Remote Desktop Reporter Agent Deployment Guide

Table of Contents
Overview .............................................................................................................................. 2
Agent Components ........................................................................................................... 2
Agent Security .................................................................................................................. 2
Windows Firewall Considerations .................................................................................... 3
Installation Procedure and Configuration Parameters ....................................................... 3
  Installation Package Location ......................................................................................... 3
  Installation Package Prerequisites .................................................................................. 3
  Installation in a VDI environment (e.g. Citrix XenDesktop Workstation OS, Citrix XenDesktop Server OS, or equivalent) .......................................................................................... 3
  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) ................................................................. 3
  Unattended Installation / Customizing Agent Behavior With Command-Line Arguments ................................................................. 3
Do I Need to Deploy the In-Session Agent via a Logon Script? .............................................. 4
Launching the In-Session Agent via Logon Scripts, and Configuring What Metrics It Monitors ...................................................................................................................... 5
  Quick Start Cheat Sheet for Monitoring Levels in Different Environments .................. 5
  In-Session Agent Monitoring Levels .............................................................................. 5
  Invoking the In-Session Agent With a Logon Script ....................................................... 6
Using Group Policy To Associate Different Monitoring Levels With Specific Classes of Users ................................................................................................................................. 7
Using the Profile Tab in Active Directory Users and Computers OR Computer Management To Associate a Monitoring Level With A Specific User ................................................................................................................................. 10
Trademark Notice ........................................................................................................... 12
Overview

The Remote Desktop Reporter Agent software is an add-on package that can be installed in several different types of virtualized and non-virtualized environments to both gather and/or enhance reporting features in the main Remote Desktop Reporter application. These include environments where remote desktop connections are not made, such as exclusively on-premise networks and hosted virtual desktops using VDI. Examples of such environments include:

- An on-premise network that utilizes Windows 7 and Windows 8 desktop workstations, where management wants to monitor productivity and other activity.
- An MSP run, cloud-based network that provides Virtual Desktops (e.g. via Citrix XenDesktop or equivalent) to various clients.
- An MSP run, cloud-based network that offers hosted SBC (Server Based Computing) environments (e.g. via Citrix XenApp, XenDesktop Server, Microsoft RDS or equivalent).
- An on-premise corporate network that facilitates telework via designated shared computing environments (e.g. via Citrix XenApp, XenDesktop Server, Microsoft RDS or equivalent).

Once installed, the Remote Desktop Reporter Agent collects basic reporting metrics, such as session duration, idle/active time, processes running, and can also be configured to collect advanced reporting metrics, such as process performance, inbound/outbound TCP and UDP connections, and even periodic screen captures of user session activity.

*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 for each session on the system, as well as connecting UDP/TCP connections from each session. In advanced monitoring scenarios, it also can gather metrics from the Remote Desktop Reporter In-Session Agent Processes loaded into one or more user sessions running on a Windows server/workstation. Ultimately, the Agent Service the sends its data to the main Remote Desktop Reporter Service located on the computer where the Remote Desktop Commander Suite was installed, for inclusion in the 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. Using Group Policy in combination with logon scripts, you can control the level of information it gathers, as well as the type of users it will monitor.

*Note: You do not need to deploy the In-Session Agent Process via logon scripts if you are running an RDS/XenApp environment and are only interested in performance and connection metrics. 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 Remote Service Management exception in Windows 7 / Windows 8 / Windows Server 2012, and in the case of earlier Windows operating systems like Windows 2008, the Remote Administration exception as well.

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 Reporter installation directory, which by default is \Program Files (x86)\RDPSoft\Remote Desktop Reporter. 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 (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 120 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, or Windows Server OS with the RDS role enabled), 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 the server can support. The default is 50.

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

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

If you will be monitoring session activity on RDS servers, Citrix XenApp servers, or VMWare Horizon View servers, 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.

If you will be monitoring session activity on RDS servers, Citrix XenApp servers, or VMWare Horizon View servers, where all activity will take place via remote sessions, AND you want to perform session recording (e.g. screenshot 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.

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.

**Launching the In-Session Agent via Logon Scripts, and Configuring What Metrics It Monitors**

**Quick Start Cheat Sheet for Monitoring Levels in Different Environments**

If you are monitoring physical workstations and/or VDI workstations, and you want to see idle/active time, CPU and memory performance, and network activity, use **level 7 (RDRLevel7Logon.bat)**.

If you are monitoring physical workstations and/or VDI workstations, and you want to perform session recording (e.g. screen captures) in addition to all of the other metrics listed above, use **level 15 (RDRLevel15Logon.bat)**.

If you are monitoring RDS servers, Citrix XenApp servers, or VMWare Horizon View servers (e.g. Windows servers in a session host role), and you wish to perform session recording (e.g. screen captures) as well as gather all of the other performance metrics and networking metrics, use **Level 15 (RDRLevel15Logon.bat)**. However, only deploy this to the logon script of users who require this level of monitoring to minimize CPU and memory consumption.

**In-Session Agent Monitoring Levels**

The In-Session Agent has several levels of monitoring it can perform. The degree of monitoring is controlled by adding up the monitoring level numbers, and passing that number as a command-line argument to the In-Session Agent as part of a logon script or similar mechanism.

**LEVEL 1 – Basic Session Monitoring**

This level captures basic session activity, such as idle time, active time, disconnected time, username, and in the case of Citrix XenDesktop environments, other details like client name, client address, initial program, and working directory. This information is only captured for console sessions – if the session is a RDS / Citrix XenApp session, the Remote Desktop Reporter will obtain it directly from the RDS management interfaces.

**LEVEL 2 – Advanced Process Monitoring**

This level captures advanced process information, such as process name, process identifier, CPU usage, memory usage, process window caption, path to process image on disk, and other similar metrics.
LEVEL 4 – Advanced Connection Monitoring
This level captures advanced TCP and UDP connection data, such as local and remote IP address and port information.

LEVEL 8 – Advanced Session Recording (Screen Captures)
This level does periodic screen captures of the user’s session, transferring the image data and related metadata to the main Remote Desktop Reporter location.

Note: This monitoring level is the most resource intensive, so it should be used selectively for subsets of users, and/or the CAPTUREINTERVAL should be adjusted as appropriate to reduce CPU load based on the hardware/resources allocated to the monitored computer/virtual machine.

Invoking the In-Session Agent With a Logon Script

Three pre-built logon scripts are installed by default under the AgentInstaller directory in the Remote Desktop Reporter installation directory – RDRLevel1Logon.bat, RDRLevel3Logon.bat, RDRLevel7Logon.bat, and RDRLevel15Logon.bat.

Here is the default script syntax:

@echo off
SET RDRAGENTFILE="C:\Program Files\RDPSoft\Remote Desktop Reporter Agent\RDPRDRAgent.exe"
if exist %RDRAGENTFILE% (
    start "" %RDRAGENTFILE% 1
)

where 1 represents the aggregate monitoring level selected in the above example.

This batch file first attempts to see if the In-Session Agent (RDPRDRAgent.exe) exists in the C:\Program Files\RDPSoft\Remote Desktop Reporter Agent directory. If it does, it starts it, using a monitoring level of 1 (Basic Session Monitoring). If you have installed the In-Session Agent to another directory on your virtual machines, you will need to change the path referenced in the SET RDRAGENTFILE command. Similarly, you can adjust the monitoring level. A monitoring level of 3 (1+2) does basic session monitoring and advanced process monitoring. A monitoring level of 7 (1+2+4) does basic session monitoring, advanced process monitoring, and advanced connection monitoring. A monitoring level of 15 (1+2+4+8) would do complete monitoring of all metrics, including session recordings.

You can utilize Active Directory to associate certain logon scripts with certain users, or you can similarly use Group Policy to associate logon scripts with certain classes of users.
Using Group Policy To Associate Different Monitoring Levels With Specific Classes of Users

To invoke the In-Session Agent with a logon script, you will need to take the following actions in order:

1.) Create one Global Security Group per Monitoring Level in Active Directory. If your AD structure already has Global Groups that contain users that correspond to the different monitoring levels you plan to use, you can skip this step.

2.) Place the corresponding users into the Global Groups you created in Step 1 above.

3.) Determine which monitoring levels you want Remote Desktop Reporter to use. (e.g. Level 1, Level 3, Level 7, or Level 15). Place the corresponding logon scripts (e.g. RDRLevel1Logon.bat, RDRLevel3Logon.bat, RDRLevel7Logon.bat, and RDRLevel15Logon.bat) into a globally-accessible location (e.g. \domain.com\netlogon, or \\domain.com\SysVol\doriangateway.com\Policies\{GUID OF GPO\User\Scripts\Logon)
4.) Using the Group Policy Management Console, create one GPO per Monitoring Level. Place each GPO at either the top level of the domain forest, or at the top level OU/Container that houses the corresponding users. If you do not already have the Group Policy Management Console installed, download it from Microsoft (http://www.microsoft.com/en-us/download/details.aspx?id=21895) or, in later operating systems, install it via PowerShell (http://technet.microsoft.com/en-us/library/cc725932.aspx)
5.) Edit each newly created GPO, and under User Configuration -> Windows Settings, expand the Scripts (Logon/Logoff) node. Click the Standard tab, and then double-click on the Logon section. Click “Add” to add a reference to the appropriate logon script you placed in a global folder in Step 3.
6.) Restrict the users that each GPO will apply to, by using the **Scope tab** in the Group Policy Management Console. Under **Security Filtering**, *remove Authenticated Users*, and then add the corresponding Global Security group you created in Step 1 to the GPO.

![Group Policy Management Console](image)

7.) Now, when a user logs on to any physical desktop, virtual desktop, or server-based computing system (e.g. RDS/XenApp/Horizon View), the RDPRDRAgent.exe In-Session Agent process will be launched with the appropriate monitoring level, and will begin transmitting information to the Remote Desktop Reporter Agent Service and on to the main Remote Desktop Reporter database.

**Using the Profile Tab in Active Directory Users and Computers OR Computer Management To Associate a Monitoring Level With A Specific User**

In certain situations, you may want to setup an elevated monitoring profile for a specific user. You can do so very easily as follows:

1.) First, remove them from any Global Group that is tied to a GPO Logon Script that automatically launches the Remote Desktop Reporter In-Session Agent (see steps 1-7 above).
2.) If a domain user, add a direct reference to the logon script (e.g. `RDRLevel15Logon.bat`) you want to run when that user logs on in the Profile Tab for the user in the Active Directory Users and Computers snap-in.

![Xen Desktop User Properties](image)

3.) If a local user, add a direct reference to the logon script you want to run when that user logs on in the Profile Tab for the user in the Computer Management snap-in.

**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 Reporter Admin Client, 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 Admin Client – this must be completed before they can use the Remote Desktop Commander Client from their systems.
Trademark Notice

Remote Desktop Reporter, Remote Desktop Commander, and the Service Provider License Tracker are trademarks of RDPSoft. Microsoft Windows and Microsoft SQL Server are registered trademarks of the Microsoft Corporation. XenApp and XenDesktop are registered trademarks of Citrix. Horizon View is a registered trademark of VMWare.