DEPLOYING THE QUALYS CLOUD AGENT (QAGENT) ON WINDOWS BASED DEVICES

White Paper | Version 01.00

ROHDE&SCHWARZ

Make ideas real

CONTENTS

1 INTRODUCTION

The Qualys Cloud Agent (QAgent for short) is a suite of tools that can be deployed on Microsoft Windows based devices. The agent allows execution of vulnerability or compliance scans. Using an agent eliminates the need to share credentials for authenticated scans.

2 DISCLAIMER

Using any security solution that consumes device resources is not recommended in production or lab environments where reliability and data consistency are of utmost importance. This white paper describes how a QAgent deployment might be handled to lessen the impact on production or lab environments. Rohde&Schwarz does not assume liability for any damage or harm resulting from the use of this white paper, particularly since the deployment of third-party software and its behavior on specific devices are not subject to the control and responsibility of Rohde&Schwarz.

Although this white paper was written on the basis of Qualys Cloud Agent version 5.4.0.10 and Windows 10 IoT Enterprise LTSC 21H2, Rohde&Schwarz does not assume any liability for the correctness or proper functionality for these specific versions nor for any other combination of versions. This white paper is provided solely on a best effort basis.

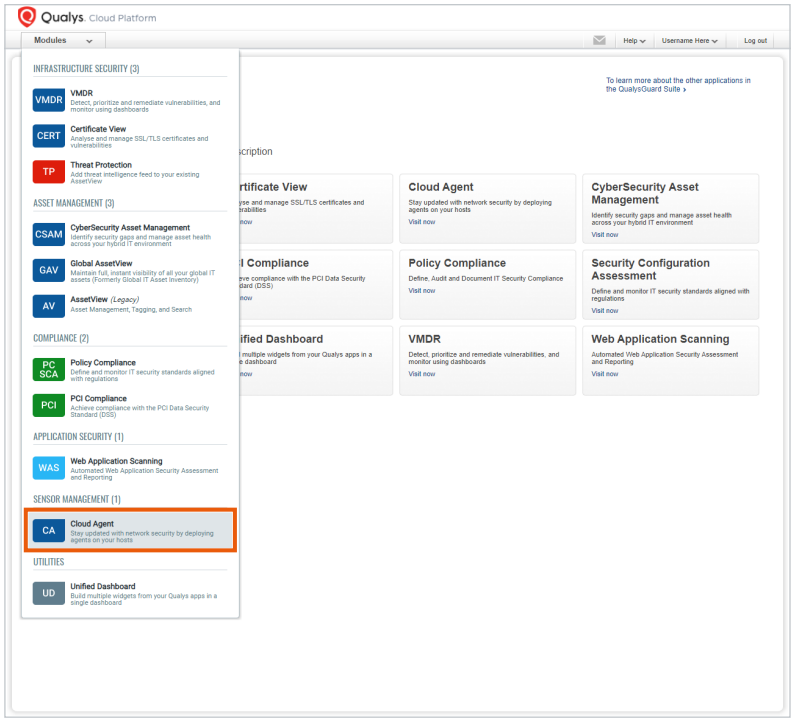
3 PREPARATIONS

It is assumed you have a valid Qualys subscription, portal access with the correct permissions and are familiar with the Qualys platform. If you cannot follow along because certain options or menus are not available, consult with your Qualys administrator to obtain the appropriate permissions or have them follow this white paper to configure it for you.

4 QUALYS PORTAL

After signing into your Qualys portal, you will find the “Cloud Agent” module in the left-hand corner. Select the highlighted menu item.

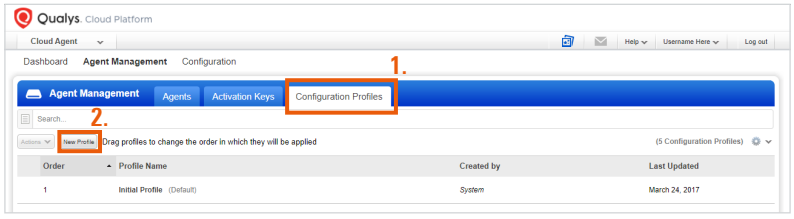
Figure 1: Selection of the Cloud Agent module in the Qualys portal



4.1 Cloud Agent overview – profile creation

In the Cloud Agent portal, go to the “Configuration Profiles” tab and create a new profile.

Figure 2: Creation of configuration profile



4.1.1 General information

Give the profile any name that fits your company naming scheme. Here are some examples you might find appropriate:

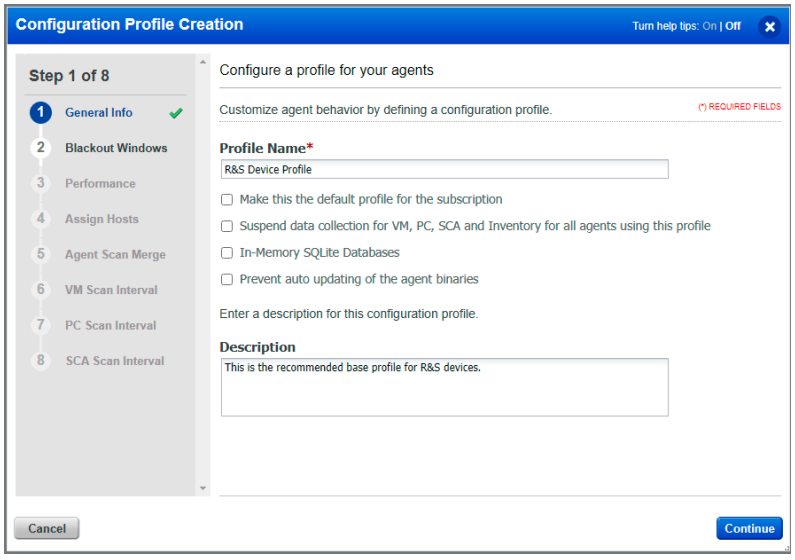
- Device type or product name specific designation:
  R&S <device type/product name> Profile
  - R&S RTO20xx Profile
  - R&S ZNLxx Profile
  - R&S FSWxx Profile

- Business case or production function based designation:
  <your company name> <business case> Profile
  - ACME ProductionTestingLine01 Profile
  - ACME TestAutomation02 Profile

- For a larger and geographically diverse deployment of devices, a location and function based naming scheme is recommended, e.g.:
  - ACME_DE_MU_LINE_01_SIGGEN_PROFILE
  - R&S_US_NY_TA_02_NETANALYSIS_PROFILE
  - R&S_US_NY_TA_02_SIGGEN_PROFILE

This white paper uses the generic name "R&S Device Profile". The description is optional but recommended.

Figure 3: Configuration of profile for the agent (step 1 of 8)



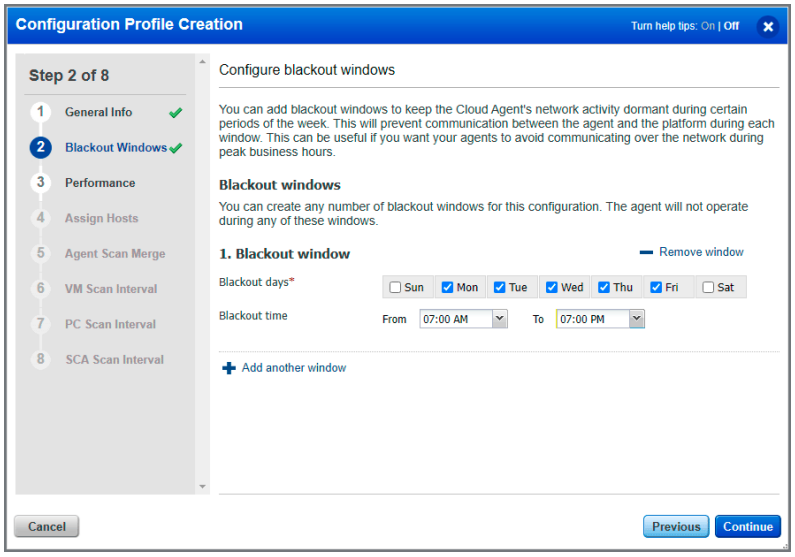
For specific Rohde&Schwarz devices, the user manual contains sections (e.g. "installation of third-party software") describing additional performance tuning requirements that must be observed during the following Qualys Cloud Agent profile creation.

4.1.2 Blackout windows

Configuring blackout windows involves a risk tradeoff between device performance, timeliness and accuracy of security information about the device. Using blackout windows is recommended if performance issues are discovered during usage of the device.

If you want to be sure that measurements and performance of a device or a device group are not negatively impacted by the Qualys Agent, blackout windows during the utilization time of devices may be configured in advance. Be careful to not blackout a device completely since the cloud agent will not be able to contact its controller. Do use blackout windows as you require them. The time zone is always the local time of the agent. Network time synchronization is recommended if this feature is used.

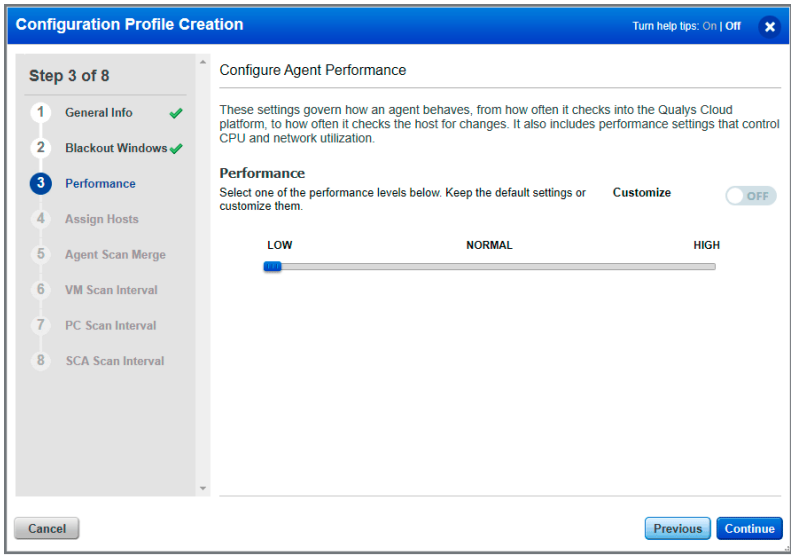
Figure 4: Configuration of blackout windows (step 2 of 8)



4.1.3 Performance

In general, the low performance setting has proven to be a good starting point. It can be customized to further decrease the strain/load the cloud agent generates on the device. Using these settings requires a hands-on, workload-specific tuning, testing and monitoring effort.

Figure 5: Configuration of agent performance (step 3 of 8)

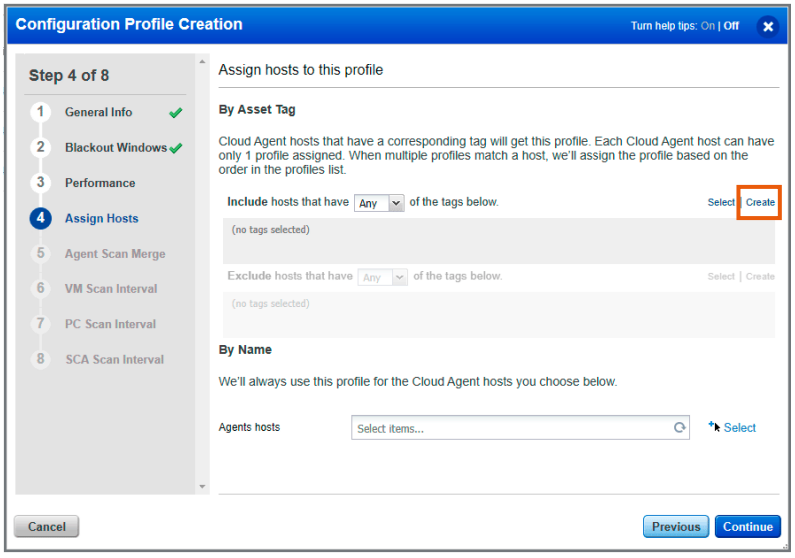


4.1.4 Assign hosts

The Qualys platform provides many ways to assign specific hosts to a profile, but it is recommended to use tags. Qualys can use various data sources depending on which ones are configured, e.g. a configuration management database (CMDB) or an IP address management (IPAM) system. The configuration of such systems is outside the scope of this white paper.

You can select a predefined tag with "Select" or create a new one. Creation of a new tag is covered next.

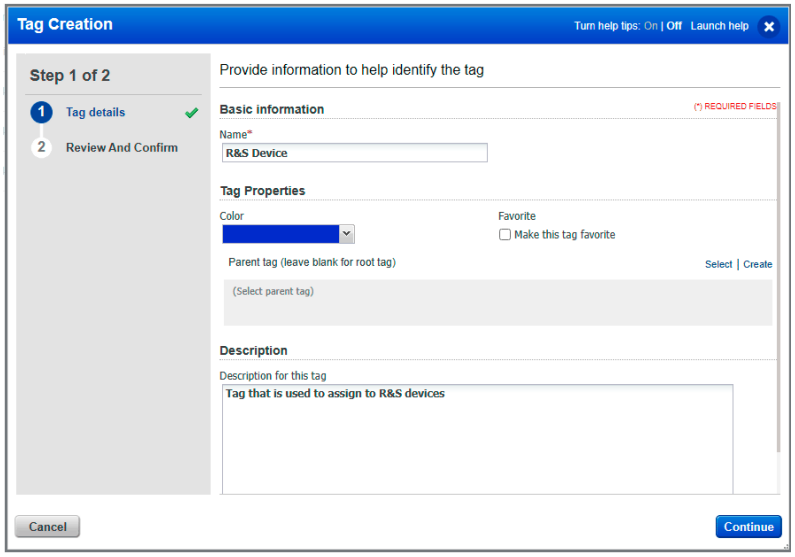
Figure 6: Assignment of hosts to the profile (step 4 of 8, part 1)



4.1.4.1 Create tag

In the tag creation dialog, select a meaningful name. A color may be useful to indicate business criticality or groups of assets for a quicker overview. The description is optional but recommended.

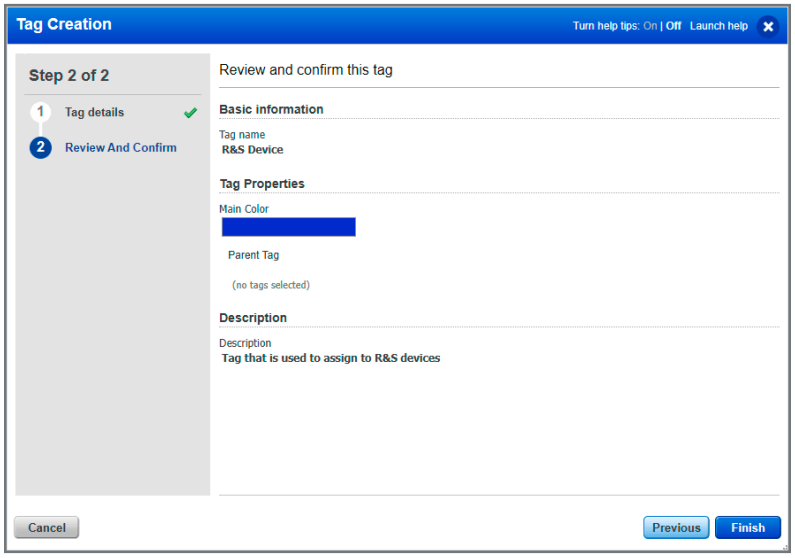
Figure 7: Creation of tag (substep 1 of 2)



4.1.4.2 Review and confirm

The second dialog step allows you to confirm your choices and brings you back to the "Assign Hosts" dialog.

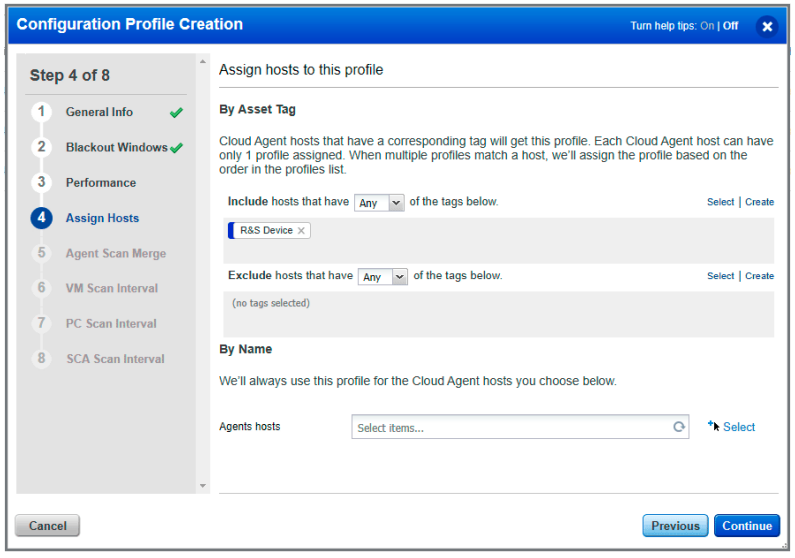
Figure 8: Review and confirmation of tag (substep 2 of 2)



4.1.5 Assign hosts with new tag

After completing the "Tag Creation" dialog, the newly created tag is assigned to the "Include hosts …" field.

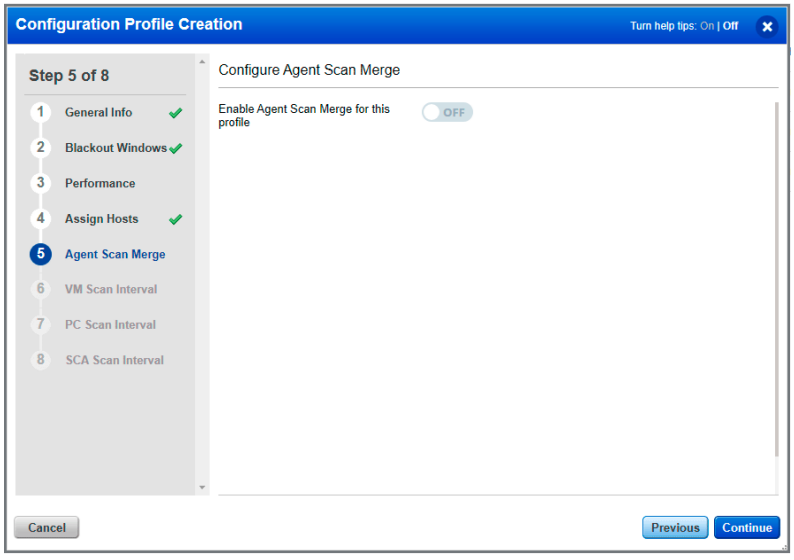
Figure 9: Assignment of hosts with new tag to the profile (step 4 of 8, part 2)



4.1.6 Agent scan merge

The agent scan merge feature can be used when other network based scans are used. It allows the Qualys platform to merge the results and ensure the same asset has been scanned multiple times.

Figure 10: Configuration of agent scan merge (step 5 of 8)



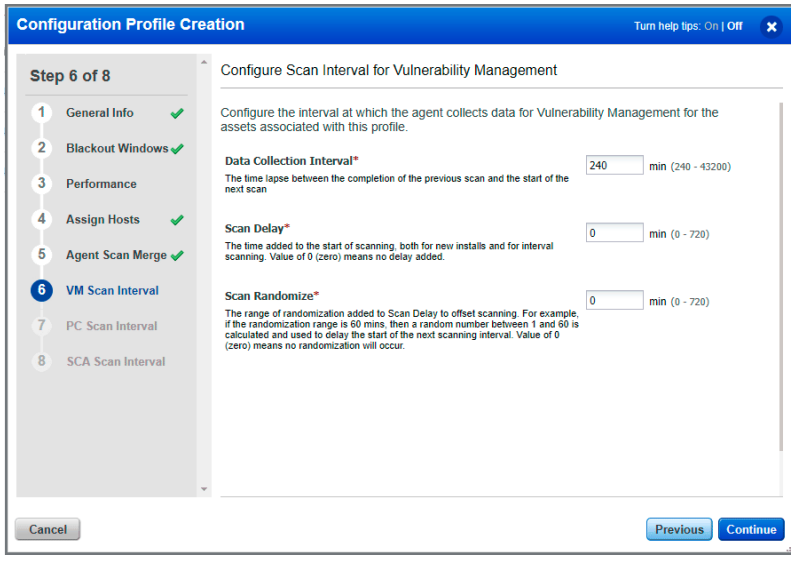
4.1.7 Vulnerability management (VM) scan interval

Vulnerability management (VM) scans can be configured to your requirements. The default is a time lapse between scans of 240 minutes, e.g. 4 hours. This is a recommended baseline. To roughly obtain a daily scan, a value of 1200 minutes should be used and the blackout windows must be factored in if configured.

Delaying a scan is not required; the default value of 0 is acceptable.

Adding a randomized value for the delay of a scan is only useful if this profile targets hundreds or thousands of devices that will all start at the same time and then will want to deliver their report at roughly the same time. The default value of 0 is acceptable.

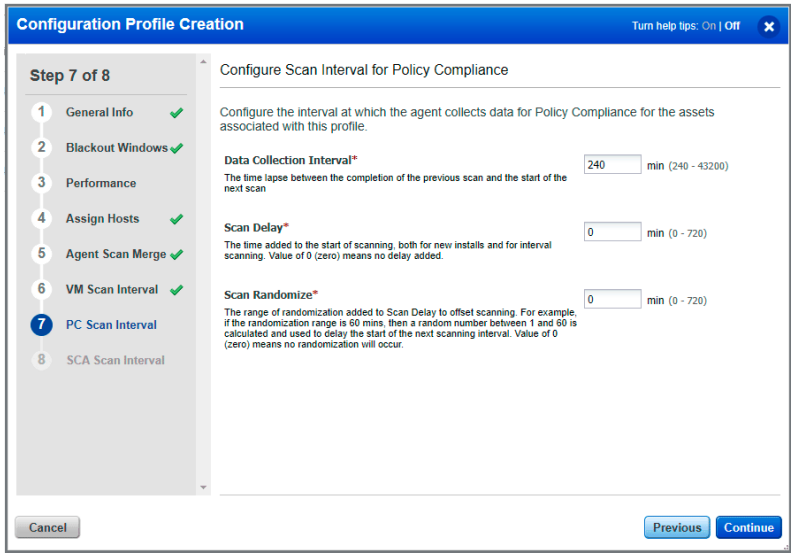
Figure 11: Configuration of scan interval for VM (step 6 of 8)



4.1.8 PC scan interval

The same recommendations from the “VM Scan Interval” apply here as well.

Figure 12: Configuration of scan interval for policy compliance (step 7 of 8)

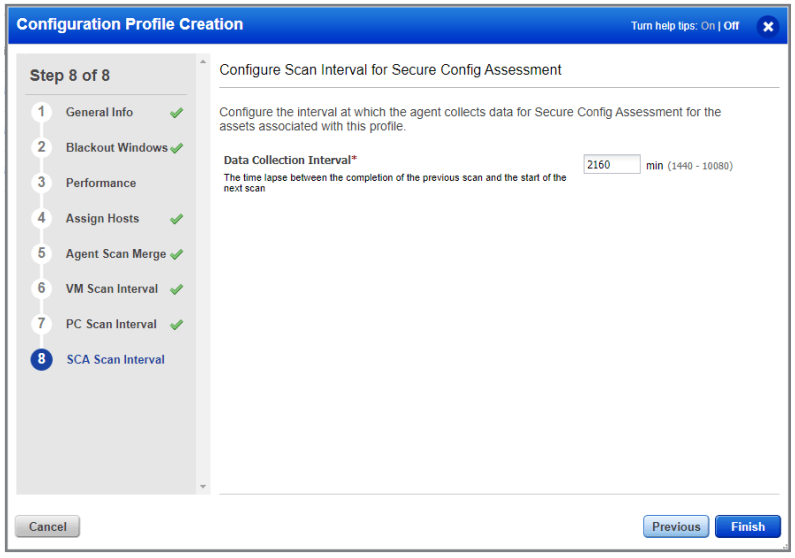


4.1.9 Secure configuration assessment (SCA) scan interval

The same recommendations from the “VM Scan Interval” apply here as well.

Clicking the “Finish” button completes the “Profile Creation” dialog.

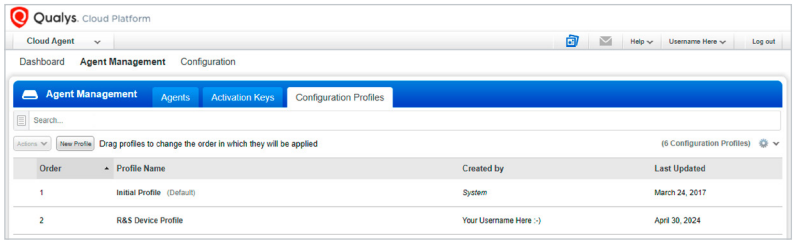
Figure 13: Configuration of scan interval for SCA (step 8 of 8)



4.1.10 Profile creation finished

After successfully completing the “Profile Creation” dialog, the newly created profile is available in the listing under the “Configuration Profiles” tab.

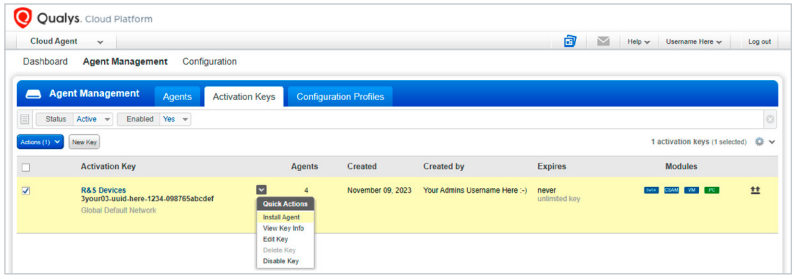
Figure 14: New profile is available



4.2 Activation keys

The cloud agent must be downloaded and installed on the target device. By switching to the “Activation Keys” tab, selecting an available “Activation Key” and clicking the drop-down menu to select “Install Agent”, you will reach the dialog that contains the deployment options and further information.

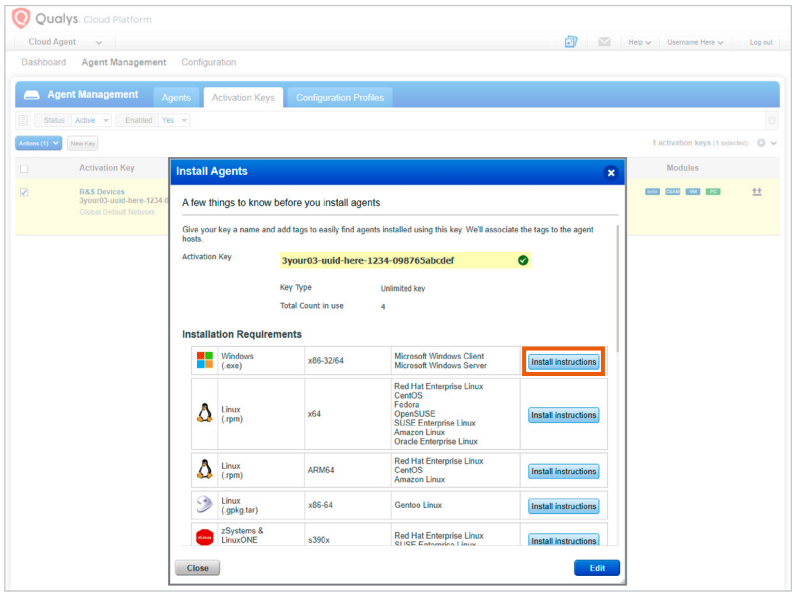
Figure 15: Activation keys



4.2.1 Install agents (1)

The “Install Agents” dialog gives you an overview of the installation requirements and accompanying installation instructions. Since this white paper is only concerned with Microsoft Windows, clicking the “Install instructions” button will bring you to the next step.

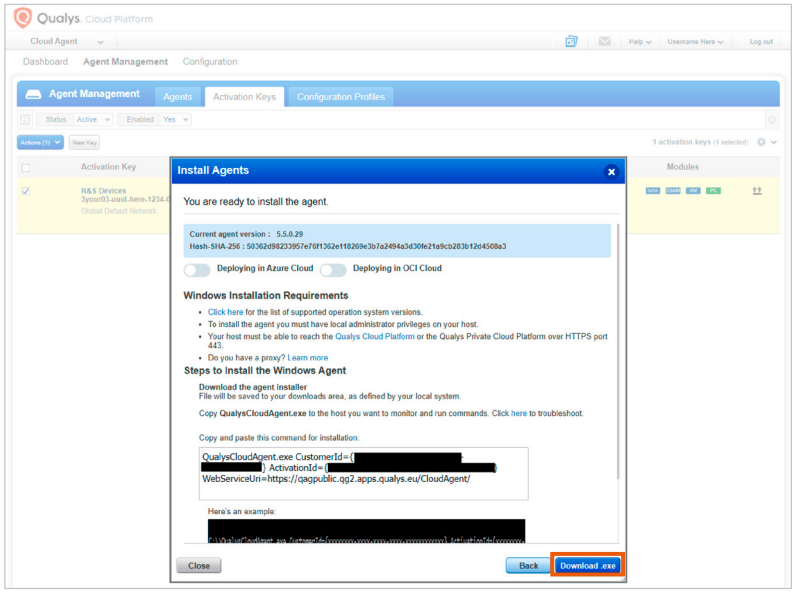
Figure 16: Installation of agents (step 1)



4.2.2 Install agents (2)

The "Install instructions" button will change the content of the "Install Agent" dialog box to show more information, including further links to configure network proxies and copy&paste command line code to execute in an administrative "cmd.exe". Save these instructions in a text file and transfer it to the device with the binary of the cloud agent that can be obtained by clicking the "Download .exe" button. This will give you the required executable that needs to be transferred to the device.

Figure 17: Installation of agents (step 2)



The next steps need to be performed on the device and are described in the following section.

5 INSTALLATION ON ROHDE&SCHWARZ DEVICE

This white paper covers a manual way of deploying a Qualys cloud agent on a device. Other methods may be appropriate for a large-scale deployment, but they are outside the scope of this white paper.

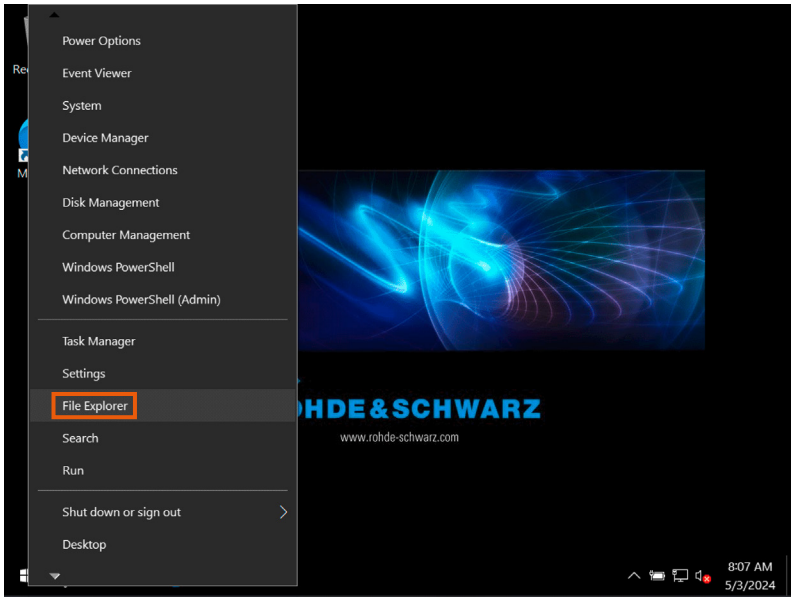
Put the TXT file and the Qualys cloud agent executable on a USB flash drive and connect it with the device.

Connect a mouse and keyboard to it as well.

5.1 File explorer to check USB flash drive

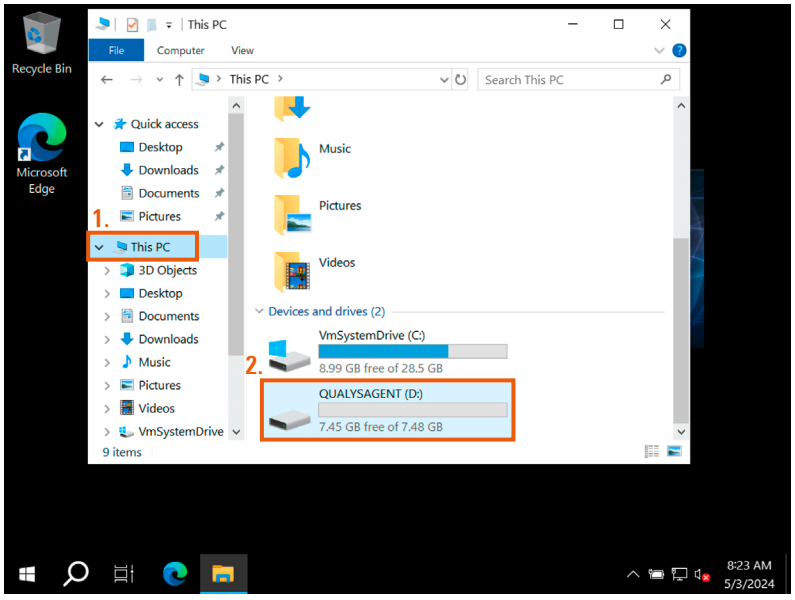
Press the “Windows key” and then right-click the “Start menu” button. From the context menu, select “File Explorer”.

Figure 18: Installation on a Rohde&Schwarz device (step 1)



In the Explorer window, select “This PC” and scroll down to your USB flash drive.

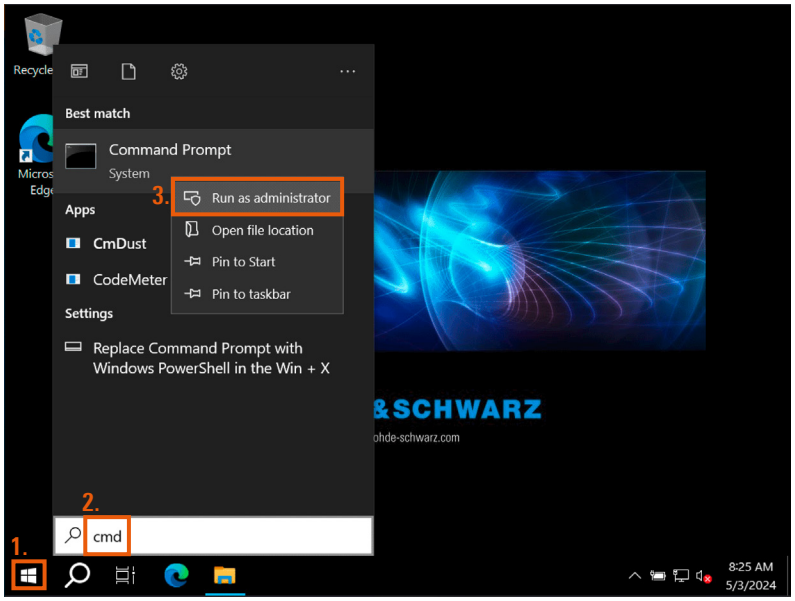
Figure 19: Installation on a Rohde&Schwarz device (step 2)



5.2 Administrative command line

Press the “Windows key”, open the “Start menu” and type “cmd.exe”. Then right-click and select “Run as administrator” from the context menu.

Figure 20: Installation on a Rohde&Schwarz device (step 3)



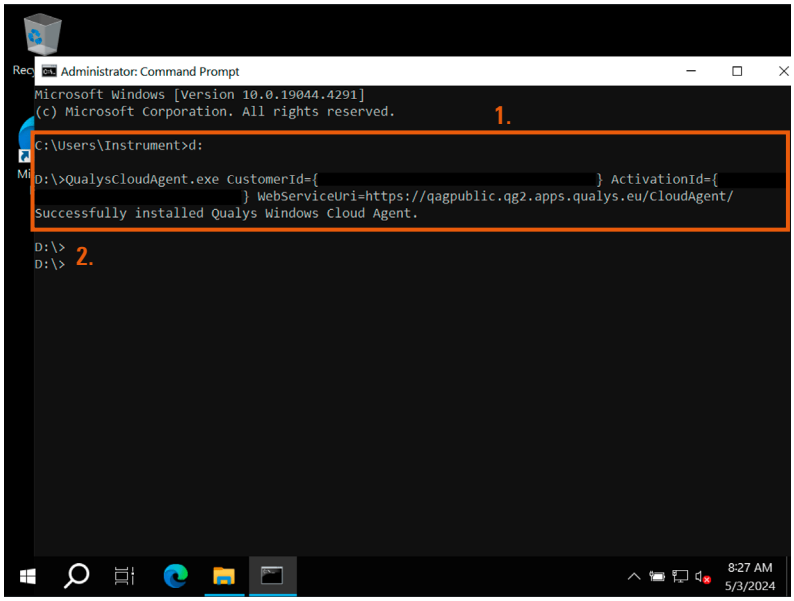
Depending on your device, you may be asked to provide “Administrator” credentials. Contact Rohde&Schwarz Customer Support to obtain the required access.

5.3 Administrative command line to install agent

In the administrative command line, enter your USB flash drive letter followed by a ":".

Then copy the previously saved command line from the TXT file, paste it in the CMD and hit "enter" to execute it. The image below shows a successful installation.

Figure 21: Installation on a Rohde&Schwarz device (step 4)



Configuring a proxy server or other special environment conditions are outside the scope of this white paper. Refer to your Qualys documentation or reach out to your Qualys customer support contact.

6 TROUBLESHOOTING OF QUALYS CLOUD AGENT

For troubleshooting and advanced configuration needs, refer to the official Qualys documentation which can be found at the following links [1]:

Getting started
https://cdn2.qualys.com/docs/qualys-cloud-agent-getting-started-guide.pdf

Troubleshooting
https://docs.qualys.com/en/ca/portal/latest/#t=agents%2Ftroubleshoot.htm

Agent management
https://docs.qualys.com/en/ca/portal/latest/#t=agents%2Fmanage_agents.htm

7 SERVICE, BACKUP OR FACTORY RESET

During service, a device may have a newer Windows image installed, which will remove any third-party or after-sales software. The same applies to backup/restore or factory reset operations on devices. It is the responsibility of the customer to remove and reinstall any third-party software such as Qualys Cloud Agent on the device.

8 SUMMARY

Following along this white paper should help you to deploy Qualys Cloud Agent on the Rohde&Schwarz devices you manage. Where applicable, baseline recommendations are given, but your lab or production use of devices may require additional optimization depending on your specific environment. Keep in mind that according to our disclaimer (see page 3), it is your responsibility to ensure the appropriate performance and reliability when using third-party software components.

If you encounter any issues with this white paper or have suggestions to improve security features of our products, send an email to our product security team at productsecurity@rohde-schwarz.com.

[1] Note: All links have been checked and were functional when this document was created. However, we cannot rule out subsequent changes to the links.

Rohde & Schwarz

The Rohde & Schwarz technology group is among the trailblazers when it comes to paving the way for a safer and connected world with its leading solutions in test & measurement, technology systems and networks & cybersecurity. Founded 90 years ago, the group is a reliable partner for industry and government customers around the globe. The independent company is headquartered in Munich, Germany and has an extensive sales and service network with locations in more than 70 countries.

www.rohde-schwarz.com

Rohde & Schwarz customer support

www.rohde-schwarz.com/support

PD 3684.1550.52 | Version 01.00 | July 2024 (ch) | White Paper
Deploying the Qualys Cloud Agent (QAgent) on Windows based devices
Data without tolerance limits is not binding | Subject to change