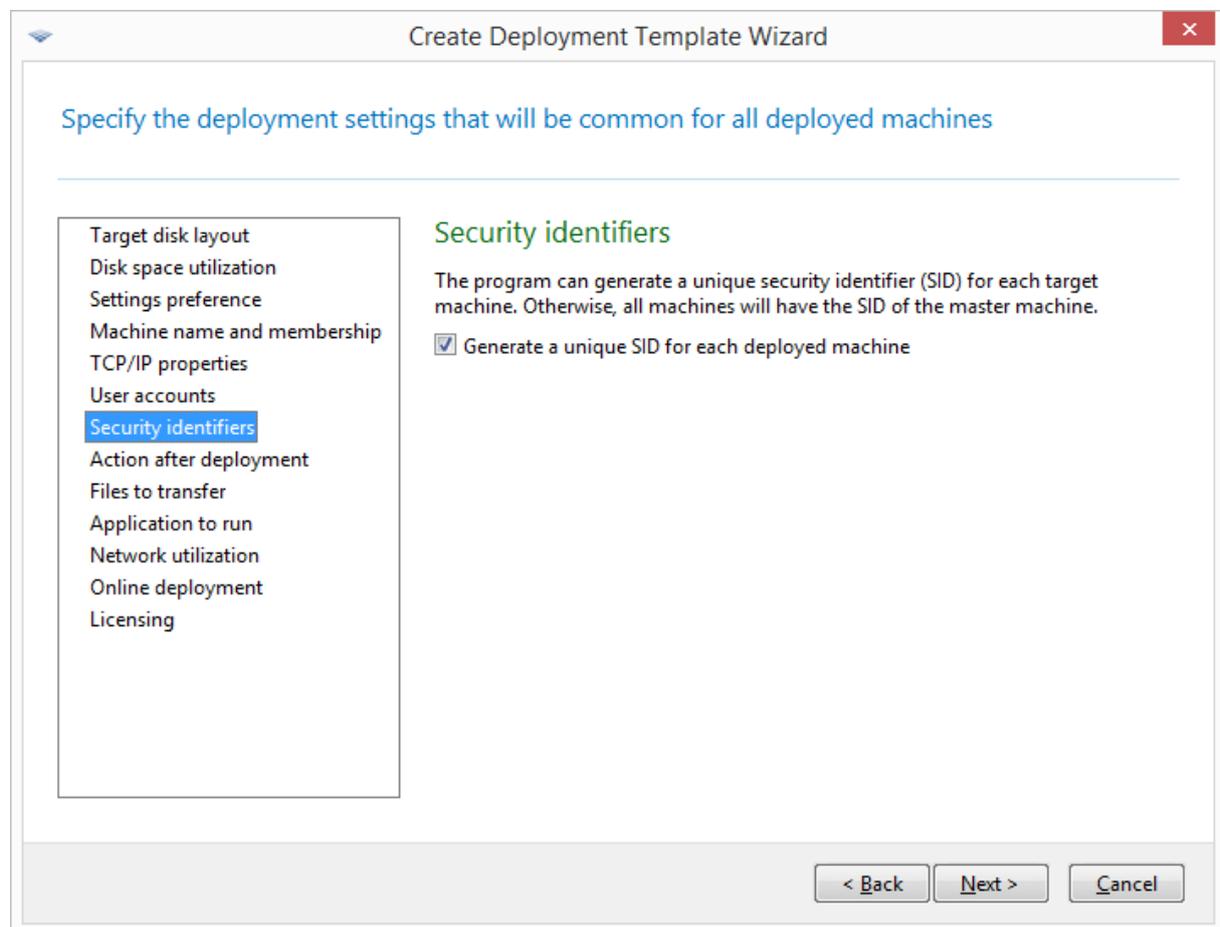
Note

SID will not be changed if master image contains a server with Domain Controller role enabled: Domain Controller server stores domain SID which should be the same on all domain machines and therefore is not supposed to be altered.

Action after deployment

The **Action after deployment** setting determines what target machines do upon completion of deployment and all associated operations (such as transferring files).

The options for this setting are:

- **Shut down**

  Target machines shut down.

  > **Note**
  > This is the default option.

- **Reboot**

  Target machines reboot.

- **Return to Ready For Deployment**

  Target machines return to a ready state.

- **Exit the application**

  - For deployments performed via WinPE-based bootable media, Acronis Snap Deploy 6 closes on target machines

    (i.e., the machine returns to the WinPE environment).

    > **Important**
    > If deployment was successful, the `%errorlevel%` variable is set to 0.
    > Any non-zero value for the `%errorlevel%` variable indicates that deployment on the target machine was unsuccessful.

  - For deployments performed via **non**-WinPE bootable media, target machines reboot.

    (i.e. for non-WinPE bootable media, this option is the same as the **Reboot** option).

Files to transfer

This setting determines the list of files, such as installation files, to be transferred to all target machines after the deployment.

Each file must be located in a network folder. When adding the file, specify the credentials to the network folder.

The destination of each file must be on one of the volumes you are deploying.

To run the file after it is transferred, select the **Run the file on target machines** check box. The file will run when Windows first starts on the target machine.

Example

You want the target machines to use a particular Plug and Play device driver, such as a video adapter driver, so that Windows automatically recognizes the device at boot. In this case, do the

following:

1. Create a network folder, such as \\server\share, and place the driver files to it. Driver files usually include an .inf file and a .sys file.
2. Specify both files in the **Files to transfer** setting, with the following paths in the **Destination** field:
   - For the .inf file: **C:\Windows\inf**
   - For the .sys file: **C:\Windows\System32\drivers**

   If the operating system in the master image resides on a different volume, change the drive letter in these paths accordingly.

During the deployment, the files are placed in the corresponding folders. When starting on the target machine, Windows discovers the new device and finds your driver for it.

Applications to run

This setting determines non-interactive applications, such as Windows services or applications executing scripts, that will run on the target machines after the deployment is complete.

Warning!
Scripts must not launch interactive applications; for example, notepad.exe. Otherwise, it will not be possible to log in to the deployed operating system.

To add an application, click **Add**, and then specify the path to the application and the parameters the application will run with.

The application and script files, if any, must be located on one of the volumes you are deploying.

The application will run when Windows first starts on the target machine.

Network utilization

This setting determines the data transfer mode for the deployment.

The preset is: **Multicast**

With the **Multicast** transfer mode, OS Deploy Server sends data to a group of recipients simultaneously.

Using the **Unicast** transfer mode, the server sends a copy of the data to each recipient. This can significantly reduce the deployment speed.

For example, suppose that you have a bandwidth of 100 MB per second, and you want to deploy a system to 10 target machines.

- With the **Unicast** mode, the server divides the speed among 10 machines. Therefore, the data transfer speed will be 10 MB per second for each target machine.
- With the **Multicast** mode, the server sends one copy of data to a multicast address, and each client will receive data at a speed of 100 MB per second.

Multicast configuration has a parameter that specifies the time to live (TTL) for multicast packets. Use this parameter to limit multicast packets distribution via gateways.

The default value is 15. In practice, this enables the packets to pass up to 15 hops which may be treated as an unlimited distance. The minimal value 1 will limit the packets circulation to one subnet.

By setting the permitted bandwidth, you can limit the network usage during deployment. The default value is 1 gigabit (Gbit) per second.
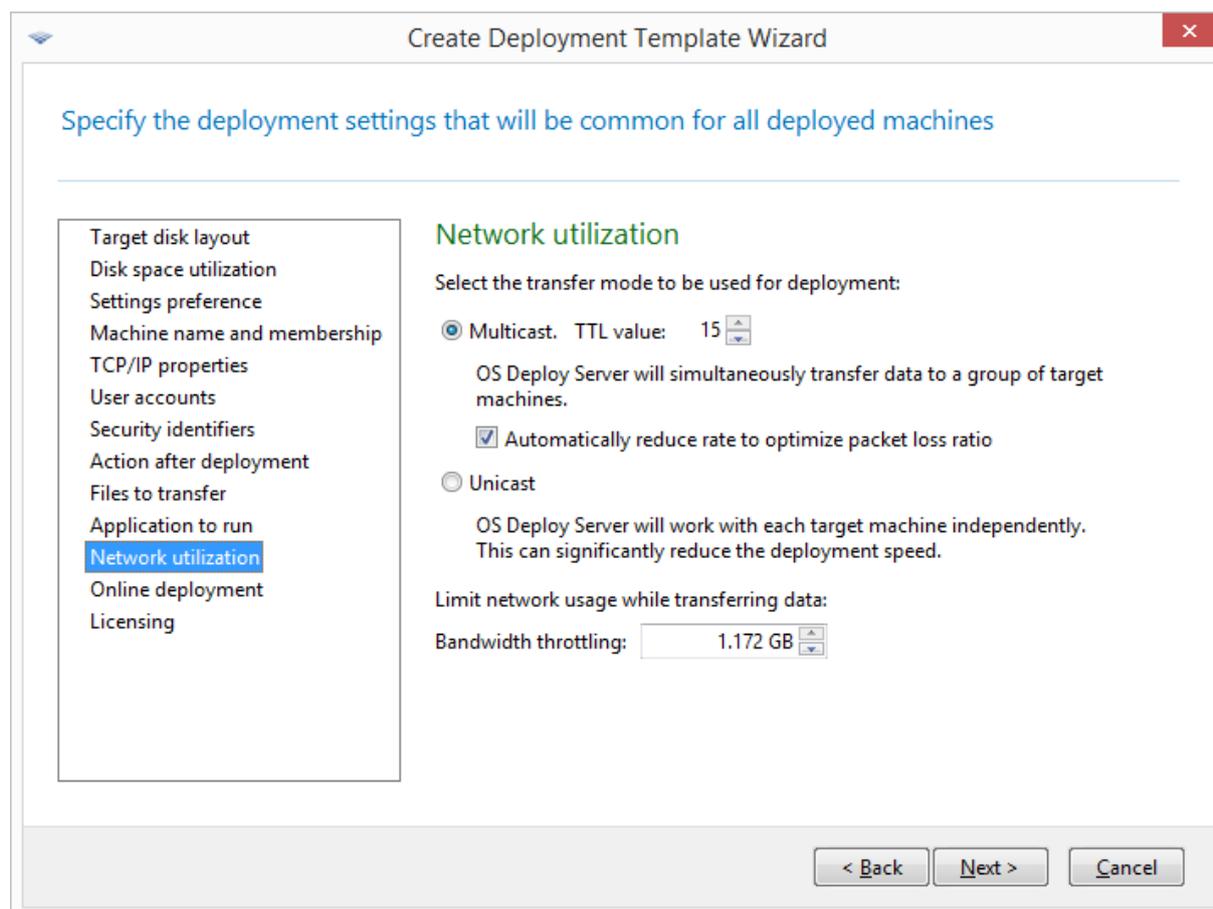
Adjusting network utilization settings

Acronis Snap Deploy 6 uses Internet Group Management Protocol (IGMP) for multicasting. Therefore, all network hardware (such as routers or network switches) must be IGMP-capable and correctly configured. The specific information on configuring any particular router or network switch is usually available in the documentation provided with the hardware.

If there is no IGMP-capable hardware (or you cannot configure it correctly) in the network, use the **Unicast** data transfer mode.

Licensing

This setting determines which type of license to use for deployment to a target machine and what to do when no appropriate license is available on the license server.

The preset is:

- Use a deployment license of the corresponding type (a server license or a workstation license)
- If no such deployment license is found, use a machine license of the same type
- Stop deployment otherwise
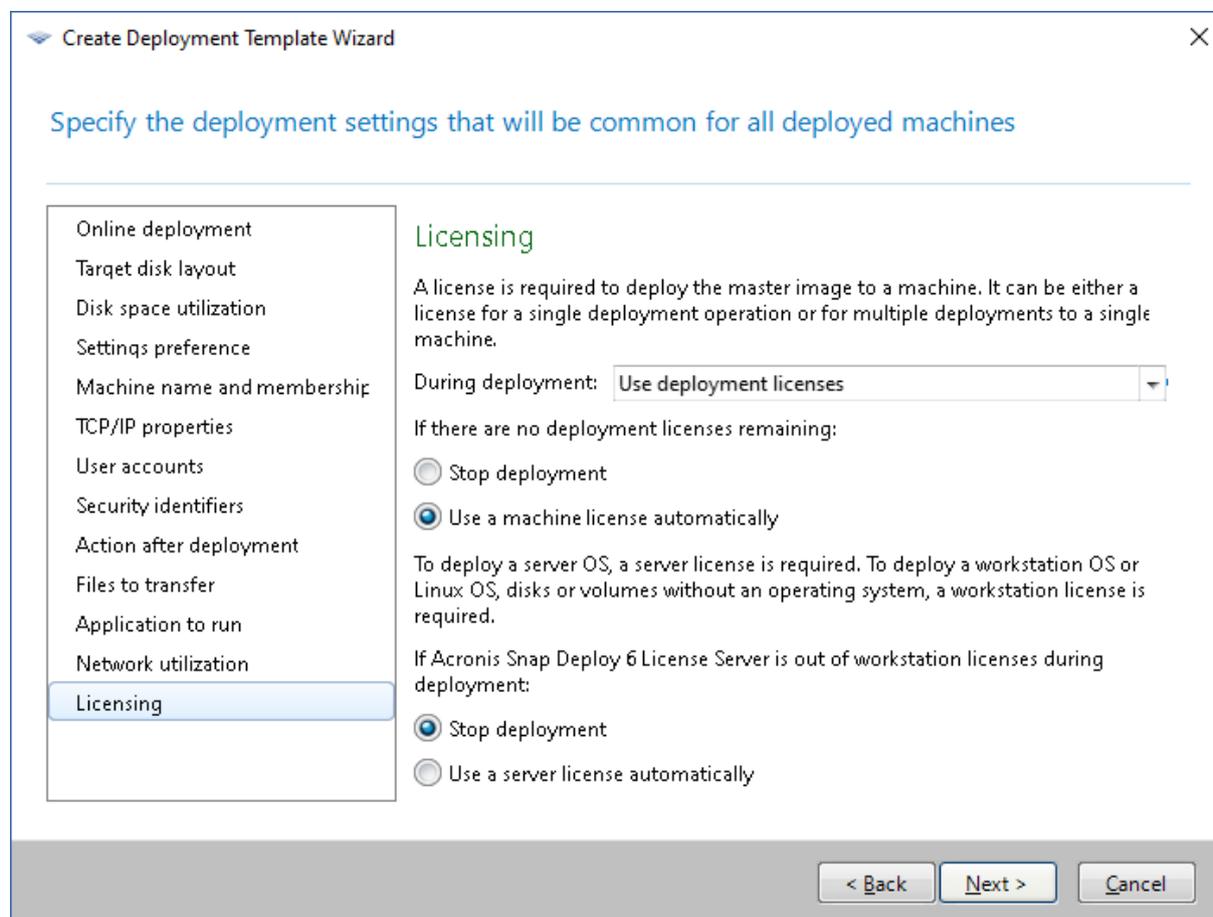
Specifying licensing settings

Based on your selection, the software will use a deployment license (which enables a single successful deployment) or a machine license (which enables an unlimited number of deployments to a machine). Based on the operating system you are deploying, a workstation license or a server license will be used.

If no appropriate license is available on the license server, the software can either stop deployment to the machine, or use an alternative license.

Note
To force a machine license to be used for a particular machine, you can specify the **Licensing** setting as an individual setting for that machine.

When you deploy a workstation operating system and you selected the **Use a server license automatically** option, the software will use a server license if no workstation license can be used.

Example

Suppose that you are deploying a workstation operating system. Consider the following settings:

- During deployment: **Use deployment licenses**
- If there are no deployment licenses: **Use a machine license automatically**
- If the license server is out of workstation licenses: **Use a server license automatically**

With these settings, the software will use a license based on the following priority:

a. Deployment workstation license
b. Machine workstation license
c. Deployment server license
d. Machine server license

If you change the second setting from **Use a machine license automatically** to **Stop deployment**, the software will use only deployment licenses. The software will use the following priority:

a. Deployment workstation license
b. Deployment server license

Using Acronis Universal Deploy

Specify whether you want to use Acronis Universal Deploy during deployment.

To configure this setting

1. Select whether to use Acronis Universal Deploy.

    Acronis Universal Deploy will help you to create a bootable Windows or Linux clone on different hardware by automatically installing the necessary system drivers. Use Acronis Universal Deploy when deploying the operating system to a machine with a dissimilar processor, different motherboard, or other mass-storage device than in the imaged system. For detailed information, see "What is Acronis Universal Deploy".
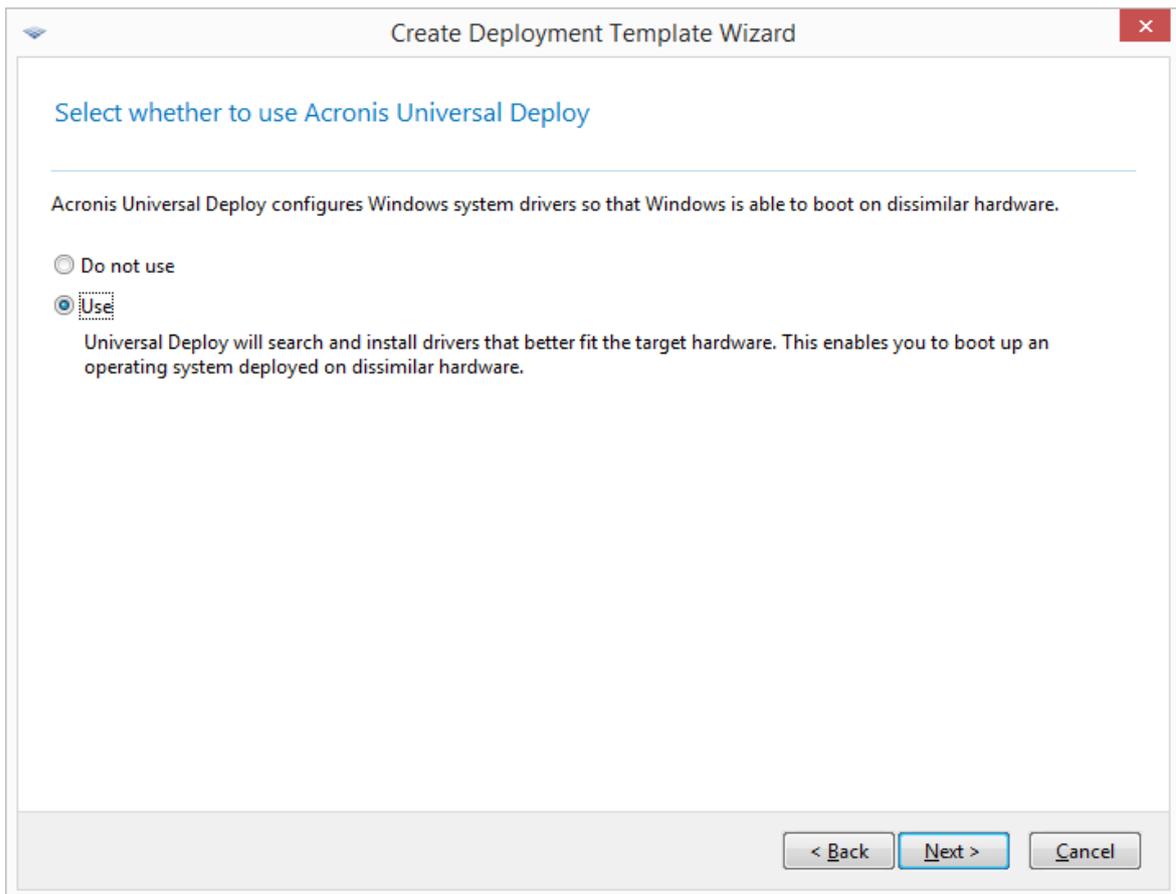
Select whether to use Acronis Universal Deploy

In Windows, Acronis Universal Deploy uses three sources for drivers:

- The Windows default driver storage folder (in the master image being deployed)
- The driver repository, which is one or more network folders or removable media
- The mass-storage device driver specified by the user

The software will find the most suitable drivers of all available drivers and install them into the deployed system. However, the driver defined by the user will have the priority. It will be installed, with appropriate warnings, even if the software finds a better driver.

In Linux, Acronis Universal Deploy will find the necessary modules in the **/lib/modules** directory. The steps below will be skipped.

2. [Optional] Specify the driver repository.

   Specify a driver storage to search for HAL and storage device drivers during the automatic search-and-install procedure. You can add network locations and enable a search of removable media for drivers.
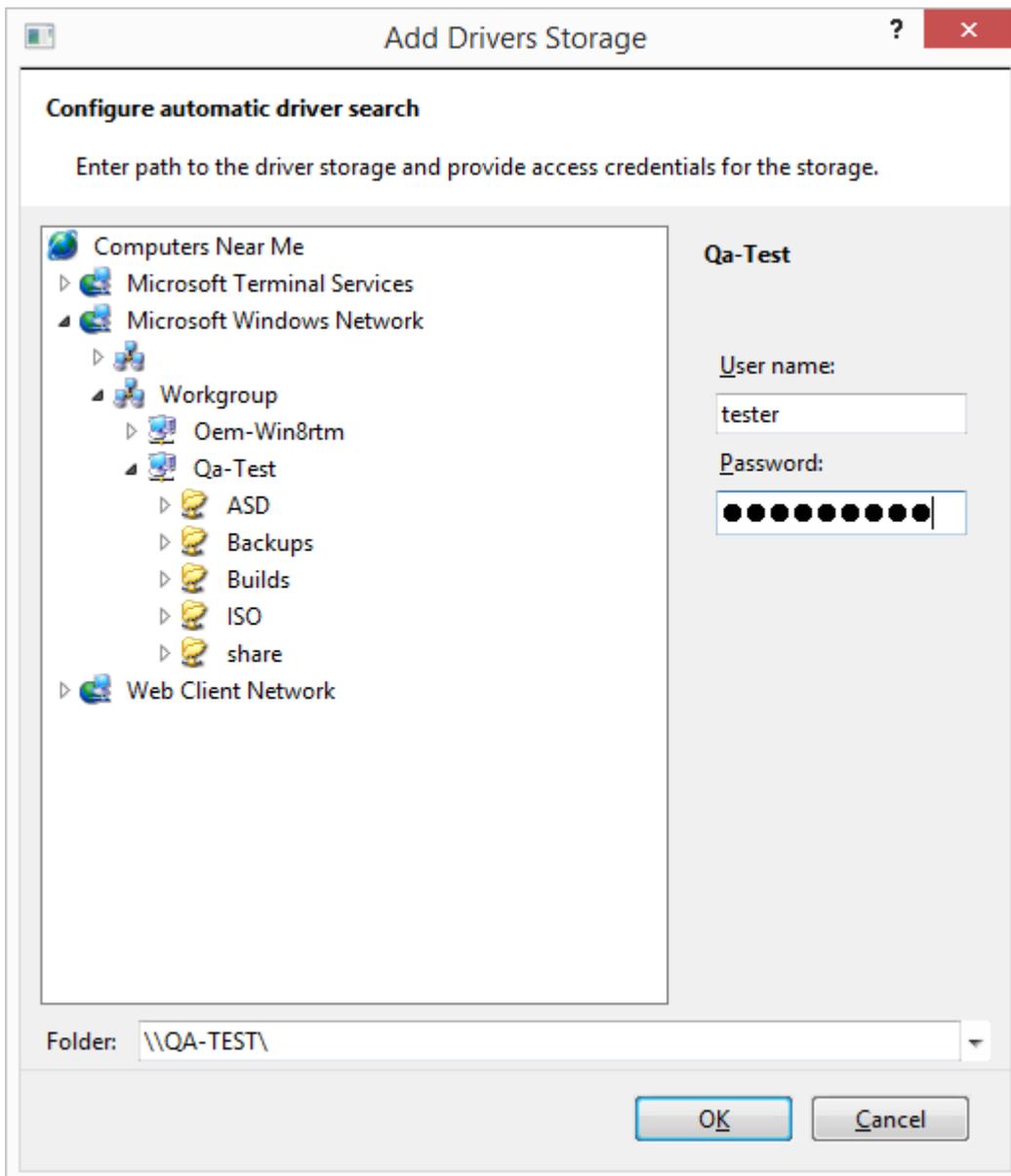
Adding a driver storage

3. [Optional] Specify the mass-storage driver.

If the target hardware has a specific mass-storage controller (such as a SCSI, RAID, or Fibre Channel adapter) for the hard disk, explicitly specify the appropriate driver for that controller. The driver will be installed in any case, bypassing the automatic driver search-and-install procedure.

Use this option only if the automatic search-and-install procedure was unsuccessful.

Note

When deploying the system to a virtual machine that uses SCSI hard drive controller, make sure to specify SCSI drivers for the virtual environment. For example, VMware requires Buslogic or LSI logic drivers. Use drivers bundled with your virtualization software or download the latest driver versions from the software manufacturer's Web site.

Summary window

Check your settings in the summary window, and then click **Save**.
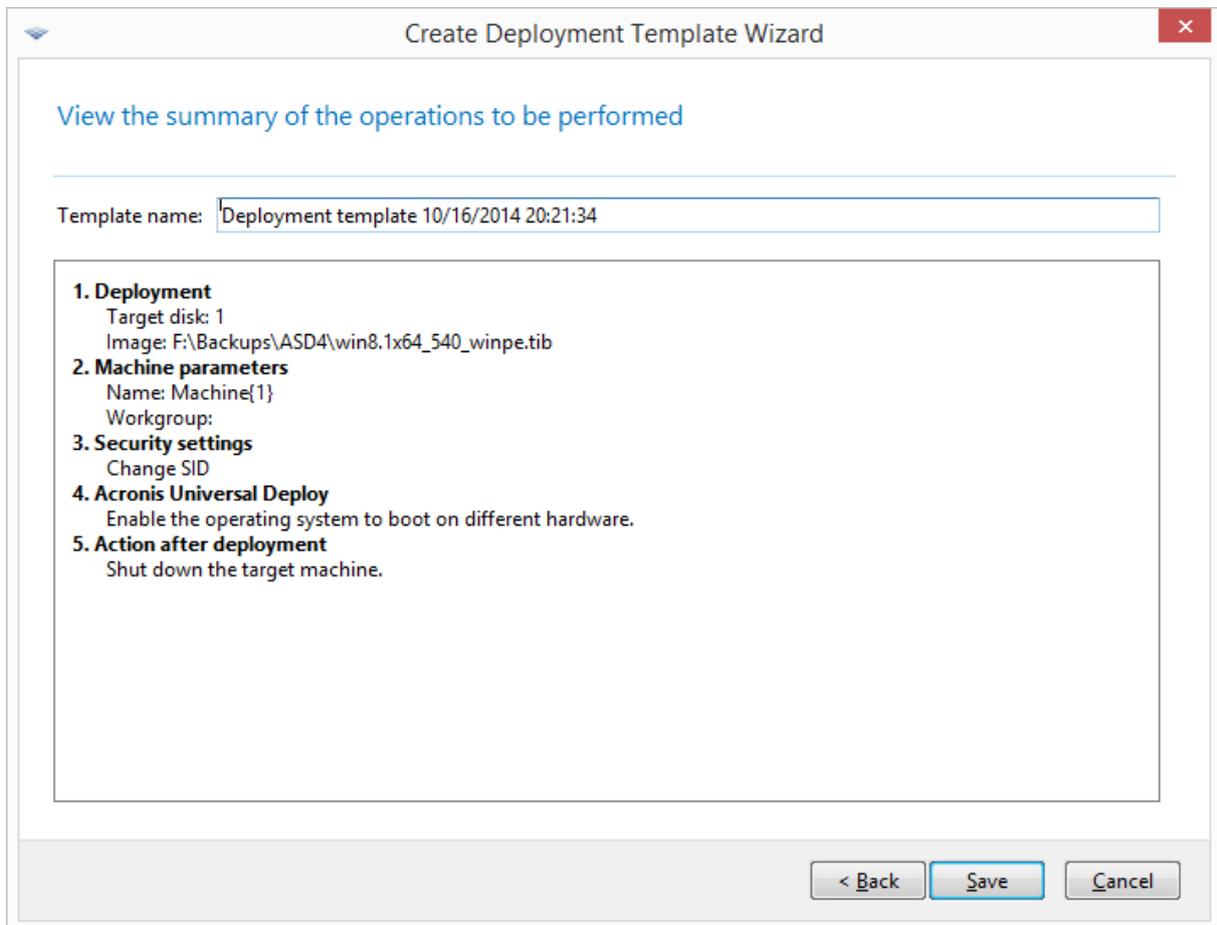
The summary window

Configuring default deployment settings

In the **Default Deployment Settings** window, you can specify the values that will be used by default when you create a deployment template.

To view or change the default deployment settings

1. Start Management Console.
2. On the **Tools** menu, click **Configure default settings**. If prompted, specify the name or IP address of the machine where OS Deploy Server is installed, and the user name and password of an administrator on that machine.

Each default setting has a preset value. To reset all default settings to their preset values, click **Reset all**.

List of default settings

The following is the list of default deployment settings and their preset values.

- **Target disk layout**

  The preset is: Perform deployment to the first hard disk in the BIOS

- **Disk space utilization**

  The preset is: Extend or reduce the volumes being deployed, according to the available space on the target disk

- **Machine name and membership**

  The preset is: The same as of the master system

- **TCP/IP properties**

  The preset is: The network settings of the master system

- **User accounts**

  The preset is: Create no additional user accounts

- **Security identifiers**

  The preset is: Generate a unique security identifier (SID) for each target machine

- **Action after deployment**

  The preset is: Shut down the machine after the deployment

- **Network utilization**

  The preset is:
  - Perform deployment by using multicast

- **Licensing**

  The preset is:
  - Use a deployment license of the corresponding type (a server license or a workstation license)
  - If no such deployment license is found, use a machine license of the same type
  - Stop deployment otherwise

Managing deployment templates

In the **Templates** window, you can create, view, edit, and delete the deployment templates that are saved on OS Deploy Server.

To open this window, click **Actions -> Manage templates**. If prompted, specify the name or IP address of the machine with the deployment server, and the user name and password of an administrator on that machine.

To create a deployment template

1. Connect the management console to OS Deploy Server.
2. On the **Actions** menu, click **Manage templates**.
3. Click **Create new**, and then follow the steps of the Create Deployment Template Wizard.

Deployment through a deployment task

By using a deployment task, you can perform deployment in either of these ways:

- Deployment to a specified list of machines. Acronis Snap Deploy 6 will use the Wake-on-LAN functionality to wake up the machines that are turned off and thus are not ready for deployment.
- Deployment as soon as a specified number of any machines become ready for deployment. You (or users in your organization) will need to make the machines ready.

A machine becomes ready for deployment after it boots into an agent from a bootable media or a PXE server, and then connects to OS Deploy Server.

Note
If the machine does not boot into the agent and the machine has Secure Boot enabled, we recommend disabling Secure Boot on this machine as a workaround.

In addition, you can run any deployment task manually from the **Deployment tasks** view.

A deployment task runs according to a deployment template. When creating the task, you can create a deployment template or specify an existing one.

Prerequisites

Before proceeding with the deployment, make sure that:

- You have installed the following components: Management Console, License Server, OS Deploy Server, and (optionally) Acronis PXE Server. All these components are already installed if you performed a typical installation.
- You imported a sufficient number of licenses to License Server.
- You created a master image by using either bootable media (offline imaging) or Management Agent (online imaging).

Procedures in this section assume that you have performed these steps.

Deployment to specific machines

Deployment to a specified list of machines can run immediately, manually, or on a schedule.

When the deployment is about to start, the software uses the Wake-on-LAN (WOL) functionality of the BIOS to wake up (turn on) the machines in the list.

Acronis Snap Deploy 6 wakes up each machine by sending a special packet, called the *magic packet*, to all network adapters of the machine.

Machines in another subnet can be woken up through the Acronis Wake-on-LAN Proxy component, which is delivered with Acronis Snap Deploy 6.

The woken-up machines then boot into Agent.

You can manually boot machines that do not support Wake-on-LAN, before the task starts. Such machines will also be deployed, provided that they are listed for deployment.

A best practice for this type of deployment is to use Acronis PXE Server for booting the machines. Also, you can boot the machines by using a bootable media.
Alternatively, you can configure online deployment to the target machines.

Preparation steps

This section describes how to prepare deployment to a specified list of machines.

Getting MAC addresses

Media Access Control address (MAC address) is a 48-bit physical (hardware) address of a network device. In Windows, the physical address can be obtained by running the command `ipconfig /all` or by selecting **Local Area Connection -> Status -> Support -> Details** (in Windows 7, you can access this option from the Network and Sharing Center).

MAC addresses for bare metal are usually supplied by the hardware manufacturer. You can get the MAC address of any PC-compatible hardware by entering the network configuration menu of any Acronis bootable component, such as Master Image Creator.

An administrator can execute a script that collects the MAC addresses of all machines on the network and saves the MAC addresses to a text file. This can be a plain text file, such as the following:

```
00-01-23-45-67-1A
02-01-23-45-67-1B
```

You can then specify this file when creating the deployment task or in the **Machines** view when adding machines.

You also will be able to provide each MAC address manually.

Enabling Wake-on-LAN on target machines

Make sure that Wake-on-LAN is enabled on the target machines. Enter the machine BIOS and set **Power -> Wake On PCI PME -> Power On**. The exact names might vary depending on the BIOS version.

To enable the Wake-on-LAN feature on a machine running Windows, set the network adapter (NIC) properties on the machine as follows:

Select **Control Panel -> System -> Device Manager -> Network adapters ->** select the network adapter **-> Properties -> Advanced**:

- **Enable PME->Enabled**
- **Wake On Link Settings-> OS Controlled**
- **Wake On Settings->Wake On Magic Packet**

The exact names of the controls may differ depending on your operating system.

If you cannot or do not wish to use Wake-on-LAN on some or all of the target machines, you will have to boot them into Agent manually before the scheduled time comes.
Alternatively, you can configure online deployment to the target machines.

Installing and configuring the PXE server

For the machines to automatically boot over the network into Agent when the scheduled time comes, do the following:

1. Install Acronis PXE Server. If you performed a typical installation, the PXE server is already installed together with OS Deploy Server.

   > **Note**
   > If all of the target machines are located in one subnet, but OS Deploy Server is installed in a different subnet, we recommend installing a separate PXE server in the target machines' subnet. For details, see "Deployment in another subnet".

2. Connect the management console to the PXE server.
3. Do one of the following, as described in "Configuring Acronis PXE Server":
   - Upload the agent to the PXE server by clicking **Upload components**.
   - Upload a Preinstallation Environment (PE) image to the PXE server by clicking **Upload PE image to PXE**. For information about creating a PE image (a WIM file), see "Adding Acronis Snap Deploy 6 components to WinPE".

   When uploading the agent or the PE image:
   - Set **Start operating system** as the default boot menu option.
   - Set up a reasonable time-out so that the operating system can start automatically. You can leave the default setting for the time-out.

Without a PXE server, you will need to boot the target machines manually before the deployment task starts.
Alternatively, you can configure online deployment to the target machines.

Setting up a machine to boot from PXE

For bare metal, it is enough that the machine BIOS configuration supports network booting. This is because no operating system is present on the hard disk, so the machine will boot from the network even if the hard disk drive is the first device in the boot sequence.

On a machine that already has an operating system on the hard disk, the BIOS must be configured so that the network adapter is either the first boot device, or at least precedes the Hard Drive device in the boot sequence.

The following example shows one of the reasonable BIOS configurations. Unless you insert a bootable media, the machine will boot from the network.
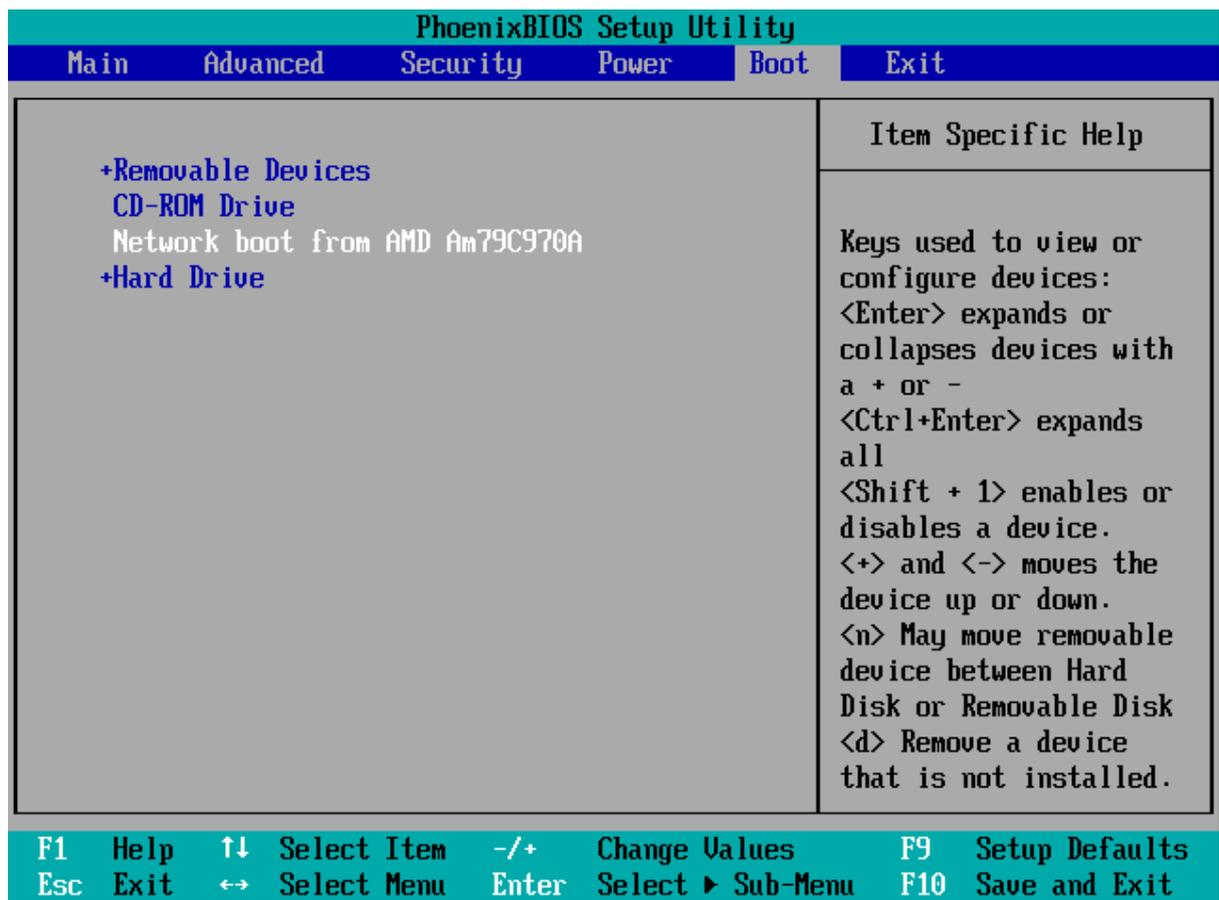
Example of setting up the BIOS for network booting

In some BIOS versions, you have to save changes to BIOS after enabling the network adapter so that the network adapter appears in the list of boot devices.

If the hardware has multiple network adapters, make sure that the network adapter supported by the BIOS has the network cable plugged in.

Creating the deployment task

When the deployment is about to start, OS Deploy Server wakes up the turned-off target machines in the list you specify. The machines turn on, boot into Agent from the PXE server, and connect to the deployment server.

When all (or some, depending on your choice) target machines connect, the deployment server starts deployment. Deployment is usually performed by multicasting.

The following picture illustrates deployment to specific machines within a single subnet. If the target machines are located in another subnet, you may need to perform additional steps before creating the deployment task.
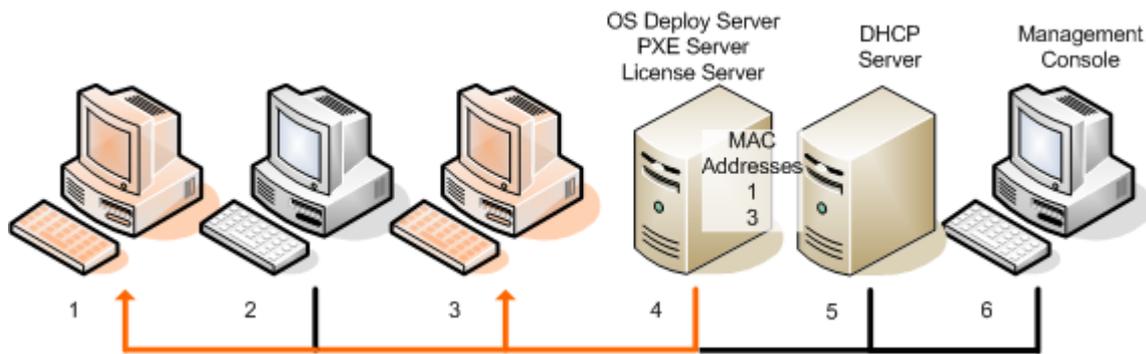
Deployment to specific machines within one subnet

To create a deployment task for specific machines

1. Make sure that you have completed the preparation steps.
2. Start the Management Console.
3. In the welcome screen, click **Deploy image**. If prompted, specify the machine where OS Deploy server is installed.
4. In **Deploy to**, select **The machines listed below**.
5. Select **Add machines -> From file**, and then specify the file with the MAC addresses you created.

   You can also specify the MAC addresses manually (select **Add machines -> By MAC address**) or select machines that are currently listed in the **Machines** view (select **Add machines -> From machine list**).
6. Tune the PXE server as follows:

   a. Select the **Use PXE server for booting into agent** check box, and then click **Specify**.

   b. Specify the name or the IP address of the machine with the PXE server, and the user name and password of an administrator on that machine.

   Tuning the PXE server ensures that the machines in your list boot into Agent when the task starts (even though you selected **Start operating system** as the default boot menu option), and boot to the operating system after the task finishes.

   Machines that are not in your list are not affected: they boot according to the default boot menu option.

   The PXE server remains tuned until the task finishes. It becomes tuned again the next time the task starts.

Note

Tuning the PXE server is not effective if you uploaded the bootable components to the PXE server directly (using the **Acronis PXE Server** setting) when creating a WinPE-based bootable media. This is because choosing a default boot menu option is not available in this case. You need to create a PE image first (using the **WIM image** setting), and then upload the PE image to the PXE server.

---

7. If the machines are located in a different subnet than the deployment server, specify the Wake-on-LAN proxy installed in that subnet, as follows:

   a. Expand **Show Wake-on-LAN Proxy settings**, and then click **Specify**.

   b. Specify the name or the IP address of the machine with Acronis Wake-on-LAN Proxy, and the user name and password of an administrator on that machine.

8. Click **Next**.

9. Create a deployment template or select an existing one.

10. Specify when to run the task (set up the deployment schedule):

    - **Now**: The task will run immediately after you create it.
    - **Once later**: The task will run once at the specified date and time.
    - **Daily**: The task will run at the selected times every day or every few days.
    - **Weekly**: The task will run on the selected days every week or every few weeks.
    - **Monthly**: The task will run on the selected day every month.
    - **Manually**: The task will run only when you start it manually.

    If prompted, specify the credentials for running the task.

    Important
    When the scheduled time comes, the target machines must be turned off or booted into Agent.

    With any deployment schedule, you will be able to start the task manually by selecting it in the **Deployment tasks** view and clicking **Run** on the toolbar.

11. Specify a time-out for waiting for all listed machines to become ready, and the action after the time-out.

    In practical situations, some of the listed machines might not connect to the deployment server at the scheduled time. For example, they may be in use at that time. The task waits for listed machines to become ready for the time you specified. As soon as all machines are ready, the task starts deployment.

    If not all machines are ready after the time-out, the task can:

    - Perform deployment to the machines that are currently ready.
    - Stop without performing deployment to any machine. The task will start at its next scheduled time and will again begin waiting for the readiness of all machines.

Start condition for deployment

12. Review the task summary, and then click **Create** to create and save the task.

The task appears in the **Deployment tasks** view. When the task is started, the connected machines' IP addresses and the task progress are displayed in that view.

When the task is finished, its log entries will be available in the log of the deployment server.

Deployment in another subnet

Machines in another subnet (behind a network switch or router) can be woken up through the Acronis Wake-on-LAN Proxy component.

If OS Deploy Server is installed in one subnet (Subnet 1) and the target machines in another subnet (Subnet 2), prepare deployment as follows:

1. Install Acronis Wake-on-LAN Proxy in Subnet 2.
2. Prepare Acronis PXE Server in either of these ways:
   - Install the PXE server in Subnet 2 and configure that PXE server. This way, only machines in Subnet 2 can boot to the PXE server.

   OR
   - Install the PXE server in Subnet 1. Enable this PXE server to also work in Subnet 2 by configuring the network switch to relay the PXE traffic. The PXE server's IP addresses are

configured on a per-interface basis using IP helper functionality in the same way as DHCP server addresses. For more information, see this article from Microsoft. This way, machines from both subnets can boot to this PXE server.
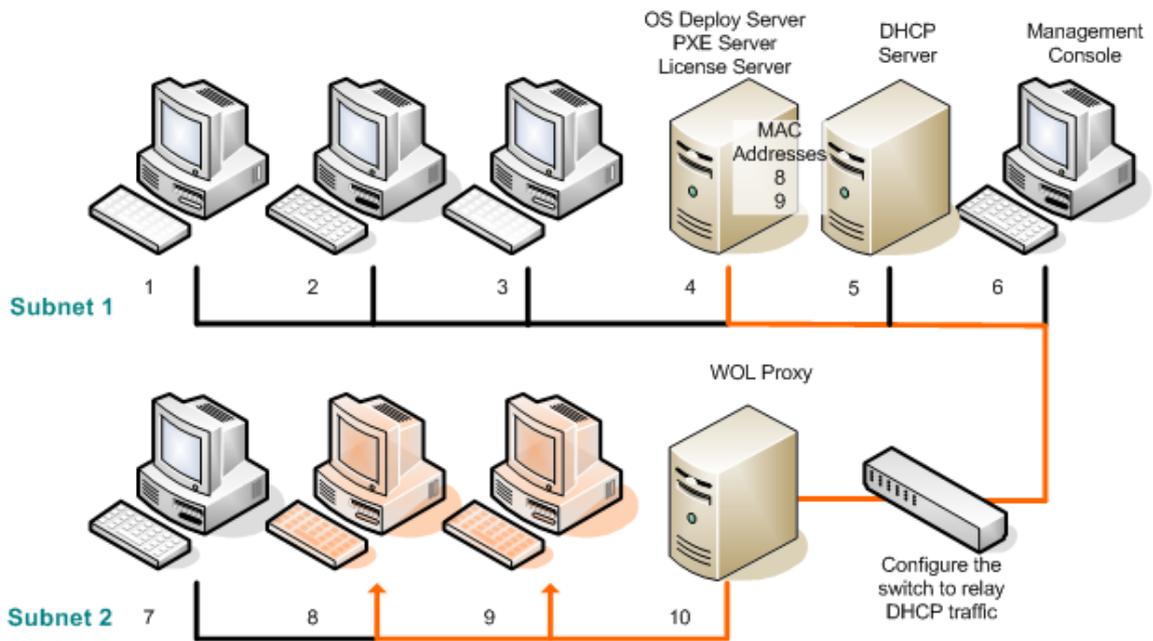
Deployment in another subnet by using Acronis Wake-on-LAN Proxy. The network switch is configured to relay the PXE traffic and DHCP traffic.

3. Create the deployment task. When creating the deployment task, specify the Wake-on-LAN proxy and specify the PXE server that you prepared in the previous step.

Note

If your router also acts as a Network Address Translation (NAT) device, see also "Deployment behind an NAT device".

Deployment to any ready machines

Deployment to any ready machines starts when a specified number of machines becomes ready. OS Deploy Server counts how many machines have connected to it, and starts deployment when a specified number of machines is reached. Deployment is usually performed by multicasting.

You can specify a time-out period. After the time-out, deployment will start anyway on the machines that will be ready at that moment.

This way of deployment decouples configuring the deployment operation from booting the target machines. You configure the deployment first, no matter whether the target machines are ready or not, and then boot the machines. The operation will start as soon as the target machines are ready or (optionally) on a time-out.

To create a deployment task for any ready machines

1. Do one of the following:
   - Create a bootable media with Agent.

OR

- Connect the management console to Acronis PXE server and upload Agent.

2. Start Management Console.

3. In the welcome screen, click **Deploy image**. If prompted, specify the machine where OS Deploy server is installed.

4. In **Deploy to**, select **Any machines ready for deployment**.

5. Select the condition that triggers the deployment:

   - Specify the number of machines that you need to deploy; for example, 70 machines.

   - Choose whether you want the deployment to start anyway after a time-out.

     If you do not specify a time-out (clear the **Deploy anyway after** check box), the deployment server will wait until any 70 machines boot into Agent and connect to the deployment server.

     If you specify a time-out, the deployment will start either when any 70 machines connect, or when the time runs out and at least one machine is connected. If no machine is connected, the task will stop.
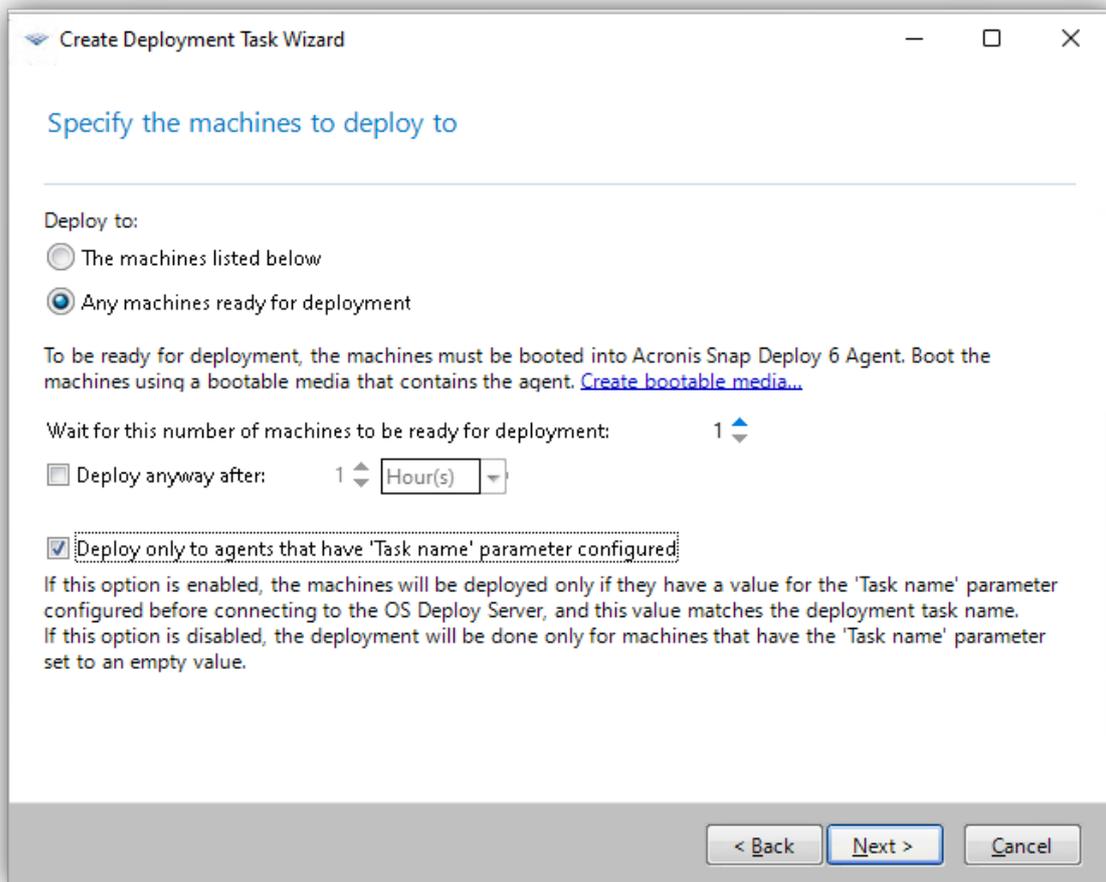
Triggering conditions for the deployment

6. [Optional] To limit the deployment only to machines that have a task name value equal to the name of the deployment task, select **Deploy only to agents that have "Task name" parameter configured**.

Use this option to ensure that a particular master image will be deployed only to selected target machines. This is especially handy when you perform multiple parallel deployments of different master images.

> **Note**
> This option requires that the **Task name** value is set in the Acronis Snap Deploy agent configuration on those machines. See "Booting the target machines" (p. 131).

When the deployment task runs, the server checks the **Task name** value retrieved from all agents connected to the OS Deploy Server. The deployment is performed only to machines where the **Task name** value matches the name of the deployment task.

If this option is disabled, the deployment is performed only to machines that have no value set in the **Task name** field of the Snap Deploy agent configuration.

> **Note**
> This functionality is not supported for online deployments.

7. Click **Next**.
8. Create a deployment template or select an existing one.
9. Review the deployment operation summary and click **Create** to create and save the deployment task. You can see the task in the **Deployment tasks** view. The task will be in the **Waiting for machines** state until the specified number of machines is connected.
10. Boot the target machines into Acronis Snap Deploy 6 from the bootable media or the PXE server.

As the target machines connect to the deployment server, they appear in the **Machines** view with a state of **Ready**.

While the deployment server is waiting, you are able to cancel the deployment by selecting the task and then clicking **Stop** on the toolbar.

As soon as the triggering condition arises, the available machines become engaged in the deployment, and their state changes to **Running**.

Booting the target machines

You need to manually boot the target machines into Agent in the following cases:

- To perform deployment to any ready machines
- To perform deployment to the specific machines that do not support the Wake-on-LAN functionality

You can boot the machines by using a bootable media or Acronis PXE Server. Alternatively, you can configure online deployment to the target machines.

To boot a target machine

1. Do one of the following:
   - Create a bootable media with Agent.

OR

- Connect the management console to Acronis PXE Server and upload Agent.

Note

When creating the bootable media or uploading Agent to the PXE server, you can configure the agent to start automatically after a time-out.

2. Boot the target machine into Agent from the bootable media or the PXE Server.
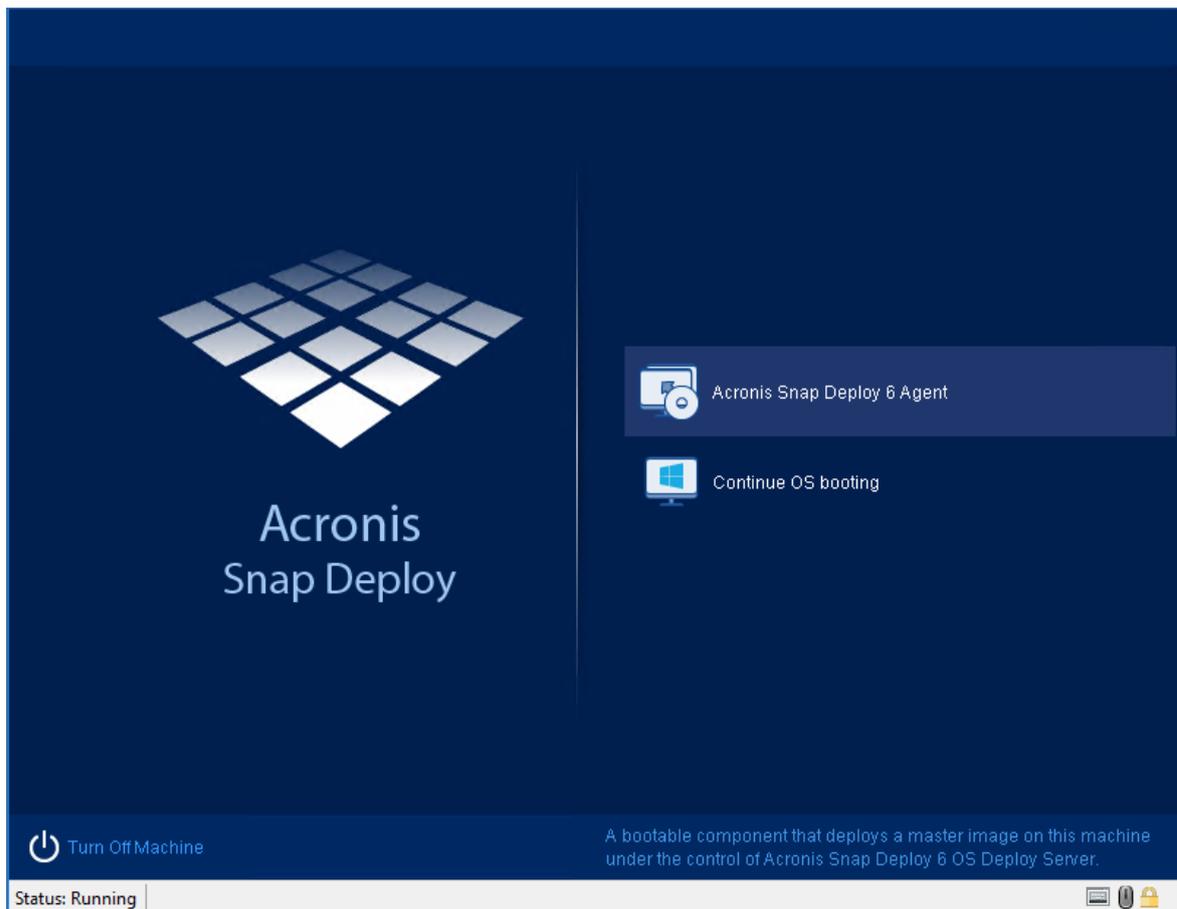
The boot menu on the target machine's side

3. Select Agent in the boot menu. You can skip this step if you configured the agent to start automatically.

4. [Optional.] Choose whether you want to configure the agent. The agent configuration includes the network settings and the address of OS Deploy Server. A dialog box comes up suggesting that you configure the agent.

   To load the agent with the default configuration (recommended in most cases), click **Cancel** or wait until the dialog box disappears after the time-out. To configure the agent before loading (recommended if your network does not have a DHCP server), click **OK**.
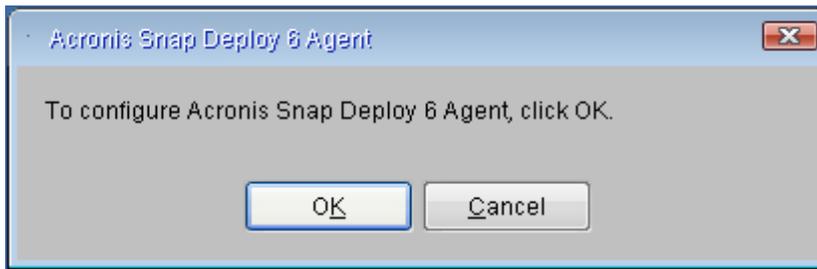
Prompt for configuring the agent on the target machine's side

With the default configuration, the agent:

- Takes the network settings, such as the IP address, from the DHCP server (uses DHCP auto configuration).
- Connects to the OS Deploy Server that you specified when creating the bootable media or uploading the agent. If you did not specify a deployment server, the agent connects to the first deployment server it finds on the network.

You can load the agent with the default configuration if there is a DHCP server and only one OS Deploy Server on the network.

To configure the agent

You can configure the following settings for the agent.

Configuring the OS deployment server

- In the **Server address** field, enter the DNS name or IP address of the deploy server the agent will connect to.
 This option enables you to have multiple deployment servers that perform different functions on the same network. If you leave this field empty, the software will search for the deployment server automatically.

Note
Acronis bootable media uses NetBIOS networking protocol to resolve OS Deploy Server in a network. NetBIOS protocol uses ANSI characters for host names. So, machines that have non-English characters in their names cannot be accessed from Acronis bootable media. If the name of the OS Deploy Server machine contains non-English characters, use the machine's IP address to specify it in the network.
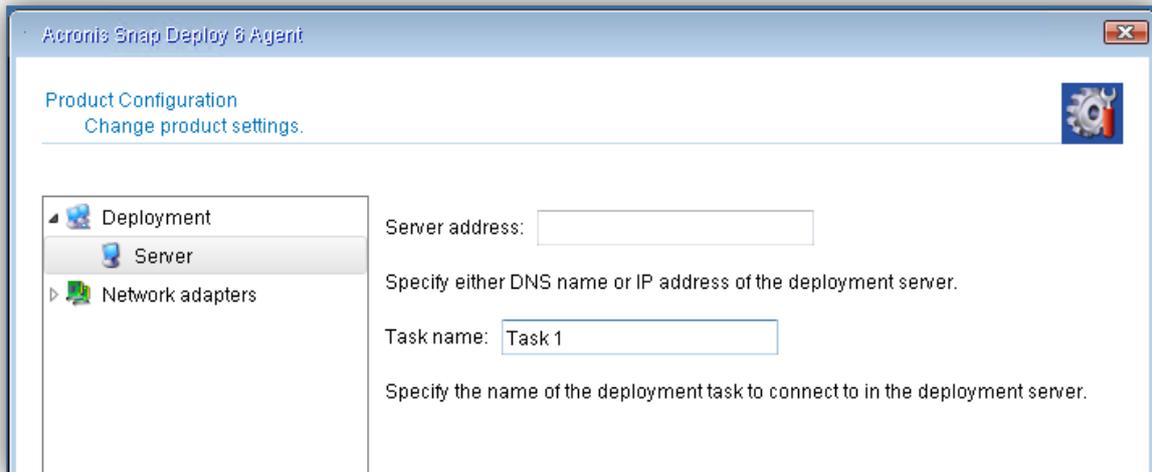
Configuring a deployment task name

- To configure the agent to allow deployments by a specific deployment task only, enter the name of that deployment task in the **Task name** field. See "Creating the deployment task" (p. 125).

Note
The option **Deploy only to agents that have 'Task name' parameter configured** must be enabled in the deployment task with that name.

When the deployment task runs, the server checks the **Task name** value retrieved from all agents connected to the OS Deploy Server. The deployment is performed only on machines where the **Task name** value matches the name of the deployment task.

If you leave the **Task name** field empty, all deployment tasks that do not have the option **Deploy only to agents that have 'Task name' parameter configured** enabled will perform deployment of the master image to this machine.

Note
This functionality is not supported for online deployments.

Configuring the network settings

You can configure the network settings for each network adapter of the target machine. This option enables you to manually specify network configuration if automatic configuration is not possible (for example, if no DHCP server is present on your network).

- To change the network settings for a current session, click **Acronis Snap Deploy 6 Agent** in the startup window. The **Product configuration** window that appears will allow you to configure network settings for each network interface card (NIC) of the machine.

Changes made during a session will be lost after the machine reboots.

Adding VLANs

- In the **Product configuration** window, you can add virtual local area networks (VLANs). Use this functionality if you need access to a backup location that is included in a specific VLAN.

Note

The VLAN settings configured on the Windows machine where you run the Media Builder are included in the created Linux-based media automatically, so you do not need to create them manually after booting from that media.

VLANs are mainly used to divide a local area network into segments. A NIC that is connected to an access port of the switch always has access to the VLAN specified in the port configuration. A NIC connected to a trunk port of the switch can access the VLANs allowed in the port configuration only if you specify the VLANs in the network settings.

Configuring Wi-Fi settings

You can configure Linux-based media to connect to a Wi-Fi network after booting. Thus, on machines with no Ethernet connection, the media can connect the machine to an OS Deploy Server via Wi-Fi and start the deployment from there.

If the Wi-Fi connection details have been included in the Linux-based media during media creation the machine will connect to the specified WI-Fi network automatically.

- In the **Product configuration** window, click **Wi-Fi settings** and select one of the available Wi-Fi networks. A dialog will prompt you to enter the password. Enter the password and click **Join**.

To enable access to a VLAN via a trunk port

1. Click **Add VLAN**.
2. Select the NIC that provides access to the local area network that includes the required VLAN.
3. Specify the VLAN identifier.

After you click **OK**, a new entry appears in the list of network adapters.

If you need to remove a VLAN, click the required VLAN entry, and then click **Remove VLAN**.

Configuring the agent on the target side

Set the preferable values, and then click **OK**.

When Agent starts and the target machine is ready for deployment, the target machine displays the following window:
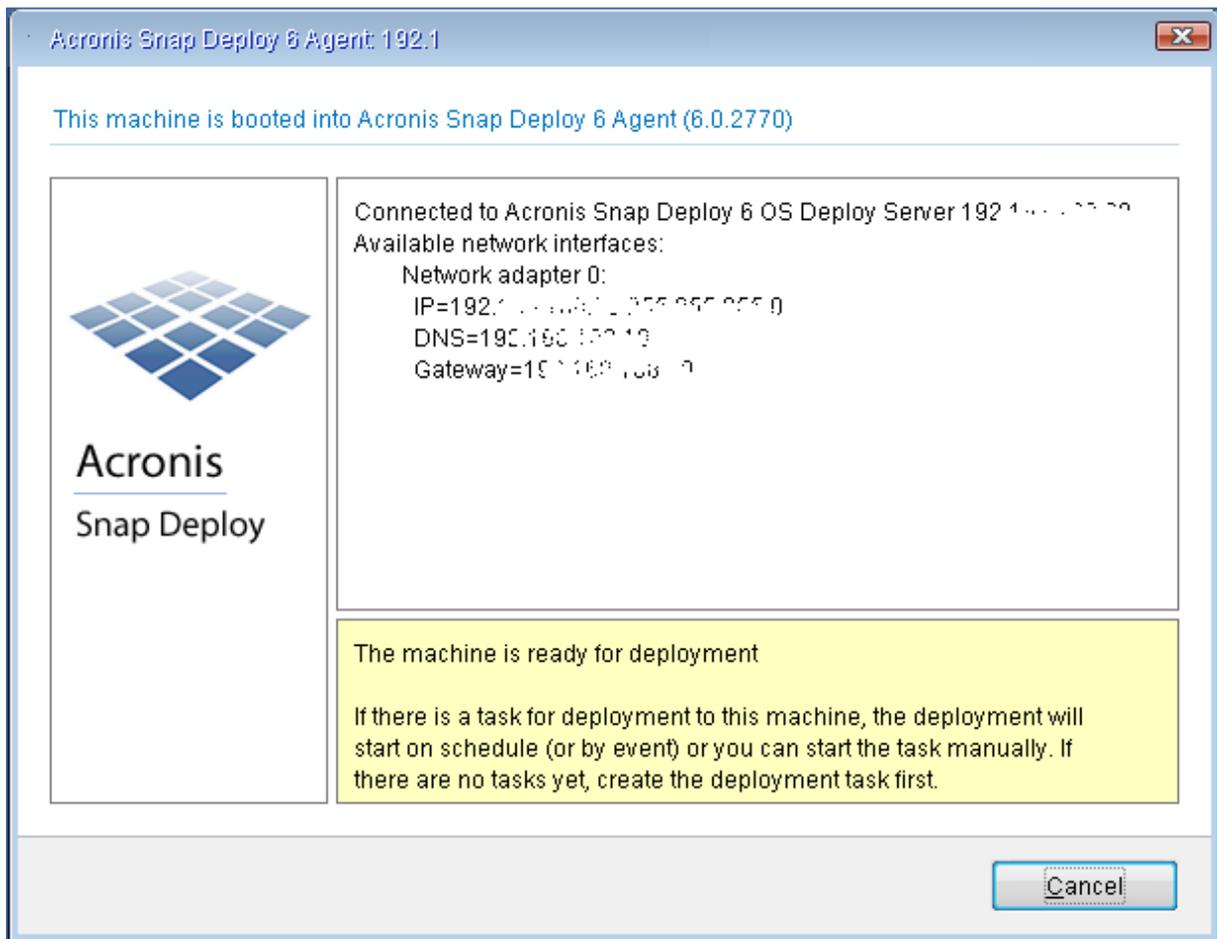
Agent: ready for deployment

Configuring online deployment

OS Deploy Server can automatically reboot online target machines (running Windows) into Agent and make them ready for deployment every time the deployment starts.

To configure online deployment

1. Install Management Agent on the target machines.

   The machines will appear in the **Machines** view and will have the **Online** state.
2. Start Management Console.
3. In the welcome screen, click **Deploy image**. If prompted, specify the machine where OS Deploy server is installed.
4. In **Deploy to**, select **The machines listed below**.
5. Select **Add machines -> From machine list**, and then select machines that have the **Online** state in the **Machines** view.
6. Click **Next**.
7. Create a deployment template or select an existing one.
8. Configure the **Online deployment** setting in the deployment template.

9. Specify when to run the task (set up the deployment schedule):

- **Now**: The task will run immediately after you create it.
- **Once later**: The task will run once at the specified date and time.
- **Daily**: The task will run at the selected times every day or every few days.
- **Weekly**: The task will run on the selected days every week or every few weeks.
- **Monthly**: The task will run on the selected day every month.
- **Manually**: The task will run only when you start it manually.

If prompted, specify the credentials for running the task.

Important

When the scheduled time comes, the target machines must be turned on.

With any deployment schedule, you will be able to start the task manually by selecting it in the **Deployment tasks** view and clicking **Run** on the toolbar.

10. Specify a time-out for waiting for all listed machines to become ready, and the action after the time-out.

In practical situations, some of the listed machines might not connect to the deployment server at the scheduled time. For example, they may be in use at that time. The task waits for listed machines to become ready for the time you specified. As soon as all machines are ready, the task starts deployment.

If not all machines are ready after the time-out, the task can:

- Perform deployment to the machines that are currently ready.
- Stop without performing deployment to any machine. The task will start at its next scheduled time and will again begin waiting for the readiness of all machines.

Start condition for deployment

11. Review the task summary, and then click **Create** to create and save the task.

The task appears in the **Deployment tasks** view. When the task is started, the connected machines' IP addresses and the task progress are displayed in that view.

When the task is finished, its log entries will be available in the log of the deployment server.

Operations with deployment tasks

Once a deployment task is created, it appears in the **Deployment tasks** view.
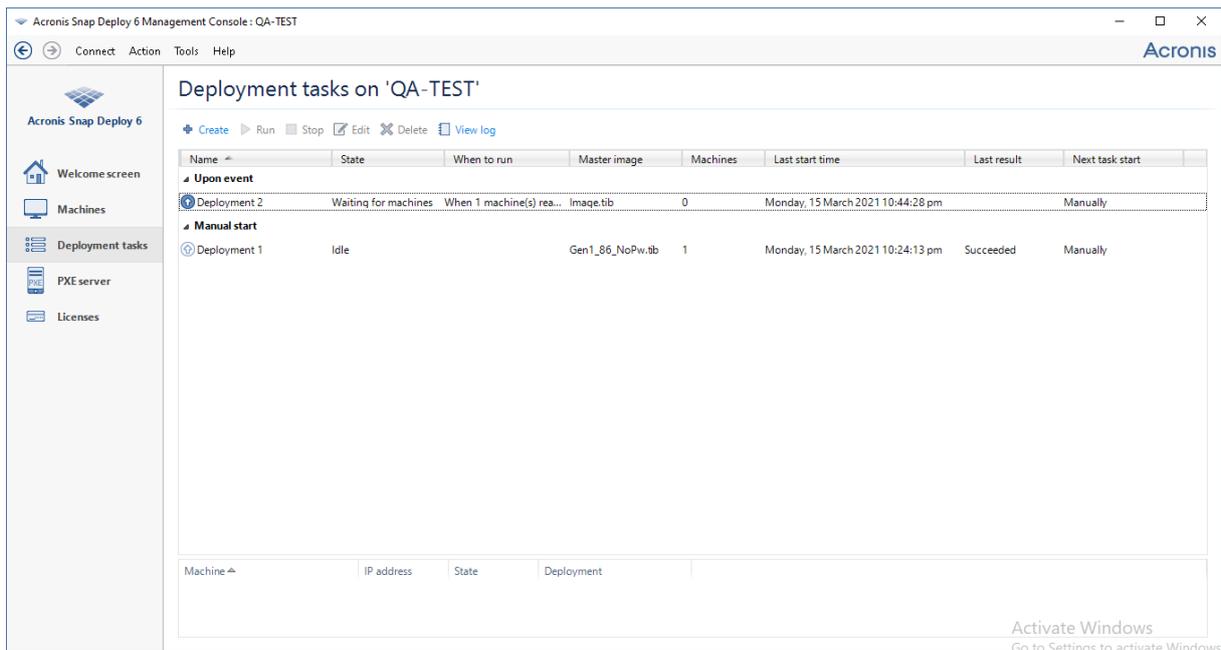
List of deployment tasks

To edit a task (for example, to change its schedule), select it and click **Edit**. Editing is performed in the same way as creation; but, the previously selected options are already set, so you need to enter only the changes.

Any task stays on the deployment server until you delete it. To delete a task, select the task and then click **Delete**.

To run a task immediately, select the task and then click **Run**. The task schedule remains unchanged.

You cannot edit or delete a task while it is running.

Deployment behind an NAT device

Successful deployment is not guaranteed if OS Deploy Server and the target machines are separated by a Network Address Translation (NAT) device. A typical router usually acts as an NAT device.

All machines behind an NAT device normally form a separate subnet and appear to the deployment server as having the same IP address. This may lead to problems when connecting to components of Acronis Snap Deploy 6 and when showing the deployment progress for each target machine.

To avoid these problems, we recommend installing OS Deploy Server in the same subnet as the target machines.

If installing the deployment server in that subnet is not possible, configure the NAT device as follows:

1. Set up *port forwarding* for the NAT device:
    *   If Acronis Wake-on-LAN Proxy is installed in that subnet, forward the TCP and UDP ports 9876 to the machine with the Wake-on-LAN proxy.
    *   If Acronis PXE Server is installed in that subnet, forward UDP ports 67, 68, and 69 to the machine with the PXE server.
2. When creating the deployment task, specify the IP address of the NAT device when asked about the address of the PXE server and/or of the Wake-on-LAN proxy.

Even after you configure the NAT device this way, you might still receive inconsistent information about the deployment progress for each machine.

User-initiated deployment (custom deployment)

Acronis Snap Deploy 6 can be configured in such a way that users will be able to deploy and re-deploy their machines with one click on the boot menu.

User-initiated deployment is also called custom deployment.

Understanding user-initiated deployment

An administrator creates a set of deployment templates that meet the organization's needs and assigns to each template a name that can be easily understood by a user.

The administrator creates an Acronis bootable media with these templates or uploads these templates to a PXE server. The administrator then switches on the user-initiated deployment mode.

Users who need to redeploy their machines boot the machines from the bootable media or the PXE server, and select the template by name from the boot menu.

Note
If a machine does not boot from the bootable media or the PXE server and the machine has Secure Boot enabled, we recommend disabling Secure Boot on this machine as a workaround.

The deployment starts immediately and proceeds independently on each machine.
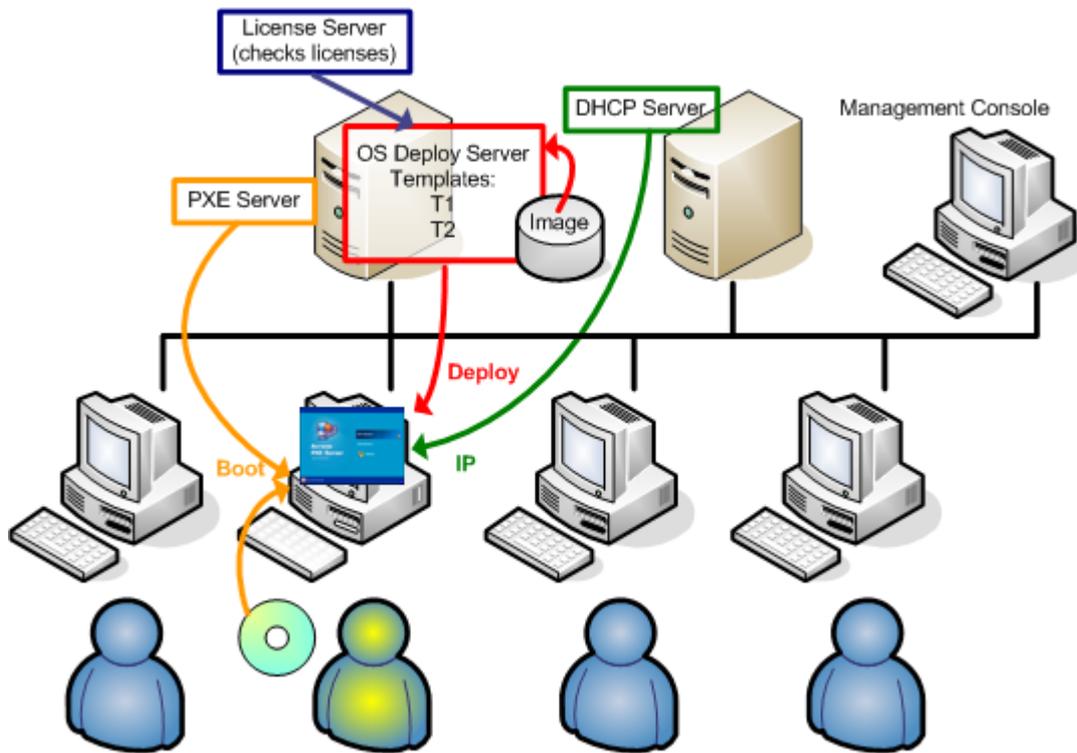
User-initiated deployment mode: a user starts deployment.

In software testing labs, the choices can be various operating systems, various editions of the same operating system, or the same operating system with various settings or applications. In a university or school lab, the choices can be various exercises that students have to explore, or the initial system image for the purpose of self-restore.
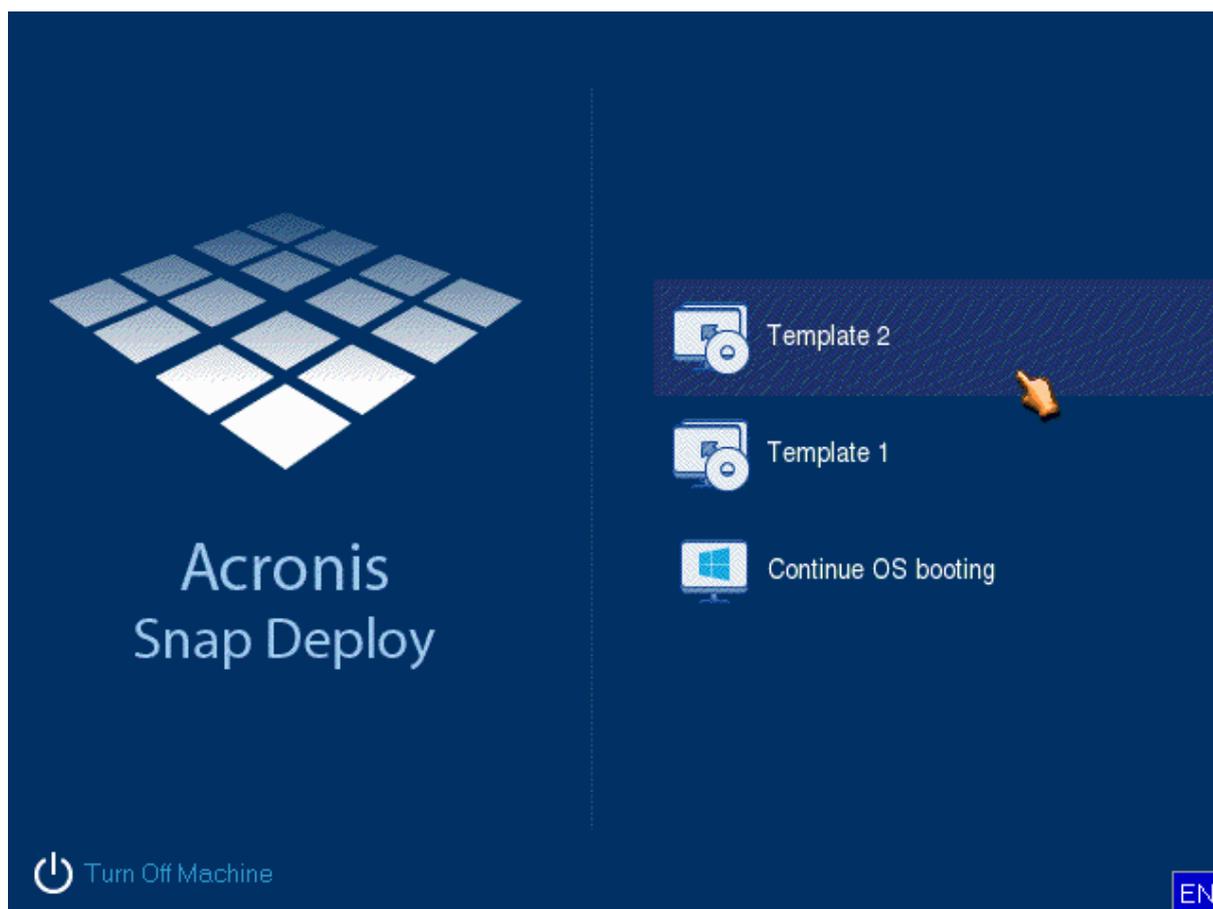
The custom boot menu. A user can start deployment with any of the two templates or boot into Windows.

Note

To find a template in the custom boot menu, press a letter key which corresponds to the first letter of the template name. The cursor will jump on the first template whose name starts with the pressed letter.

Important

If the user-initiated deployment uses a PXE server, machines that are deployed through deployment tasks will not be able to boot from that PXE server. However, deployments to such machines will be possible if they boot from a bootable media.

The user-initiated deployment mode is primarily intended for continual work without the administrator's assistance. Only users (the ones on the target side) will be able to initiate deployment. However, the administrator can view logs, create new deployment templates, change the user-initiated deployment configuration (add, edit or remove boot menu items) and perform other management operations except initiating the custom deployment.

Considerations when using a PXE server

When enabling or configuring the user-initiated deployment mode with Acronis PXE Server, the software first **removes all bootable components** (Agent, Master Image Creator, and the PE image)

from the PXE server, because users might be confused by the unknown items appearing in the boot menu. Then, the software uploads to the PXE server the templates selected by the administrator. So **you will have to upload the bootable utilities again,** if they are needed after switching off the user-initiated deployment mode.

If you need to perform both user-initiated deployment and deployment through a deployment task, you can use the PXE server for the former and bootable media for the latter.

Alternatively, you can use another OS Deploy Server to perform deployment through deployment tasks, while one OS Deploy Server is in the user-initiated deployment mode. To do so, ensure that the target machines connect to the appropriate deployment server, by specifying the deployment server when creating the bootable media or by configuring Agent at boot. Two deployment servers cannot use the same Acronis PXE Server.

Setting up the user-initiated deployment mode

Preparation

1. Install Management Console and License Server. Import licenses to the license server. Install OS Deploy Server and Acronis PXE Server. All these components are already installed if you have performed a typical installation.
2. Configure and image the master system (or systems), either from a bootable media with Master Image Creator or by using Management Agent.

To set up user-initiated deployment

1. Start Management Console.
2. In the welcome screen, click **Configure user-initiated deployment**. If prompted, specify the machine where OS Deploy server is installed.

    Note
    If you are planning to use an Acronis PXE Server with user-initiated deployment and there are active operations that use that PXE server, either cancel those operations or wait until they are completed, before proceeding. See also "Considerations when using a PXE server".

3. Create the deployment templates according to your organization's needs. Assign to each template a name that can be easily understood by the users. Select one or more templates to be added to the boot menu.
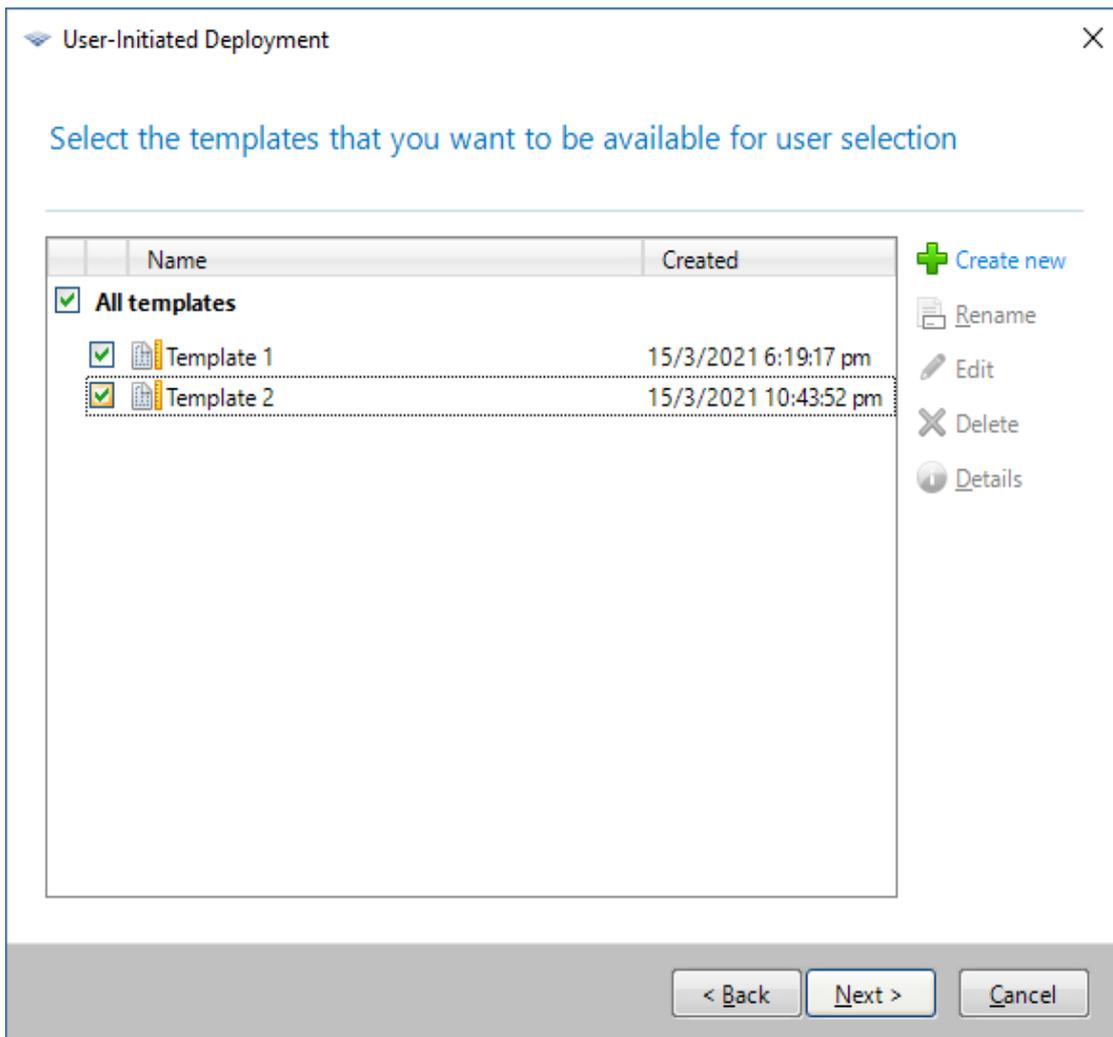
Adding templates to the boot menu

4. Select how to display the boot menu. For example, you can choose to start a particular deployment template automatically after a time-out.

5. Select whether you want to create an Acronis bootable media (a removable media or an ISO file of the media) or to upload the templates to Acronis PXE Server.

    • Having saved the ISO file, you can create as many media copies as the users need by using third-party CD/DVD burning software. When creating a bootable media for user-initiated deployment, you can specify network settings, such as the name of the deployment server, in the same way as when creating any other bootable media. For details, see "Creating an Acronis bootable media".

    • The templates being uploaded to the PXE server can be protected with a password to prevent the templates from unauthorized execution. A password prompt will come up when the user selects a template in the boot menu. No password will be required to start the operating system.

6. Review the operation summary and then click **Switch on** to proceed. The software creates the media with the custom boot menu. OS Deploy Server switches to the user-initiated deployment mode.
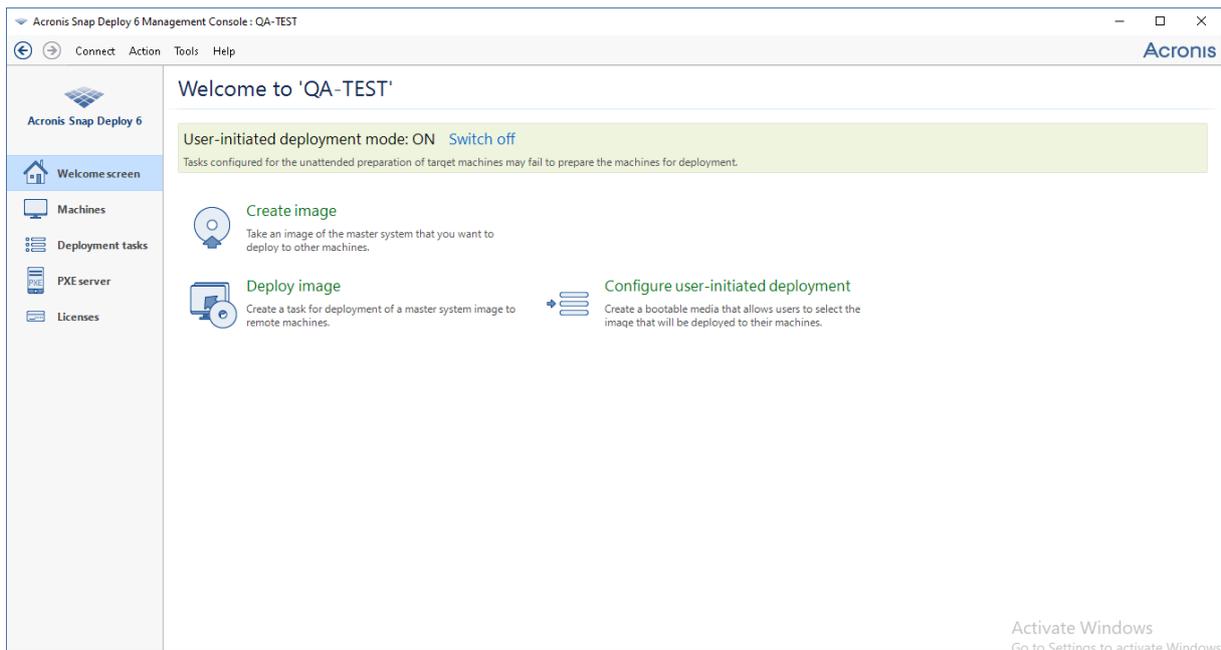
OS Deploy Server in the user-initiated deployment mode

In the **Machines** view, the administrator can see the status of the user-initiated deployment for each machine.

While the deployment server is in the user-initiated deployment mode, the administrator can:

- Change parameters of the user-initiated deployment mode.
- Create a new media for the user-initiated deployment mode.
- Stop the selected operation, if need be, by right-clicking the corresponding machine in the **Machines** view, and then clicking **Cancel deployment**.
- Switch off the user-initiated deployment mode.

The user who requested deployment sees the following screen while the deployment is in progress.
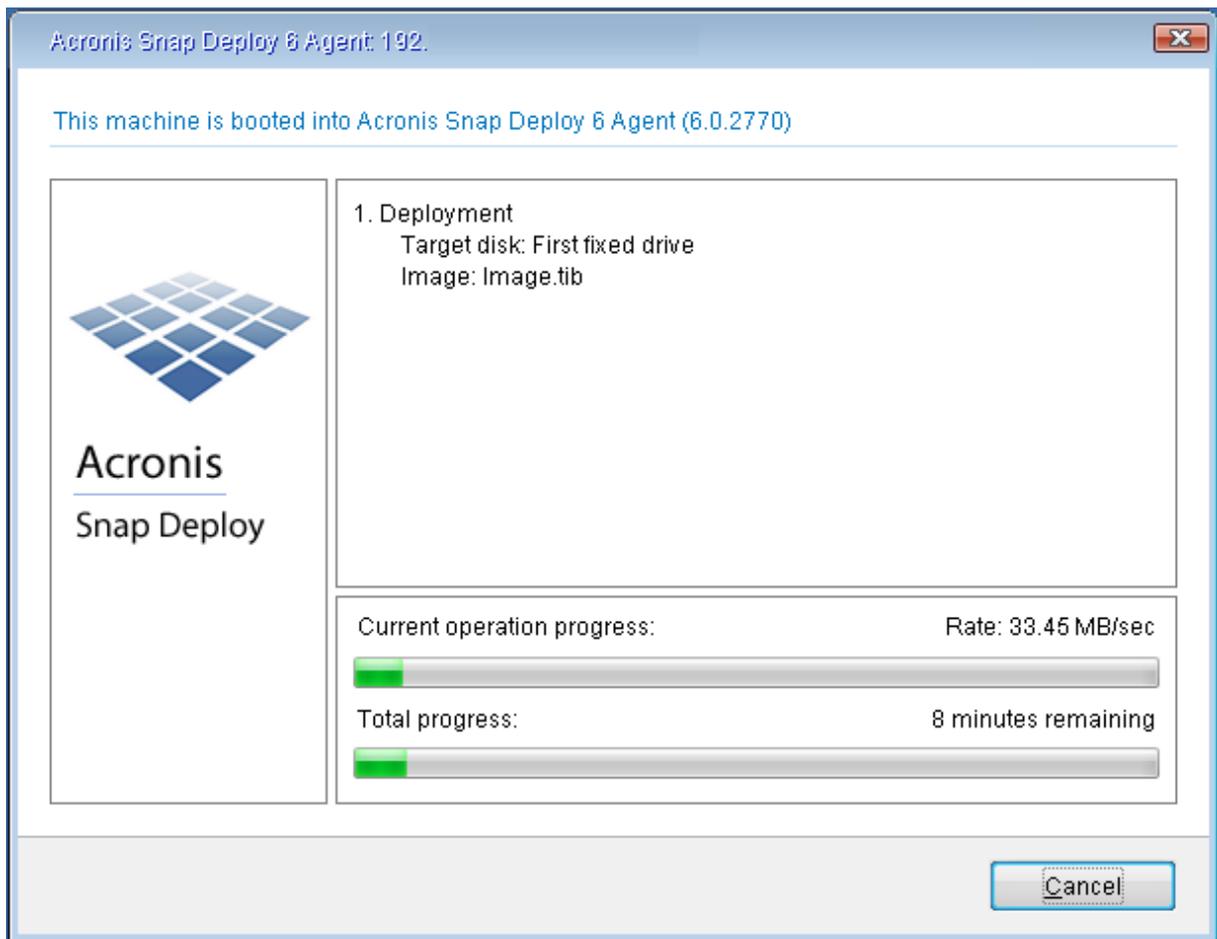
User-initiated deployment in progress: view on the target machine's side

Changing parameters of the user-initiated deployment mode

To change the templates or the boot menu password used in the user-initiated deployment mode, you need to reconfigure the user-initiated deployment mode.

1. If some user-initiated deployment operations are active, either stop the operations or wait until the operations are completed.
2. In the welcome screen of the management console, click **Configure user-initiated deployment**, and then repeat the procedure described in "Setting up the user-initiated deployment mode". The earlier selected options will be set, so you have to enter only the changes.

Switching off the user-initiated deployment mode

To switch off the user-initiated deployment mode

1. If some user-initiated deployment operations are active, either stop the operations or wait until the operations are completed.
2. In the welcome screen of the management console, in the **User-initiated deployment mode** area, click **Switch off**.

3. If the user-initiated deployment mode uses Acronis PXE Server, the software needs to remove the custom deployment templates from the server. If prompted, specify the credentials for the PXE server (the user name and password of an administrator on the machine with the PXE server).

Stand-alone deployment

Stand-alone deployment is deployment to a machine that is isolated from the network or included in a network without Acronis Snap Deploy 6 infrastructure (to be exact, without OS Deploy Server). Stand-alone deployment is performed locally by using the bootable component called Standalone Utility.

To perform a stand-alone deployment

1. Install Management Console.
2. Create an Acronis bootable media with Master Image Creator and Standalone Utility.

> **Note**
> Standalone Utility can be placed on a physical media only. This component is not designed to boot from a PXE server.
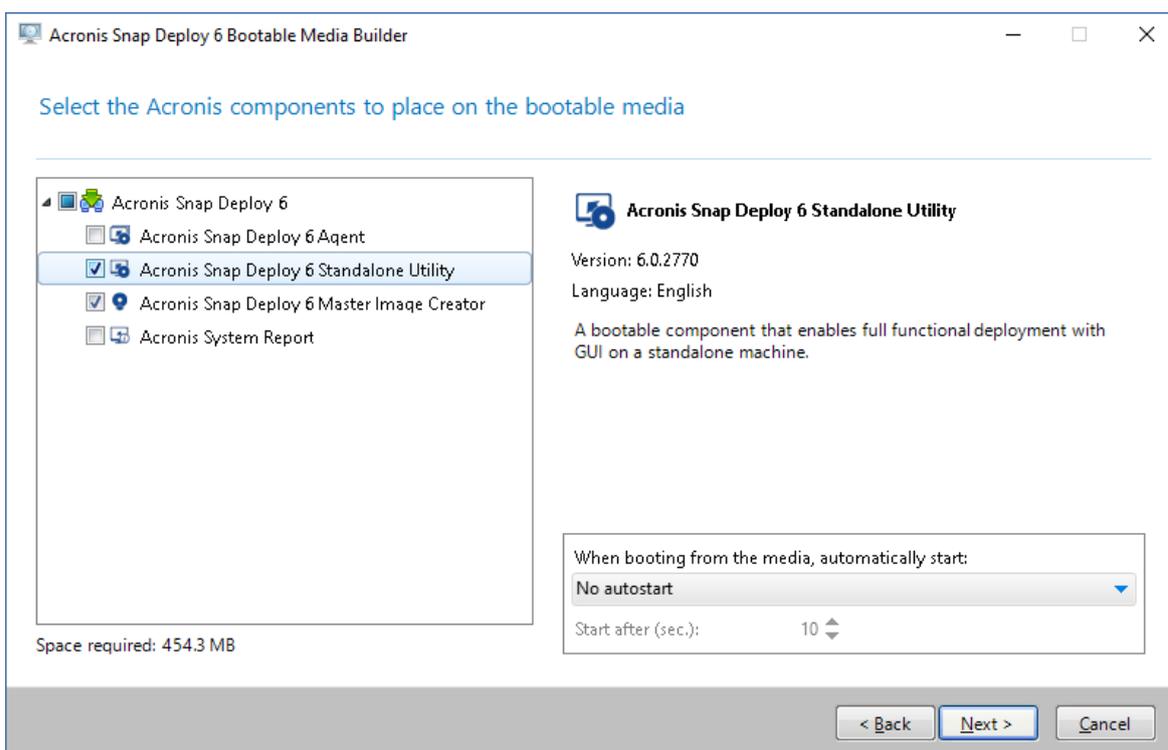
The Acronis stand-alone components to be placed on the bootable media

3. Configure the master machine.
4. Boot the master machine into Master Image Creator. If the machine fails to boot into the master image creator and the machine has Secure Boot enabled, we recommend temporarily disabling Secure Boot on this machine as a workaround.

5. Create an image of the master machine and save it to a network folder, detachable media, or removable media. You should not save the image to an internal hard disk of the target machine, because it cannot be accessed during the stand-alone deployment.

6. Boot the target machine into Standalone Utility. If the machine fails to boot into the stand-alone utility and the machine has Secure Boot enabled, we recommend temporarily disabling Secure Boot on this machine as a workaround.

7. If you saved the master image to a media, attach or insert the media.

   Standalone Utility can deploy an image located:

   • In a network folder.

   • On a USB or FireWire (IEEE-1394) storage device (such as a flash drive) attached to the target machine.

   • On DVD+R/RW, DVD-R/RW, CD-R/RW, or recordable Blu-ray Discs (BD-R, BD-RE) loaded in the target machine's media drive.

8. Configure the deployment operation as described in "Creating a deployment template". Note that the template cannot be saved because the stand-alone utility does not access OS Deploy Server.

9. Review the deployment settings, and then start the stand-alone deployment.

Deploying BIOS-based systems to UEFI-based and vice versa

Acronis Snap Deploy 6 supports transferring 64-bit Windows operating systems between BIOS-based hardware and hardware that supports Unified Extensible Firmware Interface (UEFI).

How it works

Depending on whether the machine uses BIOS or UEFI firmware for booting, the disk with the system volume must have a specific *partition style*. The partition style is master boot record (MBR) for BIOS, and GUID partition table (GPT) for UEFI.

In addition, the operating system itself is sensitive to the type of firmware.

When performing a deployment to a machine that has a type of firmware that is different from the firmware of the original machine, Acronis Snap Deploy 6:

• Initializes the disk to which you are deploying the system volume either as an MBR disk or as a GPT disk, depending on the new firmware.

• Adjusts the Windows operating system so that it can start on the new firmware.

For details, including the list of Windows operating systems that can be adjusted this way, see "Deploying volumes" and "Deploying disks" in this section.

Recommendations

- Deploy the entire system onto uninitialized disks.
- When migrating to UEFI-based hardware, use Acronis bootable media or WinPE-based bootable media of versions later than 4.0. Earlier versions of WinPE do not support UEFI.
- Remember that BIOS does not allow using more than 2 TB of disk space.

Limitations

Transferring a Linux system between UEFI and BIOS is not supported.

Transferring a Windows system between UEFI and BIOS is not supported if a master image is burnt to an optical disc (a CD, a DVD, or a Blu-ray disc).

When transferring a system between UEFI and BIOS is not supported, Acronis Snap Deploy 6 initializes the target disk with the same partitioning scheme as the original disk. No adjustment of the operating system is performed. If the target machine supports both UEFI and BIOS, you need to enable the boot mode corresponding to the original machine. Otherwise, the system will not boot.

Deploying volumes

Let's assume you have created a master image of the system and boot volumes (or the entire machine) and want to deploy these volumes to a different platform. The ability of the deployed system to boot up depends on the following factors:

- **Source operating system:** is the OS convertible or non-convertible? Convertible operating systems allow changing the boot mode from BIOS to UEFI and back.
  - 64-bit versions of all Windows operating systems starting with Windows Vista SP1 are convertible.
  - 64-bit versions of all Windows Server operating systems starting with Windows Server 2008 SP1 are convertible.

  All other operating systems are non-convertible.
- **Source and target disk partition style**: MBR or GPT. System and boot volumes of BIOS platforms use MBR disks. System and boot volumes of UEFI platforms use GPT disks.

  When selecting a non-initialized target disk for deployment, this disk will be automatically initialized either to GPT or to MBR depending on the original disk partitioning style, the current boot mode (UEFI or BIOS) and the type of operating systems (convertible or non-convertible) that are located on this volume.

  If the initialization may result in bootability loss, the software takes the partitioning style from the source volume ignoring the target disk size. In such cases, the software can select the MBR partitioning style for disks whose size is more than 2 TB; however, the disk space beyond 2 TB will not be available for use.

  If required, you can initialize the target disk manually by using a third-party partitioning tool, such as Microsoft Disk Management or Acronis Disk Director.

The following table summarizes whether it is possible to retain the system bootability when deploying boot and system volumes of a BIOS-based system to UEFI-based and back.

- A green background means that the system will be bootable. No user action is required.
- A yellow background means that you need to perform additional steps to make the system bootable. These steps are not possible on some machines.
- A red background means that the system will not be able to boot due to BIOS and UEFI platform limitations.

Original system	Target hardware			
	BIOS Disk: MBR	BIOS Disk: GPT	UEFI Disk: MBR	UEFI Disk: GPT
BIOS OS: convertible		**Solution** Deploy the operating system to an MBR disk or to an uninitialized disk.	*The target machine must support BIOS.* **Additional steps** Before deployment, turn off the UEFI mode in BIOS	The convertible OS will be automatically converted to support UEFI booting.
BIOS OS: non-convertible			Perform the deployment under the bootable media. or After deployment, turn off the UEFI mode in BIOS.	**Solution** Deploy the operating system to an MBR disk or to an uninitialized disk.
UEFI OS: convertible	The convertible OS will be automatically converted to support BIOS booting.	*The target machine must support UEFI.* **Additional steps** Before deployment, turn on the UEFI mode in BIOS. Perform the deployment under the bootable media. or After deployment, turn on the UEFI	**Solution** Deploy the operating system to a GPT disk or to an uninitialized disk.	

UEFI OS: non-convertible	**Solution** Deploy the operating system to a GPT disk or to an uninitialized disk.	mode in BIOS.		

Deploying disks

Let's assume you have created a master image of a whole disk (with all its volumes) and want to deploy this disk to a different target platform.

The ability of the deployed system to boot up in different modes depends on the operating systems installed on the source disk. Operating systems can be **convertible** i.e. allow changing the boot mode from BIOS to UEFI and back, or **non-convertible**. For the list of convertible operating systems, see "Deploying volumes".

- When a source disk contains one or more operating systems and *all* of them are convertible, the boot mode can be automatically changed. Depending on the current boot mode, the target disk may be initialized either to GPT or to MBR partitioning style.
- If *at least one* operating system on a source disk is non-convertible (or the source disk contains any boot volumes of the non-convertible OSes), the boot mode cannot be changed automatically and the software will initialize the target disk as the source one. To boot up the target machine, you have to turn on/off the UEFI mode in BIOS manually. Otherwise, the deployed system will not boot.

The following table summarizes all cases of deploying disks of a BIOS-based system to UEFI-based and vice versa.

- Green background means that the system will be bootable. No user action is required.
- Yellow background means that you need to perform additional steps to make the system bootable. These steps are not possible on some machines.

Original system	Target hardware	
	BIOS	**UEFI**
BIOS **OS: convertible**		The target disk will be initialized as GPT. The OS will be automatically converted to support UEFI booting. If you want to deploy the source disk "as is": Turn off the UEFI mode in BIOS. Boot from a bootable media, and perform the deployment.

BIOS **OS: non-convertible**		The target disk will be initialized as the source one (MBR). *The target machine must support BIOS.* **Additional steps** Turn off the UEFI mode in BIOS. Boot from a bootable media, and perform the deployment.
UEFI **OS: convertible**	The target disk will be initialized as MBR. The OS will be automatically converted to support BIOS booting. If you want to deploy the source disk "as is": Turn on the UEFI mode in BIOS. Boot from a bootable media, and perform the deployment.	
UEFI **OS: non-convertible**	The target disk will be initialized as the source one (GPT). *The target machine must support UEFI.* **Additional steps** Turn on the UEFI mode in BIOS. Boot from a bootable media, and perform the deployment.	

Deployment to large disks in BIOS

After a deployment to a BIOS-based system, the target system disk is initialized as MBR. Because of disk size limitations in BIOS, if the disk is larger than 2 TB, only the first 2 TB of disk space will be available for use. If the machine supports UEFI, you can overcome this limitation by turning on the UEFI mode and then performing the deployment. The disk is initialized as GPT. The 2-TB limitation for GPT disks does not exist.

Managing the list of machines (the Machines view)

The **Machines** view shows a list of machines for which you can set up deployment by using OS Deploy Server.

A machine is determined by the MAC address of its network adapter. A MAC address is a set of six hexadecimal numbers, such as: 01-35-79-BD-F1-23.

The list of machines includes:

- The machines that you added to the list. For example, you can add machines by using a file with MAC addresses.
- The machines that have ever connected to the deployment server.

The lower part of the window shows details about the selected machine and enables setting up individual deployment settings for it.

To open the Machines view

1. Start Management Console.
2. Click **Machines**. If prompted, specify the name or IP address of the machine with OS Deploy Server.

Adding machines

To add one or more machines to the list, do either of the following:

- Install Management Agent on the machines. The machines will be automatically added to the list.
- Click **Add machines** on the toolbar and add the machines in either of these ways:
  - **By MAC address**: Type the MAC address of the machine.

    Optionally, provide a label that will be shown in the **Machine** column.
  - **From file**: Specify a text file with the list of MAC addresses, one machine per line. If the machine has more than one network adapter, separate the MAC addresses for each adapter with a semicolon (;). No space character is allowed between the MAC addresses.

    The hexadecimal numbers in a MAC address can be separated by a colon (:) or a hyphen (-), or have no separator.

    Optionally, provide a label that will be shown in the **Machine** column. The label must follow the MAC address (or addresses). The label and the MAC address must be tab separated. In text editors such as Notepad, you can normally insert a tab character by pressing the TAB key. The label itself cannot contain a tab character.

    The following is a sample file:

    ```
    00:01:23:45:67:1A
    02-01-23-45-67-1B        My machine
    ```

```
010203040506    Machine 2
00-11-22-33-44-55;AA-BB-CC-DD-EE-FF      Machine 3
```

In either case, the label that you provide is unrelated to the network name of the machine. If no label is provided, the **Machine** column will contain the MAC address of the machine.

> **Note**
> Make sure that you specify the MAC address correctly. Any set of six hexadecimal numbers is recognized as a valid MAC address of a machine, even if a network adapter with that address does not actually exist.

- Import individual deployment settings from a file. The list will be automatically updated with machines that are specified in this file but are not present in the list yet. Specifying labels for the **Machine** column is not supported.

Groups of machines

Using groups helps you to organize the list of machines.

For example, you can create a separate group for each department in your organization. You can then perform deployment to some or all machines of a department by selecting them in the corresponding group.

Each machine can be a member of one or more groups.

To create a group, click **Create group** on the toolbar, and then type the name of the group.

To add one or more machines to a group, select them in the list, click **Add to group** on the toolbar, and then select the group to add the machines to.

A group itself cannot be specified for deployment.

To create a deployment task for all machines that are *currently* in a group, right-click the group, and then click **Deploy image**. Subsequent changes to the group do not affect the list of machines in the deployment task.

In addition to the groups you create, there is the **All machines** built-in group. It contains the entire list of machines.

Actions on machines

To perform an action on a machine, right-click that machine in the list. Most actions are also available when you select more than one machine.

The actions are the following:

- **Deploy image**: Starts the Create Deployment Task Wizard. By default, the deployment task is being created for the selected machine (or machines).
- **Cancel deployment**: Cancels the currently running deployment for the selected machine.

- **Add to group**: Adds the selected machines to a group you previously created.
- **Remove from group**: For the selected machines in a group, removes them from that group.
- **Delete**: Removes the selected machines from the list. The machine will reappear in the list the next time it connects to the deployment server.
- **Deny deployments**: Excludes the selected machines from any deployment through the deployment server. As a result:
  - Any deployment tasks do not apply to the machine. However, the list of machines in those tasks is not affected.
  - User-initiated deployment for the selected machines is not possible.
  - Stand-alone deployment for the selected machines is possible, because it does not use the deployment server.
- **Allow deployments**: Undoes the exclusion of the selected machines that was previously done by the **Deny deployments** action.
- **Set label**: Sets the label that is shown in the **Machine** column. For example, you can use the network name of the machine as the label. If no label is provided, the **Machine** column shows the MAC address of the machine.

States and results for machines

The **State** column shows the current state related to deployment.

The state can be one of the following:

- **Not ready**: The machine is not connected to the deployment server; for example, the machine is turned off.
  For deployment to specific machines, the deployment server will wake up the turned-off machine when the scheduled time comes or when you start the task manually.
  For deployment to any ready machines, you will have to boot the machine into Agent.
- **Online**: The machine is turned on and will automatically reboot into Agent and connect to the deployment server when the deployment task starts.
- **Ready**: The machine is booted into Agent and is connected to the deployment server, so the machine is ready for deployment.
- **In progress** (shown as percentage complete): A deployment is currently being performed to the machine.
- **Deployments denied**: You excluded the machine from deployment (see the **Deny deployments** action).

The **Last result** column shows the result of the last deployment operation on the machine.

The result can be one of the following:

- **Never deployed**: No deployment has yet been performed on the machine since it was added to the deployment server.
- **Succeeded**: The deployment to the machine finished successfully.

- **Failed**: The deployment to the machine failed. For example, no available license for performing deployment has been found on the license server. If performing the deployment started but did not finish successfully, the target disk or volume may be empty or contain inconsistent information.
- **Canceled**: You stopped the deployment task that was performing deployment to the machine (see the **Stop** action). The master image was not deployed to the machine. The target disk or volume may be empty or contain inconsistent information.

Individual deployment settings

By using individual settings for a machine, you can override one or more deployment settings of a deployment template.

Example. You created a deployment template to perform deployment to 100 machines. For one of those machines, however, you need to perform deployment to a different hard disk than the one prescribed by the template. You override the **Target disk layout** setting for that machine.

By default, all templates recognize individual settings. You can set up a particular template to ignore any individual settings.

Enabling, disabling, and resetting individual settings

To enable an individual setting for a machine

1. In the **Machines** view, click the machine for which you want to set up individual settings.
2. On the **Individual settings** tab, click **Configure**.
3. Click the setting that you want to override.
4. Select the **Enable this setting to override the common deployment setting** check box.
5. Specify the individual setting.

To disable an individual setting for a machine

1. In the **Machines** view, click the machine for which you want to disable an individual setting.
2. On the **Individual settings** tab, click the setting that you want to disable.
3. Clear the **Enable this setting to override the common deployment setting** check box.

> **Note**
> The value that you specified for the individual setting is still remembered, so you can easily re-enable the setting by reselecting the check box.

To reset individual settings for a machine

1. In the **Machines** view, click the machine for which you want to reset individual settings.
2. On the **Individual settings** tab, click **Reset**.

    As a result, all individual settings are disabled, and all values are returned to the preset settings. The preset settings are the same as for the default deployment settings.

List of individual settings

The following are the individual settings that you can specify. The description of these settings is similar to that of the common deployment settings, with the differences described in this section.

- **Windows activation key**

    By default, Windows is not activated after the deployment of a new machine.

To activate Windows on the machine as part of the deployment process, enter the key in the **Activation Key** text box.

- **Online deployment**
- **Target disk layout**
- **Disk space utilization**
- **Machine name and membership**

    Specify the machine name in the **Machine name** text box or select the **Preserve original machine name** check box. When **Preserve original machine name** is selected, the Management Agent for Windows installed inside the machine reads the current machine name defined in Windows, and applies it to this machine after the deployment of the new image.

    Because this is an individual machine name, the use of name patterns is not available.

- **TCP/IP properties**

    If you choose to use a specific (static) IP address, specify that address in **IP address**. Because this is an individual address, use of IP address range is not available.

- **User accounts**
- **Security identifiers**
- **Action after deployment**
- **Licensing**

    By selecting the **Use machine license** check box, you force using a machine license for the machine, even if the template prescribes using deployment licenses.

    If no machine license is available, the software will act according to the setting in the template: it will either stop deployment to the machine, or use a deployment license.

    A machine license enables an unlimited number of deployments. A deployment license enables a single successful deployment.

    This individual setting cannot be changed if the machine already uses a machine license.

Exporting and importing individual settings

To export individual settings for machines

1. In the **Machines** view, select the machines with the individual settings you want to export.
2. Click **Export**.
3. Specify the file folder and name.
4. Click **OK**.

    The file will be saved to the specified location and will have the .config extension. If your selection contains machines that have no individual settings enabled, these machines will be skipped in the file. User names and passwords specified in the **Machine name and membership** and **User accounts** settings will be encoded.

    You may view this file by using any advanced text editor (for example, WordPad or Notepad++).

To import individual settings for machines

1. Prepare a valid .config file with the individual machine settings.
2. In the **Machines** view, click **Import**.
3. Specify the file path.
4. Click **OK**.

    The individual settings for machines in the **Machines** view will be updated according to the file. Any disabled settings will be enabled if they are specified in the file. Machines that are specified in the file but are not present in the **Machines** view will be automatically added.

The configuration file format

A file containing individual settings must have the JavaScript Object Notation (JSON) format and `.config` extension.

Structure of a `.config` file

Top-level object

Pair		Required	Description
Name	**Value type**		
`machines`	array of objects	Yes	The machines for which you want to enable individual settings. Each machine should be represented as an object (see the table below).

Machine object

Pair		Required	Description
Name	**Value type**		
`bios id`	string	No	BIOS ID is not mandatory in the .config file as long as there is MAC address specified. BIOS ID and MAC address uniquely identify a machine. If both BIOS ID and MAC address values are not present, the import of the .config file will fail.
`mac address`	string	Yes	A MAC address of a machine for which you want to enable individual settings. The hexadecimal numbers in a MAC address can be separated by a colon (:) or a hyphen (-), or have no separator. Any set of six hexadecimal numbers is

			recognized as a valid MAC address of a machine, even if a network adapter with that address does not actually exist.
parameters	object	Yes	Any individual settings that you want to enable for this machine. The value must be a set of the following pairs: the string identifier of a setting (as in the list of individual settings) and the object containing the setting options (see the table below).

Setting object

Pair		Required	Action during importing
Name	**Value type**		
Online deployment			
`activate_to_ win_pe`	`true` or `false`	Yes	`true`: Select the **WinPE-based media** option. `false`: Select the **Acronis media** option.
`win_pe_image_ path`	string	Yes, if `activate_ to_ win_pe` is `true`	A non-empty value: Select the **Specify a path to the media** option and specify this value in the **WinPE image path** field. An empty value: Select the **Use the media from the master image** option.
`inject_manage ment_agent`	`true` or `false`	No	Select (`true`) or clear (`false` or not specified) the **Install agent** check box.
Windows activation key			
`activation_key`	string	No	A non-empty value: specify a Windows activation key. An empty value: ignore the setting.
Target disk layout			
`target_disk_ number`	string	Yes	"1": Select the **Default disk** option. Any other numeric string: Select the **Disk number in BIOS** option and specify this value.
`target_disk_`	string	Yes	"0": Select the **Erase the target disk data...**

`partition`			option. Any other numeric string: Select the **Replace volume** option and specify this value.
Disk space utilization			
`entirely_disk_ space_occupy`	`true` or `false`	Yes	`true`: Select the **Resize volumes to fit target disk** option. `false`: Select the **As in the master image** option.
Machine name and membership			
`computer_name`	string	Yes	Specify this value in the **Machine name pattern** field.
`domain_member ship_name`	string	Yes, if adding the machine to an Active Directory domain	Select the **Domain** option and specify this value as a domain name.
`domain_user`	string		Specify the user name of a domain administrator.
`domain_ password`	string		Specify the password of a domain administrator.
`domain_ encoded`	`true` or `false`		Encode the values specified in the `domain_user` and `domain_password` names. This name must have the `false` value if you specify or modify the `domain_user` and `domain_ password` names. Otherwise, the target machine will not be added to the domain.
`work_group_ membership`	string	Yes, if adding the machine to a workgroup	Select the **Workgroup** option and specify this value as a workgroup name.
TCP/IP properties			
`use_master_ image_network_ settings`	`true` or `false`	Yes	Select (`true`) or clear (`false`) the **Use the settings from the master image** check box.

gateway	string	Yes, if use_master_image_network_settings is false and any of these names are specified	Specify the default gateway (`gateway`), IP address (`static_ip_address`), and subnet mask (`static_ip_mask`). If you want to obtain an IP address for the machine automatically, do not specify these names.
static_ip_address	string		
static_ip_mask	string		
dns_ip_address	string	Yes, if use_master_image_network_settings is false and any of these names are specified	Specify the DNS server IP address (`dns_ip_address`), name (`dns_host_name`), and domain name (`dns_domain`). If you want to obtain a DNS server address for the machine automatically, do not specify these names.
dns_host_name	string		
dns_domain	string		
User accounts			
user_accounts	object	Yes	Add user accounts. The value must be a set of the following pairs: a group name and an array of objects containing the `Username`, `Password`, and `Encoded` names. A group name can be any of the following: `Administrators`, `Power users`, or `Users`. The `Username` and `Password` names must have string values. The value of the `Encoded` name must be `false`.
Security identifier			
sid_changing	true or false	Yes	Select (`true`) or clear (`false`) the **Generate a unique SID for each deployed machine** check box.
Action after deployment			
post_deployment_action	string	Yes	`"Shutdown"`: Select the **Shut down** option. `"Restart"`: Select the **Restart** option. `"StayReady"`: Select the **Make ready for deployment** option. If another value is specified, this name will be ignored.
Licensing			

license_type	string	Yes	"PerDeploy": Select the **Use deployment licenses** option. "PerMachine": Select the **Use machine licenses** option.
no_deploy ment_ license_ action	string	Yes, if license_ type is "PerDeploy"	"Stop": Select the **Stop deployment** option. "UseMachineLicense": Select the **Use a machine license automatically** option.
no_machine_ license_ action	string	Yes, if license_ type is "PerMachine"	"Stop": Select the **Stop deployment** option. "UseDeploymentLicense": Select the **Use a deployment license automatically** option.
no_work station_ license_ action	string	No	"Stop" or not specified: Select the **Stop deployment** option. "UseServerLicense": Select the **Use a server license automatically** option.

Sample .config file

```
{
    "machines": [
        {
            "mac address": "AA:AA:AA:AA:AA:AA",
            "parameters": {
                "Online deployment": {
                    "activate_to_win_pe": "false",
                    "inject_management_agent": "false"
                },
                "Target disk layout": {
                    "target_disk_number": "1",
                    "target_partition_number": "0"
                },
                "Disk space utilization": {
                    "entirely_disk_space_occupy": "true"
                },
                "Machine name and membership": {
                    "computer_name": "Computer",
                    "work_group_membership": "WORKGROUP"
                },
                "TCP/IP properties": {
                    "use_master_image_network_settings": "false",
                    "gateway": "10.0.2.1",
                    "static_ip_address": "10.0.2.32",
                    "static_ip_mask": "255.255.255.0",
                    "dns_ip_address": "10.0.2.32",
                    "dns_host_name": "TEST-HOST",
                    "dns_domain": "asd.test"
                },
                "User accounts": {
                    "user_accounts": {
                        "Users": [
                            {
                                "Password": "pass",
                                "Username": "user",
                                "Encoded": "false"
                            }
                        ]
                    }
                },
                "Security identifier": {
                    "sid_changing": "true"
                },
                "Action after deployment": {
                    "post_deployment_action": "Shutdown"
                },
                "Licensing": {
                    "license_type": "PerDeploy",
                    "no_deployment_license_action": "UseMachineLicense"
                }
```

```
                }
            }
        ]
    }
```

Managing deployment tasks (the Deployment tasks view)

The **Deployment tasks** view contains the list of deployment tasks that you previously created on OS Deploy Server.

To open the Deployment tasks view

1. Start Management Console.
2. Click **Deployment tasks**. If prompted, specify the name or IP address of the machine with OS Deploy Server, and the user name and password of an administrator on that machine.

List of deployment tasks

The upper part of the view shows the list of deployment tasks and related information, such as the name of the master image that will be deployed by the task.

The list of deployment tasks is divided into three categories:

- **Scheduled**: Tasks that will run once or more at a time you specified. For details about creating such tasks, see "Deployment to specific machines".
- **Upon event**: Tasks that will perform deployment as soon as a specified number of machines becomes ready for deployment. For details about creating such tasks, see "Deployment to any ready machines".
  One of these tasks may be already running and waiting for the machines. If none of these tasks is running, you can start any of them manually.
- **Manual start**: Tasks that perform deployment to specific machines and have no schedule. These are tasks that you chose to run **Manually**, and completed tasks that you chose to run **Now** or **Once later**.

To start any of the deployment tasks manually, select the task, and then click **Run** on the toolbar.

The lower part of the view shows the machines that are related to the selected task. The list depends on the type of task.

- For a task that performs deployment to specific machines: the list of machines to which the task performs deployment. Deployment will start on a schedule or when you start the task manually.
- For a task that performs deployment to any ready machines: the list of machines that are currently ready for deployment (have the **Ready** state). Deployment will start as soon as a sufficient number of machines become ready (or after a time-out), even if you start the task manually.

Actions on deployment tasks

To perform an action on a deployment task, select the task in the list. The available actions appear on the toolbar.

The actions are the following:

- **Create**: Starts the Create Deployment Task Wizard.
- **Run**: Starts the selected task. The task will wait for machines to become ready and then will perform deployment to them.
- **Stop**: Stops the selected task. The machines whose deployment finished by the time you stop the task remain deployed (the last result for such machines is **Succeeded**).
- **Edit**: Edits the task in the Create Deployment Task Wizard.
- **Delete**: Deletes the task from the deployment server.
- **View log**: Shows the log entries related to the selected task.

States and results for deployment tasks

The **State** column shows the current state of the task.

The state can be one of the following:

- **Idle**: The task is not running. It will run on a schedule or when a specified number of machines become ready. Alternatively, you can start the task manually.
- **Waiting for machines**: The task has started but is waiting for machines to become ready. This state occurs in the following cases:
  - A task that performs deployment to a specified list of machines waits until the machines are woken up or reboot into the bootable environment.
  - A task that performs deployment to a number of any ready machines waits until this number is reached.
- **In progress** (shown as percentage complete): The task is performing deployment. After deployment has finished on all machines, the task state becomes **Idle**.
- **Stopping**: The task is stopping after you chose to stop it or after not enough machines became ready after a time-out. The task will then enter the **Idle** state.

The **Last result** column shows the result of the deployment task.

The result can be one of the following:

- **Succeeded**: Deployment has been successful on all of the machines where it started (all of these machines have the **Succeeded** result).
- **Failed**: Deployment to one or more machines failed (a machine has the **Failed** result).
- **Stopped**: The task has been stopped. This state occurs in either of these cases:
  - You stopped the task, by using the **Stop** action.
  - The task stopped because not enough machines became ready for deployment, according to the deployment start condition you specified when creating the deployment task.

Command-line mode and scripting under WinPE

Having booted a machine in Windows Preinstallation Environment (WinPE), the administrator can perform imaging or deployment in the command-line mode or execute scripts.

Command-Line Utility is included in a WinPE-based bootable media that you can create by using Management Console.

The section "Sample scenarios" provides examples of using the command-line utility.

Limitation. Command-Line Utility can generate a new security identifier (SID) but cannot adjust other settings on the fly. To change the machine name, domain or workgroup membership, and other settings, either use the graphical user interface or apply the Microsoft System Preparation Tool (Sysprep) to the master system and specify the new settings in the Sysprep.inf answer file.

Command-line syntax

This section provides the list of commands and parameters of Command-Line Utility.

Supported commands

Command-Line Utility `asdcmd.exe` has the following format:

```
asdcmd /command /parameter1 [/parameter2 …]
```

Commands may be accompanied with parameters. Some parameters are common for most commands of `asdcmd`, while others are specific for individual commands. The following is the list of supported commands and compatible parameters.

Command	Common parameters	Specific parameters
create Creates an image of specified disks and volumes	/filename:\<file name> /password: \<password> /net_user:\<user name> /net_ password: \<password> /incremental /differential /compression: \<0…9> /split:\<size in MB>	/harddisk:\<disk number> /partition:\<volume number> /file_partition:\<volume letter> /raw /progress:\<on|off>

	`/oss_numbers`
	`/reboot`
	`/shutdown`
	`/log:<file name>`
	`/log_net_ user:<remote user>`
	`/log_net_ password: <password>`	

`deploy`
 	
Deploys disks and volumes, including the master boot record (MBR), from an image
	`/filename:<file name>`
	`/password: <password>`
	`/net_user:<user name>`
	`/net_ password: <password>`
	`/oss_numbers`
	`/reboot`
	`/shutdown`
	`/log:<file name>`
	`/log_net_ user:<remote user>`
	`/log_net_ password: <password>`
		`/harddisk:<disk number>`
		`/partition:<disk number>-<volume number>`
		`/target_harddisk:<disk number>`
		`/target_partition:<disk number>-<volume number>`
		`/start:<start sector>`
		`/fat16_32`
		`/size:<volume size in sectors>`
		`/type: <active|primary|logical>`
		`/preserve_mbr`
		`/preserve_disk_layout`
		`/resize:<yes|no>`
		`/patching_sid`
		
		`/license_server:<server IP address>`
		`/grant_server_license`
		`/use_machine_license`
		`/use_deployment_license`
		
		When using Acronis Universal Deploy:
		
		`/ud_path:<path>`
		`/ud_username:<user name>`
		`/ud_password:<password>`
		`/ud_driver:<.inf file name>`

`verify` Verifies the image integrity	`/filename:<file name>` `/password: <password>`	

	`/net_user:<user name>`
	
	`/net_ password: <password>`
	
	`/reboot`
	
	`/shutdown`
	`/log:<file name>`
	
	`/log_net_ user:<remote user>`
	`/log_net_ password: <password>`	

`list`
 	
Lists available drives and volumes. With the `filename` parameter, lists the contents of the image
	`/password: <password>`
	`/net_user:<user name>`
	`/net_ password: <password>`
		`/filename:<file name>`

`email_n`
 	
Turns on e-mail notifications about deployment
		`/email_from:<sender address>`
		`/email_to:<recipient address>`
		`/email_subject:<message subject>`
		`/email_smtp:<SMTP server address>`
		`/email_port:<SMTP server port>`
		`/email_user:<SMTP server user name>`
		`/email_password:<SMTP server user password>`
		`/email_ encryption:<no|ssl|tls>`

`email_n_test` Sends a test e-mail message		The same as for the `email_n` command

Common parameters (parameters common for most commands)

Parameter	Description	Image location
Access to images		
`/filename:<file name>`	Specifies the full path to the image, including the file name	Any
`/password: <password>`	Specifies the password for the image (if required)	Any
`/net_user:<user name>`	Specifies a user name for accessing the network drive	Network drive
`/net_ password: <password>`	Specifies a password for accessing the network drive	Network drive
Imaging options		
`/incremental`	Sets the image type to incremental. If this parameter is not specified or if there is no basic full image, a full image will be created. An incremental image stores changes to the data against the latest image. The name of an incremental image is the name you specified in the `/filename` parameter, followed by an index; for example: MasterImage2.tib, MasterImage3.tib, and so on. To deploy an incremental image, specify its name in the `/filename` parameter of the `deploy` command. Make sure that the image is in the same folder as all images it depends on.	Any
`/differential`	Sets the image type to differential. If this parameter is not specified or if there is no basic full image, a full image will be created. A differential image stores changes to the data against the latest *full* image. The name of a differential image is the name you specified in the `/filename` parameter, followed by an index; for example: MasterImage2.tib, MasterImage3.tib, and so on. To deploy a differential image, specify its name in the `/filename` parameter of the `deploy` command. Make sure that the image is in the same folder as the full image.	Any
`/compression: <0…9>`	Specifies the data compression level. The compression level ranges from 0 to 9 and is set to 3 by default	Any
`/split:<size in MB>`	Splits the image into parts of the specified size, in megabytes	Any

General options		

`/oss_numbers`	If this parameter is specified, the numbers of the volumes in the `/partition` parameter are adjusted for the MBR partition table. This means that primary volumes have numbers 1-1, 1-2, 1-3, and 1-4 (a disk cannot have more than four primary volumes); logical volume numbers start with 1-5.
	
	If this parameter is not specified, consecutive volume numbering must be used.
	
	For example, if the disk has one primary volume and two logical volumes, their numbers can appear as follows:
	
	`/oss_numbers /partition:1-1,1-5,1-6`
	
	or
	
	`/partition:1-1,1-2,1-3`
		Any

`/reboot`	Restarts the machine after the operation is completed. Cannot be used with the `/shutdown` option	Any
`/shutdown`	Shuts down the machine after the operation is completed. Cannot be used with the `/reboot` option	Any
`/log:<file name>`	Creates a log file of the current operation with the specified file name	Any
`/log_net_ user:<remote user>`	If the log file is created in a network folder, specifies the user name for accessing that folder	Any
`/log_net_ password: <password>`	If the log file is created in a network folder, specifies the password for accessing that folder	Any

Specific parameters (parameters specific for individual commands)

Option	Description
create	
`/harddisk:<disk number>`	Specifies the hard disks to include into the image. An image may contain data of more than one hard disk. In that case, separate disk numbers by commas, for example: `/harddisk:1,3` To view the list of available hard disks, use the `/list` command.

`/partition:<disk number>-<volume number>`	Specifies the volumes to include into the image file. Volume numbers are specified as `<disk number>-<volume number>`, for example: `/partition:1-1,1-2,3-1` See also the `/oss_numbers` parameter. To view the list of available volumes, use the `/list` command.
`/raw`	Use this parameter to create an image of a volume with an unrecognized or unsupported file system, or of a disk that contains such volume. With this parameter, all contents of the disk or volume will be copied sector-by-sector. Without this parameter, only the sectors containing useful system and user data are imaged (for the supported file systems).
`/progress:<on|off>`	Shows or hides the progress information (percent completed). The progress is shown by default.
deploy	
`/harddisk:<disk number>`	Specifies the hard disk in the image.
`/partition:<disk number>-<volume number>`	Specifies the volumes in the image.
`/target_harddisk:<disk number>`	Specifies the target hard disk.
`/target_partition:<volume number>`	Specifies the target volume number for deploying a volume over an existing one. If this parameter is not specified, the software assumes that the target volume number is the same as the volume number specified with the `/partition` parameter.
`/start:<start sector>`	Sets the start sector for deploying a volume to the unallocated space on the hard disk.
`/size:<volume size in sectors>`	Sets the new size of the volume in sectors. The size of a sector is considered to be 512 bytes, regardless of the physical sector size on the hard disk drive. For example, if you want the volume size to be 512 MB (a megabyte is 1 048 576 bytes), specify the size as follows: `/size:1048576` Specify this size even if you are using a hard disk drive with 4-KB sectors.

	To see the size of the volume in the master image, use the `/list` command.
`/fat16_32`	Enables the file system conversion from FAT16 to FAT32 if the volume size after deployment is likely to exceed 2 GB. Without this parameter, the deployed volume will inherit the file system from the image.
`/restore_bootable:<auto|on|off>`	Sets the rule of deployment for the master boot record (MBR) when deploying a volume (when deploying a disk, MBR is always deployed): • `auto`: Deploy the MBR only when deploying an active volume that contains an operating system. Use this setting to ensure that the operating system can boot. • `on`: Deploy the MBR when deploying any active volume, no matter whether the volume contains an operating system or not. • `off`: Do not deploy the MBR. Use this setting, for example, to preserve the Unix boot loader.
`/type:<active|primary|logical>`	Sets the deployed volume to active, primary or logical, if possible (for example, there cannot be more than four primary volumes on a disk). Setting a volume to active always sets it to primary, but a volume that is set to primary may remain non-active. If the type is not specified, the software tries to keep the target volume type. If the target volume is active, the deployed volume is set to active. If the target volume is primary and there are other primary volumes on the disk, one of them will be set to active, and the deployed volume becomes primary. If no other primary volumes remain on the disk, the deployed volume is set to active. When deploying a volume to unallocated space, the software extracts the volume type from the image. For a primary volume, the type will be set as follows: • If the target disk is the first according to BIOS and it has no other primary volumes, the deployed volume will be set to active. • If the target disk is the first according to BIOS and there are other primary volumes on it, the deployed volume will be set to logical • If the target disk is not the first according to BIOS, the deployed volume will be set to logical.
`/preserve_mbr`	When deploying a volume over an existing one, the target volume is deleted from the disk along with its entry in the target disk's master boot record (MBR). Then, with the `/preserve_mbr` parameter, the deployed volume's entry will occupy the upper empty position in the target disk's MBR. Thus, the target disk's MBR is preserved. Without this parameter, the deployed volume's entry will occupy

	the same position as in the source disk MBR saved in the image. If the position is not empty, the existing entry will be moved to another position.
`/preserve_disk_layout`	When deploying an MBR disk or volume with a convertible OS, and the target drive is larger than 2 TB, the target drive is converted to GPT by default. To disable this default behavior and preserve the MBR disk layout on the deployed machine, use `/preserve_disk_layout` parameter. This may be useful when are deploying an image to a machine that does not support UEFI architecture and thus cannot boot from a GPT volume. This parameter is an equivalent for the deployment template option: **Convert disk to GPT if target disk is larger than 2 TB**.
`/resize:<yes|no>`	Specifies whether to change the size of the volumes you are deploying, according to the available space on the target disk. This parameter is an equivalent of the **Disk space utilization** setting in a deployment template. • `yes`: The software will proportionally extend or reduce each of the deployed volumes according to the available space on the target disk. • `no`: Each deployed volume will have the same size as in the master image. Any excess available space on the target disk will become unallocated. If the target disk does not contain enough available space for placing the volumes, the deployment will fail. Without this parameter, the volumes will be resized proportionally.
`/patching_sid`	Generates a unique security identifier (SID) for the target machine. Without this parameter, the target machine will have the same SID as the master machine.

`/ud_path:<path to driver storage>`
 `/ud_username:<user name>`
 `/ud_password:<password>`
	Specifies using Acronis Universal Deploy, the path to the drivers storage (in a network folder), and the user name and password to access the folder.

`/ud_driver:<.inf file name>`	Specifies using Acronis Universal Deploy, and the mass-storage driver to be installed. The driver is specified as an .inf file.

The following parameters related to licensing are effective only when booting from Acronis PXE Server. You do not need to use these parameters when booting from a physical media.

Deployment is performed by using a deployment license or a machine license. By default, the software uses a machine license only if no appropriate deployment license is found on the license server.

By using the `/use_deployment_license` and `/use_machine_license` parameters, you can force a particular type of license to be used for performing the deployment. If you specify both of these parameters, their order will determine license priority. For example, if you specify `/use_machine_license /use_deployment_license`, the software will use a machine license; if no machine license is found on the license server, the

	software will use a deployment license instead.
`/license_server:<server IP address>`	Specifies the IP address of License Server.
`/use_deployment_license`	Forces a deployment license to be used for deployment. If no deployment license is found, the deployment will fail. By using this parameter with the `/grant_server_license` parameter, you can allow a server deployment license to be taken if no workstation deployment license is found on the license server.
`/use_machine_license`	Forces a machine license to be used for performing the deployment. If no machine license is found, the deployment will fail. By using this parameter with the `/grant_server_license` parameter, you can allow a server machine license to be taken if no workstation machine license is found on the license server.
`/grant_server_license`	Allows a server license to be taken for deploying a workstation operating system. The server license will be used if no workstation license is found on the license server. By default, when you use this parameter and deploy a workstation operating system, the software uses the following priorities for licenses, from highest to lowest: Deployment workstation licenses Machine workstation licenses Deployment server licenses Machine server licenses By using this parameter with the `/use_deployment_license` parameter, the `/use_machine_license` parameter, or both, you can force a particular type of license to be used for performing the deployment or change the priorities for licenses.
list	
`/filename:<file name>`	Displays the image content. When listing image content, volume numbers may not coincide with those in the list of disks and volumes if the image does not contain all the volumes. For example, if the image contains only volumes 2-3 and 2-5, they will be listed as 2-1 and 2-2. If the `deploy /partition` command cannot find a volume in the image by its physical number, use the `list` command to obtain the volume number in the image. Then, use the `/partition:<number in the image> /target_partition:<physical number of the target`

	`volume>` parameters. In the example above, to deploy the volume 2-5 to its original place, use: ```/partition:2-2 /target_partition:2-5```
email_n	
`/email_from:<sender address>`	Specifies the e-mail address of the sender. For example: ```/email_from:user@example.com```
`/email_to:<recipient address>`	Specifies the e-mail address of the recipient. For example: ```/email_to:admin@example.com```
`/email_subject:<message subject>`	Specifies the custom text in the subject line of the e-mail message. For example: ```/email_subject:"Deployment notification"``` In addition to the custom text, the subject line will include the MAC address and the IP address of the machine being deployed.
`/email_smtp:<SMTP server address>`	Specifies the name or IP address of the outgoing (SMTP) server. For example: ```/email_smtp:smtp.example.com```
`/email_port:<SMTP server port>`	Specifies the port of the SMTP server. For example: ```/email_port:465``` Without this parameter, port 25 is used.
`/email_user:<SMTP server user name>`	Specifies the user name to log on to the SMTP server. For example: ```/email_user:user```
`/email_password:<SMTP server user password>`	Specifies the password to log on to the SMTP server. For example: ```/email_password:MyPassWd```
`/email_encryption:<no|ssl|tls>`	Specifies the type of encryption that is used by the SMTP server. For example: ```/email_encryption:tls```

	Without this parameter, no encryption is used.
email_n_test	
Use this command instead of the `email_n` command, with the same set of parameters, to test the configuration of e-mail notifications.	

Usage examples

Example 1. The following command creates an image **arc.tib** of hard disk 1, and places the image to the network folder **\\server1\folder**. The operation log file **log1.log** is saved in another network folder: **\\server2\dir**. Credentials for both network folders are provided:

```
asdcmd /create /harddisk:1 /filename:\\server1\folder\arc.tib /net_user:user1 /net_
password:pw1 /log:\\server2\dir\log1.log /log_net_user:user2 /log_net_password:pw2
```

Example 2. The following command creates an image of the volume 1-2 sector-by-sector (in the raw mode) and saves the image to volume H:

```
asdcmd /create /filename:h:\raw.tib /partition:1-2 /raw /log:c:\log.txt
```

Example 3. The following command deploys the hard disk 2 from the password-protected image **1.tib** that is located in the network folder **\\server1\folder**, to the disk with the same number, 2.

```
asdcmd /deploy /filename:\\server1\folder\1.tib /password:qwerty /harddisk:2
```

Sample scenarios

Deploying images assigned to target machines

Scenario

An administrator needs to deploy a different master image to each target machine.

Solution

The administrator puts the images in a shared location that can be accessed from each target machine.

The administrator renames each image according to the target machine's MAC address. The image destined to the machine with MAC address **01-02-03-04-05-06** will have the name, for example, **image-01-02-03-04-05-06.tib**.

The administrator writes a deployment script that can read the target machine's MAC address and pull an image with a name corresponding to the MAC address from the shared location. The script can be executed on any number of target machines.

Sample script

```
setlocal
SET IMG_PATH=\\image_server\images
SET TMP_DRV_LETTER=h:
net use %TMP_DRV_LETTER% %IMG_PATH%
echo off
for /f "tokens=1-13 delims= " %%a in ('ipconfig /all') do (
IF %%a EQU Physical (
for /f "tokens=1-3 delims= " %%a in ('echo %%l') do (
IF EXIST %TMP_DRV_LETTER%\%%a.tib (
echo DEPLOYMENT IMAGE file: %%a.tib
asdcmd.exe /deploy /filename:%TMP_DRV_LETTER%\%%a.tib /harddisk:1 /target_partition:c
goto end
) ELSE (
echo THE IMAGE FILE %IMG_PATH%\%%a.tib NOT FOUND
)
)
)
)
:end
echo on
net use %TMP_DRV_LETTER% /d
wpeutil Reboot
endlocal
```

What this script does:

a.   Mounts the network folder containing the set of images (one image corresponds to one target machine)

b.   Retrieves the MAC address of the target machine

c.   Generates a .tib file name (if MAC address is 01-02-03-04-05-06 then the .tib file name must be 01-02-03-04-05-06.tib)

d.   Searches the network folder for an image with such name

e.   Deploys the image if found

f.   Restarts or shuts down the target machine

Environment variables:

- IMG_PATH: the path to a network folder on the deployment server.
- TMP_DRV_LETTER: the mounted drive on target side.

Creating images assigned to target machines

Scenario

The administrator needs to create an image of each machine to be able to later roll back the system to the imaged state by deploying the image to the same machine.

Solution

The administrator creates a script that:

- Creates an image of each machine.
- Names each image according to the machine's MAC address.

The images can be deployed to the corresponding target machines.

Sample script

```
setlocal
SET IMG_PATH=\\image_server\images
SET TMP_DRV_LETTER=h:
net use %TMP_DRV_LETTER% %IMG_PATH%
echo off
for /f "tokens=1-13 delims= " %%a in ('ipconfig /all') do (
IF %%a EQU Physical (
for /f "tokens=1-3 delims= " %%a in ('echo %%l') do (
echo IMAGE FILE: %%a.tib
asdcmd.exe /create /filename:%TMP_DRV_LETTER%\%%a.tib /harddisk:1 /compression:8
goto end
)
)
)
:end
echo on
net use %TMP_DRV_LETTER% /d
wpeutil Reboot
endlocal
```

What this script does:

a. Mounts the network folder
b. Retrieves the booted machine's MAC address
c. Generates a .tib file name (if MAC address is 01-02-03-04-05-06 then the .tib file name will be 01-02-03-04-05-06.tib)
d. Creates an image of the volume C of the machine, and saves the image to the network folder using the generated file name
e. Restarts or shuts down the machine

Environment variables:

- IMG_PATH: the path to a network folder on the deployment server.
- TMP_DRV_LETTER: the mounted drive on target side.

Collecting system information

The Acronis System Report tool collects information about a machine and saves this information to a file. You may want to provide this file when contacting Acronis technical support.

The tool is available:

- On a machine where Management Console is installed. The tool collects information about that machine.
- Under an Acronis bootable media. The tool collects information about the machine that is booted from the media, and saves this information to a locally-attached USB drive.

To collect system information in the management console

1. In the management console, select from the top menu **Help > Collect system information**.
2. Specify whether to split the file with system information into smaller parts. If so, specify the maximum size of such part.
3. Specify where to save the file or files.

To collect system information under an Acronis bootable media

1. Create an Acronis bootable media. When creating the media, select the **Acronis System Report** check box in the list of components.
2. Attach a USB drive to the machine for which you want to collect information.
3. Boot that machine from the media.
4. In the boot menu, click **Acronis System Report**.

The tool saves the file with system information to the USB drive. If two or more USB drives are attached, the tool saves the file to the first such drive it finds.

Index