Create New Group in the Web Control Center

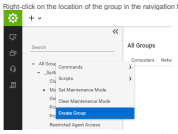
Overview

ConnectWise Automate® comes with several default groups; however, you may find that you may need to add extra groups to suit your business needs. Refer to Default Groups for a list of default groups that come pre-configured with an Ignite installation.

Add a New Group

To create a new group in the Web Control Center:

1. Navigate to **Groups**.
2. Right-click on the location of the group in the navigation tree and select **Create Group**.

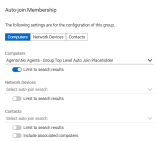


3. Enter a descriptive group name so it is easily identifiable.

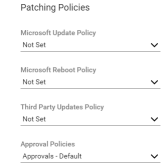
4. Select a group **Type** from the drop-down. If you are creating a sub-group, the type is inherited from the parent group. Each group type is explained in further detail below:

   - **Exclusions:** Allows you to create exclusions to limit users from specific computers. Regardless of the settings set on the Groups and Clients tab of the user configuration, if the user is a member of an exclusion group, then all computers in that group are denied to that user. For example, if the technician John Doe has been given access to the group All Agents, then he has access to every agent in Automate. However, if there are select computers that you do not want John Doe to have

access to, you can create a new group (e.g., Boss's laptop), give it a group type of Exclusion, and include John Doe in this exclusion group. Exclusion groups do not affect Super Admins or those users with the Computers > Show All > Access user class permission checked.
   - **Organizational:** Allows you to organize your groups. For example, in the initial installation or upgrade of Automate, all groups are set to original and all original and all patching groups display in the Patch Manager making the Patch Manager more time-consuming to navigate. You can change the original groups to organizational and only have the patching groups displayed in the Patch Manager.
   - **Original:** Original type does not limit the application of rules to the group. All default groups packaged with Automate have the group type original. These can be changed to any group type.
   - **Patching:** Allows you to limit the groups that appear in the Patch Manager. By utilizing the patching Type, only this group and groups with the original Type are displayed in the Patch Manager.
   - **Permissions:** Limits the security of certain groups, allowing access to other groups without granting full access. Only groups with the type permissions and original are used to locate computers to which the user has access. If a user is assigned to a specific client in the user configuration (Groups and Clients tab) and that client is not assigned to an original or permissions group, the user does not have access to that client. If a user has access to four groups and only one group is a 'permissions' group, then the user is only able to see the computers in this one group. This feature is especially useful if you have a large team of technicians that need to be able to see all groups but only need access to computers in certain groups.
5. Click **CONFIRM**.
6. Locate the newly created group in the navigation tree using the Search bar. You may need to refresh the screen for the group to appear.
7. Click the **Settings** tab.
8. Enter a **Description** for the group. This field has a maximum character limit of 1024 characters.
9. For computer groups, select the agent template to apply to this group from the **Templates** drop-down. This is the configuration template to apply to the members of this group. Template settings cascade down to all sub-groups that do not have a template set for them. For more detailed information on how to create templates and their usage, please refer to Create a New Agent Template.
   Note: For contact and network device groups, leave the template **Name** and **Priority** drop-downs as the default selection. Templates will only apply settings to agents and will not have any impact on contacts or network devices that are members of the group.
10. For computer groups, select the template priority from the **Template Priority** drop-down. If a computer belongs to multiple groups, it could have multiple templates set for them. If this is the case, the templates are merged together and applied to the computer. If there are different values for the same configuration item in the templates then the templates are applied in priority order 0-10 (with 0 being the highest priority). The default template has a priority order of 10, meaning it is applied to all agents in the group.
    Note: Templates are auto-applied to a computer or group of computers when the Update Config command is received. The configuration is updated automatically, based on the schedule set in the template. However, this can be done manually by right-clicking on the client, location, computer or group and selecting **Commands** > **Inventory** > **Update Config** for an immediate change.
11. Click to indicate if the group contains **Computers**, **Network Devices**, or **Contacts**. This also allows you to edit the related fields below.



12. Select the auto-join search to use when adding new computers, network devices, or contacts to this group from the drop-down. The **Auto Join Searches** section allows you to automatically assign members to the group based on the selected search. These search options are pulled from existing searches. Any member that is detected by the selected search will become a member of this group when the search runs, approximately every 6 minutes. Refer to Using Searches for more information on creating searches.
    Note: The **Auto Join Search** capability is important in maintaining a consistent delivery. Auto join searches give a consistent, predictable result and let you drive a consistent policy to all group members.
13. Click the **Limit to search results** toggle to enable dynamic ejection from the group of members that do not match the search criteria. When selected, members that are not detected by the selected search, are ejected from the group. Otherwise, if not selected, members are not automatically ejected based on the search.
14. For contacts, toggle the **Include associated computers** to add computers to the group that is associated with the contact found by the search. A contact is considered associated with a computer if they have logged onto the computer in the last 30 days or if the contact is assigned to the computer.
15. Groups with the type **Patching** have an additional section. Use the drop-downs to select the policies to apply to the group.



There are four types of patching policies that can be defined:

- Microsoft Update Policies - Defines the patch installation settings for Microsoft updates. You can define pre-install and post-install scripts as well as optional settings such as daytime patching and creating a restore point. Scheduling options consist of defining a specific day of the week, date(s), or day(s) along with the start time and duration.
- Third Party Update Policies - Extends your patching capabilities beyond Microsoft updates to third-party applications such as Adobe® Reader, Adobe Flash, Java™ Runtime, and more. Third Party Update Policies are integrated into Patch Manager as a licensed add-on option. If the system does not verify a valid license, this screen is disabled.
- Microsoft Reboot Policies - Defines when a reboot occurs on a device. There are four types of reboot policies, and each defines when the device is rebooted based on patching.
- Approval Policies - Controls the circumstances and conditions in which patches are approved or denied. A series of rules allows patches with a Not Set patch approval status to be automatically approved, ignored, or denied based on the patch's severity, category, title, or CVSS score.

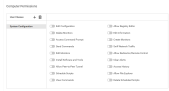
16. Groups can be synced to a client or location. Under **Linking**, select the appropriate **Company** and **Site** to add all new computers, contacts, and network devices for this client and/or location to this group. This creates an auto-join for that client/location.
    Note: If a group is linked to the client or location, when this group is double-clicked on the navigation tree, the client or location will open. Holding down the **[Shift]** key and double-clicking will allow you to edit the group settings.

17. Select a **Maintenance Window** from the drop-down, if applicable. Maintenance windows suppress incoming alert template actions at specific times on a daily or weekly basis.

- Computer groups: Select the desired maintenance window. This applies to all agents that are members of the group.
- Contact groups: The selected maintenance window applies to computers that are associated with contacts in this group. This maintenance window only applies if the computer has been added to the group by the contact using the Join Computers checkbox.
- Network Device groups: Leave the default maintenance window for network device groups as Not Selected. Maintenance windows do not apply to network devices because these assets cannot be placed into maintenance mode.
  Note: To create a new maintenance window, click **Create a New Window**. For more detailed information on how to create maintenance windows and their usage, please refer to Maintenance Windows.

18. In the **User Classes** section, click the **Add a User Class** icon and select the appropriate user class to apply to this group. After the user class has been added, select the specific Group Computer Permissions to apply using the toggles on the right. Group permissions are inherited from the group's parent (e.g., Agent Types.Windows Servers inherits its permissions from the Agent Types parent group). After permissions are defined on a group, all sub-groups inherit them. Group permissions only apply to computers that are members of the Group, not contacts or network devices.

    Note: If no permissions are assigned to the Group, it will look at the permissions set for the Client. If there are permissions assigned to the Client and to a Group, any computers that are associated with both, the permissions will be combined. For more detailed information on group permissions, refer to Assign User Permissions to a Group and for overall permissions, refer to Assign Permissions.
    Note: To remove a user class, select the user class and click Delete.



19. Click **Show advanced settings**.
20. The **Group Membership Control** section controls group membership when a member gets added to a group when it already exists in another group. There are three settings for the **Group Membership Control** section: **Regular**, **Master**, and **Non-Master**.
    - **Regular**: When a member joins a Regular group, no members are removed or added to any additional groups. This is the default setting for new groups.
    - **Master**: When a member joins a Master group, the member is removed from all other Non-Master Groups.
    - **Non-Master**: Members of a Non-Master group can be removed from the group when the member joins a Master Group.
21. Click **SAVE**.