PAESSLER PRTG

acronis.com

Acronis Cyber Cloud

Integration with Paessler PRTG

User Guide

REVISION: 3/26/2025

Table of contents

© Acronis International GmbH, 2003-2025

Introduction

Paessler PRTG (https://www.paessler.com/prtg) is a network monitoring software with a broad range of supported sensors and metrics.

The Acronis-Paessler PRTG cloud integration adds a sensor with information about the Acronis Cyber Protect agent, such as backup size, CyberFit score and time intervals between last and next backup, antivirus and antimalware scan.
Additionally, it reports information about itself as well as the agents, to the integration status collector in Acronis Cloud.

The integration is implemented as a custom EXEXML sensor (https://www.paessler.com/manuals/prtg/custom_sensors), which basically represents an executable file with Paessler PRTG-specific output data format.
The executable sensor addon uses device credentials and remote execution service to run commands on the target device.

Windows Remote Management (WinRM) is used on the Windows targets and SSH - on the Linux ones.

The addon connects to the Acronis Agent core API in order to get access to the Acronis Cloud, then extracts the protection plan, backups information and reports it in Paessler PRTG-specific format on standard output.

© Acronis International GmbH, 2003-2025

Prerequisites for addon use

The following preconditions are required:

- A probe server with a Paessler PRTG network monitor installed
- Windows user credentials (with administrator rights) for the probe server
- Administrator user credentials for the Paessler PRTG interface
- Addon executable file: `ci-addon-paessler.exe`
- One or more target devices with Windows, macOS or Linux, with or without Acronis agent
- User credentials (with administrator rights) for the Windows devices
- Version of PowerShell on the Windows target devices - at least 3.0
- User account with SSH password access for Linux/macOS target devices
- Version of `curl` at least 7.4 for Linux/macOS target devices

Usage of Paessler PRTG Hosted Monitor (PPHM)

This document describes the integration as used on a self-hosted Paessler PRTG instance.

If you are using Paessler PRTG Hosted Monitor (PPHM), you can still run this integration via Remote Probes (RP). For this purpose, simply install the integration on each of the RPs and use the corresponding RP to send monitoring information to the Core Server.

See detailed instructions on how to set up a PR.

© Acronis International GmbH, 2003-2025

Installation and configuration

The Paessler PRTG manual can be found at either of these locations:

- https://www.paessler.com/manuals/prtg
- http://{prtg-host}/help/introduction.htm, where prtg-host is a host with Paessler PRTG instance installed.

Installation of executable file

1. Go to the **Acronis Management portal** > **Integrations**. Click on the **PRTG Network Monitor** tile.

   

   See more information about enabling and managing integrations.
2. Download the `ci-addon-paessler` addon executable file from the **Download Scripts** tab.
3. Copy this file to the `<PRTG program directory>\Custom Sensors\EXEXML\` folder where `<PRTG program directory>` is `C:\Program Files (x86)\PRTG Network Monitor\` by default.
4. The addon should be now accessible in the custom sensor creation dialog in the Paessler PRTG interface.

Target device creation in Paessler PRTG

The target device can be discovered automatically by Paessler PRTG or created manually: https://www.paessler.com/manuals/prtg/create_objects_manually

Manual device creation:

1. Open the **Devices** tab in the Paessler PRTG web interface.
2. Click the (**+**) button at the top-right of the device tree.
3. Select **Add device**.
4. Select a device group in the tree, for example "`Root->Network Discovery->Windows->Servers`".
5. Click **OK**.
6. For each device, do the following:
   a. Provide device name and IPV4 address/DNS name.
   b. For the **Credentials for Windows Systems** parameter, clear the **Inherit from Servers** checkbox.
   c. Enter user credentials for the target device:
      - Domain/Computer name
      - User name
      - Password

© Acronis International GmbH, 2003-2025

Sensor configuration

To create addon sensor for the target device, do the following:

1. Open the **Devices** tab in the Paessler PRTG web interface.
2. In the device tree, locate and click the target device.
3. Click the (**+**) button at the top right of the device information pane.
4. Select **Add sensor**.
5. In the **Search** field, enter "`exe`".
6. From the below list, select **EXE/Script Advanced** and open a sensor creation dialog.
   a. Enter a meaningful **Sensor Name**, for example: Acronis Agent.
   b. From the **EXE/Script** drop-down list, select **ci-addon-paessler.exe**.
   c. Optionally, set additional command line parameters in the **Parameters** section, which is usually empty.
   d. Select the **Set placeholders as environment values** radio-button.

      Note
      This is the most important setting as it passes target device data to the addon through process environment.

   e. Set the **Timeout(Sec.)** option, for example to 300, in order to allow for some network and target device delays tolerance.
   f. To save sensor result data for additional troubleshooting, set **Result handling** to **Store result in case of error**. The saved sensor data can be found at the following directory on the probe server: `C:\ProgramData\Paessler\PRTG Network Monitor\Logs\sensors`.
   g. For **Scanning Interval**, clear the **Inherit from** checkbox and change this propery to a value, suitable for production. For testing purposes, leave it as is (60 seconds).
   h. Click **Create**.

Sensor settings can be changed later by clicking on the particular sensor in the tree or its device data and opening the **Settings** tab.

Addon command line

The addon gets its connection mode and credentials from environment variables with `prtg_` prefix, set by the Paessler PRTG probe service on custom sensor process execution:

- `prtg_host` - target device address or DNS name
- `prtg_linuxpassword`
- `prtg_linuxuser`
- `prtg_version` - Paessler PRTG probe version
- `prtg_windowsdomain`

© Acronis International GmbH, 2003-2025

- `prtg_windowspassword`
- `prtg_windowsuser`

  The connection mode is automatically selected by a non-empty `prtg_linuxuser (ssh)` or `prtg_windowsuser (winrm)` variable.

  It is possible to run the `ci-addon-paessler.exe` file manually or change the additional parameters in the sensor config:

```
Usage:
ci-addon-paessler [-m mode] [-P port] [-l level] -u username -p password target-host
Examples:
ci-addon-paessler.exe 127.0.0.1 - poll local windows machine
Flags:
-a, --authmode string authentication and encryption mode (unencrypted|sspi|internal) (default "unencrypted")
-d, --domain string domain
-h, --help help for ci-addon-paessler
-l, --loglevel string enable log with level (debug|info|warn|error)
-f, --logtofile enable logging to file
-m, --mode string connection mode (auto|winrm|ssh|mock) (default "auto")
-p, --password string password
-P, --port int target port
-t, --timeout int WinRM timeout, seconds (default 30)
-u, --user string username
-v, --version version for ci-addon-paessler
```

  - target-host is the target device DNS name or network address
  - -d, --domain [domain]
    credentials for target device:
    -u, --user [user]
    -p, --password [password]
  - -P, --port parameter that allows to make the remote connection port different from the default one (5985 for winrm and 22 for ssh)
  - -l, --loglevel switch on logging that also sets the log filter level
    In the Paessler PRTG sensor configuration, it should be used only with a `logtofile` flag, because the log output breaks the Paessler PRTG sensor data parser.
  - -f, --logtofile change log output from `stderr` to a file in the `LOCALAPPDATA` folder

© Acronis International GmbH, 2003-2025

- for Paessler PRTG sensor: `C:\Windows\System32\config\systemprofile\AppData\Local\[datetime]_[pid]_addon_paessler.log`
- for manually started addon: `C:\Users\[username]\AppData\Local\[datetime]_[pid]_addon_paessler.log`

- -m, --mode allows to change the connection mode from automatic selection to explicit winrm or ssh setting
- -t, --timeout changes the operation timeouts for the winrm client
  It should be changed together with the timeout parameter in the sensor configuration. The sensor timeout should be longer than 4x winrm timeout.
- -a, --authmode parameter selects ON/OFF encryption/authentication modes:
  - unencrypted (default) - use Windows SSPI API to perform Negotiate authentication and no encryption
  - sspi - use Windows SSPI API to perform Negotiate authentication and encryption
  - internal - use internal NTLM authentication without encryption

For the first and third options to work, `AllowUnencrypted=True` should be configured on the target device winrm service.

Encryption mode

It is necessary to allow unencrypted connection to the WinRM service by setting the `AllowUnencrypted` parameter to `True`:

```
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

PowerShell version check on target device

Run PowerShell on the target device and enter the following:
`$PSVersionTable`

It should show PSVersion 3.0 or higher:

COMMAND OUTPUT

NAME	VALUE
PSVersion	3.0
WSManStackVersion	3.0
SerializationVersion	1.1.0.1
CLRVersion	4.0.30319.36543
BuildVersion	6.2.9200.16398
PSCompatibleVersions	{1.0, 2.0, 3.0}
PSRemotingProtocolVersion	2.2

© Acronis International GmbH, 2003-2025

See "Links" (p. 14) for Windows 2008 PowerShell installer links.

© Acronis International GmbH, 2003-2025

Windows Remote Management setup on target device

- run command prompt as administrator on the target machine
- run the following command in a prompt:

winrm configuration command

```
winrm quickconfig
```

- Check the access to the target device from the addon:

manual addon run

```
ci-addon-paessler.exe -u username -p password target_device
```

- Troubleshoot connection issues:
  - Is the winrm service running on the target?
  - Is the target accessible from a network?
  - Does the firewall allow connection to port 5985 from the probe server?
  - Are the target user credentials correct?
  - Does the target user have administrator rights?

Known issues

WinRM operation blockage

When using the `sspi` authentication (+encryption) method, the WinRM service on the target machine sometimes blocks and pauses, and the sensor fails with a timeout in WinRM call. On the sensor graphs, this appears as red "Downtime" dots and sensor data absense intervals.

Possible workaround: enable unencrypted access to the WinRM service and switch to `unencrypted` or `internal` authentication.

Kerberos encryption not supported

When using `-a sspi` authentication with full domain credentials and DNS name for localhost, Kerberos encryption is not supported. The target device should have `AllowUnencrypted` set to `true` and the addon should be used with the default (`-a unencrypted`) authentication mode.

NTLM authentication restrictions

If `ci-addon-paessler.exe` and `winrs` cannot execute commands on the target device with error messages like:
"**WinRM cannot process the request. The following error with error code 0x80090322 occurred while using Negotiate authentication**"
OR

© Acronis International GmbH, 2003-2025

"**Remote machine network connection failed: ctx.Update failed on step 0: The function requested is not supported**",
it is possible for the Paessler PRTG probe machine to have NTLM authentication restrictions set up in group policies.

To check the NTLM policies on the probe server:

1. Click **Win+R** or the **Start** button together with **Run**.
2. Input the `gpedit.msc` file and run it.
3. Go to **Local Computer Policy** → **Computer Configuration** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options**.
4. Locate the "**Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers**" setting. If its value is set to **Deny all**, then the NTLM authentication will not work.
5. Locate the "**Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication**" setting. It contains a list of server addresses with NTLM authentication enabled, even when **Deny all** is set.

Possible workarounds:

- Add target device addresses or host names to the "**Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication**" setting.
- Enable `AllowUnencrypted=true` on the target devices and use the `-a internal` command line option in addon command line, in order to have internal NTLM implementation, instead of Windows SSPI.
- If both the probe server and the target device are on the same domain, then use host and domain names to access the target machine with Kerberos protocol, instead of NTLM.
  - From **Device settings**, set the following properties of the target device:
    - DNS name
    - domain
  - Set `AllowUnencrypted` to `true`, as Kerberos encryption is not supported.

Additional security hardening

It is possible to further enhance the security of the WinRM service, at the expense of some additional configuration of the target device.

- Change the WinRM security exception scope and allow access only from the Paessler PRTG probe machine address
- Use HTTPS listener (For target configuration example, see https://github.com/ansible/ansible/blob/devel/examples/scripts/ConfigureRemotingForAnsible.ps1)
- Use Kerberos or CredSSP for authentication, instead of Negotiate.

Linux/macOS SSH access configuration

To access Linux or macOS target devices, the following is required:

© Acronis International GmbH, 2003-2025

- Working SSH daemon
- User account with rights to access password-protected devices by SSH
- At least version 7.4 of `curl` installation

In the Paessler PRTG UI, user account credentials should be set up in the device or device group configuration:

- **Credentials for Linux/Solaris/MacOS (SSH/WBEM) Systems** field group
- **User name** field - user account name
- **Authentication method** radio box - password
- **Password** field - user account password

Addon execution flow

- Connect to the target machine through WinRM or SSH.
- Execute the `aakore info --raw` command from the default path on Windows or without path on Linux.
- Extract the `aakore local HTTP REST API` endpoint address, port and agentId.
- Get temporary API client credentials from `aakore /idp/clients endpoint`.
- To execute http requests on `aakore` or cloud, a proxy script is used. For Windows, the script is implemented in PowerShell and for Linux - a `` `curl` `` utility invocation is used.
- Exchange credentials for access token in `aakore /idp/token endpoint`.
- Data exchange with the cloud is performed through `aakore` endpoint, used as intermediary.
- Get `resourceId` from `/api/resource_management/v4/resources`.
- Get backup size from `/bc/api/vault_manager/v1/stats` by `resourceId`.
- Get resource protection status from `/api/resource_management/v4/resource_statuses` by `resourceId`.
- Calculate the CyberFit score from status.
- Report agent status to `/api/integration_management/v2/status`.
- Format report and print on `stdout`.

On any error execution, there is a stop and some error information is returned to Paessler PRTG on `stdout`.

By default, no other information is printed on `stdout` or `stderr` as it brokes the Paessler PRTG sensor data parser.

© Acronis International GmbH, 2003-2025

Supported sensor channels and monitoring data limitations

In the current integration version, only the following sensor channels are supported:

- on Windows
  - CyberFit score
- on all platforms
  - Backup size
  - Last backup
  - Next backup
  - Last antimalware scan

An antivirus protection policy is included at **Protection plans** > **Antivirus & Antimalware protection** and returned as **Last antimalware scan**.

The Microsoft Defender or Security Essentials antivirus protections are disabled after default installation of Acronis Cyber Protect agent, so usually this policy cannot be applied.

© Acronis International GmbH, 2003-2025

Links

Paessler PRTG

https://www.paessler.com/prtg

https://www.paessler.com/manuals/prtg

https://www.paessler.com/manuals/prtg/custom_sensors

https://www.paessler.com/manuals/prtg/create_objects_manually

Windows Remote Management

https://docs.microsoft.com/en-us/windows/win32/winrm/about-windows-remote-management

https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/how-to-enable-windows-remote-shell

https://docs.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management

https://github.com/ansible/ansible/blob/devel/examples/scripts/ConfigureRemotingForAnsible.ps1

PowerShell installers for Windows 2008

3.0: http://www.microsoft.com/en-us/download/details.aspx?id=34595

4.0: http://www.microsoft.com/en-us/download/details.aspx?id=40855

https://social.technet.microsoft.com/wiki/contents/articles/21016.how-to-install-windows-powershell-4-0.aspx

© Acronis International GmbH, 2003-2025