Agency Administrator Tools

Sabre Red Workspace User Guide

INTRODUCTION

The Agency Administrator Tool is a feature of The Sabre® Red™Workspace designed for agency administrators. Due to the complexity and power of this tool, it is designed for administrators who have a strong understanding of Sabre Red Workspace and have educated themselves on how to best use the Agency Administrator Tool to benefit their agency.

The Agency's "Ordering Agent" should order this product from Agency eServices.

Change configuration settings

Configuration settings make products available (ON) or not available (OFF) to agents. *Sabre* applies configuration settings to all agencies; however, *Sabre* allows some settings to be optional. In other words, the agency administrator can override *Sabre's* default setting for optional products.

Example:

Sabre turns ON products A and B for your agency, where product A is required and product B is not. All agents in the agency must have product A. However, if the agency administrator does not want the agency's agents to have product B, he/she can turn it OFF to override *Sabre's* default setting. Product B will not install on the agents' workstations.

Activate authorized *Sabre Red Apps* for users

Configuration settings also allow *Sabre Red Apps* that have been acquired via the *Sabre Red App Centre* to be made available (ON) to designated agents. After a *Sabre Red App* has been entitled (authorized) for an agency, it is set to (OFF) for all agents. The agency administrator can then decide which agents will have the *Red App* activated (ON).

Example:

The agency buyer on the *Sabre Red App Center* acquires *Red App* A. Once that app is authorized for the agency, the agency administrator uses the Agency Administrator Tool to activate (turn ON) the app for a designated group of agents. After this step is performed those agents will see the *Red App* appear in their Workspace.

Establish default user settings

Default values can be set for several pre-defined user properties and also allow or deny the user the ability to modify those settings.

Example:

The agency wants to establish a consistent default path for Scribe compilations and force Java TA sharing for all users and prohibit those users from adjusting these settings.

Control when agents receive *Sabre Red Workspace* software updates

Updates are software components that download and install on the agents' workstations. Updates can include a new software release, a fix to a known problem, or a critical update to protect the stability of the *Sabre Red Workspace* application or your data. The agency administrator can lock agents from receiving updates for a period of time to allow the agency more time to test or to verify the changes.

Example:

Sabre announces a new release coming on July 1. On June 30, the agency administrator locks all but three agents. On July 1, only the three agents receive the new updates. The three unlocked agents perform testing, while the other agents continue work without the updates. On July 12, the three agents complete testing. The agency administrator unlocks the remaining agents so they receive the new changes. Then, all agents have the same version.

Allow or block access from designated IP addresses

IP Allow or Deny enables agency administrators the capability to restrict access to *Sabre Red Workspace* unless the user is on an allowed IP address.

Example:

The agency decides they only want agents accessing *Sabre Red Workspace* from within their office headquarters. The agency administrator uses the IP Allow/Deny feature to create a policy of restricting access for all IP addresses except for those utilized by headquarters. As a result of this policy, when a user tries to access the *Workspace* from any other IP address, they will be denied access.

If an agency does not have an agency administrator, the agents within that agency can still use *Sabre Red Workspace*. The differences are described in the table below:

	Without an agency administrator	**With an agency administrator**
Configuration settings	Agents receive products according to *Sabre's* default settings, which consider the agent's geographical location and any contractual obligations	Agents receive products according to *Sabre's* default settings for fixed products. Also, the agency administrator can turn ON or OFF products that *Sabre* deems optional.
Sabre Red Apps	Agents are unable to take advantage of the extended capabilities that can be provided by *Sabre Red Apps*	The agency administrator can determine which *Red Apps* should be active in the agent's *Workspace* and take full advantage of the additional capabilities of *Sabre Red Apps*
Software updates	Agents receive updates as soon as *Sabre* makes the updates available.	The agency administrator can lock one or more agents so they will not receive any available updates. After the agents are unlocked, those agents will receive the updates.
Allow or deny access by IP address	Agents with valid credentials can access *Sabre Red Workspace* from any location	The agency administrator can enact rules to restrict access to *Sabre Red Workspace* based on IP address in accordance with the agency's policies.

BECOMING AN AGENCY ADMINISTRATOR

After an agency decides who will fulfill the role of agency administrator, the agency site administrator must submit a request form via *Agency eServices* at https://eservices-beta.sabre.com/Manager/Ordering/Sabre-Red-Workspace-Agency-Administrator-Order-Form.aspx for each person who needs to be an agency administrator.

Note: More than one person can be an agency administrator for the same agency.

Within three business days, *Sabre* will grant access to the PCC and Agent ID (EPR) provided by the site administrator in each request form.

ACCESSING THE AGENCY ADMINISTRATOR TOOLS

After *Sabre* sets up your PCC and Agent ID with agency administrator rights, you must do the following:

1. Launch *Sabre Red Workspace* (if it is not already running).

2. Download updates in any of the following ways:

    a. Click **Help** on the menu bar, and then click **Check for Updates**

    b. Wait approximately 20 minutes after launching *Sabre Red Workspace*. Then, updates download automatically.

Wait for a few hours with *Sabre Red Workspace* running. Then, updates download automatically.

Note: A message informs you when *Sabre Red Workspace* checks for updates. After the check completes, another message informs you whether updates are downloading or updates are not available.

3. After the download completes, a message asks you to restart *Sabre Red Workspace*. Click to restart.

4. After *Sabre Red Workspace* restarts, the **Admin** menu will be accessible from the Application Launcher Bar at the top of the *Sabre Red Workspace* main window (just below the menu bar). [Note: This menu may have already been available if you had any other administrative tools activated.]

Select the **Admin** menu and then **Agency Admin Tools**. A new tab opens and you see the Agency Administrator Tools main dashboard.

MAIN DASHBOARD

The Agency Adminstrator Tools main dashboard allows you to select an option, depending on the function you want to perform. You can:

1. Manage Groups

    Groups are a method the agency administrator uses to group together agents to later facilitate changing configuration settings or controlling updates against the group.

2. Manage Configurations

    Set-up products, settings, and *Red App* configurations for user groups.

3. Manage Updates

    Lock agents from receiving updates to *Sabre Red Workspace* for a period of up to 30 days.

4. View Change History

    View and export logs of previous changes to configurations and update locks.

5. Allow/Deny Access

Establish rules to prohibit access to *Sabre Red Workspace* based on IP address.

MANAGE GROUPS

The Agency Administrator Tool list all the agents in an agency. For agencies with many agents, these lists can be very long. Trying to change configuration settings for only certain agents or locking only certain agents takes time when finding them in a long list.

Therefore, the Agency Administrator Tools let you put agents into groups that are more manageable than one long list of all agents. You can decide how you want to group your agents together, so that you can change configuration settings or control software updates for an entire group (instead of for each agent individually). At any given moment, you can assign an agent to one group only. Also, to ensure optimal performance, groups sizes should be kept to a manageable size not to exceed 1,000 users per group.

In order to change any configuration settings for any of your agents, you must create at least one group. However, you can lock and unlock one or more of your agents without creating a group.

DECIDING WHETHER TO USE GROUPS

Not every agency needs to create groups. To make this decision, consider:

1. Learn as much as you can about how groups work by reading the documentation and getting familiar with the Agency Administrator Tool.
2. Decide whether you want to change any configuration settings, including the activation of any acquired *Red Apps,* for any of your agents.
    a. If YES, you must create a least one group so that all of your agents are in a group.
    b. If NO, then groups are optional for you.
3. Decide whether you want to lock or unlock your agents to control when they receive *Sabre Red Workspace* software updates.
    a. If YES, then you should consider the number of agents in your agency and the number of agents you will lock and unlock at one time.
    If these numbers are similar to each other, then you may not need to create groups. If the numbers are very different, it will save you time if you create groups and apply locks against those groups.
    For example, if you have 500 agents and you plan to lock all of them at once except for two agents for testing purposes, then you may not need to use groups. On the other hand, if you want to lock all agents except for one agent at each of 30 office locations, then you should create groups to save time while locking and unlocking your agents.
    b. If NO, then groups are optional for you.

ORGANIZING YOUR AGENTS INTO GROUPS

If you decide that you want to create groups, you should plan a strategy for what groups to create. Here are some ideas to consider when determining your strategy:

Who will administer each group	If multiple people will have agency administrator access, you will want groups to reflect their scope of authority or jurisdiction. If the same person is the agency administrator for all groups in your agency, then this consideration is not important. Although multiple people can have agency administrator access, the information each agency administrator sees in the Agent Admin Tools is the same. Each agency administrator sees all groups created for your agency. It is your responsibility to enforce rules with each other so that each agency administrator knows which groups he or she should maintain or own. For example, you may need three groups if your agency has nine office locations and Sue will administer five, Joe three, and Maria one. Each person must know the name of the groups to which they should make changes. Each person should understand that he/she should not make changes to the groups for which he or she is not responsible. Enforcing these rules will prevent one agency administrator from making a change and another agency administrator undoing that change.
Your organizational structure	If certain office locations have a different business model than other locations, then you may want to create a group for each model.
Geographical locations	If your agency will have agency administrators in multiple office locations that can easily be distinguished from each other, then you may want to create groups to match the geography. Examples include: • North, South, East, West • Germany, Italy, France
Type of business function or persona	You may have a mix of business functions and want to create groups that reflect these differences, such as Leisure, Corporate, and Marketing.

If you plan to lock agents while other agents perform additional testing of new software updates, you may want to create two groups: one group of test agents and one group of remaining agents. This will let you lock all the remaining agents and simply leave the group of test agents unlocked.

After you consider how your agency needs to administer your agents and you determine a strategy, you can create groups.

TO CREATE A NEW GROUP

1. From the Agency Administrator Tools main dashboard, select **Create new group** in the **Manage Groups** section and click **Next**.	The Create New Group window opens. The left pane (‘Ungrouped Agents’ section) lists all agents who are not yet assigned to a group. The names are sorted alphabetically by the agent’s last name.
2. In **Group Name**, type a name for the group.	The name you type must be unique. You cannot have more than one group with the same name. Also, you can use

characters only. No special characters or spaces are allowed.

3. In the left pane, locate an agent to add to the group. You can:

   - Scroll down if the list has more rows than will fit in the pane.

   Click a column header. The up or down arrow indicates the column currently sorted and the direction of the sort. You can click the same column header to reverse the sort order; or, you can click a different column header.

   - Select a **Filter by** item from the pull-down menu, type text into the text box, and click **Filter**. The filter applies to any letters or numbers you type. You can click **Clear Filter** to return to all ungrouped agents.

     For example, if you select ‘Agent Last Name’, type ‘bom’, and click **Filter**, the filtered results will show all names that contain ‘bom’.

4. As you locate an agent you want to add to the group, move the agent to the right pane to include them in the group.

   - Click a single row in the left pane (‘Ungrouped Agents’ section) and click **Add**.
   - Select multiple random rows in the left pane by clicking one row, and then pressing the **CTRL** key while you click another row. Both rows are selected. You can repeat this for multiple rows. Then, click **Add**.
   - Select a range of rows in the left pane by clicking on the first row, pressing the **Shift** key while you click the last row in the range. The rows you clicked and the rows in between are selected. Then, click **Add**.
   - Click **Add All** to move all agents shown in the left pane to the right pane. If you have applied a filter, only the filtered agents move to the right pane.

5. If you make a mistake, you can:

   - Click **Undo** to cancel your most recent add.
   - Select one or more rows in the right pane and click **Remove**.
   - Click **Remove All** to move all agents shown in the right pane to the left pane. If you have applied a filter to the right pane, only filtered agents move to the left pane.
   - Click **Cancel** to close this window and discard all changes you made.

6. After the right pane contains only the agents you want to include in the group, click **Save.**

7. A message informs you that *Sabre Red Workspace* will process your request. Click **OK**.

The Agency Administrator Tools main dashboard appears.

Note: All Agency Administrator Tool windows that have an **Undo** button now include a **Redo** button. These windows are: Create New Group, Edit Group, Manage Existing Groups, and Lock or Unlock Agents. The Redo button is inactive until you click Undo. After the Redo button becomes active, it remains active only until you click another arrow key. If you select another user and click an arrow key to move him to the left or right, then the Redo button again becomes inactive. If you made three changes and then clicked **Undo** three times, you can then click **Redo** three times to reapply those changes that you previously undid.

TO EDIT AN EXISTING GROUP

1. From the Agency Administrator Tools main dashboard, select **Manage existing groups** in the **Manage Groups** section and click **Next**.

   The Manage Existing Groups window opens and lists all groups in alphabetical order by group name.

2. Select the group you want to edit and click **Edit**.

3. If you want to change the name of the group, type a new **Group Name**.

4. If you want to add one or more agents to the group, locate the agent in the left pane (‘Ungrouped Agents’) and move the agent to the right pane (the group). You can use the same methods as described in “To Create a New Group”.

5. If you want to remove one or more agents from the group, locate the agent in the right pane (the group) and move the agent to the left pane (‘Ungrouped Agents’). You can use the same methods as described in “To Create a New Group”.

6. After the right pane contains only the agents you want to include in the group, click **Save**.

7. A message informs you that *Sabre Red Workspace* will process your request. Click **OK**.

The Manage Existing Groups window appears. You can perform other functions or you can click **Cancel** to return to the Agency Administrator Tools main dashboard.

TO EDIT AN EXISTING GROUP

1. From the Agency Administrator Tools main dashboard, select **Manage Existing groups** in the **Manage Groups** section and click **Next**.

   The Manage Existing Groups window opens and lists all groups in alphabetical order by group name.

2. Select the group you want to delete and click **Delete**.

3. A confirmation message appears. You can:

   - Click **Delete** to delete the group. The agents that were assigned to this group will become unassigned. If you create a new group or edit a different group, you will see these agents in the left pane (‘Ungrouped Agents’).

Next, a message informs you that *Sabre Red Workspace* will process your request. Click **OK**.

- Click **Cancel** to disregard your request. The group will remain.

The Manage Existing Groups window appears. You can perform other functions or you can click **Cancel** to return to the Agency Administrator Tools main dashboard.

TO FIND THE GROUP ASSIGNMENT OF AN AGENT

You can view a list of all agents already assigned to a group. If you see an agent assigned to a group that you want to remove, you can remove the agent.

1. From the Agency Administrator Tools main dashboard, select **Manage existing groups** in the **Manage Groups** section and click **Next**.

   The Manage Existing Groups window opens and lists all groups in alphabetical order by group name.

2. Select the **Find the group assignment of an agent** option.

   The Manage Existing Groups window lists all ungrouped agents in the left pane and all grouped agents in the right pane. For each agent that is assigned to a group, the right pane shows the group name.

3. In the right pane, locate an agent. You can:

   - Scroll down if the list has more rows than will fit in the pane.
   - Click a column header. The up or down arrow indicates the column currently sorted and the direction of the sort. You can click the same column header to reverse the sort order; or, you can click a different column header.
   - Select a **Filter by** item from the pull-down menu, type text into the text box, and click **Filter**. The filter applies to any letters or numbers you type. You can click **Clear Filter** to return to all grouped agents.

     For example, if you select 'Agent Last Name', type 'bom', and click **Filter**, the filtered results will show all names that contain 'bom'.

4. As you locate an agent, you can see the group to which the agent is assigned in the **Group Name** column. Do one of the following:

   - If you want to return to the Agency Administrator Tools main dashboard, click **Cancel**.
   - If you want to remove one or more agents from the group, you can do any of the following:
     - Click a single row in the right pane ('Grouped Agents' section) and click **Remove**.
     - Select multiple random rows in the right pane by clicking one row, and then pressing the **CTRL** key while you click another row. Both rows are selected. You can repeat this for multiple rows. Then, click **Remove**.
     - Select a range of rows in the right pane by clicking on the first row, pressing the **Shift** key while you click the last row in the range. The rows you

clicked and the rows in between are selected. Then, click **Remove**.

- Click **Remove All** to move all agents shown in the right pane to the left pane. If you have applied a filter, only the filtered items move to the left pane.
- If you make a mistake, you can click **Undo** to undo your most recent move, or click **Cancel** to close this window and discard all changes you made.

- After the right pane contains only the agents you want to include in the groups, click **Save**. A confirmation message appears. You can:
  - Click **Remove** to remove the agents from the group. The agents that were assigned to this group will become unassigned. If you create a new group or edit a different group, you will see these agents in the left pane ('Ungrouped Agents').

    Next, a message informs you that *Sabre Red Workspace* will process your request. Click **OK**.
  - Click **Cancel** to disregard your request. The agents will remain in the group.

The Agency Administrator Tools main dashboard appears.

Note: Deleted PNRs and or PCCs will automatically be removed from the Agency Administrator Tool and new EPRs will come into the tool as ungrouped.

MANAGE CONFIGURATIONS

After you create at least one group, you can view the configuration settings *Sabre* applied to your agency. *Configuration settings* make products available or not available to agents. *Sabre* applies three types of configuration settings:

Fixed settings

These settings are required.

Settings you can change

These settings are optional. The agency administrator can override these settings.

User properties you can override

These are individual user properties that you can override to a default setting.

A fourth type of configuration setting for *Sabre Red Apps* may be available if you have at least one *Red App* entitled (authorized) for use by at least one user in your agency.

When viewing current settings, you can see how many agents have a product or *Red App* turned ON out of the total number of *entitled* agents. An agent is *entitled* to have a product according to geographical location, whether or not your agency has

contractual agreements with *Sabre*, or whether or not a *Sabre Red App* has been authorized for use by your agency via the *Sabre Red App Centre.*

For example, your group may have eighteen agents, where six are located in Country A and the remaining twelve are in Country B. If you view the setting for a product that applies to only Country A, then the number of entitled agents would be six. The remaining twelve are not entitled to have the product.

If you choose not to change the configuration settings, then your agents will receive the default *Sabre* settings.

TO VIEW CONFIGURATION SETTINGS FOR A GROUP

1. From the Agency Administrator Tools main dashboard, select **Change Sabre Red Workspace settings for my agents** in the **Manage Configurations** section and click **Next**.

2. Select the group for which you want to view or change settings, and click **Next**.

3. The Manage Configurations window shows the total number of agents in the group, *Workspace* settings you can change, *Red Apps* settings you can change, fixed settings, and user properties you can override. From this window, you can open or close any of these sub-menus by clicking the arrows.

   Note: The "Configure settings for Workspace" submenu will already be expanded. Collapse this menu to quickly locate the other menus.

4. After a section is expanded, you see a list of products. For each product, you see the number of agents out of the total number of entitled agents that have the product turned ON.

The Manage Configurations window opens and lists all groups in alphabetical order by group name.

- Click the right arrow (▶) to expand a section so you can see the products in that section. While expanded, you see the down arrow (▼).
- Click the down arrow (▼) to collapse a section so you no longer see the products in that section. While collapsed, you see the right arrow (▶).

TO CHANGE THE CONFIGURATION SETTINGS FOR A PRODUCT OR RED APP

1. While viewing configuration settings for Workspace or Red Apps (see "To View Configuration Settings for a Group"), you will see a column next to each product or *Red* App which has the following options:

2. If you click the **ON** or **OFF** option, that setting will be applied to all entitled agents in the group.

3. Click **Save** to apply any setting changes you made.

- **ON** or **OFF** in the 'Change setting to' section

  Note: If an option is already set, it appears inactive. For example, if you already have 10 of 10 entitled agents ON, then the **ON** option is inactive.

- **Keep current setting** is unselected when you change the **ON** or **OFF** setting. This behavior lets you easily see which settings you have changed by looking down the column.

4. A confirmation window appears which lists the changes you requested.
5. A message informs you that *Sabre Red Workspace* will process your request. Click **OK**.

The Agency Administrator Tools main dashboard appears.

- To change the settings, click **Apply Changes**.
- To cancel the changes, click **Cancel**.

TO REVIEW FIXED SETTINGS

1. Expand the “Fixed settings” submenu to see a list of all products that cannot be modified.

TO OVERRIDE DEFAULT USER PROPERTIES

1. While viewing the “Override User Properties” sub-menu, you will see the list of properties you can establish default settings for.

2. Determine if you want to allow the end user to modify (override) your default setting.

- For settings that have predefined values, choose the desired setting from the drop down menu located under the “Override Setting to” column.
- For settings that require a file path, enter the file path into the free text box located under the “Override Setting to” column.
- Select **YES** from the “Allow User Override” column to enable end user overrides.
- Select **NO** from the “Allow User Override” column to restrict changes to your default values.

MANAGE UPDATES

Updates are *Sabre Red Workspace* software components that download and install on the agents’ workstations. Updates can include a new software release, a fix to a known problem, or a critical update to protect the stability of the *Sabre Red Workspace* application or your data.

An agent receives *Sabre Red Workspace* updates as soon as the updates become available from *Sabre*, unless the agent is locked. A *lock* prevents the agent from receiving any software updates for a period of time. There are two kinds of locks:

Sabre lock

Sabre may lock an agent or agency while researching a reported problem.

Agency lock

The agency administrator may lock one or more agents to prevent them from receiving update

For example, an agency wants two agents to receive the updates to validate that the update is safe for the agency environment. In this case, the agency administrator locks all of the agents (except for the two test agents) to prevent them from receiving the updates. The two test agents receive the updates. After they complete their validation and deem the update safe, the agency administrator unlocks the remaining agents so they can receive the updates.

IMPORTANT NOTE: *Sabre* will unlock agents locked by the agency administrator only upon the agency’s request or if a critical update is needed that could impact the security or integrity of the *Sabre Red Workspace* application or its data.

Both of these locks are independent of each other. If either or both locks are enabled, then the agent will not receive *Sabre Red Workspace* updates until both locks are disabled.

If the agency administrator chooses not to lock any agents and *Sabre* has not locked the agents, then those agents will receive *Sabre Red Workspace* updates as the updates become available.

UNDERSTANDING EXPIRATION DATES

An *expiration date* is a date when the lock expires. When the lock expires, the agent will receive all pending software updates. Although the duration between the lock date and the expiration date can vary, the default is 30 days.

A *Sabre* lock may or may not have an expiration date, depending on the reason why the agent was locked. An agency lock always has an expiration date.

The agency administrator can unlock an agent he/she previously locked at any time before the expiration date arrives, or just wait for the expiration date to unlock the agent automatically.

All dates appear in GMT -5 (US Daylight Savings Time or GMT -6 (US Central Standard Time), whichever applies.

UNDERSTANDING RELOCK DATES

After the agency administrator unlocks an agent or the agency lock expires, a relock date is calculated. A *relock date* is the date when an agent can be locked again after being unlocked. Although the duration between the unlock date and the relock date can vary, the default is 5 days.

During the time after the expiration date passes, but the relock date has not yet arrived, the agency administrator cannot lock the agent. The agent does not appear in the list of agents who are not locked.

All dates appear in GMT -5 (US Daylight Savings Time or GMT -6 (US Central Standard Time), whichever applies.

TO LOCK OR UNLOCK ONE OR MORE AGENTS

1. From the Agency Administrator Tools main dashboard, select **Lock or unlock agents from receiving Sabre Red Workspace software updates** in the **Manage Updates** section and click **Next**.

   The Unlock or Lock Agents window opens. The left pane (‘Agent NOT locked by Agency’ section) lists all agents who are unlocked. The right pane (‘Agents Locked by Agency’ section) lists all agents who are currently locked by the agency administrator. The names in both panes are sorted alphabetically by the agent’s last name.

2. If any agents are locked by a *Sabre* lock, an icon appears in the **Sabre Lock** column. To view information about this lock

   1. Click to highlight the row that contains the *Sabre* lock icon.
   2. Click **View Sabre Lock Details**.

      The Lock Details window opens and shows the date the agent was locked and the expiration date. If the expiration date is ‘None’, then the agent will remain locked until *Sabre* unlocks the agent.
   3. Click **Close**.

3. To lock an agent:

    1. In the left pane, locate an agent you want to lock. You can:

        - Scroll down if the list has more rows than will fit in the pane.
        - Click a column header. The up or down arrow indicates the column currently sorted and the direction of the sort. You can click the same column header to reverse the sort order; or, you can click a different column header.
        - Select a **Filter by** item from the pull-down menu, type text into the text box, and click **Filter**. The filter applies to any letters or numbers you type. You can click **Clear Filter** to return to the original list.

          For example, if you select 'Agent Last Name', type 'bom', and click **Filter**, the filtered results will show all names that contain 'bom'.

    1. As you locate an agent you want to lock, move the agent to the right pane to include them in the list:

        - Click a single row in the left pane ('Agents NOT Locked by Agency' section) and click **Add**.
        - Select multiple random rows in the left pane by clicking one row, and then pressing **CTRL** key while you click another row. Both rows are selected. You can repeat this for multiple rows. Then, click **Add**.
        - Select a range of rows in the left pane by clicking on the first row, pressing the **Shift** key while you click the last row in the range. The rows you clicked and the rows in between are selected. Then, click **Add**.
        - Click **Add All** to move all agents shown in the left pane to the right pane. If you have applied a filter, only the filtered agents move to the right pane.

4. To unlock an agent, repeat the above steps except use the names in the right pane instead of the left pane, and use the **Remove** and **Remove All** buttons instead of **Add** and **Add All**.

5. If you make a mistake, you can:

    1. Click **Undo** to undo your most recent move.
    2. Select one or more rows in either pane and click **Add** or **Remove**.
    3. Click **Add All** or **Remove All** to move all agents shown in the pane to the opposite pane. If you have applied a filter to the source pane, only filtered agents move to the opposite pane.
    4. Click **Cancel** to close this window and discard all changes you made.

6. After the left pane contains only the agents you want unlocked and the right pane contains only the agents you want locked, click **Save**.

7. A message informs you that *Sabre Red Workspace* will process your request. Click **OK**.

   Note: Be aware that lock requests happen very quickly; however, it takes more time to process unlock requests.

   Note: Once a lock request is saved, and followed subsequently by an unlock request, the "relock" process described under "Understanding Relock Dates" applies.

8. The Agency Administrator Tools main dashboard appears.

TO VIEW AGENTS YOU CANNOT LOCK UNTIL THE RELOCK DATE ARRIVES

1. From the Agency Administrator Tools main dashboard, select **View agents you cannot lock** in the **Manage Updates** section and click **Next**.

   The Agents You Cannot Lock window opens. All agents appear in alphabetical order by last name.

2. You can sort and filter by using the same methods as described in "To Lock or Unlock One or More Agents".
3. After you locate the agent, you can see the relock date in the right column.
4. When you finish, click **Close**.

The Agency Administrator Tools main dashboard appears.

After the relock date passes, these agents appear automatically in the 'Agents NOT Locked by Agency' section of the Unlock or Lock Agents window.

TO VIEW CHANGE HISTORY

To view a list of changes made by your agency in the last 30 days

1. From the Agency Administrator Tools main dashboard, select **View history of group and setting changes** in the **View Change History** section and click **Next**.

   The View history of group and setting changes window opens. This table lists the last 1,000 changes made by all users assigned to the agency's administrator role. These changes include altering groups or configuration items. The default sort order displays the most recent entries at the top. Click any column header to sort the contents in the order of the column selected. Click the column header again to sort in the opposite direction.

Date/Time	The date and time the entry occurred.
Edited By ID	The Sabre ID of the person at the agency who made the change.
Edited By Name	The last name, first initial of the person at the agency who made the change.

Change Type	Create, Update, Delete, Assign, or Unassign.
Group Name	The name of the agency group.
Agent Name	The Last name, first initial of the agent who was assigned to or removed from the agency group. This column is blank when you create the group.
Agent ID	The Sabre ID of the agent who was assigned to or removed from the agency group. This column is blank when you create the group.
Product Name	The Product name if you change a configuration setting. This column is blank otherwise.
New Setting	The new configuration setting for a Product. This column is blank otherwise.

2. From the Agency Administrator Tools main dashboard, select **View history of lock and unlock changes** in the **View Change History** section and click **Next**.

The View history of lock and unlock changes window opens. This table lists the last 1,000 changes made by all users assigned to the agency's administrator role. These changes include applying or removing agency locks. The default sort order displays the most recent entries at the top. Click any column header to sort the contents in the order of the column selected. Click the column header again to sort in the opposite direction.

Date/Time	The date and time the entry occurred.
Edited By ID	The Sabre ID of the person at the agency who made the change.
Edited By Name	The last name, first initial of the person at the agency who made the change.
Agent Name	The Last name, first initial of the agent who was locked or unlocked.
Agent ID	The Sabre ID of the agent who was locked or unlocked.
Change Type	Lock or Unlock

3. Click **Export Log** to export the Change History data for configuration changes or locks into a fil in *.csv format.

4. Click **Close** to return to the main Agency Administrator Tool dashboard.

TO RESTRICT ACCESS TO SABRE RED WORKSPACE BASED ON IP ADDRESS

NOTE: The IP Allow/Deny capabilities are highly technical and are geared toward admins that have a thorough understanding of IP addresses and agencies with the technology requirements (such as a fixed public IP address) to leverage it. Without this understanding and setup, users may be locked out of the Sabre Red Workspace erroneously.

To set up access policies based on the users IP address:

1. From the Agency Administrator Tools main dashboard, select **Create/Update access policy** in the **Allow/Deny Access** section and click **Next**.

   The "Create/Update access policy" window opens.

2. To add a rule, select "Add Rule" from the top left corner of the window.

3. Click the space labeled "<click here to add users and/or PCC's>" under the "PCCs and/or User IDs" column.

   The "Choose users and PCCs for this rule" pop-up will appear.

   - The list will have any PCCs and the respective users you can control within the Agency Administrator Tool
   - The list starts with the PCC and then is followed by the users in the PCC. If you have access to control more than one PCC, the subsequent PCCs and users will appear after the first group.

   Select the PCCs and/or individual users for this rule.

4. Select to create a "Deny" or "Allow" rule under the "Action" column.

   An **ALLOW** rule will enable access to the defined list of PCCs or users only if they are accessing the *Sabre Red Workspace* from one of the defined IP addresses. Access is prohibited for these PCCs or users on all other IP addresses.

   A **DENY** rule will prohibit access to the defined list of PCCs or users if they try to access the *Sabre Red Workspace* from any of the defined IP addresses. Access is allowed for these PCCs or users on all other IP addresses.

5. Enter the IP Address or IP Address Range for this rule by clicking on the space labeled "<click here to add IP addresses>" under the "IP Addresses or IP Address Range" column.

   To enter a single IP address rule, just enter the desired IP address, i.e. 10.10.10.10

   To enter an IP address range, enter the first IP address of the range followed by a dash (-) followed by the last IP address of the range, i.e. 10.10.10.10-10.10.10.99.

   - This rule would apply to all IP address from 10.10.10.10 through 10.10.10.99. For example 10.10.10.50 would be included in this rule.

6. To save and activate the rule, select "Save."

7. To cancel your work on this rule, select "Cancel."

8. To delete any rule in the list, select the rule by clicking on any component of the rule, and then select “Delete Rule” from the top left corner of the window.

IP ALLOW / DENY RULE CONFLICT RESOLUTION

The IP allow / deny functionality allows for multiple rules to be established for an individual user. For example, you may set up one rule for an entire PCC and another rule for a specific individual within that PCC. The table below depicts which rule would apply when conflicts exist.

	I-A-U	I-A-P	E-A-U	E-A-P	I-D-U	I-D-P	E-D-U	E-D-P
I-A-U		Allow	Allow	Allow	Allow	Allow	Deny	Deny
I-A-P	Allow		Allow	Allow	Allow	Allow	Deny	Deny
E-A-U	Allow	Allow		Allow	Allow	Allow	Allow	Allow
E-A-P	Allow	Allow	Allow		Allow	Allow	Deny	Allow
I-D-U	Allow	Allow	Allow	Allow		Deny	Deny	Deny
I-D-P	Allow	Allow	Allow	Allow	Deny		Deny	Deny
E-D-U	Deny	Deny	Allow	Deny	Deny	Deny		Deny
E-D-P	Deny	Deny	Allow	Allow	Deny	Deny	Deny	

Legend:

- E = Explicit – A rule that has been directly associated to a user or PCC, i.e. an “Allow” rule assigned to user ABC on IP address 10.10.10.10, is an explicit allow rule for user ABC only for IP address 10.10.10.10.
- I = Implicit – A rule that has been indirectly attributed to a user of PCC, i.e. an “Allow” rule assigned to user ABC on IP address 10.10.10.10, creates an implicit “Deny” rule for user ABC on all other IP addresses.
- A = Allow - Allow access based on the IP addresses entered.
- D = Deny – Deny access based on the IP addresses entered.
- U = User – This is a rule applied to the user, i.e. an “Allow” rule assigned to user ABC.
- P = PCC – This is a rule applied to an entire PCC, i.e. an “Allow” rule assigned to a PCC.

For an example of how this conflict resolution works, assume we have two rules that have been created.

Rule 1: A “Deny” rule for user ABC on IP address 10.10.10.10.

Rule 2: An “Allow” rule for PCC XYZ1 (which includes user ABC) on IP address 10.10.10.10.

Based on the conflict resolution table, Rule 1 is an explicit deny rule for a user (E-D-U), while Rule 2 is an explicit allow rule for a PCC (E-A-P). If we look at the table above where these two rule types intersect (highlighted in yellow), we will see that this user will be denied access. That is because the explicit rule assigned to the user holds a higher priority than the explicit rule applied to the entire PCC.

NOTE: You should always be aware that for every explicit rule created, an implicit rule is also put into effect. Using Rule 2 from above as an example, an implicit Deny rule has been created for all users within PCC XYZ1 on all other possible IP address except 10.10.10.10.