



# Program Administrator's Guide

[www.rsiguard.com](http://www.rsiguard.com)

## Table of Contents

<b>1</b>	<b>Deploying RSIGuard .....</b>	<b>3</b>
1.1	RSIGuard Standalone vs. RSIGuard+myCority .....	3
1.2	RSIGuard Component Overview.....	4
1.3	The Overall Deployment Process .....	6
1.4	System Requirements to Use RSIGuard .....	7
1.5	Choosing Default User Settings .....	9
1.6	Choosing Administrative Configuration Settings .....	9
1.7	Network Folder Setup.....	10
	a) Selecting a Root Network Folder Path .....	10
	b) Creating the Needed Subfolders.....	11
	c) Folder permissions on Linux/Mac.....	12
	d) Changing the Root Network Folder Path.....	12
	e) Internet Access/Proxy Server Setup .....	14
1.8	HR Data, Administrator Console and Status Reports .....	15
	a) HR Data Integration .....	15
	b) Administrator Console Configuration .....	18
	Call Center Integration .....	20
1.9	Software Package Delivery .....	21
1.10	Operating System Support .....	21
1.11	Software Installation.....	22
	a) Standard Installation .....	22
	b) Server Installation for Citrix/Thin Clients .....	22
	c) Server Installation for Linux.....	23
1.12	English-Only vs International Edition .....	23
<b>2</b>	<b>Introducing Users To RSIGuard &amp; RSIGuard Pilots.....</b>	<b>24</b>
2.1	Welcome Email & Introductory Tutorial .....	24
2.2	Self-Installation Assistance .....	25
2.3	Resources for New Users .....	25
<b>3</b>	<b>Ongoing Management of RSIGuard .....</b>	<b>26</b>
3.1	Viewing DataLogger Data .....	26
3.2	Viewing Aggregate Data with GroupInsight Reports .....	28
3.3	Viewing Data with Other Applications.....	31
3.4	myCority Integration.....	32
3.5	Managing the BreakTimer .....	34
3.6	Managing ForgetMeNotes.....	34
3.7	Managing AutoClick .....	35
3.8	Managing KeyControl.....	36
3.9	Restricted Settings/Features/Menu Items & Administrator Access.....	36
3.10	Modifying an Individual's Settings Locally & Remotely.....	38
3.11	RSIScript Scripting Language .....	39
3.12	Global and Group Modification of Settings .....	40
3.13	Software Updates .....	41
3.14	Additional Support .....	41

# 1 Deploying RSIGuard

## 1.1 *RSIGuard Standalone vs. RSIGuard+myCority*

RSIGuard is used by organizations in two product configurations.

- 1) RSIGuard as a standalone application: This solution includes the BreakTimer, ForgetMeNots, KeyControl, ErgoCoach, AutoClick, Work Restrictions and DataLogger. It is a desktop application for Windows or Mac (limited Linux support). It can be used by any size of organization. It includes reporting tools UserInsight and GroupInsight.
- 2) RSIGuard integrated with myCority: This solution is appropriate for larger organizations. It includes training, assessment, program management, ergonomic evaluation management, reporting in a SaaS environment. It includes all RSIGuard standalone functionality, but some of the features are enhanced due to the integration with myCority.

The primary application, RSIGuard.exe, is physically the same for both RSIGuard (standalone) and RSIGuard+myCority configurations. However, the two configurations have technical differences that are discussed throughout this document.

When the term RSIGuard is used, the information applies to either configuration. If the term “RSIGuard Standalone” or “RSIGuard+myCority” is used, then it is referring to a particular configuration.


See section 3.3 for additional details about the differences between RSIGuard Standalone and RSIGuard+myCority.

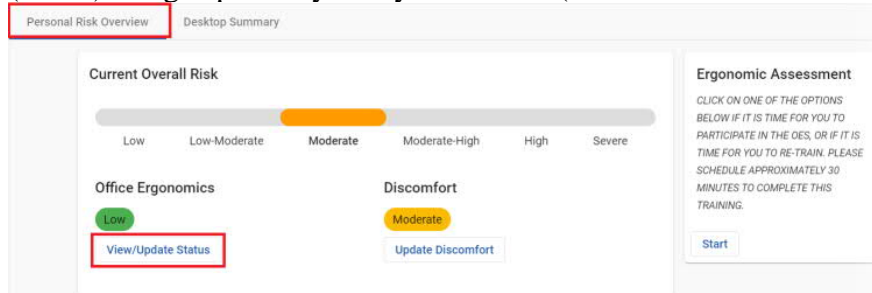
## 1.2 RSIGuard Component Overview

RSIGuard is an ergonomic software package composed of several components:

- **RSIGuard** (RSIGuard.exe) is the application that is installed on each employee's computer. It can be configured in different user-interface modes to present different feature sets:
  - **RSIGuard Mode** - All features are available (BreakTimer, ForgetMeNots, AutoClick, KeyControl, DataLogger, ErgoCoach, Work Restrictions). However, individual features can be included/excluded by configuration at your organization's discretion. The GUI is configurable and looks like this:



- **RSIGuard+myCority Mode** – Like RSIGuard mode, except the Data icon (  ) brings up the myCority dashboard (instead of the data menu).



- **UserInsight** (UserInsight.exe) is the application that allows an employee or an administrator to view graphs of DataLogger data for an individual user. It is primarily for RSIGuard Standalone, but is accessible in RSIGuard+myCority by pressing CTRL while clicking on the dashboard icon.
- **GroupInsight** (GroupInsight.exe) allows a manager or EH&S staff to view aggregate data reports based on DataLogger data (*RSIGuard Standalone only*).
- **Administrator Console** (part of RSIGuard.exe) is the tool that provides administrators a single console for accessing all management functions (e.g., remote settings control, reporting).

- ***RSIGuard Web Reporting tools*** (a component of the SaaS GX2 application) allows a manager or EH&S staff to view aggregated and individualized reports for employees. (*RSIGuard+myCority only*)

Except for hosted RSIGuard+myCority reporting tools, these components are delivered in MSI installation packages (DMG for Mac).

- Your organization will install RSIGuard's user components on employee computers with a client installation package that includes ***RSIGuard*** and ***UserInsight***. This package will be named RSIGuard-Install-vVersion.msi if you use a standard installation, or RSIGuard-YourOrganization-vVersion.msi if you use a custom installation.
- Organizations that use RSIGuard Standalone will install RSIGuard's administrator components on manager/EH&S staff computers with an installation package (<http://www.rsiguards.com/admintools>) that includes ***UserInsight*** and ***GroupInsight***. It is also required that you install RSIGuard's user components on a manager's computer alongside the manager components as this is required to access the ***Administrator Console*** and for automatic configuration of ***GroupInsight***.

Two standard configurations of the RSIGuard client are available. Either can be modified in endless ways, but these are a starting point for many situations.

- RSIGuard Stretch Edition – this edition is used by most organizations and is applicable in most office environments.
- RSIGuard Call Center Edition – this edition is optimized for employees with customer-facing jobs such as in call centers, medical facilities, etc. Call Center Edition provides less intrusive defaults designed to accommodate the call center environment. See section 1.10 for more information.

### 1.3 The Overall Deployment Process

RSIGuard deployment is generally quite simple and typically involves these steps:

1. Verify that your organization's computers can run RSIGuard by reviewing **System Requirements to Use RSIGuard** (section 1.4). Conduct any organization-specific IT or security procedures.
2. Safety staff should review **Choosing Default User Settings** (section 1.5) and decide if you wish to modify any defaults.
3. Safety staff and IT Staff should review **Choosing Administrative Configuration Settings** (section 1.6) and provide the necessary information. This includes determining what reporting functionality your organization wishes to utilize.
4. After receiving a draft settings spreadsheet from your organization (<http://www.rsiguards.com/documents/program/ConfigurationSettings.xls>), Cority will review your settings specifications. If needed, a followup call/email with your IT/Safety may be helpful. Within 3 business days, Cority will provide you with your MSI software installation package. See **Software Package Delivery** (section 1.10).
5. If appropriate to your configuration, IT staff reviews the **Network Folder Setup** (section 1.7) section and configures any necessary network resources (e.g., creating network folders and setting permissions – no server software is used).
6. If your organization will utilize HR data for reporting (GroupInsight) and central settings management (Admin Console) (RSIGuard standalone only), the HR data should be created and placed in the location defined in step 3 (see section 1.8a). If your administrators will have different levels of access to administrative functions, you need to configure that as well (see section 1.8b).
7. If your organization will utilize any internet-based features, IT staff should review **Internet Access Setup** (section 1.7e) to ensure necessary internet access is available.
8. If your organization will utilize RSIGuard's discomfort surveys (HSRs), IT staff should review **Configuring GroupInsight for Health Status Reports** (section 1.8c). (RSIGuard Standalone only)
9. Inform your employees when RSIGuard will be installed and provide introductory information. See **Introducing Users to RSIGuard** (section 2).
10. Deploy the MSI package through your organization's preferred software distribution mechanism. See **Software Installation** (section 1.11).
11. Deploy the Administrator Tools to the appropriate RSIGuard administrator(s) if reporting and remote settings management functionality is desired by safety staff. The MSI package is discussed in the **RSIGuard Component Overview** (section 1.2).

## 1.4 System Requirements to Use RSIGuard

The following list documents the necessary environment for using RSIGuard.

- Operating System: Windows 10, 8.1, 8, 7, Vista. Macintosh OSX 10.4 or later. RedHat Linux RHEL4, 5, 6 or 7.
- Processor Requirements: No minimum required.
- Memory Usage: RSIGuard typically uses between 40-50MB of RAM, however this may increase to 60-90MB when the user is directly interacting with RSIGuard (adjusting settings, in a break, in the dashboard). On most systems, this is a minimal/small memory footprint.
- CPU Usage: Background RSIGuard CPU usage is <1%, and does not impact computer performance. CPU usage increases when the user is directly interacting with RSIGuard.
- Disk storage: Installation of RSIGuard Stretch Edition/Call Center Edition v6.0 requires 300MB of disk space. Data stored by RSIGuard uses about 175KB per year per user (i.e., a negligible amount of space).
- Registry Access Rights: RSIGuard users must have access to HKEY\_CURRENT\_USER\Software\RSIGuard in the registry. This is the case in virtually all Windows environments for Standard or Admin users.
- Folder Access Rights: RSIGuard users need read/write access to the C:\Users\Public\Documents\RSIGuard folder (Windows 7 and later). This is the normal Windows configuration. In the unlikely scenario where write access isn't available, an administrator account should launch RSIGuard once after installation.
- Network compatibility: RSIGuard is compatible with all standard networks and can be operated over a terminal-based system (e.g., Citrix, Remote Desktop). Please see **Server Installation** (section 1.11b) for an additional discussion of server installations.

Although RSIGuard can be used without network access, if network features are utilized (e.g., roaming profiles/data), users need the ability to read/write/delete from a network drive. RSIGuard requires no other network services. Management of network file security is done using Windows file system security to ensure reliability and utilize existing IT resources.

- Network traffic: Network traffic varies based on numerous factors. In a typical configuration, in which the client is installed on the user's local hard drive, but data and configuration information are stored on a network drive, traffic typically involves 3 or 4 network transmissions per hour per user of a few thousand bytes (i.e., a negligible quantity of bandwidth usage for most computing environments). Because frequency of transmissions varies based on user activity, the theoretical bandwidth range could average as low as 3K per hour (6bps), with peaks up to 300K per hour (600bps) per user.

If data and configuration information and software are stored on the local machine, network bandwidth usage is zero.

If users are on thin clients (e.g., Citrix machines with no local hard drives) or if for some other reason the software is installed on a server instead of the local machine, and if stretches are enabled during breaks, then bandwidth will increase because the video stretches will need to be transmitted over the network (assuming the stretch option is enabled). If the bandwidth requirements (approximately 1MB per hour per user) are too high for your environment, lower bandwidth videos are available. Please provide us with acceptable bandwidth levels so we can provide appropriate video content.

- Software compatibility: RSIGuard is compatible with virtually any application. RSIGuard does not install, modify, or remove any system DLLs when installed and therefore will not affect other applications that depend on these DLLs. Cority tracks, investigates, and attempts to resolve any report of software incompatibility. There are currently no reported software compatibility issues.



## **1.5 Choosing Default User Settings**

RSIGuard is highly configurable to meet user needs. When you deploy RSIGuard to your organization, you may want to use RSIGuard “out of the box” with our suggested default settings, or you may wish to change default settings.

Although our experience has led to default settings that are optimal in most situations, each organization has unique needs (e.g. a particular break regimen, or inclusion of additional ForgetMeNot messages). Thus, you can specify different defaults. For any setting:

- You can use our default setting or change to a different default setting
- You can let users freely adjust a setting, lock it in place, or define a validation rule (e.g. a range) over which a user can vary a setting. This can apply to the Settings screens and/or the initial Setup Wizard.
- For each groups of settings (e.g. BreakTimer, KeyControl, ForgetMeNots, etc.) you can hide/show the settings and hide/show the entire feature
- You can create different default configurations for different groups of users based on a wide variety of trigger criteria (e.g. location, HR data if available, risk, etc.)

To specify alternative default user settings, add notes to the “User Settings” and the “ForgetMeNots” sections of the Configuration Settings spreadsheet -

<http://www.rsiguards.com/documents/program/ConfigurationSettings.xls>

## **1.6 Choosing Administrative Configuration Settings**

Administrative Configuration Settings control organization identification, network configuration, reporting configuration, etc. These settings are not normally adjusted by end users, but rather are pre-specified for entire groups of employees or for the entire organization.

Specifying these settings generally requires input from both IT and safety staff. Safety staff should determine what type of reporting functionality they need. Key questions include:

- Do you want to be able to do aggregate networked reporting and have networked profiles? If so, where will the networked data/profiles be stored? Should all administrators have access to all reporting data and the ability to adjust user profile settings, or do you need an access hierarchy?
- Will you collect HR data by exporting from an HR system or will you prompt users to initially provide needed HR data? What fields will benefit the reporting process?
- What features/screens are available to/hidden from users?

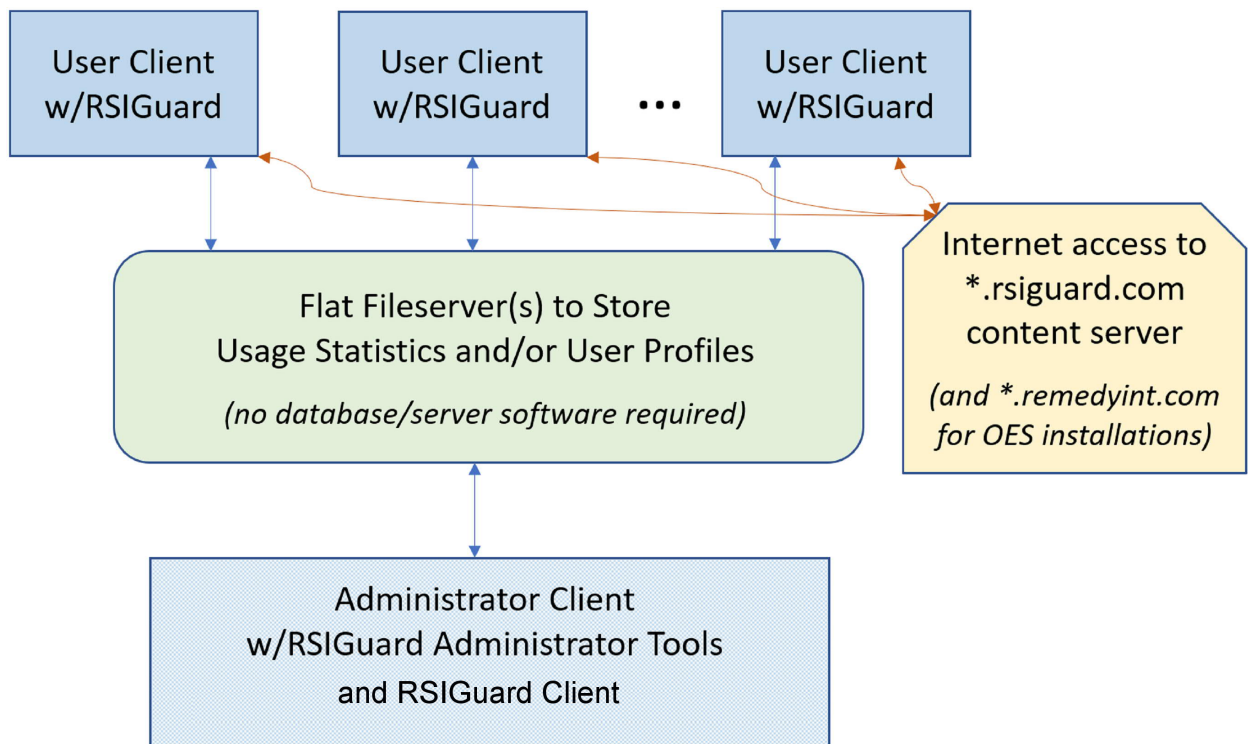
IT technical staff input is typically not necessary for RSIGuard+myCority since data is not stored on a network and HR data is based on myCority/GX2 HR data.

To specify administrative configuration settings, complete the “Admin Settings” section of the spreadsheet - <http://www.rsiguards.com/documents/program/ConfigurationSettings.xls>

## 1.7 Network Folder Setup

RSIGuard stores and reads several types of data (e.g, DataLogger data and user profile settings). By default, single-copy installations of RSIGuard store this data in the %appdata%/RSIGuard folder and the HKEY\_CURRENT\_USER section of the registry. In this configuration, an administrator or ergonomist can't view user data and can't view/change user settings because the data is not networked.

However, RSIGuard can store some, or all, of this data on a network fileserver. This enables central management of settings, and/or central reporting of RSIGuard data. No server software is needed because data is read/stored in binary files directly by the RSIGuard client.



*Architecture Diagram of RSIGuard Installation with networked data/profiles*

If your organization uses myCority, you will not need to create any servers to enable this functionality. Cority will create a custom version of RSIGuard that stores data/settings in the SaaS environment.

If your organization uses RSIGuard without myCority, you'll need to create a file server to store data and/or settings to enable this functionality. This section explains how to configure and name a network folder hierarchy and how to manage file access security of the data.

### ***a) Selecting a Root Network Folder Path***

In most cases, it makes organizational sense to put all RSIGuard data that is to be stored on a file server under the same root path. Ideally you should select a network root path that all

users can access (e.g., a mapped drive like S:\Space\RSIGuard or a UNC path like \\AcmeSharedDrive\RSIGuard). If your users are distributed in several locations that do not share a common network file server, you may need to identify multiple root paths, or create a mapped drive name in each location that refers to an acceptable root path for that location. Another alternative is to use a roaming folder (e.g., if all users have a P: drive that maps to a personal network location, you could use P:\RSIGuard).



*In some network environments, there are significant time delays (up to 1 or 2 seconds) to initially access a UNC-specified networked file. If this is the case with your network, and you configure RSIGuard to store data to a UNC-named folder, your users may experience delays when RSIGuard writes to the network (although RSIGuard tries to mitigate this by writing when users are idle). In most networks, mapped drives are significantly faster to access than UNC paths, and are thus preferable. If a mapped drive is not possible, and users only use 1 computer each, you may wish to store data locally and use the “Daily Backup” feature to copy data to a network location once a day.*

### ***b) Creating the Needed Subfolders***

Within the selected root path, you will create some or all of these 4 subfolders:

1. **Data** (e.g., S:\RSIGuard\Data): This folder stores the usage data (TID and KUF files) created by RSIGuard client installations (i.e DataLogger data). For information about this data, please see <http://www.rsiguards.com/documents/help/DataLoggerAnalysis.pdf>. Users need read/write/delete permission to at least their personal data files within this folder. Personal data files are named *Username.tid* and *Username.kuf*, where *Username* is the user’s login name. For example, if a user logs in as “jdoe”, their data will be stored as “jdoe.tid” (for daily usage information) and “jdoe.kuf” (for long-term keyboard statistics). If usernames are not guaranteed to be unique in your organization, you should read the end of the “HR Data Integration” section in 1.9. Users do not need the ability to view a directory listing of the folder. You may wish to give all users read/write access to the folder and prevent folder listing, or you may wish to set permissions for each data file separately to give each user access to only their 2 files (e.g., with Creator Owner – see <https://technet.microsoft.com/en-us/library/cc754178.aspx?f=255&MSPPErrors=-2147217396> for information on this security model). Ergonomic administrators who have permission to view DataLogger data (using UserInsight or GroupInsight) need read privileges in this folder, but do not need any write privileges. Most organization’s (except those who use myCority) will need this folder.
2. **Config** (e.g., S:\RSIGuard\Config): This folder is used to store RSIGuard settings. Filenames are named RSIGuardRoamingProfile- *Username.rni* where *Username* is the user’s Windows login name. Privileges for this folder are the same as the Data folder, except that Ergonomic administrators who have permission to remotely modify user settings also need write and delete privileges in this folder. Most organizations will need this folder.
3. **HRData** (e.g., S:\RSIGuard\HRData): This folder holds your HR database information (see section 1.9 for more information about HR data). In most installations, this data should only be readable by RSIGuard administrators. Write access is only necessary for the person (or automated process) responsible for keeping the HR data up to date.

4. **Scripts** (e.g., S:\RSIGuard\Scripts): This folder provides a place for scripts such as the Startup.txt script (and potentially other scripts as well) as described at <http://www.rsiguard.com/RSIScript>. RSIGuard users should have read permission only. Only administrators who are authorized to make global changes to RSIGuard configuration should have write access to this folder. Note that if your organization chooses to store these scripts on your web server, on a Cority web server, or on the local hard drive, then this folder is not necessary. Also, in most deployments, this folder will be empty until some point in the future when scripts become necessary (e.g. to make a global change to RSIGuard configuration). The primary reason to create this folder during initial deployment is so that you don't need to do it later if it becomes necessary to add scripts.

#### ***c) Folder permissions on Linux/Mac***

If data is stored on a Windows server but accessed from a Mac, you may simply reference your drive via smb: (e.g. [\\OurServer\RSIGuard](http://OurServer/RSIGuard) becomes smb://OurServer/RSIGuard). However, this section applies if data is stored on a Unix file server.

Unix-based permissions are different than Windows permissions. If your data files are stored on a Unix-based filesystem (e.g. Linux, Mac), this section describes the desired file and folder permissions.

If all users are in the same usergroup as the owner of the Data, Config and Reports folder, then the minimum permissions for those folders should be set to 730 (drwx-wx---). If users might not be in the same usergroup as the owner of the Data and Config folder, then permissions for those folders should be set to 733 (drwx-wx-wx). This allows users to create, modify, rename and delete files in the Data, Config and Reports folders, but does not give them permission to view a list of files. If desired, for simplicity you can create these folders with read permissions, e.g. 777 or 773. This allows users to view the contents of the folders (e.g. using cd / ls).

A user's umask must be set to give appropriate permissions to files those users create. The default user umask of 0002 is appropriate. This gives rw to user and group, and r to all. However, depending on your user architecture, you could reduce permissions to increase security (e.g. to remove write permissions from group, or even read permissions from group and/or all depending on the needs of the user(s) who may be running reports on data in the Data folder).

As in Windows, the HRData folder generally need only be accessible to administrators. The Scripts folder might also have permissions set to 733, but files within the folder need only give users read access.

#### ***d) Changing the Root Network Folder Path***

If after deploying RSIGuard, you need to relocate RSIGuard data, there are 2 key considerations.

- 1) How to get RSIGuard to point to the new server
- 2) Migrating data from the old server to the new server

Pointing to the new server:

If you are preparing to install a new version of RSIGuard, then simply inform us of the new network folder path. We'll update your installation package for the new version, and when it's installed, it will point RSIGuard to the new location. If you don't want to install a new client, and your old network path will still be valid for some period after the new path is accessible, then another option is to use the "Startup.txt" script to issue a command to RSIGuard to change the location. The Startup.txt file is located at *OldNetworkFolderPath/Scripts/Startup.txt*. It would contain commands like:

```
update datafolder NewNetworkFolderPath/Data
update profilefolder NewNetworkFolderPath/Config
```

#### Migrating data:

If the old server is available to RSIGuard when RSIGuard moves to the new server, RSIGuard will automatically transfer data to the new server if the "update" command is used. In this case, you should not move any data. If the old server is not available, but you have backups of the data, you can manually prepopulate the new server with the historical data. In this case you would not use the update command (please discuss this option with RSIGuard support for details if you plan to use it).

Once users are pointing to the new server, access to the old server can be removed.

### ***e) Internet Access/Proxy Server Setup***

Several features of RSIGuard take advantage of web access if it exists:

- myCority functionality depends heavily on access to \*.cority.com for configuration, reporting, and messaging
- Online registration/license tracking, RSIGuard online documentation, ErgoCoach training content, BreakTimer YouTube channels, RSIGuard update functionality depend on access to \*.rsiguard.com

If your organization requires any of these features, your users need to access these webservers. If you have internet access restrictions for employees, then access must be granted to \*.rsiguard.com on port 443 (https) . In addition, if your organization uses RSIGuard+myCority, then access must be granted to \*.cority.com on port 443.

Some features *do* transmit personally identifiable information such as network login ID and RSIGuard profile name. This information is only used as follows: in online registration/license tracking, this information is only used to track the usage of an organization's license (per section 4.3 of the RSIGuard license agreement); in establishing an initial connection to myCority, some agreed-upon token will be transmitted to myCority in non-SSO configurations.

If your organization uses a proxy server in the Windows or Mac environment, RSIGuard will use proxy settings from the OS. In general, no RSIGuard-specific proxy server configuration should be required.

If your organization uses a proxy server in the Linux environment, you will need to define a proxy server string. You can either provide the proxy string to Cority (to be embedded in your custom RPM installation package) or place it in the environment variable, HTTP\_PROXY. The format for the string is [[username:password]@]server:port. Here are some examples:

- 168.192.0.1:3128 – server is 168.192.0.1 and port is 3128. No authentication required.
- @168.192.0.1:3128 – server is 168.192.0.1 and port is 3128. Authentication is required and the user will be prompted for credentials.
- joesmith:secret123@168.192.0.1:3128 – server is 168.192.0.1 and port is 3128. Authentication is required and RSIGuard will use the provided credentials. This method is frequently inappropriate for security reasons.

## **1.8 HR Data, Administrator Console and Status Reports**

### ***a) HR Data Integration***

The Administrator Console in RSIGuard and the GroupInsight reporting application provide more sophisticated functionality if you integrate HR data for your employees into RSIGuard. For example, GroupInsight lets you generate reports based on parameters such as employee location, department, supervisor, or whatever other fields you may wish to use. In addition, GroupInsight lets you send email to groups of users who meet your selected criteria – and those criteria can include HR criteria if HR data is integrated. The Administrator Console lets you manage groups of users (e.g. changing settings) based on this data if available.

Ideally your organization provides an HR database that contains all the fields you want to be available – however some limited functionality is also possible in a scenario where you can't create such a database and end users provide the data via a survey when they first install RSIGuard. A user survey is less preferred because of likelihood of user error, the additional time demands placed on the user, the lack of a system to keep data up to date, and because some functionality requires an actual HR database file.

The HR database is generally created by your organization from your organization's HR system (or an IT system such as Outlook), and never needs to be transmitted outside your organization. The database is a text-based CSV file and should be stored in the location specified in your RSIGuard Configuration Settings spreadsheet. The file is ideally updated through an automated periodic export process from your HR system, or alternately, a less frequent manual export process.

The file is in the following format.

Line 1 of the file is a header line that specifies the fields (columns) that appear in the rest of the CSV database file. Here is a sample header line, followed by an explanation.

PKEY=login,First Name,Last Name,Email,EmployeeID,Key=Department,Key=Building,Key=Supervisor,Key=Job Type

Each field name on the header line is separated by a comma. The first field must be a primary key (PKEY) which is an identifier that is guaranteed to uniquely identify an employee. To specify the primary key, you specify 'PKEY=' followed by the PKEY's name. Generally, this must be PKEY=login (see below for exception), which defines that the first field of each line will be the user's network login ID. Each subsequent field is optional, and you can add or remove any other field you want to use. If the field name is prefixed with 'KEY=', it means that the Administrator Console will allow you to group users by that field and GroupInsight will let you compare users based on that field. Typically, you would only make fields that have a "many users to one value" relationship a key. For example, "Location" is a logical choice for a key, whereas email address or name would not be a logical choice for a key. Use whichever fields you need/want.

You may also omit line 1 to use RSIGuard's default database format. If you omit line 1, RSIGuard acts as if you had the following header line:

PKEY=login,Name,UserEmail,EmployeeID,Key=Location,Key=Department,Script

Lines 2 thru the end of the file contain the data for your employees – each line (record) corresponds to one employee. Here are some sample lines of data:

gvoenel78,Gary,Voenel,gvoenel78@acme.com,651-07-789,Management,M1,Mark Winters,Consultant  
dgenowitz75,Douglas,Genowitz,dgenowitz75@acme.com,903-72-709,Engineering,P1,Mark Winters,Consultant  
csatelli53,Christie,Satelli,csatelli53@acme.com,726-70-905,Production,S2,Mark Winters,Full time  
akevner65,Aster,Kevner,akevner65@acme.com,506-37-987,Fab-Plastic,P1,Mark Winters,Full time  
emartin43,Elaine,Martin,emartin43@acme.com,524-34-961,Administration,S1,Mark Winters,Full time  
clocatelli77,Carol,Locatelli,clocatelli77@acme.com,815-66-081,Fab-Metal,S3,Mark Winters,Full time  
rnelson76,Rebecca,Nelson,rnelson76@acme.com,063-15-849,Fab-Plastic,B1,Mark Winters,Full time  
maustin29,Madison,Austin,maustin29@acme.com,499-04-088,Engineering,P1,Mark Winters,Full time  
rkevner68,Rebecca,Kevner,rkevner68@acme.com,673-89-577,Fab-Plastic,S2,Mark Winters,Part time  
kfelt87,Kelvin,Felt,kfelt87@acme.com,921-49-417,Fab-Plastic,M1,Mark Winters,Full time  
cbaker46,Chris,Baker,cbaker46@acme.com,514-48-274,Management,P1,Mark Winters,Full time  
bgilmore93,Bill,Gilmore,bgilmore93@acme.com,001-57-159,Marketing,S1,Chris Baker,Consultant  
pbaker17,Paul,Baker,pbaker17@acme.com,971-87-171,IT,B1,Chris Baker,Full time

If you would like a test database file, you can download a sample file at  
<http://www.rsiguard.com/help/UserMgmt/SampleHRData.csv>.

The data in the HR database file may be encrypted (by Cority, or by your organization using a tool provided by us) before being placed on your server to provide additional privacy/security. This is generally not necessary because the HR data file is generally only available to administrators. However, all administrators must have read access to the HR database file, and if this is a security concern, encryption may be appropriate. The encryption tool, HRDBEncoder.exe can be used either as a Windows application or as a command line application. To use as a command line application, the usage is:

HRDBEncoder [/q] INFILE OUTFILE

where INFILE is the clear text CSV file, and OUTFILE is the encoded DAT file. The /q option disables any error messages about a missing INFILE or a non-writeable OUTFILE.

As stated above, the first column generally must be defined as PKEY=login. However, in the rare situation that an organization does not have unique logins for each user (or recycles logins when an employee leaves) you have options. Usually the PKEY is a Network Login ID (NLI or username). The reason for this is that RSIGuard will save data in files whose names are based on this value (e.g., if your NLI/username is "jsmith", your RSIGuard data file would be "jsmith.tid"). Furthermore, RSIGuard knows the NLI/username because it can query Windows for it. Thus, RSIGuard automatically knows the PKEY value for any logged in user. In the HR database, the PKEY must match (i.e. jsmith). If NLI's are recycled, then, unless data/config files are deleted before the NLI is reused, the old data/config would be inherited by the new user of the NLI (e.g. current employee Jan Smith (jsmith) would inherit from former employee John Smith (jsmith)).

If your organization is in this rare situation, RSIGuard allows you to define an alternate mechanism for naming data/config files (and thus the value of the PKEY for each user). For example, you could use "Employee ID" (EID). But, since RSIGuard can't simply query Windows for an EID, it would typically need to get it via another mechanism. One possible mechanism is that when RSIGuard first starts, it could ask the user for their EID, and then, that would be their PKEY – which would then also need to be the PKEY in the HR database. The downside of this method is that the user has to manually enter their EID, and inevitably, mistakes will be made. A user could enter an EID that was someone else's (in which case two employees would be set up with the same PKEY) or could enter an invalid EID. In either case, it would be difficult to track down such errors. Ideally, whatever PKEY you use,



RSIGuard should be able to get the value without asking the user. For example, RSIGuard can use registry values, environment variables, or query URLs. For example, if HKEY\_CURRENT\_USER\Acme\EmployeeID is available, or if the Environment Variable EmployeeID is set, or if there were a URL that converts current NLI's to EID's (e.g. <http://www.acme.com/hrquery?nli=jsmith> returns the EID "12345678") RSIGuard can use such a mechanism to automatically get EIDs (or whatever field you wish to use in place of NLI).

### ***b) Administrator Console Configuration***

Because the Administrator Console is part of RSIGuard, a manager using the Administrator Console normally does not need to perform any specific configuration. It automatically looks for data and network profiles in their default network locations. It automatically looks for the HR database in the specified location and builds the user interface accordingly. The only aspect of Administrator Console configuration that requires explicit configuration is the creation of Access Controls.

Access Controls define which users a particular administrator is allowed to view, and also defines which users have access to the Administrator Console. RSIGuard can be configured to turn Access Controls off (in which case any user who enters the administrative password can access the data and settings of all users) or on (in which case administrators can only access those users they are explicitly given permission to view).

Access controls can also limit what an administrator can do, e.g. view user data, change user settings, configure where HR data is located, view the “overall user report.”

To define Access Controls, you must create a UMAccess.txt file in the same folder as the HR database is located. This file should be read only to all users except to the administrator who defines access rights. Each line of the UMAccess.txt file grants access to one administrator.

Each line is in the format:

NETWORKLOGIN,+/-,+/-FIELD=VALUE,+/-FIELD=VALUE,+/-FIELD=VALUE...,+/-ACCESSTYPE

The first value is the network login of the administrator (e.g. jsmith). The next value (the “base access value”) is either a + or – symbol. If it is the + symbol, it means start by granting access to all users (subsequent values on the line can then be used to selectively remove access to groups of users). If it is the – symbol, it means start granting access to no users (subsequent values on the line can then be used to selectively add access to groups of users).

For example:

jsmith,+,-Location=Chicago

bsanchez,-,+Location=Chicago

tchan,-,+Building=B25,+Building=B27,-Department=IT,+Supervisor=Doug Jones

means that administrator jsmith has access to all users except those in Chicago, bsanchez has access only to users in Chicago, and tchan has access to all users in building B25 and B27, unless they are in the IT department, and all users who report to Doug Jones. In this last example, because the +Supervisor value comes after –Department=IT, IT staff who report to Doug Jones *would* be included. If the –Department=IT came after the +Supervisor value, then no IT staff would be included.

In addition, you can add or remove access types by using +/- followed by:

- Unknown – to give access to users who are not in the HR database. By default, this is enabled if the “base access value” is + or disabled if it is -. In the above examples, jsmith could access users who aren’t in the HR database, but bsanchez and tchan could not.
- ViewUserData – to control access to the UserInsight data (enabled by default).

- ViewGroupData – to control access to the GroupInsight data (enabled by default).
- Settings – to control access to remotely changing other users's settings (enabled by default).
- UserReport – to control access to the Overall RSIGuard Usage Report (enabled by default).
- Config – to control access to the settings that change where HRData and UMAccess data is stored (disabled by default unless access string is limited to +).

Some examples:

abaker,+ (give abaker access to all users and controls except Advanced Config settings)

tmeyer,+,-ViewGroupData (don't let tmeyer view GroupInsight reports)

phansen,+,-Settings (don't let phansen adjust the values of user settings)

jsmith,+,+Config (give jsmith full access including ability to change location of HR & UMAccess database)

When Access Controls are enabled, a user who does not appear in the UMAccess.txt database will not have any administrative access.

### ***Call Center Integration***

RSIGuard Call Center Edition is designed for the call center environment in the following ways:

1. The setup wizard asks questions that are more appropriate to the call center environment than to the office environment and is much shorter than the Stretch Edition wizard.
2. Default settings are geared towards the time-sensitivity demands of the call center environment (e.g. shorter break durations).
3. Default settings are geared towards non-intrusiveness based on the requirement in call centers that agents never be interrupted during calls. Warnings are provided if settings are modified in ways that might be incompatible with call center work.
4. RSIGuard Call Center Edition breaks can be globally controlled to reduce the frequency of agent breaks as a function of call load (e.g. so that during heavy call periods, breaks are reduced or eliminated). This is typically controlled manually (e.g. by a call center manager) using a separate tool called RSICallVol (see item 6 for automated alternative).
5. Breaks can be balanced to insure that there are never large percentages of agents taking breaks at any particular time.
6. RSIGuard Call Center Edition can optionally be integrated with call center software if your call center software provides the necessary APIs. If integrated, RSIGuard can:
  - a. Automatically adjust break levels based on call volumes as described in item 4 above.
  - b. Automatically take agents offline after a call completes when a break is needed, and automatically return them online when the break completes.

If your organization wishes to pursue integration with your call center software, your call center IT department should do the following:

1. Provide Cority with a list of call center software technologies used at your organization's call centers.
2. Provide Cority with support contacts for your call center software. This means either:
  - a. Someone at your organization who is familiar with the APIs to the call center software, or
  - b. Contacts to appropriate call center software vendor support.

The call center software API's/services that RSIGuard needs to access include those accessible to desktop software (either via the desktop or via web protocols) to:

- Identify call load levels
- Identify agent status (e.g. on a call, waiting for a call, offline)
- Modify agent status (e.g. switch to offline, switch to online)

## **1.9 Software Package Delivery**

RSIGuard is delivered via download from the [www.RSIGuard.com](http://www.RSIGuard.com) web server via a custom link (for custom installations) or a standard link (for non-custom installations). You can provide the download URL to end users (and optionally require users enter an email address), or your IT staff can download the MSI and make it available to users (e.g., via advertised software, by using a software distribution tool to push RSIGuard onto the desktops of new RSIGuard users, or by reinstalling it on new computers).

Customize MSI packages are preset with your organization's chosen configuration (specified via <http://www.rsiguard.com/documents/program/ConfigurationSettings.xls>). Customizations might include configuration for your network, default settings for features, settings restrictions, custom questions to ask users on setup, and software registration.

Our MSI packages are created to not require any keyboard/mouse interaction. Upon launching the installation package, RSIGuard is installed to the installation folder (by default, "C:\Program Files\RSIGuard" on 32-bit Windows, or "C:\Program Files\RSIGuard (x86)" on 64-bit Windows). The software is optionally launched when installation completes (per specification in Configuration Settings). The MSI package contains a visible user interface that shows the installation progress. If you want to hide this, use the /qn MSI option (e.g., `msiexec RSIGuard-Acme-v6SB.msi /qn`) and the installation will be performed silently in the background.

By default, RSIGuard installs a shortcut in the "All Users" Startup folder (or the personal Startup folder if rights to the "All User" folder are not available at installation), so after RSIGuard is installed, it will run automatically every time a user logs in. If you want RSIGuard to be installed only in a particular user's Startup folder, you can use the MSI command argument `ALLUSERS=""` (e.g., `msiexec RSIGuard-Acme-v5SB.msi ALLUSERS=""`).

## **1.10 Operating System Support**

RSIGuard is currently available for Microsoft Windows, Apple OSX, and to a limited degree for RedHat Linux.

## 1.11 Software Installation

### *a) Standard Installation*

In most environments, it is desirable to install RSIGuard on each user's computer. You can use standard software distribution tools to push RSIGuard onto desktops, or put RSIGuard on your standard desktop image. You can also install RSIGuard manually on each computer, or have users install it themselves (see **Self-Installation Assistance** (section 2.2)). The RSIGuard installation is portable, and therefore it is possible to install it on a server and have users launch it in a login script via reference to the server installation. It can even be installed on portable media such as a USB or thumb drive.

### *b) Server Installation for Citrix/Thin Clients*

If your users use thin clients (e.g., Citrix), you can install RSIGuard on the thin client itself (uncommon) or on the Citrix server(s) (common).

If installing on the server, the issues to consider are:

- Where will the RSIGuard application be, and how will it be launched?  
RSIGuard can be installed on a file server that is read-accessible to users. You can install by simply copying the contents of a standard installation (e.g. c:\Program Files\RSIGuard) to a network folder. Then, RSIGuard can be launched during startup (either with a login script, or by placing a shortcut in the Startup folder).
- Where will RSIGuard store user data?  
If %appdata% is on the network, then data will, by default, be stored in a networked location, as this is RSIGuard's default data location. If you want data stored in another location, it can be specified (see section 1.7).
- Where will RSIGuard store user settings?  
If HKEY\_CURRENT\_USER is on the network, then settings will, by default, be stored in a networked location, as this is RSIGuard's default settings location. If you want data stored in another location, it can be specified (see section 1.7)
- Is RSIGuard in a same or superior context to other applications?  
In order to track activity (or for features like AutoClick or KeyControl to work), RSIGuard must be at the same level or higher than the applications in use. For example, if computer A runs RSIGuard, and you remote desktop to B, A can track activity on B. However, if RSIGuard is only installed on B, that instance of RSIGuard can't track activity on computer A. In some cases, you may want to install RSIGuard at multiple levels and use the Virtual Computing feature of RSIGuard to automatically enable/disable RSIGuard as appropriate.

There are various combinations of server installations, virtual machines, virtualized applications, remote desktop connections, etc. that can complicate RSIGuard deployment – but are typically all possible. These may require additional support from Cority. But, generally speaking, the 4 issues described above are the key issues to consider.

### ***c) Server Installation for Linux***

When installing RSIGuard in a Linux environment, you can also install RSIGuard on a server. This makes updating RSIGuard for all users simpler as the executable, libraries, and resources only need be updated once. To accomplish this:

1. Install RSIGuard on an IT computer. You'll use this base installation to grab the files you need to put on the server.
2. Create a folder on the server, e.g. /acme-server/RSIGuard. You'll need to set the environment variable `RSIGUARD_HOME` to this folder for each client machine.
3. Then, within `RSIGUARD_HOME`, create a bin subfolder, and copy /usr/bin/RSIGuard to `$RSIGUARD_HOME/bin`.
4. Copy the /usr/share/rsiguard/Resources folder (and subfolders) to `$RSIGUARD_HOME`
5. Copy the libraries from /usr/local/lib/libwx\* to your preferred location on your server (it can be in a location like `$RSIGUARD_HOME/lib`, but it doesn't have to be). Use `ldconfig (/sbin/ldconfig $RSIGUARD_HOME/lib)` or another mechanism to add this folder to your users's dynamically linkable libraries.
6. In your users startup process, make sure that `$RSIGUARD_HOME/bin/RSIGuard` is launched. For example, in a bash script, you could use "`RSIGuard &`" or "`$RSIGUARD_HOME/bin/RSIGuard &`" to launch RSIGuard in a separate process to the executing script.

## ***1.12 English-Only vs International Edition***

Microsoft Windows users can utilize either RSIGuard English-Only or International Edition.

RSIGuard English-Only is the best choice for an English-speaking population. Because this edition is not designed to be internationalized or work on multiple platforms, it offers an optimized RSIGuard experience for English speakers using Windows. New features for RSIGuard generally are first available in this edition. RSIGuard International Edition is, however, the best choice for a population that speaks other languages.

If you have a mix of English-speaking and non-English-speaking populations, you can use both editions. In that case you have two deployment options:

- 1) We can provide 2 MSI's (one for each edition). You need to push the correct MSI out to the correct users. This has the advantage that pushed packages are smaller and installation is faster. It's a good choice if you have a clear delineation of who gets what (e.g. in US, use English only, and outside US use International Edition).
- 2) We can build a single MSI with both editions. You push the MSI to all users. This MSI is roughly twice as large and takes about 2-3 times longer to install. But, it's simple in that you can push the same package to all users. All users must select their preferred language. When English is selected, English-Only edition runs. Otherwise, International edition runs. The language can be changed by the user at any time.

All Apple OSX and RedHat installations use RSIGuard International Edition.

## 2 Introducing Users To RSIGuard & RSIGuard Pilots

### 2.1 Welcome Email & Introductory Tutorial

We encourage you to help your employees get familiar with RSIGuard before it is installed on their computer by sending them an invitation letter. The letter should describe:

- Why employees should use RSIGuard
- What RSIGuard is
- A link to an introductory tutorial

A sample introductory letter is shown below (and related resources are available on our support pages at <https://www.rsiguard.com/support/pilot.htm>).

Dear Employee,

As part of our continuing effort to keep our workplace safe, we will be adopting the use of a software application called RSIGuard from Cority, Inc., which is designed to help prevent discomfort associated with computer use.

RSIGuard will be installed on your computer in the near future, and we encourage you to use it to help you maintain healthy work habits at your computer.

RSIGuard has many exciting features:

- BreakTimer will remind you to give your body enough time to rest between prolonged periods of computer use. It will also show you demonstrations of stretches you can do while resting.
- ForgetMeNots will help keep you aware of how you are physically working at the computer by prompting you with ergonomic tips during brief rests.
- ErgoCoach will help you get the most out of sit-stand desks and optimize your use of multiple monitors, notebook computers and shared workspaces.
- ErgoAnswers will help teach you healthy ways to work at your computer.
- DataLogger helps safety staff understand how to reduce your organization's risk and boost wellness.
- Health Status Reports gives you an easy way to keep us informed about how you're doing at your computer from a health perspective.
- AutoClick and KeyControl are features some of you may wish to use to reduce the strain of using a computer by reducing the number of keystrokes and mouse actions necessary to perform many actions.

We encourage you to view a brief RSIGuard introduction at <http://www.rsiguard.com/intro>.

RSIGuard is designed to work with your needs in mind. We selected this particular package because it is very user friendly, very customizable to individual needs, and because it sensitively balances ergonomic principles with the reality of how you work on your computer.

If you wish to know more about RSIGuard, please ask your supervisor.

Sincerely,

Your Health & Safety Team



## **2.2 Self-Installation Assistance**

In most organizations, IT staff will install RSIGuard for users. However, if your users will be installing RSIGuard themselves, you can help them by giving them some simple installation instructions.

A sample letter that guides them through the process is provided below (and is available online in editable form at <http://www.rsiguard.com/InstallationInstructions.doc>):

Dear Employee,

Thank you for choosing to use RSIGuard. RSIGuard will help to keep you more comfortable at your computer.

This email provides instructions on how to download, install, register, and setup RSIGuard on your computer.

1. It is a good idea to first close any applications you currently have open.
2. Visit the RSIGuard download page at <http://www.rsiguard.com/install> and follow the instructions there for downloading and installing RSIGuard.
3. After installation completes, RSIGuard will automatically launch (and will launch automatically every time you restart your computer).
4. When RSIGuard begins, it will give you the option of Registering RSIGuard or starting a 45-day trial. Choose "Register RSIGuard", click "I have my registration code for this copy of RSIGuard", and carefully enter the following registration code:  
xabc123 *<replace with your organization's registration code>*
5. RSIGuard will begin the setup wizard to help you configure your RSIGuard preferences. The setup wizard is self-explanatory, but if you'd like additional help, see <http://www.rsiguard.com/documents/help/GettingStarted.pdf>

At this point RSIGuard is running! Enjoy RSIGuard. Remember, it is there to help you work with less discomfort and avoid becoming injured. If you have questions or feedback, please contact your help desk support or email [support@rsiguard.com](mailto:support@rsiguard.com).

Thank you for using RSIGuard!

## **2.3 Resources for New Users**

Although RSIGuard is designed to be self-teaching, several resources are available for users at <https://rsiguard.com/help/>

- Web-based tutorial that introduces RSIGuard concept and features.
- Online version of the help system that is accessible directly from RSIGuard's Help menu.
- FAQ about RSIGuard.
- Several videos, brochures, and PowerPoint presentations for end-users and RSIGuard presenters.
- Many more resources

## 3 Ongoing Management of RSIGuard

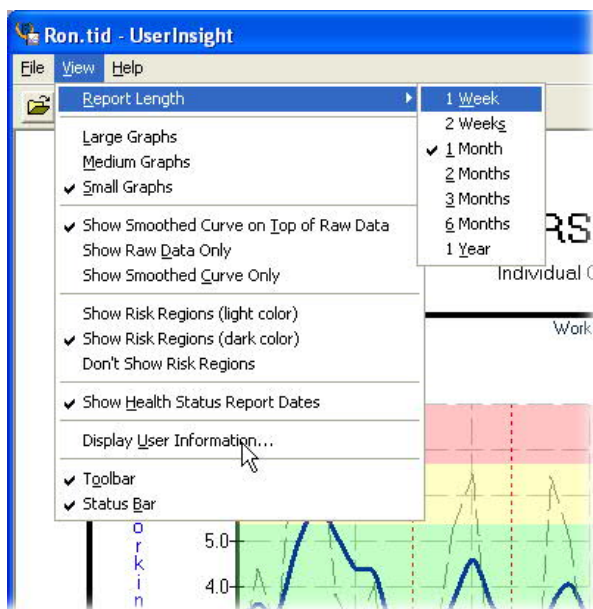
### 3.1 Viewing DataLogger Data

#### RSIGuard Standalone:

RSIGuard records statistics about how a user is working on the computer, such as time spent on the keyboard vs. mouse, strain exposures, break-taking patterns, etc. This data, which is called “DataLogger Data”, is recorded daily. Each DataLogger data file contains data about only 1 user.

To view a user’s data, you can use the RSIGuard companion application UserInsight. This application is provided both in the RSIGuard installation package as well as the Administrator Tools installation package (available at <http://www.rsiguard.com/admintools>). Although not available for Mac, Mac data files can be viewed with the Windows UserInsight application.

The main view shows graphs of each statistic and offers you several ways to view the data.



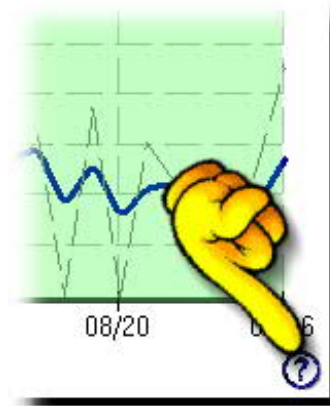
*From the view menu, you can select the period of time for which data is shown, and the graph size (zoom).*

*You can also specify if each day’s data is shown (raw data) or if a smoothed curve fit of the data is shown (smoothed). You can also view both at once.*

*If the user has submitted Health Status Reports, then you can also opt to show the dates that reports were submitted on the DataLogger graphs.*

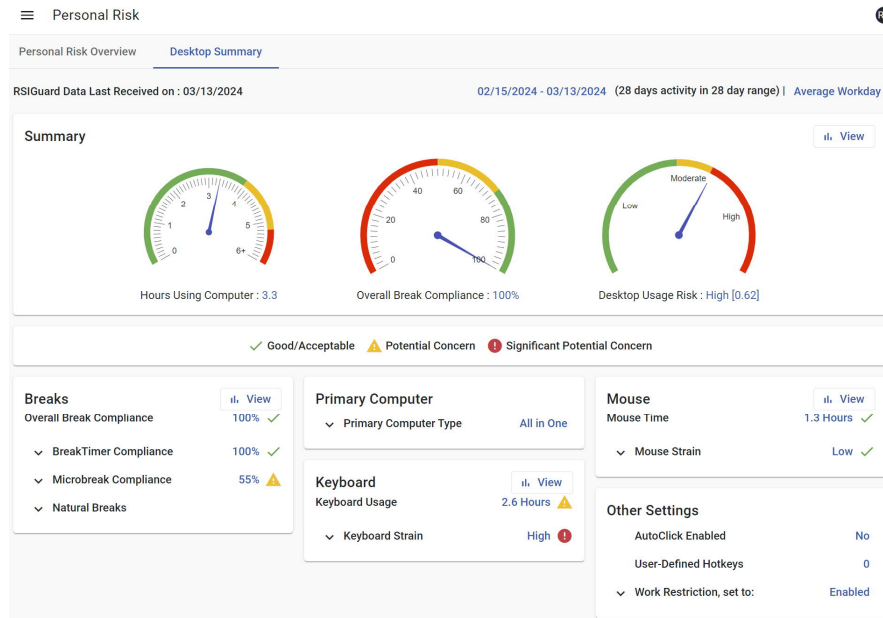
UserInsight allows each user to view their own data. However, a password is required to open up the data file of another user. By default, this password is “hsr”, but this password can be changed. In general, data files should be stored in a way that users don’t have read access to other users’ data (and at a minimum they should not have write access).

To interpret the meaning of each graph, you can click on the context Help. A window will popup with a description of how the data can be used, and how particular values/patterns should be interpreted.



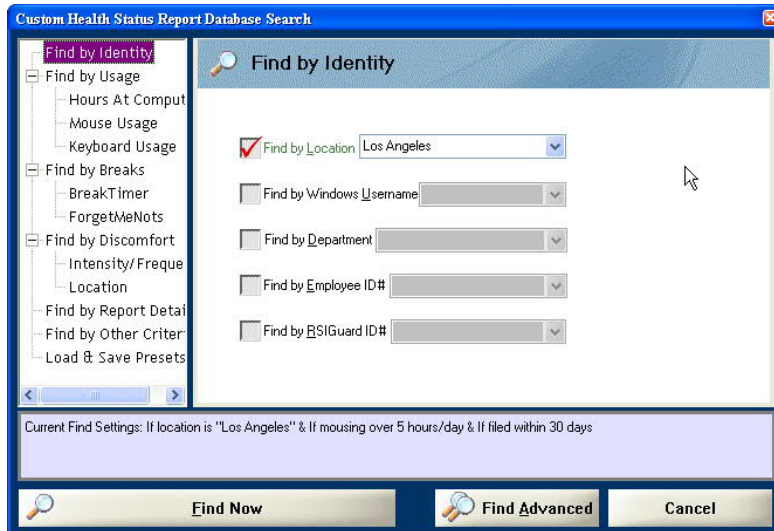
### RSIGuard+myCority:

myCority users can view their RSIGuard data (and administrators with selected roles can view employee data) by clicking on the Desktop Summary link of the dashboard:



This will give you the opportunity to view either 2-week, monthly (4-week), annual or custom summaries, as well as graphs covering those time periods.





You can select as many criteria as you wish. The blue “Current Find Settings” box at the bottom shows in plain English what the current search is as you construct it.

You can use the “Find Advanced” button to search within a current found set, or to add the results of the find to the previously found set of records.

You can also save a useful search for later use.

The most interesting search results will relate usage statistics for a particular population with discomfort to locate causal relations.

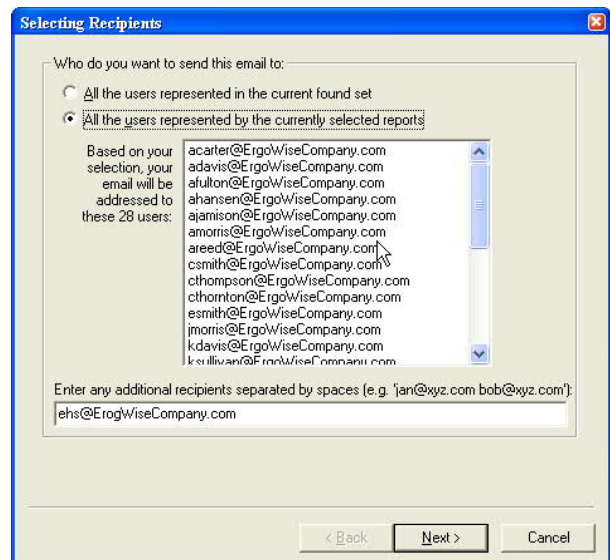
When you identify a group of employees with a particular issue, you can use the Bulk Email option in GroupInsight to send an email to each employee with ergonomic tips, product suggestions, needed workstation or work habits changes, or other relevant information.

To access this feature, click Reports, “Send Bulk Email”.

First you’ll select the users to send this email to.

You can either send the email to all of the users who were found in the most recent find (i.e. the “current found set”) or you can select a subset of the “current found set” and send just to the “currently selected recipients”.

You can also specify additional recipients (e.g., yourself, program administrators, etc.)



Next, you will compose the email you wish to send.

You'll need to specify:

- who the email is from (email address). Replies to this message will also go to this email address.
- A subject for the email
- The body of the email

When you finish, click the Next button.

In the next screen you can click the Finish button to send the email, or the Back button to make changes.

Composing the Email

Static

From: JoeSmith@ErgoWiseCompany.com (your email address)

Subject: Ergonomic keyboard available

Message (type your message below or copy and paste in a pre-written message)

Dear RSIGuard User

You have been identified as having significant typing responsibilities in your job.

As a result, you may request an ergonomic keyboard.

If you would like to request a keyboard, please visit:

<http://ErgoWiseCompany.com/ehs/ergokbd.htm>

or contact your supervisor.

Sincerely,  
Ergonomics Staff

< Back Next > Cancel

A more detailed review of GroupInsight reporting is available online at <http://www.rsiguard.com/reports>.

### **3.3 Viewing Data with Other Applications**

The UserInsight and GroupInsight applications provide extensive capabilities for reporting on RSIGuard data for organizations using RSIGuard alone. Cority GX2 reporting provides extended functionality for users of myCority (see next section). However, if you have reporting or data analysis needs that are not covered by the tools provided, there are a few options available.

Data export is possible from within the UserInsight application. All of the fields for the individual user are exported into a CSV file that can be loaded into a spreadsheet, database, or other data tool. From within UserInsight, click on the file menu and select Export Data”.

Export is possible from within the GroupInsight application as well. Click file, Export Records and select whether you want the CSV export to include all records or just the currently visible records (i.e result of last search).

If you need to programmatically access data from RSIGuard data files (TID files), Cority can provide your engineering group a DLL with an API to read the TID data files. The API provides a mechanism to open a TID file, read a header with the titles of each field, and to read sequential records (one per day) of data. The API can be utilized by any programming language that can link to and call a DLL. The DLL and documentation can be downloaded from <https://rsiguard.com/download/tools/TIDReaderLib.zip>



### 3.4 myCority Integration

myCority is a comprehensive suite of tools for managing enterprise injury prevention programs. myCority automates ergonomic self-assessments, training, risk analysis, and program management. In large organizations, RSIGuard is usually deployed as an integrated component of myCority (and is often referred to as RSIGuard+myCority). In small and mid-size organizations, RSIGuard is usually deployed as a standalone solution.

This table describes the differences in experience between RSIGuard Standalone and RSIGuard+myCority:

	<b>RSIGuard+myCority</b>	<b>RSIGuard Standalone</b>
<b>Administrators</b>	<p>RSIGuard+myCority's reporting tools are integrated with other Cority tools, and so they are seamlessly available to administrators with all the benefits of role-based-access, and web-based ease of use.</p> <p>RSIGuard's data within Cority can be used to provide a more complete risk picture (e.g. to consider a mouse-related issue resolved because this person rarely uses the mouse, or to identify them as high-risk because of excessive mouse use).</p>	<p>With RSIGuard standalone, you use our suite of desktop-based tools to do reporting (GroupInsight and UserInsight).</p>
<b>IT Staff</b>	<p>Because RSIGuard data storage is generally web-based, there is generally no need to identify any local network resources, and thus there is also no need to do any local configuration.</p> <p>RSIGuard communicates with myCority (online), so an additional configuration step is required to define how the user initially establishes a link to myCority (see discussion below).</p>	<p>If data or profiles are to be networked, some configuration work is required (e.g. creating network folders, setting appropriate access permissions).</p>
<b>Employees</b>	<p>Employee experience is customized based on their assessment-identified risk factors (e.g. ForgetMeNot messages, default settings).</p>	

If your organization uses the myCority, RSIGuard will communicate with the Cority server automatically. Depending on your organization's preferences, RSIGuard+myCority will establish a link with the user's online profile by sending their Windows login name, their email address, or some other identifying piece of information. If the HR data your



organization provides to Cority contains a piece of information that RSIGuard+myCority can determine programmatically (e.g. login name) then the synchronization is automatic. If not, then users must be queried for some piece of information that myCority can use to initially identify who the user is within the Cority (e.g. email address, employee ID).

Once a link has been established, RSIGuard will communicate with myCority daily (or on a different schedule if requested) to transmit usage data, and to receive any server instructions (e.g., new ForgetMeNotes, settings adjustments, informational messages to users) (no PII is exchanged in these daily communications).

myCority is the user-facing online solution from Cority. Cority's GX2 is the solution generally used by administrators. GX2 replaces the GroupInsight reporting tool for most organizations. Additionally, GX2 offers tools for global and group modification of settings that replace those described in this document.

### 3.5 Managing the BreakTimer

BreakTimer is a tool in RSIGuard that reminds users to take breaks when they have worked for too long without resting naturally on their own. The BreakTimer uses a sophisticated algorithm based on short and long-term typing and mousing patterns as well as natural resting patterns to determine when to suggest breaks.

Although the Setup Wizard will help your users set up an appropriate reminder schedule, if users need to fine tune the schedule, the Settings screen allows you much finer control.



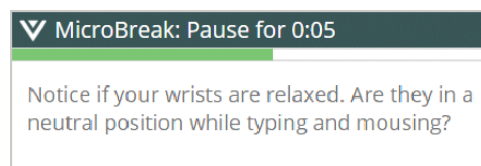
Encourage users to try explore the BreakTimer settings to make simple changes (e.g., more or less frequent breaks, or more or less intrusive breaks). If users want finer control, the settings are very flexible. There is context help throughout by clicking Help or pressing F1.

Remember that some users will resist the idea of being forced to take breaks. They can be helped by changing the Break Interruption Style. It is also important to remind users that taking breaks is proven to be an important component of preventing permanent debilitating injuries. While they may not have symptoms presently, the nature of repetitive strain injuries is that they may not present symptoms until a great deal of scar tissue damage has developed.

If RSIGuard sees a user having trouble taking breaks (e.g., skipping breaks repeatedly), RSIGuard will present the user with a wizard that will help users resolve their issues.

### 3.6 Managing ForgetMeNots

ForgetMeNots is a tool in RSIGuard that reminds users to notice how they are working (by displaying reminder messages). There are two ways that your organization can use ForgetMeNots.



1. As an awareness reminder only – when ForgetMeNots appear, they stay on the screen until the user continues working (i.e. the user need not explicitly close the ForgetMeNot window).

2. As an awareness reminder and a microbreak tool – when ForgetMeNots appear, they stay on the screen until the user stops working and rests for the specified time (by default, 12 seconds).

These “micro” breaks are given in addition to the BreakTimer breaks because research has shown increased benefit from having frequent short breaks in addition to longer, less frequent ones.

The messages ForgetMeNots shows, how it shows them, whether or not it imposes microbreaks, and various other options are configurable in the ForgetMeNots tab of the Settings screen.

For RSIGuard+myCority, ForgetMeNots messages will include messages that specifically address risk issues identified during training.

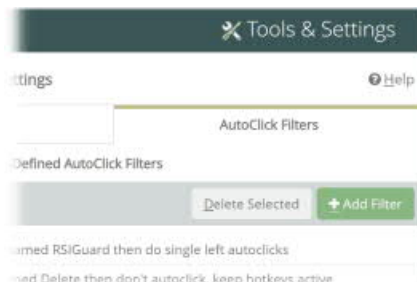
### 3.7 Managing AutoClick

AutoClick is a tool in RSIGuard that provides users a way to eliminate single clicks (and in conjunction with the KeyControl feature, to eliminate the need to click a pointing device at all). The feature works by automatically clicking when the mouse cursor is moved to a new location.

Often IT staff are resistant to provide AutoClick to users because they are concerned that users will have problems with automatic clicking. While some users will initially have trouble, there are good reasons to not only offer the feature to users, but to strongly encourage its use:

- Mouse clicking is, in many organizations, the leading cause of discomfort from computer use.
- AutoClick contains several features that make it easy to use (e.g., smart avoidance of false clicks, audio & video cues for clicks, filters that allow you to customize when AutoClick clicks and when it doesn't).
- Most users will get used to AutoClick fairly quickly if they give it a chance.
- Users can view an AutoClick tutorial during the setup wizard (or access it from the help pages at any time) to help them learn to use AutoClick.

AutoClick generally needs no additional configuration, but AutoClick filters that define when and how AutoClick works can easily be created when desired.



*A filter in the AutoClick Filters setup page that tells RSIGuard not to click on “Delete” buttons is built into the default RSIGuard configuration.*

### **3.8 Managing KeyControl**

KeyControl is a tool in RSIGuard that allows users to create powerful hotkeys that significantly reduce their use of the keyboard and mouse, while simultaneously increasing productivity. Hotkeys can perform simple functions like:

- opening a frequently accessed file
- launching a frequently visited website
- launching a commonly used application
- typing frequently typed text
- mouse-free double-clicking, right-clicking, and drag & drop operations

In addition, KeyControl hotkeys can be used to launch RSIScript macros that can perform complex functions (e.g., launching an application, then tabbing to a field, copying text from that field, switching to a different application, and pasting into that application). In general, non-technical users will require IT staff support to configure RSIScript macros. Your maintenance agreement also provides your IT staff support from Cority to help identify need for macros, and develop macros that your organization may wish to make available to groups of employees.

KeyControl also has an option to allow users to move the mouse cursor with keyboard keys.

### **3.9 Restricted Settings/Features/Menu Items & Administrator Access**

RSIGuard allows you to restrict a user's ability to modify settings. Any individual setting can be locked at a particular value. Furthermore, any individual setting can be restricted to meet any criteria that can be described using RSIScript (see section 3.10 for more information about RSIScript). Thus the value of a setting can be limited to a range, can be dependent on the value of other setting(s), can be dependent on HR data, or other logic. Defining restricted settings is typically accomplished as part of the specification of your custom MSI installation package. For assistance defining these restrictions during specification, or after deployment, please contact your RSIGuard support representative.

RSIGuard also allows you to restrict access to groups of settings (e.g. the ForgetMeNots tab), menu items, and other features, as described in the custom MSI specification spreadsheet.

If you are at a user's computer and need to access restricted functionality (e.g. to enable a feature that by default is not available to employees), you can do so by entering "Administrator Access" mode.

The typical way to authenticate for administrator access is to hold the CTRL key and click on the Toolgear menu. Then, select "Administrator's Access". Depending on how you have configured access to administrator functionality (as specified in the custom MSI spreadsheet specification), you will either be prompted for an Administrator's Access Code. The default access code is 'adminx' but this can be changed before or after RSIGuard is deployed.

Having administrator access to RSIGuard (which is not related to operating system administrator privileges) does not give you any additional security access to any other

computer functionality. And while it allows you to adjust the settings of the RSIGuard instance on the computer on which you are working, it does not increase your security privileges. In general, Cority does not suggest taking significant precautions to prevent users from accessing this mode. However, if your organization is concerned about users having full ability to adjust RSIGuard settings, you can change the access code.

### 3.10 Modifying an Individual's Settings Locally & Remotely

A user can modify their own settings for BreakTimer, Stretching Options, ForgetMeNots, AutoClick, KeyControl and Personalization Options by clicking on RSIGuard's Setup menu and selecting "Settings..."



As described in **Choosing Administrative Configuration Settings** (section 1.6), you can restrict access to some or all of these settings. Although you generally want to let your users customize RSIGuard to maximize its benefit to them, there are times when you will want to force certain settings (e.g., in a call-center, in a high-risk group that needs a certain break schedule, etc.)

There are two ways IT staff can modify an individual's RSIGuard settings.

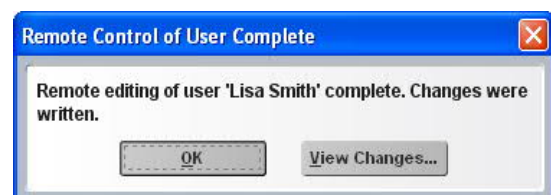
1. Change the setting at the computer (e.g., by having IT staff visit the computer or guide the user over the phone).
2. Use RSIGuard's Administrator Console.

The second option requires that your organization has configured user profiles be stored on a network (see **Choosing Administrative Configuration Settings** (section 1.6)). To modify a user's settings remotely from your own copy of RSIGuard:

1. Click the Start menu, go to the RSIGuard program group, and select Administrator's Console. Enter your admin password – 'adminx' by default). The administrator must have read access in the profiles folder.
2. Select the user to modify and click "View/Edit Settings for Selected User".
3. You will be placed in the settings screen with that user's current settings. Modify the settings you wish to change.



4. Click OK (or cancel) when done. You will see a confirmation that changes to settings were written (if any were made).



Visit the Administrator Console help ([www.rsiguards.com/help/UserMgmt](http://www.rsiguards.com/help/UserMgmt)) for more information about using the Administrator Console.

### **3.11 RSIScript Scripting Language**

In order to provide high flexibility, RSIGuard incorporates a scripting language called RSIScript. RSIScripts can be written to interact with the user, adjust RSIGuard settings, launch applications, open files and websites, perform logic and math operations, adjust the user interface, and more.

To ensure security, RSIScript is carefully designed to not provide functions that allow general read or write access to the user's hard drive or memory.

When we create an MSI installation package, the RSIGuard executable is always the standard executable. What customizes RSIGuard is a set of RSIScripts that are packaged with your installation. Therefore, you can view exactly what customizations you have in any text editor.

When the KeyControl feature is used to create macros, the macros are written in RSIScript.

When RSIGuard uses web registration codes for customization (for smaller licenses), the server responds by returning an RSIScript to customize RSIGuard.

When RSIGuard automatically runs scripts (like various startup and newuser scripts), these are all written in RSIScript.

When RSIGuard automatically runs scripts (like various startup and newuser scripts), these are all written in RSIScript.

You can launch an RSIScript manually from the Tools menu, by selecting "Run RSIScript". In administrator mode, this option will also give you the option of viewing a command line interface to directly issue commands to RSIGuard in RSIScript.

Although most clients will not learn (or need to learn) RSIScript, documentation for the language is available online at <http://www.rsiguard.com/RSIScript>.

### **3.12 Global and Group Modification of Settings**

There are two mechanisms for changing settings on a group-wide or global basis.

For most common changes, you would use the Administrator Console. To modify settings for a group of users, follow these steps:

1. Click the Start menu, go to the RSIGuard program group, and select Administrator's Console. Enter your admin password – 'adminx' by default). The administrator must have read access in the profiles folder.
2. Select the group of users to modify, and click the "Group Settings Change..." button.
3. Select the setting to adjust, the value to adjust it to, and whether or not you want to lock the value you are changing. Verify the users you are about to change (and uncheck any you don't wish to change). Click OK.

For more information on the Administrator Console, see <http://www.rsiguard.com/help/UserMgmt>.

More complex group/global settings changes can also be done that include user interaction, other extensive UI, or more complex algorithmic changes (e.g. changing a value based on an environment variable, or changing a value to be relative to the current value of a setting), can be done using an RSIScript.

When you initially configured RSIGuard, one of the settings you specified was a location for a startup script. This script is generally located on a network file server or on an internet or intranet site. Each time RSIGuard launches, it tests for the existence of this file, and if it exists, executes it.

RSIScript has a facility to specify that certain actions occur to groups of employees by username, department, location, environment variables, and various other mechanisms. Or, an action can be specified to occur to all RSIGuard users. Actions can be specified to occur once or every time RSIGuard starts.

RSIScript can change RSIGuard settings, ask users questions and perform various actions based on answers, and much more. See **RSIScript Scripting Language** (section 3.10).

RSIGuard+myCority users have additional methods of performing group settings changes and default settings changes. Please contact your support representative for more details.



### **3.13 Software Updates**

If your organization has a maintenance agreement, you will receive significant software updates via an updated MSI package (about once or twice a year). The updated package will contain any customizations that are standard for your organization as well as software release notes (which are also available online at <http://www.rsiguard.com/support>).

In addition, you have the option of letting your users download updated executables from our website. If the “Check for RSIGuard Update” menuitem is enabled, users clicking on that option will be told if an update exists. If so, they can automatically download and install it (no user-interaction is required once the user chooses to perform the update).

### **3.14 Additional Support**

RSIGuard is a powerful tool with many intuitive standard features, and a rich availability of more sophisticated tools. If your EH&S or IT staff needs assistance, we are here to help.

For support information, please visit <http://www.rsiguard.com/support>.