SOPHOS

Cybersecurity made simple.

Sophos Deployment Packager guide

product version: 1.3

Contents

1 About this guide

This guide describes how to use the free Sophos Deployment Packager tool. For information about how Managed Service Providers (MSPs) may use this tool, see the Managed Service Provider guides.

It is assumed that you are familiar with Sophos Enterprise Console and Sophos Endpoint Security and Control.

Note
Some features will be unavailable if your license does not include them.

Sophos documentation is published at www.sophos.com/en-us/support/documentation.aspx.

2 About Deployment Packager

The Deployment Packager creates a single self-extracting archive file from a set of Sophos endpoint setup files, for installing Sophos Enterprise Console on Windows endpoints. The packaged file includes configuration options such as silent/interactive installation, installation package choices and setup parameters, update path/credentials and endpoint group membership.

Packages created with the Deployment Packager always attempt to remove other potentially-clashing protection software when installed. For encryption, other potentially-clashing encryption software can be detected, but must be removed manually.

It may be necessary for you to produce several packages, each meeting the requirements of different endpoint types.

You can run the Deployment Packager tool through either its graphical user interface (GUI) or command-line interface (CLI).

- The GUI is easier for one-off deployments.
- The CLI is more versatile for repeated deployments.

  A string to invoke the command-line version with options can be stored in a text file, or regularly run from a scheduled batch file, ensuring that the installation packages are always up-to-date. So, if you're managing large numbers of computers where there is a need for frequent installation on endpoints, the CLI is preferable.

2.1 Deployment Packager known issues and limitations

- If you attempt to install Sophos Anti-Virus using a ready-made installer created by Sophos Deployment Packager and the logged on user name contains double-byte characters (for example, Japanese, Chinese), the installation does not continue.

  When the installer is run, the setup files are extracted to the `%temp%/cid_packager_temp` directory, but the installation does not continue. No errors are displayed or logged in the event logs.

  Workaround: Log on as a user with no double-byte characters in the user name.
- A "packaging failed" error message may be displayed when you try to create a package using command-line with an obfuscated password, -opwd command. If the error is displayed, ensure the obfuscated password is correct. If it is accurate and continues to display the error, enter a plain text password using the -pwd command or use the Deployment Packager user interface.

3 System requirements

The minimum requirements to run the Deployment Packager are as follows:

- Windows operating systems: see http://www.sophos.com/en-us/support/knowledgebase/118635.aspx
- Disk space: 1 GB
- Memory: 1 GB
- Processor: 2 GHz Pentium or equivalent

You should also be aware of system requirements for the packaged endpoint components. See www.sophos.com/en-us/products/all-system-requirements.aspx.

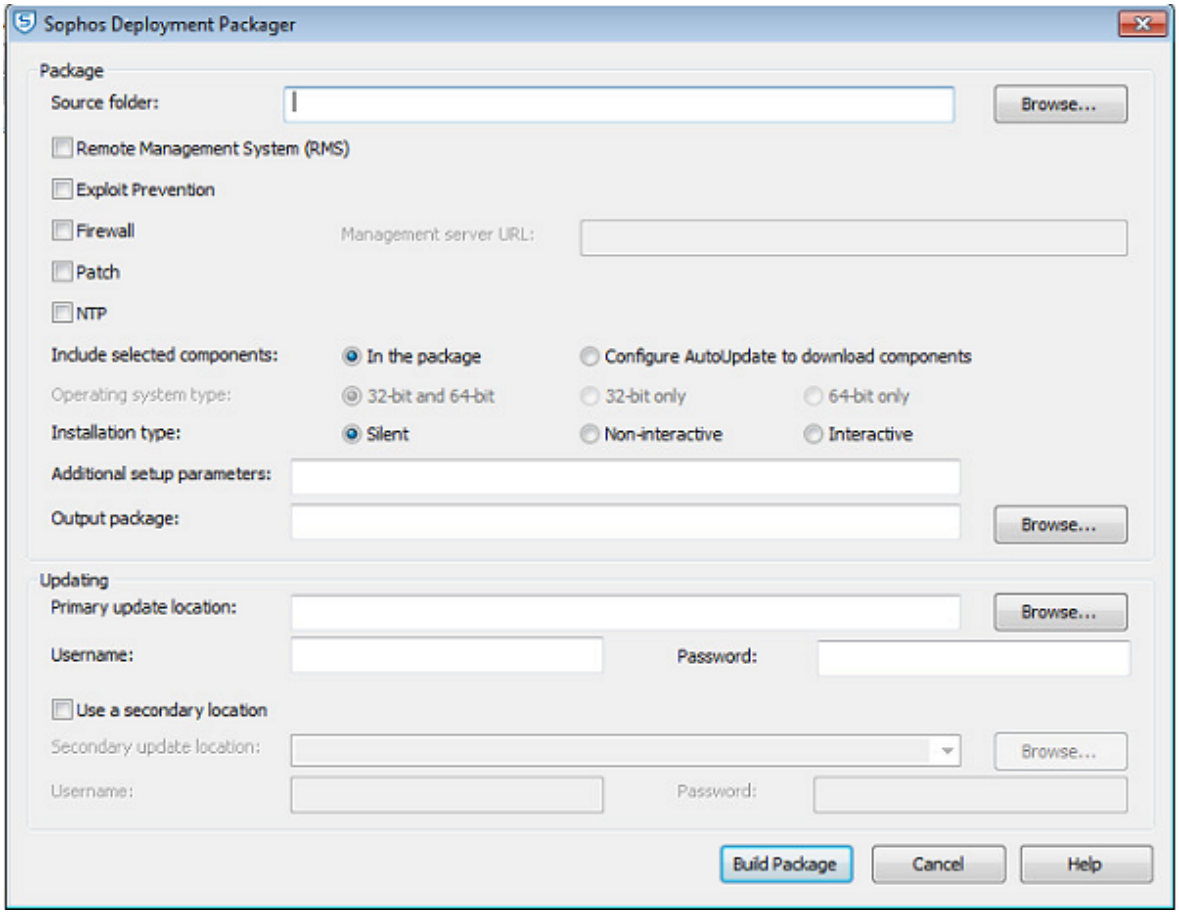
4 Create packages using the graphical user interface

Use the graphical user interface for one-off deployment. You can create an installation package for the following features:

- Endpoint protection package with anti-virus, Remote Management, Firewall, and patch management.

4.1 Create a protection package using the GUI

1. To create a protection package, run `DeploymentPackager.exe`.
   The **Sophos Deployment Packager** dialog box is displayed.



2. In **Source folder**, specify the location of the central installation directory containing the endpoint software installation files. This may be a UNC path or a local folder.
3. Select from the following:
   - **Remote Management System (RMS)**: This installs and enables the Sophos Remote Management System, which allows Sophos Enterprise Console to control Sophos Enterprise Console. For Managed systems you must enable this component.

Note
When you select this option, endpoints obtain their updating path and credentials from Sophos Enterprise Console through RMS.

- **Exploit Prevention**: This installs Sophos Exploit Prevention.
- **Firewall**: This installs the Sophos Client Firewall.

Note
If you want to install this option, check endpoint system requirements at www.sophos.com/en-us/products/all-system-requirements.aspx.

- **Patch**: This installs Sophos Patch Agent. You must also enter the address where the Management server is installed under **Management Server URL**. The address must be a fully qualified domain name. Example: http://<server name>.

  If you select this option, you can choose the **Operating system type**.
- **NTP**: This installs and enables Sophos Network Threat Protection (NTP).
- In **Include selected components** do one of the following:

  To include the selected components in the deployment package, click **In the package**.

  To download selected components from the update source, click **Configure AutoUpdate to download components**.

Note
The endpoint installer is unable to use a proxy server. If the update location is accessed through a proxy server, then the required endpoint components must be included in the package.

If you select **Remote Management System (RMS)** and then click **In the package** in **Include selected components**, the updating details are obtained from Sophos Enterprise Console.

Sophos System Protection and Sophos Endpoint Defense packages will be automatically added to the generated package (if they are part of the licensed packages) as they are not optional components.

4. In **Operating system type**, choose which operating system type to package. This option is only applicable if Patch is being installed from the deployment package. If you choose either **32-bit** or **64-bit**, the package can be installed only on specific 32-bit or 64-bit operating systems. If you choose **32-bit and 64-bit**, the package can be installed on both 32 and 64-bit operating systems, but the package size will be large.
5. In **Installation type**, select how the installation program will run on endpoint computers.
   - Select **Silent**: the program runs without any user interaction. The installation progress is not displayed on the endpoint computer.
   - Select **Non-interactive**: the program runs without any user interaction. The installation progress is displayed on the endpoint computer.
   - Select **Interactive**: the program runs with user interaction. The user can control the installation.
6. In **Additional setup parameters**, specify endpoint setup installation options. Always specify group membership using the -g option so that each installer is specific to and sets up endpoints to be members of existing groups.

The packager does not check these options for errors.

For further information, see www.sophos.com/en-us/support/knowledgebase/12570.aspx.

7. In **Output package**, specify the destination path for the output installer package. You can also specify an optional filename; if this is not supplied, the Deployment Packager will use a default filename.
8. In the **Updating** panel, for indirectly-managed endpoint packages or where remote management is enabled but not included in the package, enter the update path and credentials. You may set ":<port number>" after an HTTP URL; if unset, this defaults to 80.
    - Ensure all the components that are selected can be updated from the update location you specify (for example, Patch). If a different location is used for components, you can configure it as a secondary update location.
    - Credentials are obfuscated in the package; however, accounts set up for endpoints to read update server locations should always be as restrictive as possible, allowing only read-only access.
    - Endpoints will attempt to use their system proxy settings only if set using the environmental variables http_proxy or all_proxy. Proxy settings in Windows Control Panel Internet Options or Internet Explorer are ignored. _proxy variable values take the format _proxy=[protocol://][user:password@]host[:port], for example http_proxy=http://user:password@proxy:8080.
9. Click **Build Package** to build the self-extracting archive.

5 Create packages using the command line interface

Use the command line interface for repeated deployment. You can create an installation package for the following features:

- Endpoint protection package with anti-virus, remote management, Firewall, and patch management.

5.1 Create a protection package using the CLI

Before using this section, read Create a protection package using the GUI (page 4).

To run the Deployment Packager in command line mode, use the following format as a minimum:

```
DeploymentPackager.exe -cli -mng yes -cidpath <CIDpath> -sfxpath <SFXpath>
-crt R
```

where <CIDpath> is the path to the relevant central installation directory and <SFXpath> is the path of the output package. **-crt R** automatically removes third-party protection software.

The packager returns a value of zero when run successfully and non-zero for an error condition, together with a message to standard error method (stderr).

Command-line options

You can also use other command line qualifiers, as listed below.

-mng yes

Enable Remote Management.

-mngcfg

Specify path to custom Remote Management configuration files.

-scf

Install Sophos Client Firewall.

-ntp

Install Sophos Network Threat Protection.

-hmpa

Install Sophos Exploit Prevention.

-patch <Management Server URL>

Install Sophos Patch Agent with the Management Server address. The address should be a fullyqualified domain name. Example: http://<server name>.

-sauonly

Include Sophos AutoUpdate only (chosen remote management, firewall, NTP and SSP components are downloaded from the update source). If this option is not selected, chosen components are included in the package.

-arch <32bit, 64bit>

Specify the architecture of the package you want to create, either 32-bit or 64-bit.

> **Note**
> This option is only applicable if Patch is being installed from packaged CID. If you choose **32-bit** or **64-bit** the package can be installed only on specific 32-bit or 64-bit operating systems. If you do not specify any architecture, a single package is created which can be installed on both 32 and 64-bit operating systems, but the package size will be large.

-updp <update_path>

Updating path.

-user <username>

-pwd <password>

Username and password. The packager obfuscates these in the package. However, if you are saving a Deployment Packager command line with clear username and password in a text or batch file, ensure that it is secure.

-opwd <obfuscated_password>

Obfuscated password. For information on how to obfuscate passwords, see Knowledge Base article Obfuscating the username and password at www.sophos.com/en-us/support/knowledgebase/13094.aspx.

-s

Silent installation.

-ni

Non-interactive installation.

Other options

Any other options are packaged to be run with the installer setup file.

6 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledge base at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

7 Legal notices