

# RDPSoft Remote Desktop Commander Suite - An Introduction



Remote Desktop Commander is a comprehensive suite of solutions that provide Terminal Server / Microsoft Remote Desktop Service administrators with both an intuitive, active management interface to manage user sessions on servers in their farms, as well as a complete reporting and analysis interface where they can examine data collected over time. Not just limited to traditional Microsoft RDS Servers, Remote Desktop Commander can manage sessions from other Server-Based Computing platforms, such as Citrix XenDesktop and VMWare Horizon View. It can also manage sessions located on Windows workstations as well.

[Licensed in Lite Mode](#), Remote Desktop Commander acts as a comprehensive session management tool, allowing administrators to review and manage active and disconnected sessions in their RDS farms, in addition to the programs running within those sessions. In addition, administrators can do basic, active monitoring of session activity and resource use (e.g. RDP bandwidth, process memory, server memory, etc).

[Licensed in Fully Integrated Suite Mode](#), Remote Desktop Commander can tap into the Remote Desktop Reporter database to produce detailed reports on historic data, show detailed session activity over time (such as CPU/memory use, UDP/TCP port activity, session recordings, etc), and provide dashboards for troubleshooting and root cause analysis.

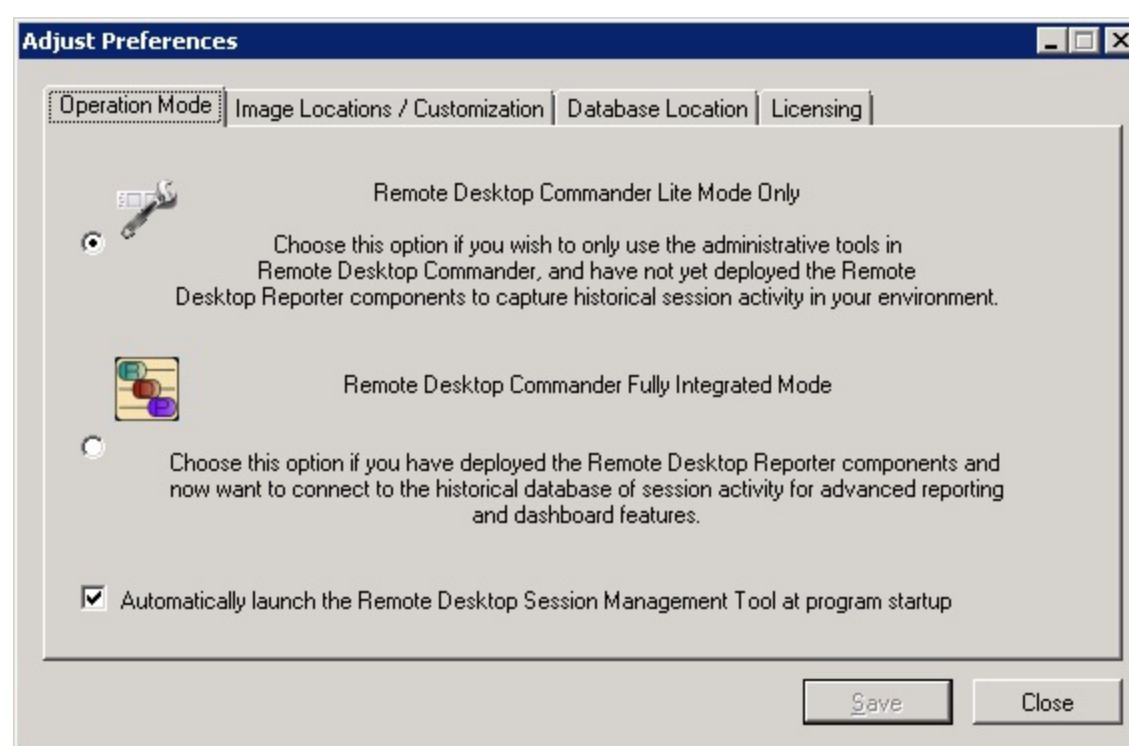
# Using Remote Desktop Commander In Lite Mode

For some server-based computing administrators, the ability to access historical session data for reporting and troubleshooting is not a high priority. Instead, they must focus on the day to day tasks of user session administration, such as:

- Messaging/alerting users
- Observing which users are idle, and if so, for how long
- Observing which users are disconnected, and if so, for how long
- Terminating hung applications or programs that have begun to use excessive resources
- Shadowing user sessions for troubleshooting/help desk purposes
- Determining if a user is utilizing too many server resources (e.g. memory or RDP bandwidth)
- Forcibly logging off or disconnecting users

If so, licensing and using Remote Desktop Commander in Lite Mode is perfect for their needs.

To place Remote Desktop Commander in Lite Mode, go to the **File Menu** and select **Adjust Application Preferences**. In the Operation Mode tab, select **Lite Mode**.



Check the **"Automatically launch the Remote Desktop Session Navigator Tool at startup"** if you want Remote Desktop Commander to immediately load active session information from your farm when it starts up. Otherwise, you can invoke the [Session Navigator](#) (including multiple instances of it from the Admin Tools menu).

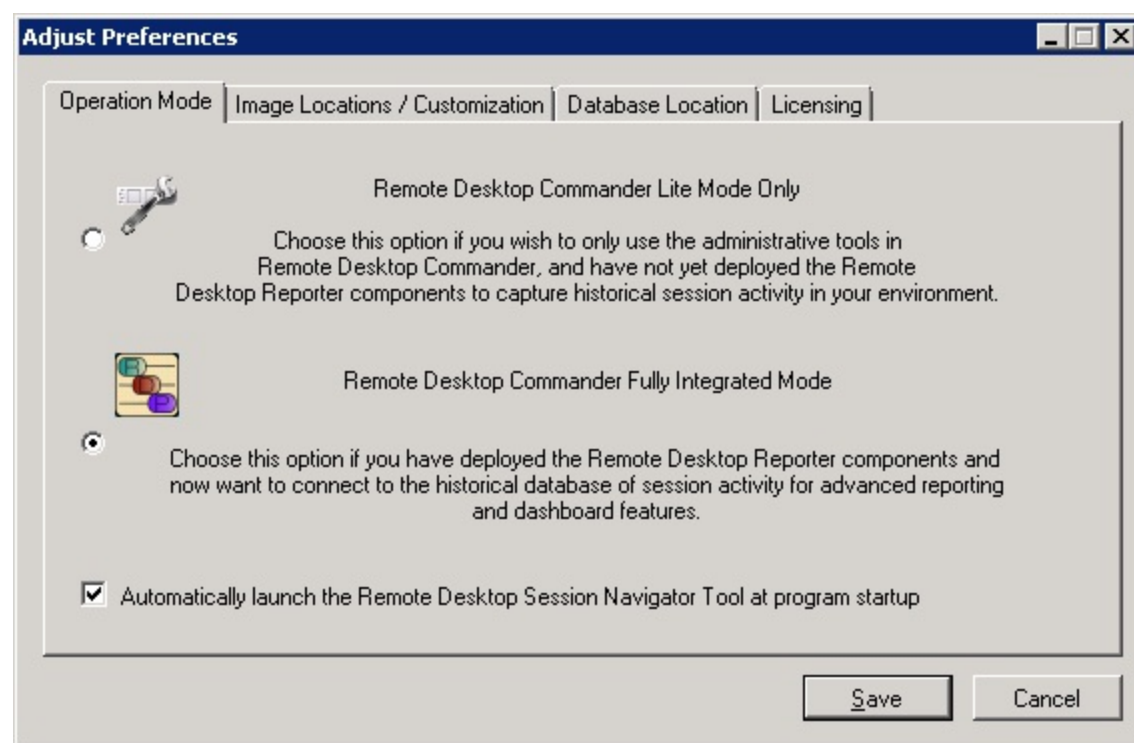
To create groupings of servers and workstations that represent your server-based computing farm (e.g. RDS/Citrix Xenapp, etc), go to the **Edit Menu**, and select **Define Computer Groups**. From here, you can create logical partitions of computers you work with on a regular basis. Computer names can be added manually, or directly from Active Directory if you have a Microsoft Windows domain environment.

# Using Remote Desktop Commander In Fully Integrated Suite Mode

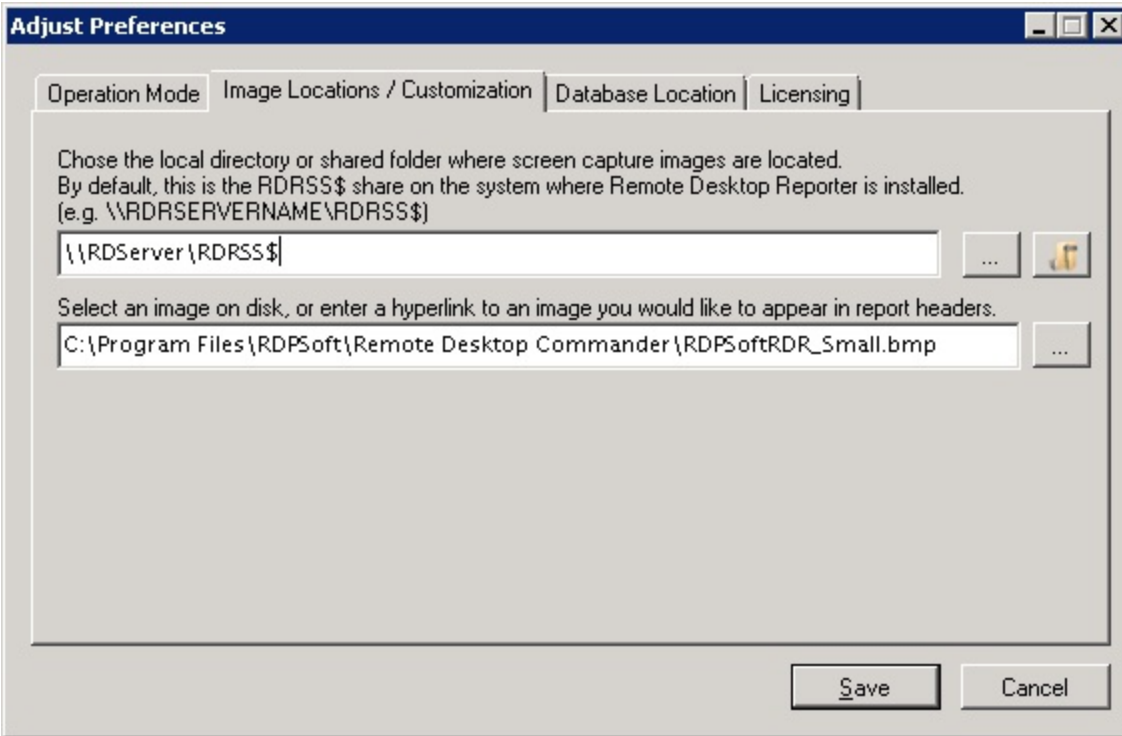
When you elect to license and use Remote Desktop Commander in Fully Integrated Suite Mode, you can leverage all of the powerful features of the Remote Desktop Commander Suite to provide total management and visibility into your server-based computing environment. For example:

- You can review historical trend reports based on data collected by Remote Desktop Reporter.
- You can leverage dashboards that show the performance impact of different users and applications on your servers.
- You can search for specific types of activity that take place in user sessions, such as network (TCP/UDP) activity, applications run, websites visited, etc.
- You can do a "deep dive" into recorded user sessions for problem root cause and analysis.
- You can review playbacks of user session recordings.
- And, just as in Lite Mode, you can actively manage and monitor sessions currently in use in your server farm.

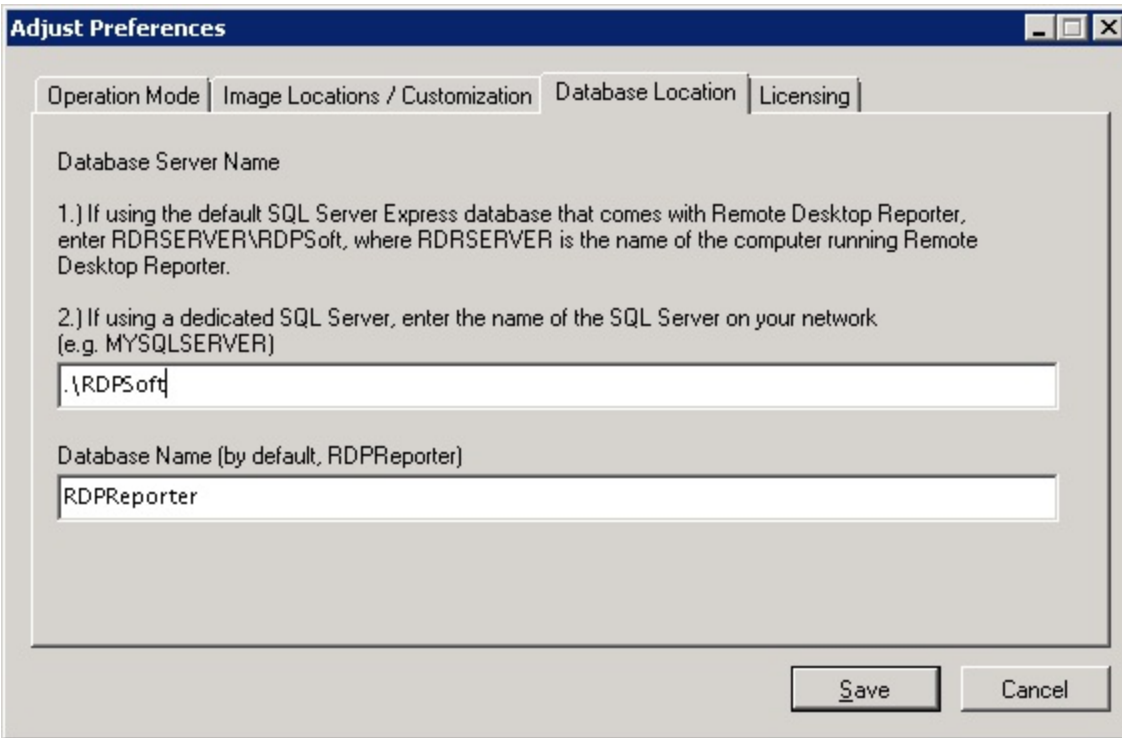
To place Remote Desktop Commander in Fully Integrated Mode, go to the **File Menu** and select **Adjust Application Preferences**. In the Operation Mode tab, select **Fully Integrated Suite Mode**.



Once this is done, go to the Image Locations tab, and set the link to the UNC share or the local path where recorded session screenshots are being stored by Remote Desktop Reporter. If you're not sure where this directory is located, open the Remote Desktop Reporter Admin Client, and visit the [Client and Agent Settings Tab](#).



Finally, select the Database Location tab, and enter in both the location of the Remote Desktop Reporter database server (and RDPSoft instance - if using the built-in SQL Server Express database), as well as the name of the database (by default, this is RDPReporter).



Click save, and then close and reopen Remote Desktop Commander. If you configured the above areas appropriately, you will now be able to access the Remote Desktop Reporter database and session recording repository to review historical trend and performance information.

# Remote Desktop Commander Menus

## File Menu

- **Application Preferences and Licensing** - Raises the Adjust Preferences Dialog, where you can change Remote Desktop Commander's operating mode, manage licensing, and inform the software where to access session screenshots and polled session data from the Remote Desktop Reporter database.
- **Exit** - Closes the Remote Desktop Commander program.

## Edit Menu

- **Define Computer Groups** - Displays the [Create and Manage Computer Groupings Dialog](#), which you use to create logical groups of computers that Remote Desktop Commander can manage in the Session Navigator Window.

## Admin Tools Menu

- **Remote Desktop Session Navigator** - Loads a new instance of the [Session Navigator Window](#), from where you can manage and monitor current session activity in your server farm.

## Reports & Dashboards Menu

- **Run Reports (Fully Integrated Mode Only)** - Loads the [Reporting Dialog](#), from where you can run reports manually or schedule them for later creation.
- **Memory and CPU By Session, Peak Memory Use By Session, Average Memory Use By Session Dashboards (Fully Integrated Mode Only - Remote Desktop Reporter Agent Required)** - Raises dashboards you can use to review and report on recent performance metrics from session data recorded by the [Remote Desktop Reporter Agent](#).

## User Session Review

- **Open Recorded Session (Fully Integrated Mode Only - Remote Desktop Reporter Agent Required)** - Starts the [Recorded Sessions Dialog](#), from where you can select review user session activity that was recently recorded by the Remote Desktop Reporter Agent.
- **Search for Session (Fully Integrated Mode Only - Remote Desktop Reporter Agent Required)** - Launches the Criteria Search Dialog, where you can search for recorded sessions by window caption, port activity, and/or program use.

## Window Menu

Displays all open child windows in the Remote Desktop Commander UI, allowing you quickly to navigate to a particular area of the program.

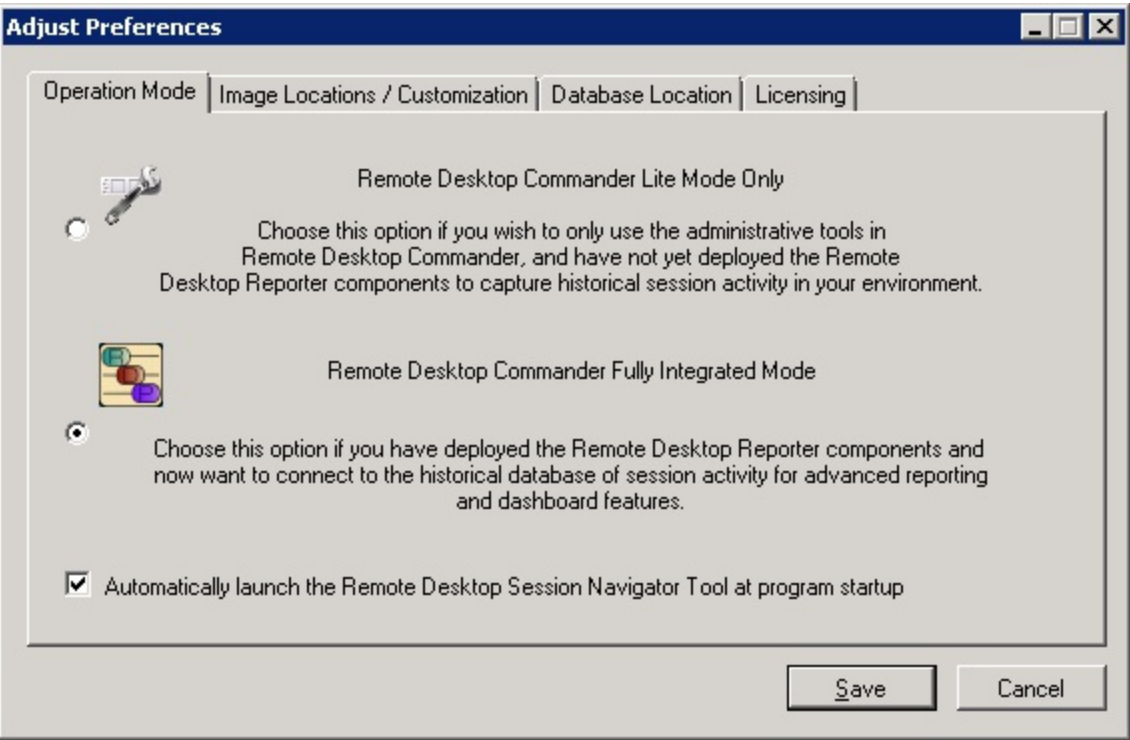
## Help Menu

- **Get Online Assistance from RDPSoft** - Connects to the RDPSoft website, where you can access the online support portal and other options.
- **Remote Desktop Commander Help** - Loads this help file.

# Remote Desktop Commander Preferences

In the File Menu -> Application Preferences and Licensing raises the Preferences Dialog for Remote Desktop Commander. Here, you can change Remote Desktop Commander's operating mode, manage licensing, and inform the software where to access session screenshots and polled session data from the Remote Desktop Reporter database.

## Operation Mode Tab

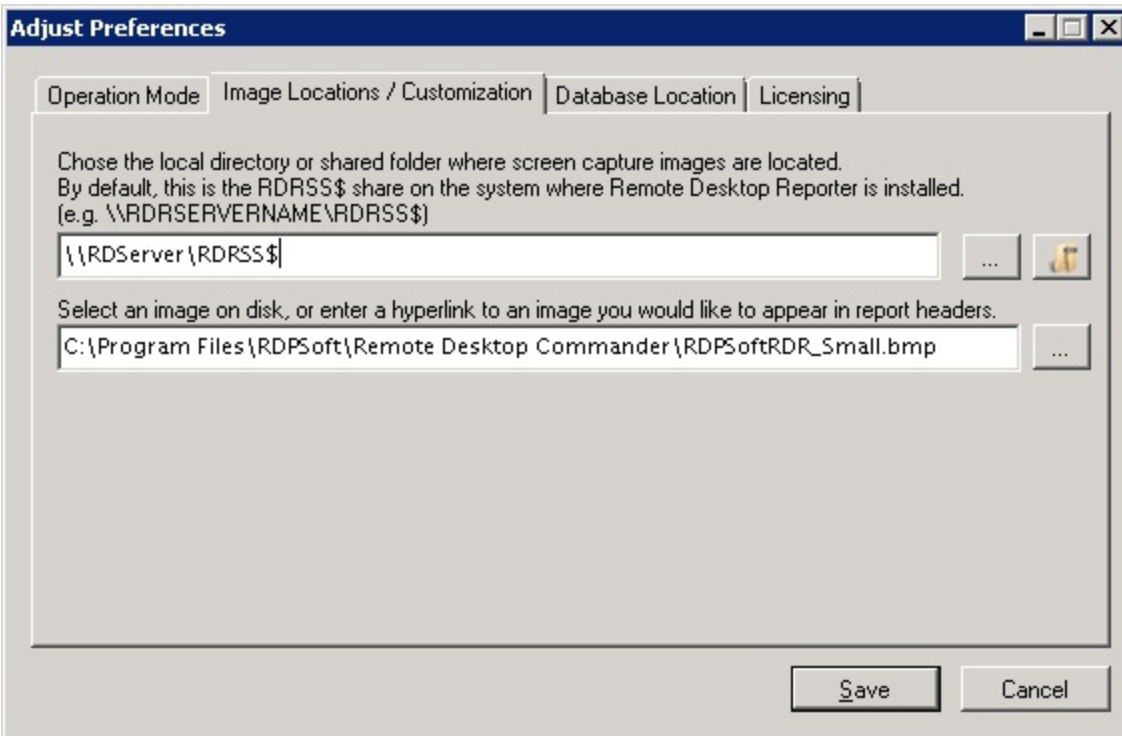


Select **Lite Mode** to only use the Administrative Tools in Remote Desktop Commander, such as the [Remote Desktop Session Navigator](#).

Select **Fully Integrated Mode** to access all of the features of the full Remote Desktop Commander Suite. **NOTE:** This requires connecting your Remote Desktop Commander instances to a Remote Desktop Reporter database, so if you have not [setup the Remote Desktop Reporter component](#) at this time, you must do so first.

Check the "**Automatically launch the Remote Desktop Session Navigator Tool at startup**" if you want Remote Desktop Commander to immediately load active session information from your farm when it starts up. Otherwise, you can invoke the [Session Navigator](#) (including multiple instances of it from the Admin Tools menu).

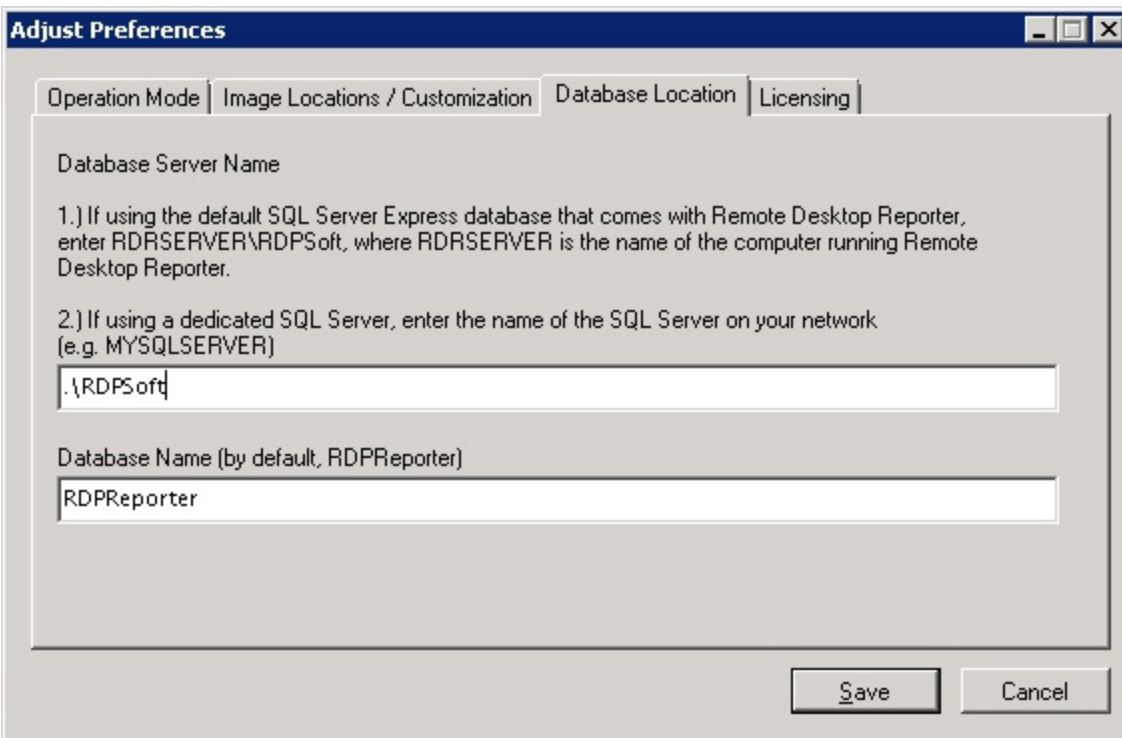
## Image Locations / Customization Tab



Here, set the link to the UNC share or the local path where recorded session screenshots are being stored by Remote Desktop Reporter. If you're not sure where this directory is located, open the Remote Desktop Reporter Admin Client, and visit the [Client and Agent Settings Tab](#). If Remote Desktop Reporter is installed on a different computer, you will need to reference a UNC path to the screen capture images folder. By default, this UNC Path is \\NAMEOFRDSERVER\RDRSS\$ unless you changed it.

Also, should you wish to change the default image used for report headers when you produce manual reports using the [Reporting Dialog](#), you can override the default image path here.

### Database Location Tab



Here, enter in both the location of the Remote Desktop Reporter database server (and RDPSoft instance - if using the built-in SQL Server Express database), as well as the name of the database (by default, this is RDPSoftReporter). By default, the database server name with instance is ".\\RDPSoft" and the database name is RDPSoftReporter. However, if the database is located on a different system, the Database Server Name must reference that system, such as RDRServer\\RDPSoft (if

using the default SQL Server instance) or SQLServer (if using your own full version of MS SQL).

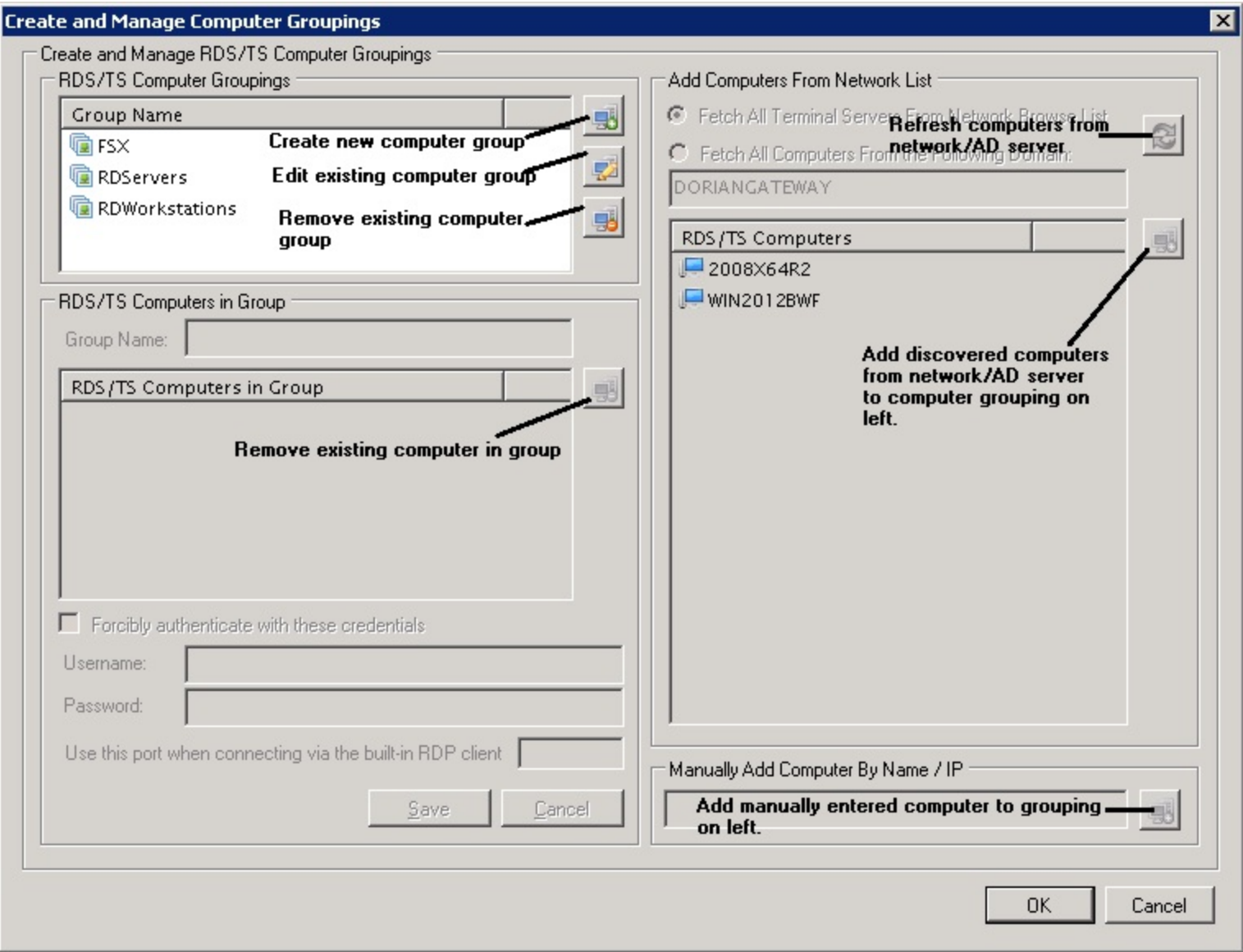
## Licensing Tab

See the [section on Licensing](#).



# Create and Manage Computer Groupings Dialog

Use this dialog to create logical groupings of Remote Desktop servers and workstations you will manage in the [Remote Desktop Session Navigator Window](#).



In the top left hand side, use the Create, Edit, or Remove buttons to create a new computer grouping, edit an existing grouping, or remove an existing grouping respectively.

In the middle left hand side, use the **Group Name** field to give your new computer grouping a name, or to change the name of an existing computer grouping.

In the right hand side, use the **Refresh** button to retrieve a list of computer names from your network. If operating in a workgroup, select **Fetch All Terminal Servers From Network Browse List**. If operating in a domain, select **Fetch All Computers From the Following Domain**, and enter in the name of your domain, if it is not already present. Select the computers from the network you wish to add via the **Add** button. If you wish to add computers manually by name or IP address, enter them in the lower right text field and click **Add Manually**.

Once you have added your computers, return the lower left hand side, and click **Save**. Alternatively, click **Cancel** to abandon your changes.

If you wish to force authentication with different user credentials for a given computer grouping, check **Forcibly authenticate with these credentials** and then enter in a valid **Username** and **Password**. Also, if you want to connect to these computers via the built in Terminal Server client, yet they use a non-standard port (as opposed to 3389 / Default RDP), enter in a new valid port number here.

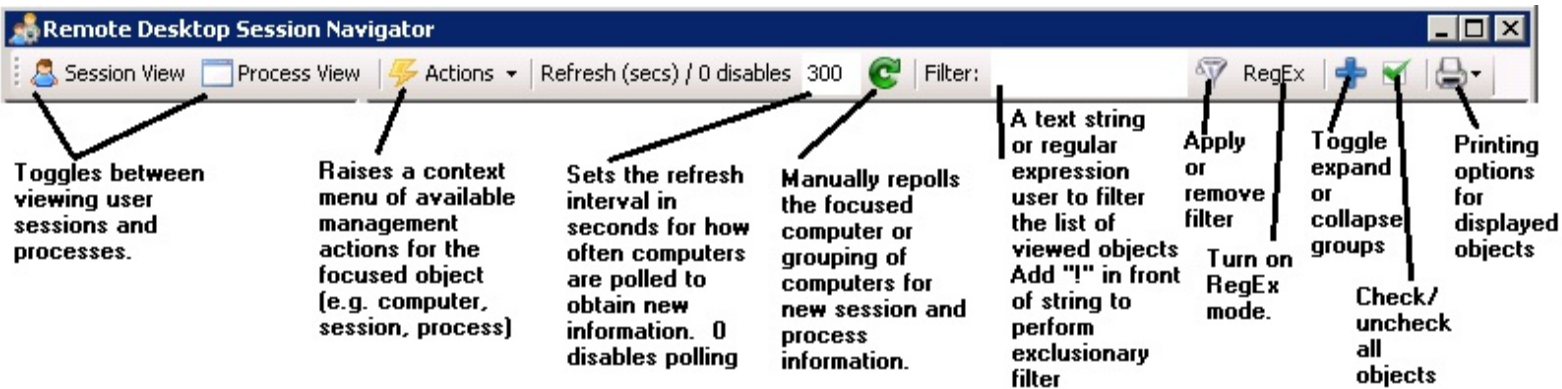
Once you have finished making changes, click **OK**. To abandon your changes, click **Cancel**. Once your changes are confirmed, any open [Remote Desktop Session Navigator Window](#) will be refreshed with your changes.

# Remote Desktop Session Navigator Window

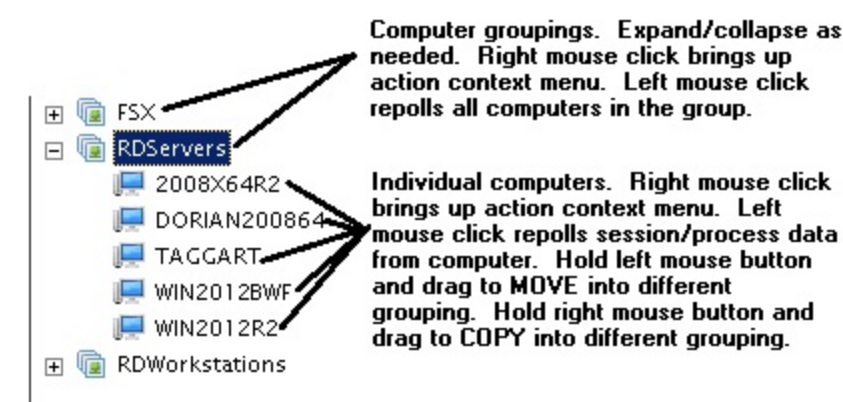
If you are using Remote Desktop Commander in Lite Mode, the Remote Desktop Session Navigator Window will be the primary area of the program you interact with on a day to day basis. The main job of the Session Navigator is to poll the computers in the groupings you created using the Create and Manage Groupings Dialog, in order to both list user session activity and process (program) activity running on those computers. The Session Navigator can be used to actively manage sessions and processes (such as disconnecting sessions, logging off sessions, sending popup messages to sessions, shadowing sessions, terminating processes, etc), and it can also be used in a monitoring role (e.g. to observe bandwidth used by specific users and memory used by specific users, processes, and computers).

Continue reading below to find out more about how to use the Session Navigator user interface.

## Session Navigator Toolbar



## Session Navigator Computer Groupings



## Session Navigator Object Listing

User	Server	Winstation	Client ID	Client Build	State	Idle Time	RDP Bandwidth (MBs)
<b>ANDY (Total Sessions: 3)</b>							
<input type="checkbox"/> ANDY	DORIAN200864	RDP-Tcp#1			008 R2	Active	00d:00h:00m:00s 6.016
<input type="checkbox"/> ANDY	WIN2012BWF	No Winstation (Discor			n: 0	Disconnected	05d:19h:41m:33s 0
<input type="checkbox"/> ANDY	WIN2012R2	No Winstation (Discor			n: 0	Disconnected	04d:21h:20m:58s 0
<b>XDUSER (Total Sessions: 2)</b>							
<input type="checkbox"/> XDUSER	DORIAN200864	RDP-Tcp#0			2003	Active	04d:20h:11m:48s 913.819
<input type="checkbox"/> XDUSER	WIN2012BWF	RDP-Tcp#3			2003	Active	05d:00h:29m:25s 0

Session ID  
 Client Device Name  
☒ User  
☒ Server  
☒ Winstation  
☒ Client IP  
☒ Client Build  
☒ State  
☒ Idle Time  
☒ RDP Bandwidth (MBs)

Polled objects, either user sessions or running processes

Object properties, via configurable columns.  
  
Click each column to group and sort by that property.

Column (e.g. object property) visibility can be toggled on/off. To control visibility, right mouse click on the columns and select/deselect as necessary.

When different columns are clicked, the objects are then sorted & grouped by that clicked column property. To collapse the group of related objects, click the plus/minus indicator on the right hand side. You can collapse or expand all of these groups by once by clicking the plus icon in the Session Navigator Toolbar (see above).

## Tips and Tricks

- For larger farms, break up servers into logical computer groupings based on functional role (e.g. Desktop Sessions, Application Sessions, etc). Then, shift focus to different groups as necessary to reduce time spent polling all servers for information.
- Leverage filters to further reduce information. Text filters are the simplest and will only bring back objects that contain the matching text. To perform an exclusionary filter, place an "!" at the beginning of the filter. So, for instance, to remove all Console sessions from view, enter in **!Console** in the filter box and click the filter icon to apply the filter. For advanced filtering, click the **RegEx** button in the Toolbar, enter in a Regular Expression in the filter box, and then click the filter icon to apply the filter.
- To perform operations on multiple objects at once (e.g. sending messages, disconnecting/logging off multiple sessions, terminating multiple processes), check all relevant objects before running an action. Alternatively, apply a filter to limit the scope of objects visible, and then click the **Check All** button in the Toolbar to select all matched, filtered objects.
- Utilize the **Intelligent Groupings** built into the Session Navigator to quickly see summarized information for similar objects. For instance, in **Process View**, click the Username column to group processes by user, so you can see the total memory utilized by user. Similarly, click the **Computer** name to group processes by computer, so you can see the total memory utilized on the server.

# Remote Desktop Commander Dashboards

When licensed in Fully Integrated Mode, and linked to a Remote Desktop Reporter database instance, Remote Desktop Commander can display historical performance data in a variety of dashboards.

**Note:** If the [Remote Desktop Reporter Agent](#) has not yet been deployed on your Terminal Servers, this data will be unavailable.

Currently, three such dashboards are offered:

- Memory & CPU Usage By Session
- Peak Memory Use By Application
- Average Memory Use By Application

Memory & CPU Usage By Session

Timeframe: Custom 01 Jul 2014 02:48 PM to 15 Jul 2014 02:48 PM

Filter By Computer: No Yes WIN7EX86 XDSRV-01

Username	Session Connect Time	Computer	Avg CPU	Max CPU	Min CPU	Avg Me...	Max Me...	Min Mem
XDUSER	7/8/2014 11:42:48 AM	WIN7EX86	1.03%	14.17%	0.10%	191.16	203.54	62.33
XDUSER	7/8/2014 10:44:27 AM	WIN7EX86	0.43%	3.85%	0.05%	101.53	105.91	88.46
XDUSER	7/2/2014 11:46:51 PM	XDSRV-01	0.22%	0.68%	0.05%	175.12	207.60	173.30
XDUSER	7/2/2014 11:45:38 PM	XDSRV-01	0.00%	0.00%	0.00%	242.21	242.21	242.21
XDUSER	7/2/2014 11:34:57 PM	XDSRV-01	0.00%	0.00%	0.00%	264.74	264.74	264.74
XDUSER	7/2/2014 10:56:05 PM	XDSRV-01	0.00%	0.00%	0.00%	169.39	169.39	169.39
XDUSER	7/2/2014 10:53:23 PM	XDSRV-01	0.42%	0.42%	0.42%	150.22	150.92	149.52
XDUSER	7/2/2014 10:47:32 PM	XDSRV-01	0.25%	0.42%	0.21%	174.73	176.92	167.80
XDUSER	7/2/2014 10:42:21 PM	XDSRV-01	0.61%	1.56%	0.21%	213.37	267.87	149.39
XDUSER	7/2/2014 9:28:18 PM	XDSRV-01	1.02%	1.77%	0.07%	427.80	433.33	351.99
XDUSER	7/5/2014 3:06:03 PM	XDWIN-01	1.77%	11.25%	0.21%	477.08	547.66	290.26

Open Selected Session Close

At the top of each dashboard, you control the **timeframe** you wish to present data from. The default timeframe is the last hour, but you can select different timeframes as desired, including custom time ranges. This is useful for tracking down the root cause of a performance issue on one of your servers.

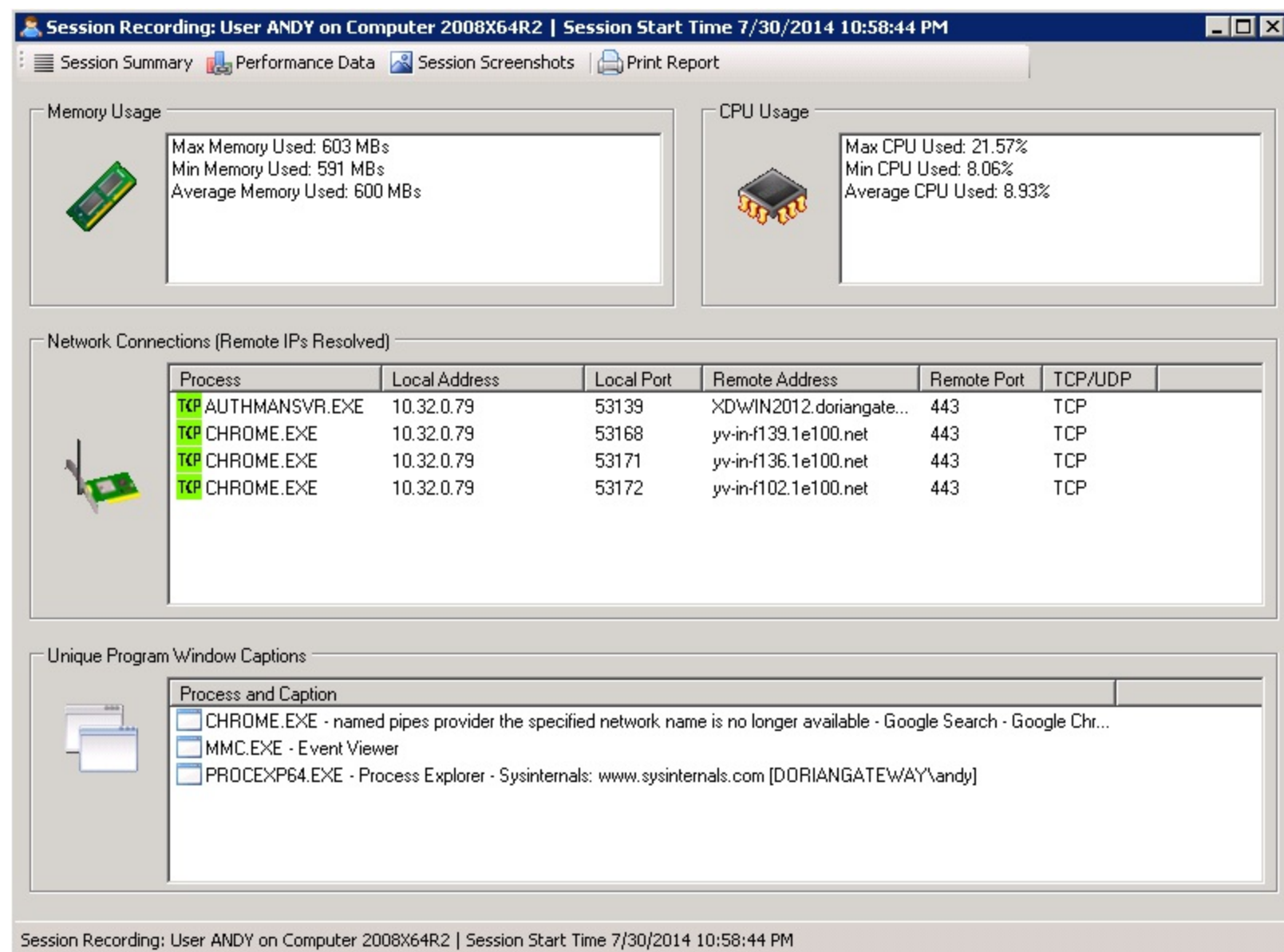
**Note:** The longer the timeframe specified, the longer it will take for Remote Desktop Commander to query the Remote Desktop Reporter database for relevant data.

You can also filter your data search by computer as needed.

In certain dashboards, you will have the ability to jump immediately into a more detailed review of the session(s) whose data (e.g. application use, memory use, etc) was featured in the dashboard. Click the **Open Selected Session** button in the lower right to launch the [Session Explorer Window](#) to start your detailed review.

Click the **Print** button in the lower right to produce a printable report in Microsoft Word, Microsoft Excel, or Adobe PDF format that summarizes the data shown in the current dashboard.

# Session Explorer Window



When licensed in Fully Integrated Mode, and linked to a Remote Desktop Reporter database instance, Remote Desktop Commander can display recorded session histories.

Use the Session Explorer Window to review detailed historical activity about a particular user session. The level of activity you will be able to review is directly dependent on the [Remote Desktop Reporter Agent Monitoring Level](#) in place on your Terminal Servers. **Note:** If the [Remote Desktop Reporter Agent](#) has not yet been deployed on your Terminal Servers, this data will be unavailable.

The **Session Summary** section displays broad aggregate data about the selected session, such as:

- Average, max, and minimum CPU usage
- Average, max, and minimum Memory usage
- Inbound/outbound TCP/UDP network connections made during the session
- Unique program window captions (e.g. all distinct title bar texts of all windowed applications running in the user's session)

The **Performance Data** section shows the amount of memory and CPU used during each monitored period in the session. By default, this is every 30 seconds, but is configurable when deploying the Remote Desktop Reporter Agent. Clicking on a **performance timeslice** (e.g. vertical CPU or memory bar) will show both the distinct processes running in the session at that time, and the performance characteristics of each process, plus the network connections each process had open at

that time.

The **Session Screenshots** section shows a chronological listing of recorded screenshots in the session. Clicking on a thumbnail will bring up the full screenshot, and you can use the navigation buttons at the top of the window to step through all session screenshots as needed, and/or optionally print out one or more in a report.

Clicking **Print Report** will prepare a detailed report of activities in the session.

### **Tips and Tricks**

- Right mouse clicking on process names in the **Session Summary** and **Performance Data** sections will raise a context menu, allowing you to research process names and remote URLs on Google.
- If the session ran for a longer period of time (e.g. greater than 8 hours), Remote Desktop Commander will automatically "window" both the **Performance Data** and **Session Screenshots**, allowing you to select the exact time range you want to review.

# Recorded Sessions Dialog

Open a Recorded Session

Filter By Date:


☐ No

☒ Yes:

01 Jul 2014 03:14 AM

to

01 Aug 2014 03:14 AM



Filter By Domain:

☒ No

☐ Yes:

Filter By Computer:

☒ No

☐ Yes:

Filter By User:

☒ No

☐ Yes:

Username	Session Connect Time	Computer
ANDY	7/30/2014 10:58:44 PM	2008X64R2
ANDY	7/29/2014 9:35:17 AM	2008X64R2
ANDY	6/12/2014 2:16:52 PM	2008X64R2
ANDY	7/24/2014 9:10:12 AM	RIMSKY
ANDY	7/8/2014 3:01:46 PM	WIN7EX86
XDUSER	7/31/2014 11:52:27 AM	2008X64R2
XDUSER	7/30/2014 1:23:42 PM	2008X64R2
XDUSER	7/30/2014 1:13:35 PM	2008X64R2

Open Selected Session

Close

The Recorded Sessions Dialog allows you to browse for all recorded user session histories stored in the Remote Desktop Reporter database. Furthermore, you can adjust the period of time you want to query for available sessions, as well as filter them by domain name, computer, or user.

**Note:** If the [Remote Desktop Reporter Agent](#) has not yet been deployed on your Terminal Servers, this data will be unavailable.

Once you have selected the session you wish to review in more depth, click the **Open Selected Session** button to raise the [Session Explorer Window](#).



# Criteria Search Dialog

Criteria Search For Sessions

Date Range to Search:

01 Aug 2014 03:23 AM

to

15 Aug 2014 03:23 AM

Search By:

Program Window Caption (Title)

☒ Find sessions with an exact window caption:

Calculator

☐ Find window captions that contain:

Search

Username	Session Connect Time	Computer
ANDY	8/1/2014 8:52:29 AM	2008X64R2

Open Selected Session

Close

In many cases, you may need to search for recorded sessions based on the activities performed in the user session. If so, use the Criteria Search Dialog to search for recorded session data by:

- Program Window Caption (e.g. Application Title Bar)
- TCP/UDP Port Activity
- Programs Run

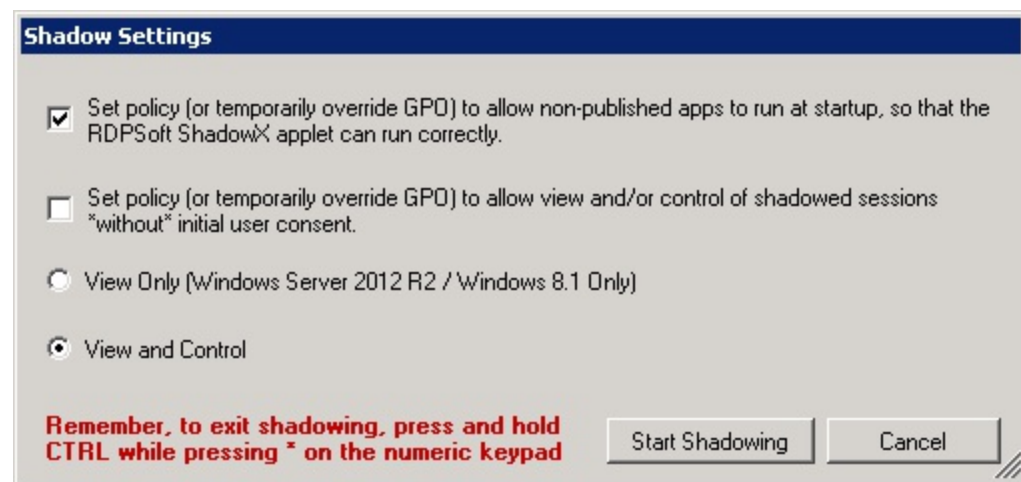
**Note:** If the [Remote Desktop Reporter Agent](#) has not yet been deployed on your Terminal Servers, this data will be unavailable.

First, select the **Date Range** to search over. Next, choose what to **Search By**.

Once you have entered in or selected your criteria, click the **Search** button.

Finally, select any session found and click **Open Selected Session** to raise the [Session Explorer Window](#).

# Shadow Settings Dialog



Remote Desktop Commander has several nice features that help facilitate an easier session shadowing process for administrators.

Shadowing support and features have changed via several subsequent Windows Server OS releases. For instance, shadowing support was dropped from Windows Server 2012, but added back to Windows Server 2012 R2.

Also, Group Policy options around shadowing and Remote Desktop Services have expanded and evolved with each new OS release.

Remote Desktop Commander attempts to take all of these items into consideration, allowing the administrator to both temporarily override certain GPO settings, as well as deploy a "shadowing helper" applet, RDSshadowX.exe, to the remote Terminal Server, prior to starting the shadowing process.

Here is a discussion of how the shadowing process works in Remote Desktop Commander:

## **If attempting to shadow a session running on a remote terminal server (e.g. on a server other than the system running Remote Desktop Commander):**

Remote Desktop Commander will attempt to remotely deploy the RDSshadowX applet to the remote Terminal Server, locating it in the C:\RDPSOFT folder on the remote system. It also will attempt to allow for the automatic running of initial programs at session initialization by setting the GPO policy allowing the running of unpublished applications. If this policy is already explicitly set to disallow running unpublished applications, it will be temporarily changed via the registry each time a shadowing attempt is initiated. Finally, it will establish a new client session on the target Terminal Server. Log on with your credentials, at which point the RDSshadowX application will launch, and attempt to start shadowing the session you originally targeted.

**Important Note 1:** The following above actions (e.g. the initial deploying of the RDSshadowX applet and the adjustment to GPO policies via Remote Registry access) requires both Administrator rights and appropriate Firewall Exceptions (e.g. Remote Service Management, File and Print Sharing, and Remote Administration) to work correctly. If you will have non-Administrators performing shadowing actions (e.g. Help Desk Members) in Remote Desktop Commander, then you need to a.) manually deploy the RDSshadowX.exe applet (located in the C:\Program Files (x86)\RDPSOFT\Remote Desktop Commander directory) to the C:\RDPSOFT directory on each Terminal Server, and b.) set your GPO policy so that either unpublished applications can be automatically started at session initialization OR explicitly publish the RDSshadowX app as a recognized published application to your Help Desk group members.

**Important Note 2:** Shadowing will only work properly if the target machine is running the full Remote Desktop Services / Terminal Services role. If the target terminal server is running in Remote Administration mode only, shadowing will not work.

**Important Note 3:** Shadowing will not work on Windows Server 2012 systems. Only Windows Server 2012 R2 edition supports shadowing. This is a fundamental limitation of the operating system.

## **If attempting to shadow a session running on the local terminal server (e.g. if Remote Desktop Commander is installed locally on a terminal server):**

Remote Desktop Commander will start the shadowing process immediately, with no additional work required.

**Configurable Shadow Settings:**

***Set policy (or temporarily override GPO) to allow non-published apps to run at startup, so that the RDPSoft ShadowX applet can run correctly*** - If checked, this option tweaks the registry on the remote machine so that programs can launch during session startup. If you do not have an existing GPO setting that permits the launch of the RDShadowX app, this setting is required.

***Set policy (or temporarily override GPO) to allow view and/or control of shadowed sessions \*without\* initial user consent*** - When checked, current GPO / per machine policies will be overridden so that sessions can be viewed and/or controlled without user notification and consent. This setting will remain in place unless the next GPO refresh interval resets it.

***View Only / View & Control*** - The option selected here determines whether or not you will have the ability to take control of the remote session during shadowing. **Note:** The ability to only view a session is a Windows 2012 R2 / Windows 8.1 feature only.

# RDPSoft Remote Desktop Reporter - An Introduction



Remote Desktop Reporter is a member component of the Remote Desktop Commander Suite. It performs the following functions:

- 1.) Polls and collects information about Terminal Services / Remote Desktop Service sessions from one or more computers on your network. The sessions tracked can be pure RDS/TS sessions established over RDP with Microsoft clients, Citrix XenApp sessions established over ICA, or VMWare Horizon View sessions established over PCoIP.
- 2.) With the use of an optionally deployable agent, polls and collects advanced information about session activity on physical workstations and virtual desktop environments, such as Citrix XenDesktop. In addition, this agent can be deployed on server-based computing (SBC) environments like TS/RDS, Citrix XenApp, and VMWare Horizon View servers in order to obtain detailed performance information about CPU and memory utilization per session, inbound/outbound TCP/UDP connections made in each session, and even session screen captures.
- 3.) Provides a reporting engine so that you can produce ad-hoc and scheduled reports covering a wide variety of user and server activity.

## Primary Application Components

Remote Desktop Reporter is built upon five key components:

**The Remote Desktop Reporter Admin Client** allows you to control all aspects of the program's operation, including configuration settings, service settings, what computers to gather information from, and report generation/scheduling.

**The Remote Desktop Commander Client** allows you and other key personnel (e.g. management) to search over, explore and report on the data collected by the Remote Desktop Reporter service (and optional deployed agents).

**The Remote Desktop Reporter Service** is responsible for polling and storing remote desktop information, maintaining the underlying SQL database, and preparing scheduled reports

**The Remote Desktop Reporter Agent** is an optionally deployable set of two components (the Agent Service and In-Session Agent) that collects detailed session and performance information from RDS/TS, XenApp, and Horizon View systems, as well as from physical workstations and virtual desktops.

**The Microsoft SQL Server Express Database Instance** holds all of the collected polling information for the purposes of reporting. Optionally, you can instruct Remote Desktop Reporter to use a full version of Microsoft SQL Server for larger, more complex networks.

# Initial Setup and Configuration

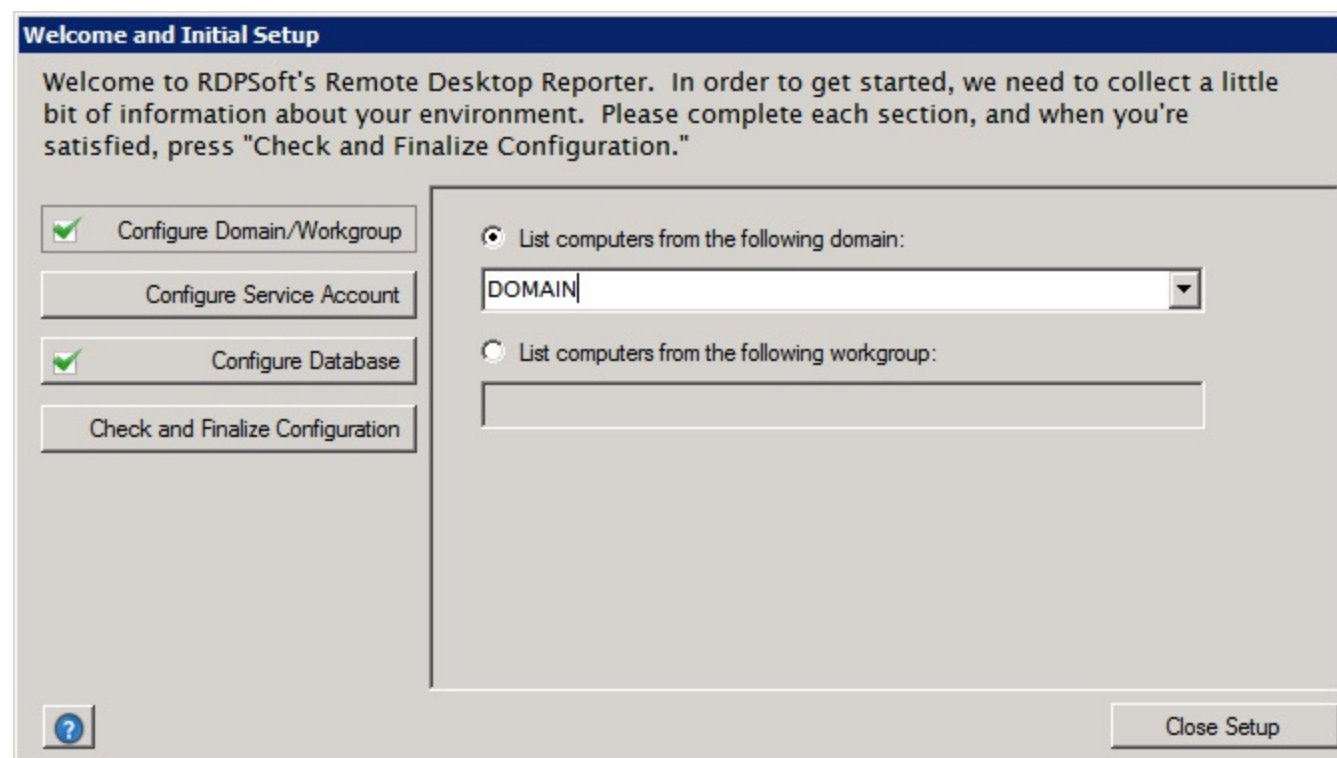
When you first run RDPSoft Remote Desktop Reporter, you will encounter the Welcome and Initial Setup Dialog. Its job is to collect the necessary information Remote Desktop Reporter needs in order to:

- 1.) Locate Remote Desktop / Terminal Services computers on your network
- 2.) Assign a service account to the Remote Desktop Reporter Service so it can poll the above computers for information
- 3.) Create a database either on the locally installed Microsoft SQL Server instance, OR create a database on a full version of Microsoft SQL Server located elsewhere on the network.

**\*\* IMPORTANT: You must be logged on with at least a local Administrator account when running the Remote Desktop Reporter software. If you plan to use a remote Microsoft SQL Server database, your interactive (logged on) account should also be an administrator on that system. Finally, the service account you choose must, at a minimum, also be an Administrator on the local machine. \*\***

Once you've completed all sections of the dialog, you can click the **Check and Finalize Configuration** button in order to configure the software to your preferences.

## Configure Domain/Workgroup Section



If the software is operating in a Microsoft Windows domain, select *"List computers from the following domain"* and select your domain from the list. If it is not present in the list, type it in using a traditional flat domain style (e.g. type DOMAIN rather than domain.com)

If the software is operating in a Microsoft Windows workgroup, select *"List computers from the following workgroup"* and type in your workgroup name.

## Configure Service Account Section

Welcome and Initial Setup

Welcome to RDPSoft's Remote Desktop Reporter. In order to get started, we need to collect a little bit of information about your environment. Please complete each section, and when you're satisfied, press "Check and Finalize Configuration."

✓

Configure Domain/Workgroup

Configure Service Account

✓

Configure Database

Check and Finalize Configuration

Username:

DOMAIN\Admin

Password:

\*\*\*\*\*

Confirm Password:

\*\*\*\*\*

If operating in a workgroup, choose a common Administrator account present on all workgroup members (e.g has the same username/password)

If operating in a domain, choose a Domain Admin account, OR 1.) a Domain User account, that 2.) is a local Administrator on this local machine, and 3.) is a member of the Remote Desktop Users group on all systems that it will report against.

?

Close Setup

Enter in the username and password you want the Remote Desktop Reporter service to run under. The service account name should be in either a *DOMAIN\Account* format if a domain account, or *COMPUTER\Account* format if a workgroup account.

**Note: Under all circumstances, this service account MUST be, at minimum, an Administrator on the local machine!**

Note 2: If operating in a domain, choose a Domain Admin account, OR 1.) a Domain User account, that 2.) is a local Administrator on this local machine, and 3.) is a member of the Administrators group on all systems that it will poll for RDP session information.

Note 3: If operating in a workgroup, choose a common Administrator account present on all workgroup members (e.g has the same username/password).

Configure Database Section

Welcome and Initial Setup

Welcome to RDPSoft's Remote Desktop Reporter. In order to get started, we need to collect a little bit of information about your environment. Please complete each section, and when you're satisfied, press "Check and Finalize Configuration."

✓

Configure Domain/Workgroup

Configure Service Account

✓

Configure Database

Check and Finalize Configuration

☒ Use the existing Remote Desktop Reporter database on the local SQL Server instance

☐ Create a new DB on the locally installed Microsoft SQL Server Express Instance

☐ Create a new DB on another Microsoft SQL Server (e.g. remote server)

☐ Use an existing Remote Desktop Reporter database on another Microsoft SQL Server

Data Files Directory

...

Server Name

Data Files Directory

...

DB Size in GBs

Server Name

?

Close Setup



Remote Desktop Reporter provides you with several options on how to store the polling data collected by the Remote Desktop Reporter Service. By default, this data is stored in a local instance of Microsoft SQL Server Express. For most small to midsized networks, this type and size of database storage should suffice. However, in larger networks, you may wish to have the data stored on a remote, dedicated version of Microsoft SQL Server that supports database sizes in excess of 10GBs. Similarly, if you choose to deploy the optional Remote Desktop Reporter agent components on systems in your network and you need data retention more than a few days, consider using a full version of Microsoft SQL Server. Later, if you want to see how much free space you have in your database at any time, simply select the Database Tab under the [Application Settings](#) area.

Once you've selected either a local instance or remote database, Remote Desktop Reporter will automatically create the database files, tables, indexes, and stored procedures necessary during the Initial Setup. Below is an explanation of the options available for additional configuration:

### **Use the existing Remote Desktop Reporter database on the local SQL Server instance**

If the Initial Setup program detects that there is already an existing Remote Desktop Reporter database defined on the local SQL instance, you can choose this option to use it.

### **Create a new DB on the locally installed Microsoft SQL Server Express Instance**

For most new setups, this will be the preferred option. The Initial Setup program will attempt to determine the default drive and directory to house the SQL MDF and LDF database/transaction log files. You can, however, change the Data Files Directory to another location on a different drive if you wish.

**Note:** The data files directory **MUST** have 11 gigabytes of space free to house both its database and transaction log files.

### **Create a new DB on another Microsoft SQL Server (e.g. remote server)**

Select this option if you want to create and house the database on a dedicated remote Microsoft SQL Server.

**Server Name** - Enter the name or IP address of the server running Microsoft SQL Server

**Data Files Directory** - Enter the path where you wish the database and transaction log files to be stored on the remote system.

**DB Size in GBs** - Enter the size in GBs (e.g. 10) you want the database to be on disk.

**Note 1:** Choosing a database size larger than 10 GBs is fine; however, it may take a while for the database server to create the MDF / LDF files on disk. So before selecting "Check and Finalize Configuration," understand that this operation could last anywhere from a few minutes to an hour or more.

**Note 2:** Currently, only Windows Integrated Security is supported for SQL Server Authentication. So make sure your current interactive account holds admin rights on both the local machine, and the remote machine where Microsoft SQL Server is running, or your operation may fail. Also, make sure that the service account you select has the ability to read data, write data, and execute stored procedures on the remote database server.

### **Use an existing Remote Desktop Reporter database on another Microsoft SQL Server**

If there is an existing Remote Desktop Reporter database defined on a SQL Server in your network (e.g. one that you've been using prior to an upgrade, or a database that was migrated to a new SQL Server), you can choose this option to use it.

**Server Name** - Enter the name or IP address of the server running Microsoft SQL Server.

**Note:** Currently, only Windows Integrated Security is supported for SQL Server Authentication. So make sure your current interactive account holds admin rights on both the local machine, and the remote machine where Microsoft SQL Server is running, or your operation may fail. Also, make sure that the service account you select has the ability to read data, write data, and execute stored procedures on the remote database server.

### **Check and Finalize Configuration**

Once you press this button, Remote Desktop Reporter's initial setup will first validate all of your selections, and then attempt to perform the various configuration actions in sequence. If there are validation errors or other problems, you will have the opportunity to go back to the relevant section and fix them before you try this option again. If all configuration actions are successful, the Initial Setup dialog will close automatically, and you will be taken into the primary user interface.



# Configuring Application Settings



## Polling Tab

Enter the number of seconds between polls of information on monitored servers and workstations. The recommended minimum polling interval is 60 seconds (1 minute), and the recommended maximum polling interval is 600 seconds (10 minutes).

**Note** - the shorter the polling interval, the greater the amount of database storage consumed over a given amount of time, but the reporting results will be more precise.

## Reporting Tab

Here you will enter the details that govern where and how reports are generated.

Select a directory where you want scheduled reports to be stored. You can specify a local path or a UNC path if you wish to store the reports on a file or web server.

**NOTE:** Mapped network drives are not available to our service account, so to store reports on a remote server, please specify a UNC path (e.g. \\SERVERNAME\ShareName)

If you would like to replace the default image displayed in the report header of each report, you can specify a local path to an image file on disk (e.g. c:\myimage.jpg), OR you can enter a path to an image file on a webserver (e.g. http://www.mydomain.com/myimage.jpg)

Finally, select the format(s) in which you would like your scheduled reports to be generated. Available formats include PDF, Microsoft Word, and Microsoft Excel.

If you would like to have your scheduled reports emailed to one or more recipients after they are produced, enable that option. If enabled, you must provide the following information about how to relay mail:

**SMTP Server:** Enter the IP address or fully qualified domain name of the email server that will relay your mail. Verify that this server will allow relay from the IP address of the computer running Remote Desktop Reporter.

**Port:** By default, this port is 25. However, you can assign a different port if required by your mail server.

**Sender Address:** Enter a valid email address that is allowed to relay email through your SMTP Server (e.g. myname@mydomain.com)

**Recipient Addresses:** Enter one or more email address(es) of the parties who will receive the scheduled reports after they are generated. If sending to more than one address, separate each address with a comma (,).

**Authenticate with mail server when sending mail:** If you check this option, the Remote Desktop Reporter Service will attempt to pass username and password credentials before sending email. To protect this authentication exchange, you should also turn on the *Use SSL Encryption* option.

**Use SSL Encryption:** If enabled, this will make the Remote Desktop Reporter service use SSL when exchanging message details with the mail server. As a result, this will protect both the contents of the message being sent, as well as the authentication sequence when a username and/or password is exchanged.

**NOTE:** The Remote Desktop Reporter Service uses "Explicit SSL" when communicating securely with specified mail servers. This means that if you select "Use SSL Encryption," you **MUST** use port 25 above. Encryption is then negotiated over port 25 before message data is exchanged securely.

**Username:** If you have selected the *Authenticate with mail server* option, supply the username to be used for authentication with the mail server. Sometimes this will be in a simple "username" style format; in other cases, you may need to supply a complete email address (e.g. myusername@mymaildomain1234.com). If uncertain, check with your mail administrator.

**Password:** Likewise, if you have enabled mail server authentication, enter the password that corresponds to the username you have supplied.

## Monitoring Tab

The Remote Desktop Reporter Service can also keep tabs on the availability of your Terminal Servers and whether or not they are still responding to incoming client connections. This monitoring and alerting is done at two different levels, for maximum protection:

1.) If the server cannot be contacted via its management interfaces (e.g. the Remote Desktop Reporter Service cannot successfully poll for session information after previously doing so), an alert will be dispatched via email to one or more administrators.

2.) If the server **\*can\*** be contacted via its management interfaces, but cannot be contacted over the TCP port used for incoming client connections (e.g. Port 3389), an alert similarly will be dispatched via email to one or more administrators.

**Send alerts when a TCP connection cannot be made on port XXX** - Check this option to enable management and port monitoring on your Terminal Servers. By default, Microsoft Terminal Services uses port 3389, and Citrix Metaframe/XenApp server utilizes 1494.

**Alert Recipient Email Addresses:** Enter one or more email address(es) of the parties who will receive the alerts when they are generated. If sending to more than one address, separate each address with a comma (,).

## Database Tab

In order to keep your Microsoft SQL Server Express database instance from filling up, enter a daily time when database maintenance will be performed. During database maintenance, records older than a certain number of days from the current date (that you specify) will be purged. You will notice two different sets of **lookback days** when setting the database grooming options.

**Purge Session Data Older Than X Days** - Enter in the aging threshold in days Remote Desktop Reporter will use when determining which database data is old enough to remove. **Session Data** as specified here is the basic level of data Remote Desktop Reporter collects regarding session activity, idle/active time, and process usage.

**Purge Agent Data Older Than X Days** - Similar to the aging threshold above, **Agent Data** as specified here is the advanced level of data collected by the optionally-deployable Remote Desktop Reporter Agent components, such as CPU utilization, memory utilization, TCP/UDP connection information, and session screen captures. Note that the setting here will also remove any older session screen capture images from disk as referenced in the database.

**Note** - The storage requirements for agent data are much more intensive than the standard session data above. In even medium sized networks, this data can exceed a gigabyte per day. Therefore, the default agent data purging interval is only 7 days. If you would like a larger retention interval for this data, please consider having Remote Desktop Reporter utilize a full version of Microsoft SQL Server that supports database sizes in excess of 10 gigabytes.

In this area, you can also verify the total amount of space allocated for your database, as well as the current free space available. Click **Refresh** to update the amount of free space available in your database.

Finally, should you wish to choose a new database server to store your Remote Desktop polling data, you can click the **Change Database Server** button, and confirm that you want to change database servers. The next time you start the Remote Desktop Reporter, you will be taken back into the Initial Setup Wizard, where you can specify a different database server

**Note** - Changing to a different database server does not migrate your existing database - it only allows you to create a new database on a separate, dedicated Microsoft SQL Server. Migrating existing databases is beyond the scope of support for the solution. Please contact a professional DBA should you wish to migrate your database.

# Domain/Workgroup Tab

Here you control how Remote Desktop Reporter builds lists of computers for the [Add/Manage Servers](#) and [Add/Manage Workstations](#) sections of the program. Indicate whether you are running a Windows workgroup or domain environment, and the name of said domain/workgroup. If you are running a large domain, you can further limit your computers to only one or more Organizational Units in that domain.

The **Refresh OUs** button will requery your Active Directory server in order to rebuild the tree of OUs and containers within your root domain. Pressing the **Save Changes** will commit any changes you've made to your Application Settings and also restart the Remote Desktop Reporter Service. Selecting **Revert** will revert your settings back to the way they were before you started making changes.

# Licensing Tab

By default, all evaluation copies of Remote Desktop Report ship with a fully functional, 30-day evaluation license file. Once you purchase the software, RDPSoft will provide you with a non-expiring, perpetual license file for the quantity of servers/workstations you bought. This license will remain valid for the current major version of the software. Shoud you wish to upgrade to a new major version of the software, and you currently own an active maintenance plan, you will need to request a new license file during the upgrade process from RDPSoft Customer Service.

Clicking the **Install/Update Licensing** button launches the RDPSoft Remote Desktop Reporter licensing tool. In order to install a new license, you will need to supply the following pieces of information to this tool:

- 1.) The location of the license file provided to you by RDPSoft.
- 2.) The primary email address associated with your customer account.
- 3.) The Customer Service Number provided to you by RDPSoft.

If all of the above information is valid, your new license will be installed, which you can verify next time you start the Remote Desktop Reporter.

# Client and Agent Settings Tab

In this Settings area, you can change the default directory where recently processed screen capture images are stored, and also can control who (besides Administrators) can access the Remote Desktop Reporter database using the Remote Desktop Commander Client operating in Fully Integrated Mode.

**Choose a directory where recorded session images will be stored** - By default, this is the *ImageRepository* subdirectory located under the Remote Desktop Reporter installation directory. If you select any local directory, a special hidden share called RDPSS\$ will automatically be created to allow the Remote Desktop Commander tool to access these images remotely. When you change the local path, the effective access rights of this share and folder contents are always adjusted so that:

- Local Administrators have Full Control
- The Local System Account (e.g. operating system) has Full Control
- Any other users that have been assigned access to the database will have Read rights (see below)

You can also specify the UNC path to a share on a different file server to store your images. When you do this, Remote Desktop Reporter will attempt to adjust the underlying NTFS permissions of the shared folder to match those listed above. However, you will need to make sure that the share you select has appropriate permissions set as well (e.g. all Authenticated Users) so that it is not more restrictive than the underlying NTFS permissions.

**Grant or remove access to the database and session image repository** - Here you can both grant and revoke access to the Remote Desktop Reporter database and session images for specific user accounts. When you add a new user, that user is granted read access to the database and the session image repository. When you remove a user, that user's database login is revoked and the user is also removed from the NTFS access control list for the session image folder.

# Configuring Service Settings



## Service Settings

In this area of the program, you can configure the account the Remote Desktop Reporter service runs under, as well as stop and restart the service as needed. In order to reduce the potential for permissions conflicts for the service as it attempts to poll information over the network, it is recommended that you choose an account in the Administrators group on the machine where it is installed, as well as in the Administrator group on each remote system that it monitors. However, if your network policies enforce a Principle of Least Privilege, you should make sure that the service is in the local Administrators group on the machine where it is installed, and that it is a simply a member of the Remote Desktop Users group on all systems that it monitors.

**NOTE:** Restricting the Remote Desktop Reporter Service to a non-Administrator account may adversely effect the different types of information it can collect from monitored servers/workstations, which may also reduce the number of reports that will contain information for said systems. Therefore, making sure that the Remote Desktop Reporter Service has full Administrator rights on the machines it collects data from is recommended.

# Configuring Computers for Monitoring



Add/Manage Servers



Add/Manage Workstations

Remote Desktop Reporter can monitor both servers and workstations on your network. You can add one or more computers from a list of devices detected on your network, or you can enter them manually by typing in their hostname or IP address. Below is a summary of the commands available to you when configuring the computers you wish to poll.



**Remove Computer(s) From Database** - Deletes one or more selected monitored from the polling database. They will no longer be polled for information.



**Refresh Monitored Computers** - Requeries the polling database and updates information about all monitored computers, such as the date/time last polled, and whether or not they are in maintenance mode. If selected for *Available Computers*, refreshes the list of servers/workstations from the network/Active Directory.



**Toggle Computer In/Out of Maintenance Mode** - Places the selected computer in/out of maintenance mode. Maintenance mode temporarily prevents a computer from being polled.



**Add Selected Computers for Monitoring** - Places the selected (or manually entered) computers into the polling database for monitoring.

## Advanced Monitoring and Monitoring of non-RDS Systems (e.g. Physical Workstations, Virtual Desktops)

If you elect to [deploy the optional Remote Desktop Reporter Agent components](#), Remote Desktop Reporter can expand both the level of detail it monitors from remote systems, as well as expand the types of devices it can monitor. Here are some of the expanded capabilities possible when using the Remote Desktop Reporter Agent.

- Non-RDS session activity on physical workstations and virtual desktops (e.g. Citrix XenDesktop or equivalent) can be monitored. This includes idle and active time of the console session.
- Detailed CPU utilization metrics, both by session and by process, on physical workstations, virtual desktops, and RDS servers (e.g. MS TS/RDS, Citrix XenApp, VMWare Horizon View)
- Detailed Memory utilization metrics, both by session and by process, on physical workstations, virtual desktops, and RDS servers (e.g. MS TS/RDS, Citrix XenApp, VMWare Horizon View)
- Detailed TCP/UDP inbound/outbound connection information, both by session and by process, on physical workstations, virtual desktops, and RDS servers (e.g. MS TS/RDS, Citrix XenApp, VMWare Horizon View)
- Session screen captures, on physical workstations, virtual desktops, and RDS servers (e.g. MS TS/RDS, Citrix XenApp, VMWare Horizon View)

[Click here for more information on how to deploy the Remote Desktop Reporter agent in your environment.](#)

# Deploying the Remote Desktop Reporter Agent Components for Advanced Analysis

## 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.***

## 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 reporting metrics from the Remote Desktop Reporter In-Session Agent Processes loaded in one or more user sessions running on a Windows server/workstation, and then is queried remotely by the main Remote Desktop Reporter Service located on the computer where the full Remote Desktop Reporter program was installed.
- \* The In-Session Agent Process is responsible for collecting session-specific metrics about user sessions running on a Windows system. This can include the console session on Windows workstations/VDIs or remote desktop sessions on Windows Servers. 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.

## 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.

### 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 In-Session Agent. 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 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), 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

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

### **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.

**Note:** On busy RDS and Citrix servers with hundreds or thousands of open connections, this monitoring level can be 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.

#### ***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 very 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**

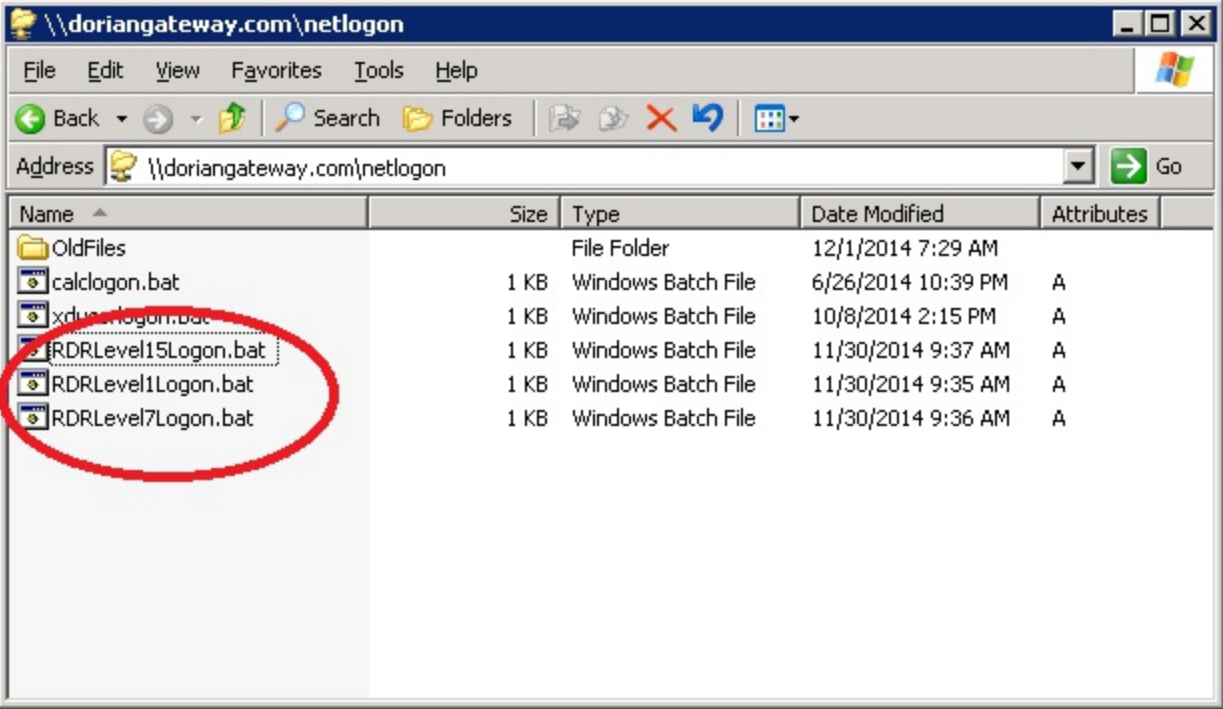
To invoke the In-Session Agent with a logon script, you will need to take the following actions in order:

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.

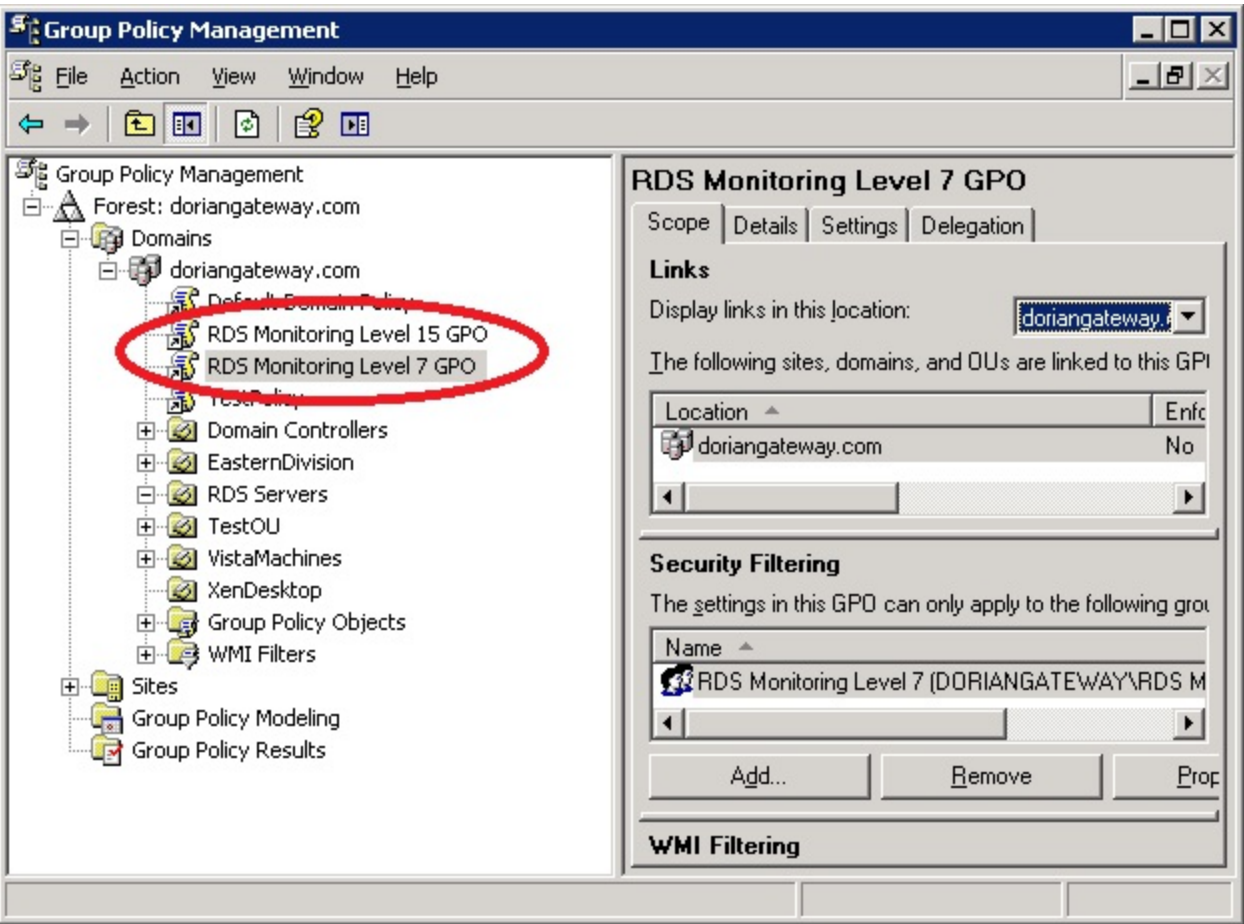


2.) Place the corresponding users into the Global Groups you created in Step 1 above.

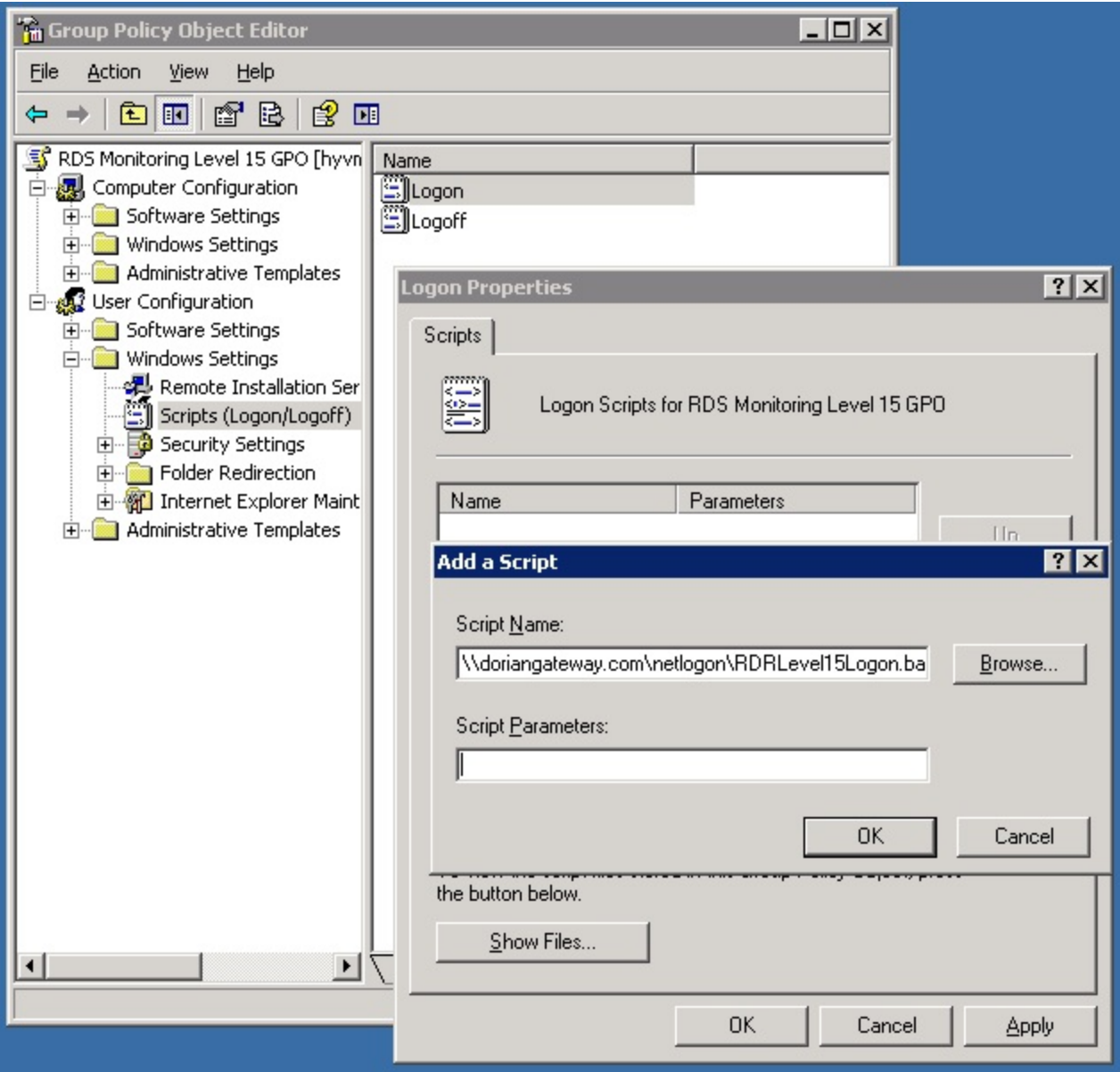
3.) Determine which monitoring levels you want Remote Desktop Reporter to use. (e.g. Level 1, Level 3, Level 7, or Level 15). Place the corresponding logon scripts (e.g. RDRLevel1Logon.bat, RDRLevel3Logon.bat, RDRLevel7Logon.bat, and RDRLevel15Logon.bat) into a globally-accessible location (e.g. \domain.com\netlogon , or \\domain.com\SysVol\doriangateway.com\Policies\{GUID OF GPO}\User\Scripts\Logon)



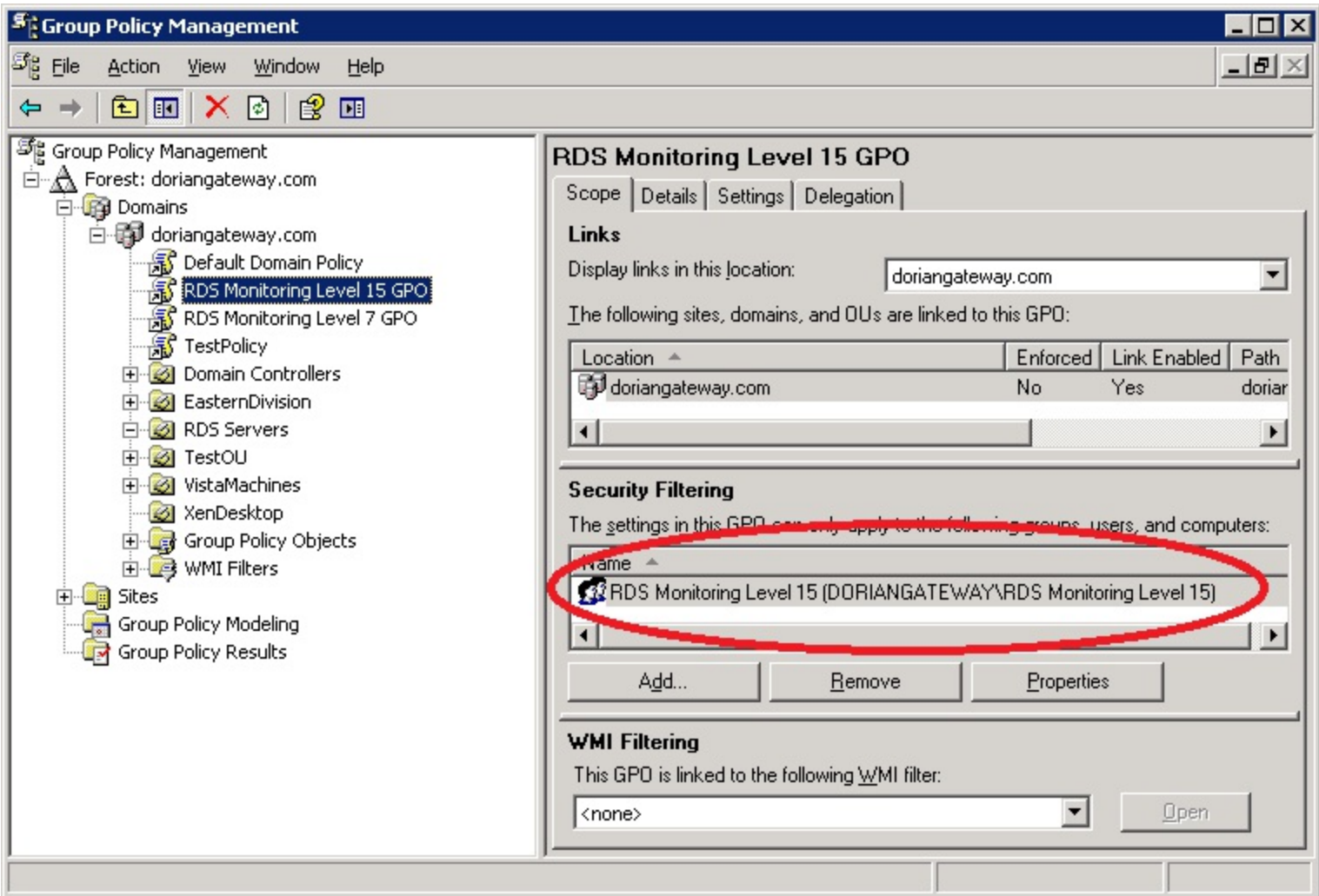
4.) Using the Group Policy Management Console, create one GPO per Monitoring Level. Place each GPO at either the top level of the domain forest, or at the top level OU/Container that houses the corresponding users. If you do not already have the Group Policy Management Console installed, download it 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.

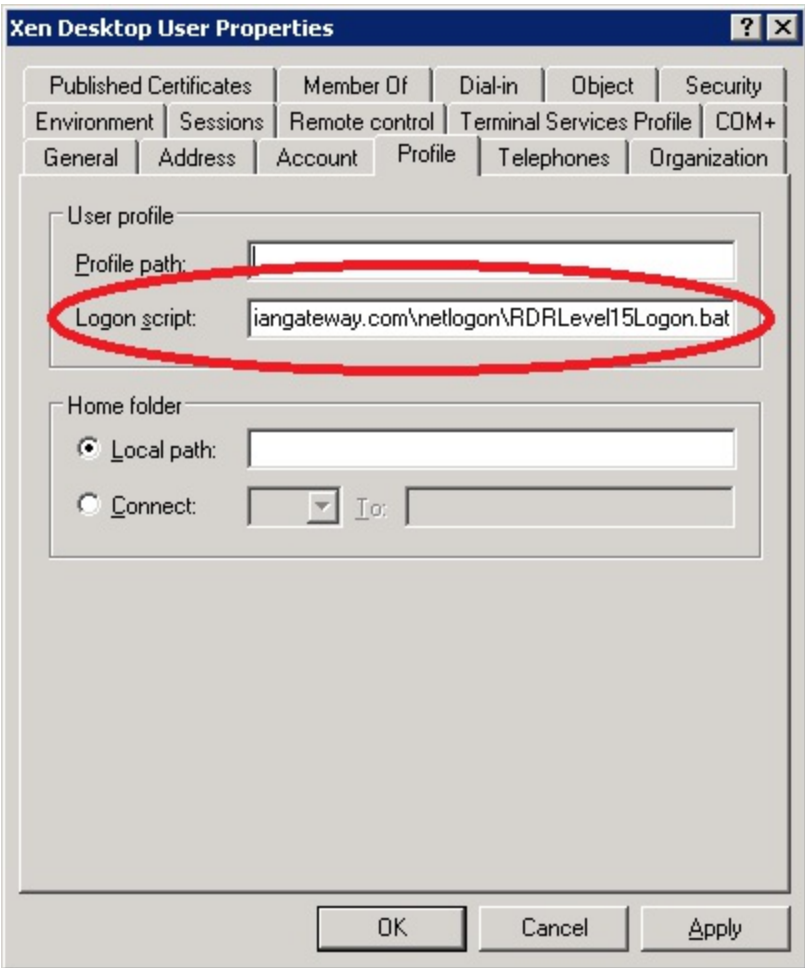


7.) Now, when a user logs on to any physical desktop, virtual desktop, or server-based computing system (e.g. RDS/XenApp/Horizon View), the RDPRDRAgent.exe In-Session Agent process will be launched with the appropriate monitoring level, and will begin transmitting information to the Remote Desktop Reporter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



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 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 Remote Desktop Commander from their workstations.

# Running, Scheduling, and Filtering Reports



## Reports and Filters

Remote Desktop Reporter allows you to produce both immediate, ad-hoc reports, as well as scheduled reports that run later. You can attach filters to both ad-hoc and scheduled reports to reduce the volume of data from the database returned to the report.

## Running Ad-Hoc Reports

To run an ad-hoc report, select a report name from the top-most listing. You can filter the reports displayed in the top-most listing by selecting a report category from the dropdown menu. Selecting "All Reports" will display all available reports in the current version of Remote Desktop Reporter, and is the default selection.

Click the **Run Report** button. The [Report Filter Selection Dialog](#) will open, allowing you to apply a quick date filter or more specialized filter to your report. If you haven't yet defined a specialized filter, you can do so in this dialog, and then apply it to the report and see the results in the Report Viewer Dialog. Alternatively, you can click the **Apply Filter** button, which will immediately raise the [Report Filter Dialog](#) and let you select or build a custom filter. Once that's done and you've applied the filter to the report, you can click **Run Report** and your filter will be preloaded in the Report Filter Selection Dialog. Should you wish to remove a filter altogether, or remove a filter before applying another one, click the **Remove Filter** button.

## Scheduling Reports

To schedule a report, select a report name from the top-most listing, then press the **Schedule This Report** button. The [Report Scheduler Dialog](#) will be displayed. Once you have selected an optional filter, the time, and the frequency you want the report to be created, press **Save** to schedule the report. Your new scheduled report will be displayed in the bottom most listing. Should you wish to change scheduling parameters later, select the report you wish to change, and click the **Update Scheduled Report** button. The [Report Scheduler Dialog](#) will reappear, allowing you to change scheduling properties. To remove a scheduled report, select the report you wish to remove, and click the **Remove Scheduled Report** button. Click the **Review Produced Reports** button to launch a Windows Explorer window displaying the contents of your Scheduled Reports folder.

# Sorting Report Data Interactively

Most all reports produced by Remote Desktop Reporter have the ability to be sorted interactively when the user creates them on demand. When a user clicks "Run Report," the Report Viewer Dialog is raised, and after the report data is obtained from the database, the report is then displayed on screen.

At the top of each report, you will see small up/down arrows in many of the columns in the report. If a column has an up/down arrow, that means it is sortable. Here's an example - you'll notice how the up/down arrows are highlighted with red circles...

Terminal Server		Day Of Activity		User Count	Username	
-----------------	---	-----------------	---	------------	----------	---

Clicking the up/down arrow will toggle the sort of items in that particular column and/or grouping between an ascending sort or a descending sort.

Once you have finalized your sort preferences, you can either print out the report, or save it as a file (e.g. in PDF, Microsoft Word, or Microsoft Excel format), and the sorting will remain the way you configured it in the printed output or file.



# Report Scheduler Dialog

Report Scheduling Options

Report Name:

Client Data – Client Utilization By Server

Applied Filter:

{NONE}

Run Report at:

11:11 PM

Daily

☐

Override default email recipients and send to:

?

Save

Cancel

The Report Scheduler Dialog allows you to specify how often a report gets generated automatically by the Remote Desktop Reporter Service. You use it when scheduling new reports and adjusting scheduling properties for previously scheduled reports.

**Applied Filter** - Select the filter you want to be applied to the report in question when it is generated by the service.

**Run Report At** - Select both the time that you want the report to run, as well as its frequency. Frequency options include daily, weekly, or monthly on specific days.

**Override default email recipients** - Normally, reports are sent to the email recipients you specify globally in the [Application Settings](#) area of the application. However, you can override those email recipients and send a scheduled report to a different group of email recipients once the report is finished. To do so, check this area and then supply one or more email addresses as needed. If sending to more than one address, separate each address with a comma (,).



# Report Filter Dialog

Select / Build Report Filters

Stored Filters

Test

Apply Filter

Create Filter

Edit Filter

Remove Filter

Define Filters

Computer Name:

Build...

Username:

Build...

Undefined:

Build...

Undefined:

Build...

Undefined:

Build...

Undefined:

Build...

Undefined:

Build...

Limit by Time Range:

☐ All Matching Events

☐ Last 24 Hours

☒ Last  Days

Filter Name:

Save Filter

Cancel/Revert

Close

Use the Report Filter Dialog to:

- 1.) Apply filters to ad-hoc or scheduled reports
- 2.) Design new filters
- 3.) Edit existing filters
- 4.) Remove filters from the filter database

The **Stored Filters** list houses all of the filters defined and stored in the filter database. To apply a filter to an ad-hoc or scheduled report, press the **Apply Filter** button. The dialog will then close and your filter will be attached to the report in question. Later, when you click **"Run Report"** to build a report manually and the [Report Filter Selection Dialog](#) is loaded, the applied filter will be preselected for you. Click the **Remove Filter** button to remove the currently selected filter from the filter database.

Similarly, click the **Create Filter** or **Edit Filter** buttons if you want to create a new filter or change the criteria of an existing filter. Pressing either button places the Report Filter Dialog into Filter Design Mode.

## Filter Design Mode

In Filter Design Mode, you can specify one or more conditions to filter results by for each of the fields that are relevant to report you are targeting. Only the fields that are relevant to the report you are targeting will be enabled. To build a set of conditions for filtering a particular field, press the **Build...** button. This will place the Report Filter Dialog into Condition Builder Mode (see below). Once you return from Condition Builder Mode, you will see the raw T-SQL conditions displayed. [Click here for an advanced discussion of how to build filter conditions using T-SQL.](#)

**Note 1:** You can edit the raw T-SQL directly in the text field should you wish. However, you must follow appropriate T-SQL syntax rules, and bound the condition(s) in starting and closing parentheses, or the filter may not function properly.

**Note 2:** If you do not want to filter a particular field present in a report, simply leave the condition list blank for that field.

**Limit by Time Range** - Arguably, this is the most important filter criteria you should consider using in your reports. If you do not need to limit the data returned to the report based on the time when it was polled, select *All Matching Events*. If you do need to limit the data returned to the report based on when it was polled, select the *Last 24 Hours* or *Last X Days* option.

**Also Restrict By Time of Day** - Selecting this option allows you to filter out polled information that occurred outside a given time of day window. For instance, you may want to restrict data that happened during your normal work day, so you would *Only Return Activity Between Hour 9 and Hour 17* (e.g. a typical 9 to 5 workday). You could also restrict your returned data to only that activity that happened outside normal business hours, e.g. from *Hour 18 to Hour 8*.

**Filter Name** - Enter a name for the filter you are creating or editing. This name will also be displayed on produced ad-hoc or scheduled reports when they are created.

**Save Filter** - Adds a newly created filter to the database, or updates the conditions of an existing filter in the database.

**Cancel/Revert** - Takes the Report Filter Dialog back out of Filter Design Mode without making changes to the filter database.

## Filter Build Mode

Select / Build Report Filters

Stored Filters

Test

Apply Filter

Create Filter

Edit Filter

Remove Filter

Select Values to Filter On:

Computer Name	Computer Type
<input type="checkbox"/> 10.32.0.231	Workstation
<input type="checkbox"/> 10.32.0.99	Workstation
<input type="checkbox"/> 123ADD	Server
<input type="checkbox"/> KL-FR10	Server
<input type="checkbox"/> FRANK	Workstation
<input type="checkbox"/> LG-NAS	Server
<input type="checkbox"/> RMILLER	Server
<input type="checkbox"/> SWATSON	Workstation
<input type="checkbox"/> TIM	Server
<input type="checkbox"/> Timmay	Server

☒ Return ONLY the checked items ☐ EXCLUDE the checked items

OK

Cancel

Close

In Filter Build Mode, you are presented with a list of distinct values currently present in the database for the target field in question. You then select one or more of these values by placing a check mark beside them, and then deciding whether you want to only return data that matches the select values, or conversely, do NOT match the selected values. Click **OK** to return back to Filter Design Mode with the appropriate T-SQL statements generated, or press **Cancel** to return to Filter Design Mode with no underlying T-SQL generated.

## Dynamic Domain Group Member Filtering

In more complex environments, such as those maintained by Managed Service Providers and SaaS Providers, you may need to dynamically filter reports based on membership in domain groups. When you turn on dynamic domain group filtering, Remote Desktop Reporter restricts the data returned to a report based on current domain group membership at run time. In other words, it builds a dynamic SQL query when executed that will only match (or alternatively, exclude) a select list of users. This is ideal if membership in groups change frequently - whenever the report is built manually or scheduled, the Active Directory server will always be consulted to get the most up-to-date list of users for a given group.

To enable dynamic group member filtering, first select the **Username** field to filter on when in **Filter Design Mode**. Then, click the **Build...** button to build a filter based on the Username field. When in **Filter Build Mode**, check the ***Dynamically return all members from domain group*** option, and the select (or type in) the name of the AD group whose member list will be obtained when the report is run. If you want the report to only return records where the user is a member of the group, select the ***Return ONLY the selected items*** option. Conversely, if you want the report to exclude all records where the user is a member of a specific domain group, select the ***Exclude the selected items*** option.

Once you select the appropriate group, click **OK** to return back to Filter Design Mode. You will now see that there is a descriptor in the Username field that is structured like so: USERNAMEIN:[DOMAIN\GROUP NAME] or USERNAMENOTIN:[DOMAIN\GROUP NAME] ... you can use this shorthand in the future (make sure you include the USERNAMEIN or USERNAMENOTIN designator, colon, and DOMAIN and GROUP NAME bounded in square brackets.)

# Report Filter Selection Dialog

**Select a Filter To Limit Report Data**

☐ Bring back all data that was polled within a certain date range

Select starting and ending poll times:

Start: 29 Mar 2014 11:47 AM End: 30 Mar 2014 11:47 AM

☐ Bring back all data that matches a defined filter, and override the relative date range in the filter with the range below

Select filter, starting, and ending poll times:

Filter: USER = SYSTEM Adjust/Create Filter(s)

Start: 29 Mar 2014 11:47 AM End: 30 Mar 2014 11:47 AM

☒ Bring back all data that matches a defined filter, using the relative date ranges (if any) defined in the filter

Select filter:

Filter: USER = SYSTEM Adjust/Create Filter(s)

☐ Return all data from the database (Warning - Report could take a long time to generate)

OK Cancel

The Report Filter Selection Dialog is raised each time you click the **"Run Report"** button to prepare a new manual report. Using the options in this dialog, you can:

- 1.) Prepare a report with a simple, quick date filter that limits the data in the report to an explicit date range.
- 2.) Prepare a report that combines an existing filter (or a filter that you just built) with an explicit date range (overriding any "relative date filtering" already present in the saved filter).
- 3.) Prepare a report that uses an existing filter as is, including any relative date filtering already present in the filter definition.
- 4.) Prepare a report with no filtering attached (e.g. return the entire database's contents).

## Notes:

When you define a filter in the [Report Filter Dialog](#), you can create what is known as a "relative date range." A relative date range simply returns data that is within a certain number of days from the current date. E.g. the prior day, prior 7 days, etc. When you use a relative date range, the ending date of the data returned is always 11:59:59PM of the immediately preceding day. Using the Report Filter Selection Dialog, you can **override** relative date filtering and only return data that was polled within an explicit starting date and explicit ending date.

If you choose to override a relative date range in a previously defined filter with an explicit date range, any **time of day** filtering defined in the filter (e.g. only return data from 8am to 17pm) will still be maintained and enforced properly.

If you have selected a filtering option that makes reference to an existing filter, you can click the **Adjust/Create Filter** button if you wish to edit the filter parameters prior to applying it to a report. Similarly, if you need to define a new filter for use with the report, click **Adjust/Create Filter**.

Clicking **OK** applies the filter and/or an explicit date range to your report, retrieves the filtered data from the database, and then displays your report. Clicking **Cancel** closes this dialog and returns to the main Remote Desktop Reporter user interface.

# Building Advanced Filter Conditions Using T-SQL

The RDPSoft Remote Desktop Reporter utilizes an instance of Microsoft SQL Server Express to store and report on Remote Desktop data from your network computers. The default query language of Microsoft SQL Server is T-SQL, therefore, all Remote Desktop Reporter filters utilize this query language.

By default, the Report Filter Dialog will build basic filter conditions for you graphically; in other words, you select one or more values you want to be included or excluded in your filter from a list, and it will construct the T-SQL. However, there may be times when you want to design more advanced Filter conditions to restrict the data in your reports. In those cases, you will need to edit the T-SQL conditions directly.

## Example 1

For example, let's say you are running a Program Tracking report, and only want to see the Remote Desktop users who have been running OUTLOOK.EXE or REGEDIT.EXE. You can start the Report Filter Dialog, select Create Filter, and then click "Build..." next to the Process Name field. From there, you can select "OUTLOOK.EXE" and "REGEDIT.EXE" from the list, and click OK.

Once you click OK, the Remote Desktop Reporter will build and return T-SQL to reflect that filtering condition on the ProcessName. In this example, it would look like this:

```
(ProcessName = N'OUTLOOK.EXE' OR ProcessName = N'REGEDIT.EXE')
```

Let's break down the above T-SQL in more depth.

(...) - Every T-SQL condition for a particular database field must be bounded by parentheses.

**ProcessName** - This is the field name we are filtering upon. Currently, filterable field names include **ComputerName**, **Domain**, **Username**, **ProcessName**, **ClientName**, **ClientAddress**, **ClientBuildNumber**, **ClientProtocolID**, and **WinstationName**. Not every field is valid in certain reports, and the Remote Desktop Reporter will automatically limit the "selectable fields" based on the report you are trying to filter.

= - In this condition, we are using the equals sign as our comparison operator. We could also use the <> comparison operator, which means \*not equal to\*.

**N** - Remote Desktop Reporter is a Unicode-aware and friendly application, so the N is automatically included in front of any string literals (in this case OUTLOOK.EXE or REGEDIT.EXE). If you are not using UNICODE characters, you can omit the N, but it doesn't hurt anything to leave it as part of the condition.

**OR** - In this example, we are using the OR logical operator to signal that we want to only return data where the ProcessName is either OUTLOOK.EXE or REGEDIT.EXE. If we had used AND as our logical operator, no data would have been returned from the filter, because no ProcessName field in the database is equal to both OUTLOOK.EXE \*and\* REGEDIT.EXE. Another useful logical operator is the LIKE operator. We'll discuss it more in depth in a moment.

**'OUTLOOK.EXE' / 'REGEDIT.EXE'** - These are the two string literals in our condition. Notice that each string literal is bounded in single quotes (apostrophes) - this is a requirement. Also, if your string contains embedded single quotes, you will need to escape them, like so: SALLY'S would become 'SALLY"S' - notice that we escaped the inner apostrophe by using two apostrophes instead of one.

## Example 2

```
(ProcessName <> N'OUTLOOK.EXE' AND ProcessName <> N'REGEDIT.EXE')
```

In this example, we have reversed the goal of the T-SQL condition in Example 1. Now, we want to return ALL data except for records where the ProcessName is either OUTLOOK.EXE or REGEDIT.EXE. To accomplish this, all we have changed is the comparison operator (using <> instead of =), and the logical operator (AND instead of OR).

## Example 3

(ComputerName LIKE N'ACC%')

Let's say, for example, that you only want to view Remote Desktop data from the Terminal Servers in your accounting department. Your domain computer naming convention prefixes each accounting department computer with "ACC." You can use the LIKE logical operator above to make Microsoft SQL Server return all of the records where the computer name starts with "ACC."

In general, LIKE is great at matching patterns of characters in a field. Here are some more rules/ways to use it, as excerpted from Microsoft's documentation on the LIKE operator (<http://msdn.microsoft.com/en-us/library/ms179859.aspx>):

% - Any string of zero or more characters.

Example: `WHERE title LIKE '%computer%'` finds all book titles with the word 'computer' anywhere in the book title.

\_ (underscore) - Any single character.

Example: `WHERE au_fname LIKE '_ean'` finds all four-letter first names that end with ean (Dean, Sean, and so on).

[ ] - Any single character within the specified range ([a-f]) or set ([abcdef]).

Example: `WHERE au_lname LIKE '[C-P]arsen'` finds author last names ending with arsen and starting with any single character between C and P, for example Carsen, Larsen, Karsen, and so on. In range searches, the characters included in the range may vary depending on the sorting rules of the collation.

[^] - Any single character not within the specified range ([^a-f]) or set ([^abcdef]).

Example: `WHERE au_lname LIKE 'de[^l]%'` all author last names starting with de and where the following letter is not l.

## Other Notes

When building a filter, next to each field, only construct the comparison condition, bounded by parentheses. **DO NOT add the WHERE keyword in front of any condition** - Remote Desktop Reporter will do that automatically for you. It will also connect multiple conditions across different fields together for you, if you define conditions for more than one field (e.g. you decide to filter on both ComputerName AND UserName, for instance).

If you have very advanced filtering needs, please contact RDPSoft Sales at <http://www.rdpsoft.com> to obtain a quote for Professional Services related to building special filters for use inside the Remote Desktop Reporter application.



# Licensing Remote Desktop Commander

To purchase licensing for Remote Desktop Commander, including the Lite and Suite editions, please visit <http://www.rdpsoft.com/buy>.

Once you have purchased Remote Desktop Commander, perform the following steps to request licensing and activate the software:

## For Remote Desktop Commander Lite:

- 1.) Open Remote Desktop Commander from the Start Menu.
- 2.) Select the **File Menu**, and click **Application Preferences and Licensing**.
- 3.) Make a note of your **Licensing Reference Number**, and then click [Visit RDPSoft Licensing Center Online](#).
- 4.) Once you have received your requested license file from RDPSoft, click **Install/Update License** to activate the software.

## For Remote Desktop Commander Suite:

- 1.) Open the Remote Desktop Reporter Admin Client from the Start Menu.
- 2.) Go to the **Application Settings** area, and click on the **Licensing Tab**.
- 3.) Visit the RDPSoft Licensing Center Online (<http://www.rdpsoft.com/licensing>) to request licensing.
- 4.) Once you have received your requested license file from RDPSoft, click **Install/Update License** to activate the software.

**Note:** If you have multiple administrators or end users that will connect to the Remote Desktop Reporter database for advanced analysis, connect each instance of the Remote Desktop Commander program to its database in the **Application Preferences and Licensing** area under the **File Menu**. Once connected to a valid RDPSoft database, Remote Desktop Commander will automatically obtain needed licensing information.

## RDPSoft License Agreement

**THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") FOR THE LIMITED LICENSE OF CERTAIN RDPSoft ("RDPSoft") SOFTWARE ("SOFTWARE") AND RELATED DOCUMENTATION IS A LEGAL AGREEMENT, WITH IMPORTANT LEGAL CONSEQUENCES, BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ("You" or "Licensee") AND RDPSoft. THIS AGREEMENT IS PRESENTED FOR REVIEW AND APPROVAL AS A MANDATORY STEP IN THE INSTALLATION AND USE OF THE SOFTWARE. DO NOT INSTALL OR USE THE SOFTWARE UNLESS YOU HAVE READ AND AGREE TO THE TERMS OF THIS AGREEMENT. BY CLICKING THE "I ACCEPT" OPTION BELOW, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, AND ACKNOWLEDGE THAT YOU HAVE THE NECESSARY AUTHORITY TO ENTER INTO THIS AGREEMENT AND ARE OVER 18 YEARS OF AGE. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, OR IF YOU ARE AN EMPLOYEE AND DO NOT HAVE THE NECESSARY AUTHORITY TO CONTRACTUALLY BIND YOUR EMPLOYER TO THIS AGREEMENT, OR ARE UNDER 18 YEARS OF AGE, YOU SHOULD CLICK THE "I DO NOT ACCEPT" OPTION AND/OR EXIT THIS INSTALLATION PROGRAM.**

This is a license agreement and not an agreement for sale. This license agreement gives Licensee certain limited rights to use the proprietary RDPSoft Software, and any Software updates and user guides, if any (hereinafter referred to as "Software and Related Materials"). All rights not specifically granted in this Agreement are reserved to RDPSoft.

Reservation of Ownership and Grant of License: RDPSoft and its third party licensor(s), if applicable, retain exclusive rights, title, and ownership of the copy of the Software and Related Materials licensed under this Agreement and, hereby, grant to Licensee a personal, nonexclusive, nontransferable license to use the Software and Related Materials based on the terms and conditions of this Agreement. From the date of receipt, Licensee agrees to use reasonable efforts to protect the Software and Related Materials from unauthorized use, reproduction, distribution, or publication.

Copyright: The Software and Related Materials are owned by RDPSoft and its licensor(s) and are protected by United States copyright laws and applicable international laws, treaties, and/or conventions.

## Permitted Uses:

Provided all applicable software license fees are paid:

Licensee may install and use a reasonable number of copies of the Software and Related Materials



solely for its internal use.

Licensee may also store or install a copy of the Software and Related Materials on a storage device, such as a network server, for use over an internal network.

Licensee may use the Software and Related Materials in an Intranet distributed computing network or environment provided any additional license fees are paid, and further provided that commercially reasonable security measures are employed to protect the Software and Related Materials from use or access beyond that allowed under this Agreement.

Licensee may make routine computer backups of the Software and Related Materials.

Licensee may use the online documentation for Licensee's own internal use.

Uses Not Permitted:

Licensee shall not copy, reproduce, display, remarket, resell, retransmit, rebroadcast, and/or redistribute copies of the Software in any hard-copy and/or digital format(s) and/or Related Materials except as expressly set forth in the Permitted Uses section above.

Licensee shall not sell; rent; lease; sublicense; lend; assign; time-share; act as a service bureau that allows third party access to the Software or Related Materials; or transfer, in whole or in part, access to prior or present versions of the Software and Related Materials, any updates, or Licensee's rights under this Agreement.

Licensee shall not reverse engineer, decompile, or disassemble the Software except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

Licensee shall not remove or obscure any RDPSOFT or, if applicable, any of RDPSOFT's licensor(s)'s copyright, trademark, or other proprietary rights notices.

Licensee shall not alter or modify the RDPSOFT Software or prepare any derivative works from RDPSOFT Software.

Term: The license granted by this Agreement shall commence upon Licensee's receipt of the Software and Related Materials and shall continue until such time that (1) Licensee elects to discontinue use of the Software and Related Materials and terminates this Agreement, or (2) RDPSOFT terminates for Licensee's material breach of this Agreement. Upon termination of this Agreement in either instance, Licensee shall return to RDPSOFT the Software and Related Materials, and any whole or partial copies, codes, modifications, and merged portions in any form. The parties hereby agree that all provisions that operate to protect the rights of RDPSOFT and its licensor(s) shall remain in force should a breach occur.

Limited Warranty and Disclaimer: RDPSOFT warrants that the media upon which the Software and Related Materials are provided will be free from defects in materials and workmanship under normal use and service for a period of sixty (60) days from the date of receipt ("Limited Warranty").

EXCEPT FOR THE ABOVE EXPRESS LIMITED WARRANTY, THE SOFTWARE AND RELATED MATERIALS CONTAINED HEREIN ARE PROVIDED ON AN "AS IS, WHERE IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE. RDPSOFT DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE AND/OR RELATED MATERIALS WILL BE UNINTERRUPTED OR ERROR FREE.

Exclusive Remedy and Limitation of Liability: During the warranty period, RDPSOFT's entire liability and Licensee's exclusive remedy shall be for RDPSOFT to repair or replace the Software and Related Materials that do not meet RDPSOFT's Limited Warranty and that are returned to RDPSOFT or its resellers with a copy of Licensee's proof of payment, or, if neither the repair nor replacement of the Software and Related Materials is practicable, to refund the software license fees paid for the Software.

IN NO EVENT SHALL RDPSOFT, OR ITS THIRD PARTY LICENSOR(S), IF ANY, BE LIABLE TO LICENSEE FOR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOST PROFITS, LOST SALES OR BUSINESS EXPENDITURES, INVESTMENTS, OR COMMITMENTS IN CONNECTION WITH ANY BUSINESS, LOSS OF ANY

GOODWILL, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT OR USE OF THE SOFTWARE AND RELATED MATERIALS, HOWEVER CAUSED, ON ANY THEORY OF LIABILITY, AND WHETHER OR NOT RDPSoft OR ANY THIRD PARTY LICENSOR(S) HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

Waivers: No failure or delay by RDPSoft or its licensor(s) in enforcing any right or remedy under this Agreement shall be construed as a waiver of any future or other exercise of such right or remedy by RDPSoft or its licensor(s).

Order of Precedence: Any conflict and/or inconsistency between the terms of this Agreement and any purchase order or other terms shall be resolved in favor of the terms expressed in this Agreement.

Export Regulations: Licensee acknowledges that this Agreement and the performance thereof are subject to compliance with any and all applicable United States laws, regulations, or orders relating to the export of computer software or know-how relating thereto. Licensee agrees not to disclose or export any Software or documentation received under this Agreement in or to any countries for which the United States Government requires an export license or other supporting documentation at the time of export or transfer, unless Licensee has obtained prior written authorization from RDPSoft and the U.S. Office of Export Control or successor thereto.

Commercial Computer Software: The Software is "Commercial Computer Software" under DFARS 227-2702 and FAR 12.212. Any use, duplication, or disclosure by the United States Government is governed solely by the terms of this License or, if specifically required under the applicable federal contract, by the RESTRICTED RIGHTS provisions set forth in one of the following clauses: subparagraph (1) (ii) of the RIGHTS IN DATA AND COMPUTER SOFTWARE clause of DFARS 252.227-7013 (48 C.F.R. Section 252.227-7013 (OCT 1988), Alternate III (g) (3) of the RIGHTS IN DATA-GENERAL clause of FAR 52.227-14 (JUN 1987), or FAR 52.227-19 (JUN 1987).

Governing Law: This Agreement shall be governed by, and resolved in accordance with, the law of the State of Georgia, USA, without reference to its conflict of laws provisions. Neither the United Nations Convention on Contracts for the International Sale of Goods nor the Uniform Computer Information Transactions Act shall apply.

Arbitration: Any dispute or disagreement arising between RDPSoft and Licensee in connection with any interpretation of the commercial terms of this Agreement or the compliance or noncompliance therewith, or the validity or enforceability thereof, shall be finally settled under the Commercial Rules of American Arbitration Association by one (1) arbitrator appointed in accordance with the said Rules in effect on the date that such notice is given. The arbitration proceedings shall be conducted in Atlanta, Georgia. The arbitration award shall be final and binding upon the parties, and judgment may be entered thereon, upon the application of either party, by any court having jurisdiction. Each party shall bear the cost of preparing and presenting its case, and the cost of the arbitration, including fees and expenses of the arbitrator(s), will be shared equally by the parties unless the award otherwise provides.

Entire Agreement: The parties agree that this constitutes the sole and entire agreement of the parties as to the matter set forth herein and supersedes any previous agreements, understandings, and arrangements between the parties relating hereto and is effective, valid, and binding upon the parties.

# How to Purchase RDPSoft Remote Desktop Commander

Remote Desktop Commander Lite Edition is based both on a.) the number of end users (e.g. administrators) who will run it, as well as b.) the total number of computers it will manage.

Remote Desktop Commander Suite Edition is licensed based on the number of servers and workstations the Remote Desktop Reporter component collects data from, not on the number of computers where it is installed, nor the total number of administrators accessing it.

A unique computer or virtual machine running Windows Server 2000, Windows Server 2003, Windows Server 2008, or Windows Server 2012 that is polled by Remote Desktop Reporter requires a server license.

A unique computer or virtual machine running Windows XP, Windows Vista, Windows 7, or Windows 8 that is polled by Remote Desktop Reporter requires a workstation license.

Purchasing the software can be done online via our Ecommerce provider, or via purchase order. Current pricing, ordering methods, and sales contact forms can be found on our website at <http://www.rdpsoft.com/buy>. You can also reach sales directly by phone tollfree at 1-855-RD UTILS (1-855-738-8457).

# How to Obtain Support for RDPSoft Remote Desktop Commander

Complimentary web-based and phone-based support is provided for all current evaluators of our tools.

Existing customers can purchase an Upgrade Protection Agreement with either Standard (web-based ticketing) or Premium (web-based and phone-based) Support.

To open a new support ticket, please visit <http://www.rdpsoft.com/support>.