Remote Desktop Commander Agent Deployment Guide

Table of Contents

Overview

The Remote Desktop Reporter Agent extends the types of data that the Remote Desktop Commander Suite can gather and also enhances the types of dashboards and reports available in the main Remote Desktop Commander Client. It also allows Remote Desktop Commander to collect and report on data even in environments that do not use Remote Desktop Connections, such as exclusively on-premises networks with physical PCs and VDI.

Here are a few examples of environments where the Remote Desktop Reporter Agent can be useful:

- An on-premises network that utilizes Windows 7, Windows 8, or Windows 10 desktop workstations, where management wants to monitor user productivity.
- An MSP run, cloud-based network that provides Virtual Desktops (e.g. via Citrix Virtual Apps and Desktops or equivalent) to various clients.
- An MSP run, cloud-based network that offers hosted End User Computing environments (e.g. via Citrix Virtual Apps and Desktops, Microsoft RDS or equivalent).
- An on-premises corporate network that facilitates telework via designated shared computing environments (e.g. via Citrix XenApp, XenDesktop Server, Microsoft RDS or equivalent).
- A Microsoft WVD or RDS environment deployed in Microsoft Azure.

Once installed, the Remote Desktop Reporter Agent can be configured to collect various metrics, such as process and user session performance (CPU and memory consumption), inbound/outbound TCP and UDP connections, and periodic screen captures of user session activity. On physical Windows workstations or PCs that do not leverage Remote Desktop connections, the agent can facilitate the collection of metrics like session duration and idle/active time, so this information can be consolidated in the same reports that *already track* this information in Remote Desktop connections.

Note: You use the Remote Desktop Commander Client to view the special metrics and activity that the Remote Desktop Reporter Agent Service has gathered. More is mentioned about this utility in a later section.

Agent Components

The Remote Desktop Reporter Agent is comprised of two key components:

- The **Remote Desktop Reporter Agent Service** runs continuously while a Windows system is online. It collects CPU and memory performance metrics and UDP/TCP connections on a per process and per user session basis. In advanced monitoring scenarios, it also can gather metrics from the In-Session Agent Processes (see below) that are loaded into one or more user sessions running on a Windows server/workstation. Ultimately, the main Remote Desktop Reporter Service (running on the computer where the Remote Desktop Commander Suite is installed) then retrieves these gathered metrics from each agent service on each monitored computer during its regular polling interval. The Remote Desktop Reporter Service then transfers the collected data into its central SQL database.
- The **In-Session Agent Process** is responsible for collecting advanced metrics about user sessions running on a Windows system, specifically, screen captures of session activity, window caption text of session activity, and idle/active metrics about the interactive console sessions on physical workstations and VDI workstations. You use batch files to control what types of advanced metrics the In-Session Agent Process gathers, and then you associate those batch files with the login process of one or more users, so the In-Session Agent Process launches automatically when they sign in.

NOTE: You do not need to deploy the In-Session Agent Process at all if you are running a RDS, Citrix, WVD, or similar environment and are only interested in performance and connection metrics, and not interested in screenshots or other advanced user activity monitoring features. The In-Session Agent Process utilizes additional memory and CPU cycles on the target system, so it is important to be selective in how you deploy it.

Agent Security

The In-Session Agent Process cannot be terminated by non-administrator users, and will stay running until the user session ends. Similarly, the Remote Desktop Reporter Agent Service cannot be terminated by non-administrator users.

Additionally, all inter-process and network communication between the In-Session Agent, Remote Desktop Reporter Agent Service, and Remote Desktop Reporter Service are encrypted with AES256 encryption.

Windows Firewall Considerations

If your environment utilizes the built-in Windows Firewall, you must enable the following firewall exceptions, so the Remote Desktop Reporter Service can collect data from its agent service and the operating system in general.

Remote Service Management
Remote Event Log Management
WMI

You can do this manually on each host monitored by the Remote Desktop Commander Suite, or you can build or adjust a Group Policy Object that adjusts the Windows Firewall Settings for the servers being monitored.

Installation Procedure and Configuration Parameters

Installation Package Location

The Remote Desktop Reporter Agent installation package can be found under the ***AgentInstaller*** subdirectory in the Remote Desktop Commander Suite installation directory, which by default is \Program Files (x86)\RDPSoft\Remote Desktop Commander. The installation package name is ***RDRAgentSetup.exe***

Installation Package Prerequisites

In order to install correctly, the target Windows operating system must have Version 3.5, Version 4, or greater of the .NET Framework already installed. The agent installation package will automatically install the binaries that match the target Platform (32-bit or 64-bit) and available .NET Framework (e.g. Version 3.5 or Version 4).

Installation in a VDI environment or any environment that utilizes a "Golden Image VM" (e.g. Citrix XenDesktop Workstation OS, Citrix XenDesktop Server OS, or equivalent)

Start the virtual machine serving as the golden/master image for the virtualized desktops in your environment. Install the Remote Desktop Reporter Agent setup package to the golden/master image virtual machine, then shutdown that virtual machine. Then, in the VDI management software, such as Citrix Studio, update the machines accordingly so at next restart, they will have the Remote Desktop Reporter Agent installed and available.

Installation in a non-VDI environment (e.g. Citrix XenApp Server, Microsoft Windows Server with Remote Desktop Services role, or other Windows systems that do not utilize RDS)

Install the Remote Desktop Reporter Agent setup package on each server or workstation you wish to poll for session information.

Unattended Installation / Customizing Agent Behavior With Command-Line Arguments

You can perform both unattended installation and uninstalls of the agent software by passing specific command line arguments to the RDRAgentSetup installation package. Similarly, you can adjust specific agent operating behaviors by passing specific arguments to the installation package.

Basic Unattended Installation Example:

```
Rdragentsetup.exe /qn
```

The above command-line argument installs the agent software in quiet (unattended) mode.

Basic Unattended Uninstall Example:

```
Rdragentsetup.exe /x // /qn
```

The above command line argument uninstalls the software in quiet mode.

Advanced Unattended Installation Example, With Configuration Parameters:

```
Rdragentsetup.exe CAPTUREBUFFER="120" CAPTUREINTERVAL="30000" MAXSESSIONS="10"
/qn
```

The above command line argument sets three configuration parameters that control the RDR Agent Service behavior, as well as instructing the Windows Installer to install the software in quiet mode.

NOTE: In most scenarios, the default values for the configuration parameters will suffice.

All Available Configuration Parameters:

APPDIR sets the installation directory. The default is “C:\Program Files\RDPSoft\Remote Desktop Reporter Agent”

CAPTUREBUFFER determines how many collection cycles worth of data the Agent Service can hold for each In-Session Agent before having to be retrieved and cleared by the primary Remote Desktop Reporter Service. After the capture buffer limit is reached, no new metrics data will be recorded. The default is 10 collection cycles per In-Session Agent. The frequency of each collection cycle is determined by the CAPTUREINTERVAL parameter below.

CAPTUREINTERVAL, specified in milliseconds, determines how frequently the session metric data should be collected by the Agent Service, the In-Session Agent, or both. The default is 30000, or 30 seconds.

MAXSESSIONS determines how many In-Session Agent Processes the Remote Desktop Reporter Agent Service can interact with on a single system. If you are installing the Agent components on a physical Windows workstation or Windows Workstation Virtual Desktop, this number should be set to 3 or lower. If you are installing the Agent components on a hosted, shared Server OS environment (e.g. XenApp, XenDesktop Server OS, Windows Server OS with the RDS role enabled, WVD Windows 10 Multisession in Azure), AND you plan on deploying the In-Session Agent to do advanced metric collection, you must set this number to the highest potential number of simultaneous user sessions you anticipate the server will support. The default is 50.

NOCONNECTIONDATA enables or disables the collection of TCP/UDP connection data related to all users and processes running on the system. By default, NOCONNECTIONDATA is set to 0, meaning TCP/UDP connection data will be collected. If you wish to not collect this data, which can greatly increase space requirements in your SQL database and will also increase the amount of CPU used by the agent service for data collection, set this value to 1.

SERVICEDISPLAYNAME determines how the RDR Agent service appears in the list of services installed on the machine. The default is "RDPSoft RDR Agent Service." However, if you want to conceal the fact that user sessions are being monitored, you can rename our service to something else entirely.

Should you wish to change agent configuration settings *after installation*, you may do so by adjusting them directly from the following registry key: **HKLM\SOFTWARE\RDRAgent** … You can also adjust some of these behavioral settings centrally via the **Polling Rate & Agent Tuning Wizard** located under the Remote Desktop Commander Configuration Tool, under the Polling Tab.

Do I Need to Deploy the In-Session Agent via a Logon Script?

If you will be monitoring session activity on RDS servers, Citrix servers, WVD hosts, etc, where all activity will take place via remote sessions, AND you only want to collect CPU, Memory, and network connection performance data, you **DO NOT** need to deploy the In-Session Agent. Simply install the agent service via the RDRAgentSetup.exe installer, and nothing more is required.

If you will be monitoring session activity on RDS servers, Citrix servers, WVD hosts, etc, where all activity will take place via remote sessions, AND you want to perform session recording (e.g. *screenshot and window caption data* in addition to CPU, Memory, and network connection performance data), you **DO** need to deploy the In-Session Agent, but **ONLY for the users who require this advanced level of monitoring (see below)**.

If you will be monitoring activity on a physical workstation or a VDI workstation, and you wish to collect session idle/active metrics and/or session screenshot activity, you **DO** need to deploy the In-Session Agent.

How to Invoke the In-Session Agent For Specific Users, and Configuring What Metrics It Monitors

Quick Start Cheat Sheet for Monitoring Levels in Different Environments

If you are monitoring RDS servers, Citrix servers, or WVD hosts, and you wish to perform session recording (e.g. screen captures) and window caption recording in addition to standard performance monitoring, **use the Level 15 batch file (RDRLevel15Logon.bat).** However, only deploy this to the users who require this level of monitoring to minimize CPU and memory consumption. Read on below to see your options for deploying this batch file.

If you are monitoring physical workstations ***where users physically work in front of their workstations***, or utilize a VDI system ***where users do not connect via RDP*** and you only want to see their idle/active time, plus CPU/memory performance and network activity, **use the Level 7 batch file (RDRLevel7Logon.bat).** Read on below to see your options for deploying this batch file.

If you are monitoring physical workstations ***where users physically work in front of their workstations***, or utilize a VDI system ***where users do not connect via RDP*** and you want to perform session recording (e.g. screen captures) in addition to all of the other metrics listed above, **use the level 15 batch file (RDRLevel15Logon.bat).**

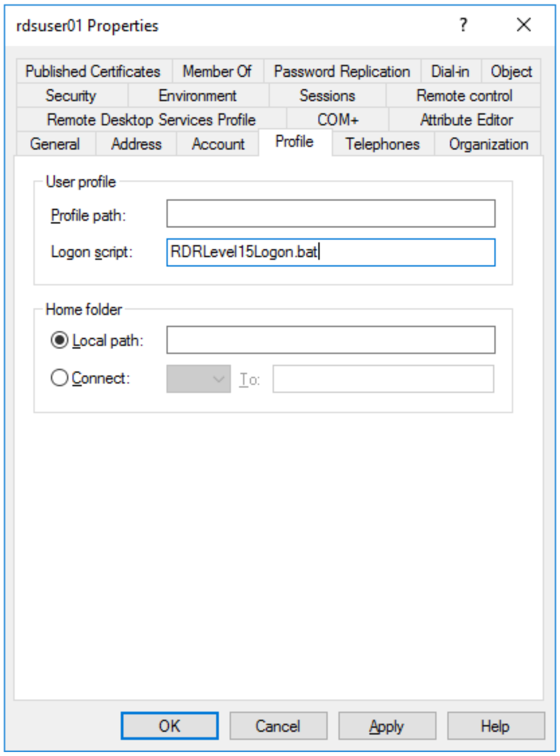
Invoking the In-Session Agent For Specific Users Via the Active Directory Users and Computers MMC Tool and the Domain NETLOGON folder

This is the easiest way to make the In-Session Agent launch specifically for specific users, when they log into a RDS/Citrix/WVD host, or physically sit down and log into a workstation. Here are the steps:

1.) Copy the appropriate batch file (e.g. RDRLevel15Logon.bat or RDRLevel7Logon.bat – see above) from the *\Program Files (x86)\RDPSoft\Remote Desktop Commander\AgentInstaller* directory into the *NETLOGON* folder of your domain controller. To access this folder, type in \\DOMAIN\NETLOGON in Windows Explorer, where DOMAIN is the name of your Windows domain.

2.) Once the appropriate batch file is copied over, launch the Active Directory Users and Computers MMC Tool, located under Administrative Tools in the Windows Control Panel of your Domain Controller.

3.) For each user who needs the additional monitoring provided by the In-Session Agent process, double click on that user, and then go to the Profile Tab. In the Logon Script field, enter in the name of the batch file to be launched when they are signed. NOTE: DO NOT enter the full path to the NETLOGON directory, ONLY the name of the batch file which is residing IN the NETLOGON folder. E.g.



Profile path:

Logon script: RDRLevel15Logon.bat

● Local path:

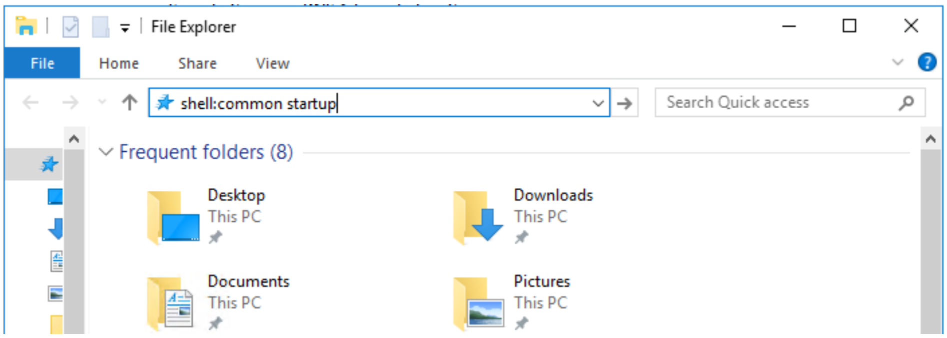
○ Connect: To:

Click “OK.” The next time the user logs in, the In-Session Agent process will start, and the additional monitoring data will be collected and transmitted to the Remote Desktop Commander application via the agent service. Later, if you want to turn off this monitoring for a user, pull up the user again in Active Directory Users and Computers, and REMOVE the reference to our batch file in the Logon Script field.

Invoking the In-Session Agent For All Users That Log Into RDS Servers, Citrix Servers, WVD Hosts, or Physical Workstations

If you want to perform enhanced monitoring for ALL users who sign into a terminal server or physical workstation, please perform the following steps. Please note that turning on screenshot recording for every single user session on a terminal server or WVD host can use a non-trivial amount of CPU, and requires nearly 30MBs of additional memory per signed on user. Therefore, if your terminal server or host is already over-subscribed with users and is "redlining" CPU or memory throughout the day, you should upgrade resources on that virtual machine before deploying the In-Session Agent for all users.

1.) Copy the appropriate batch file (e.g. RDRLevel15Logon.bat or RDRLevel7Logon.bat – see above) from the *\Program Files (x86)\RDPSoft\Remote Desktop Commander\AgentInstaller* directory into the Common Startup folder for All Users on each of your terminal servers, WVD hosts, or physical workstations. To access this folder, type in SHELL:COMMON STARTUP in Windows Explorer and hit enter, like so:



shell:common startup

Once the appropriate batch file is copied into the Common Startup folder for all users, any user who signs in on that system will have the In-Session Agent process launched in their session, with the enhanced monitoring enabled.

2.) Later, you can remove the appropriate batch file from this folder on each system if you no longer want to perform enhanced monitoring for all users.

Invoking the In-Session Agent For Users That Log Into RDS Servers, Citrix Servers, WVD Hosts, or Physical Workstations via Existing Login Scripts

If you already utilize login scripts in your environment via Group Policy or another mechanism, you can place the appropriate batch file (e.g. RDRLevel15Logon.bat or RDRLevel7Logon.bat – see above) into the folder with those login scripts, and then refer to that path and batch file to call the batch file from within your script. Please note that while this is possible, we do not offer support for these scenarios, as Group Policy and login scripts can be very finicky to configure. When in doubt, use the previous methods outlined above to deploy the In-Session Agent.

Reviewing Advanced Monitoring Metrics

In order to review the advanced monitoring metrics collected by the Remote Desktop Reporter Agent, use the Remote Desktop Commander Client. This client allows you to search for specific user sessions to review in depth, and also provides dashboards that allow you to compare resource use by user as required. Finally, just like the Remote Desktop Commander Configuration Tool, you can use the Remote Desktop Commander Client to build, review, and schedule reports on all collected monitoring data.

Note 1: If you wish to review collected data remotely, you can install the Remote Desktop Reporter Commander Client on other machines. Its install package is located under the \ClientInstaller subdirectory in the Remote Desktop Commander installation directory (e.g. C:\Program Files (x86)\RDPSoft\Remote Desktop Commander).

Note 2: Make sure you add appropriate user permissions for non-admin clients from inside the Remote Desktop Reporter Configuration Tool, Client and Agent Settings Tab – this must be completed before they can use the Remote Desktop Commander Client from their systems.

Trademark Notice

Remote Desktop Commander, Remote Desktop Reporter, and the Service Provider License Tracker are trademarks of RDPSoft. Microsoft Windows, Microsoft SQL Server, Remote Desktop Services, RDS, Windows Virtual Desktop, and WVD are registered trademarks of the Microsoft Corporation. Virtual Apps and Desktops is a registered trademark of Citrix.