Worry Free - Endpoint Management

In This Article

Overview

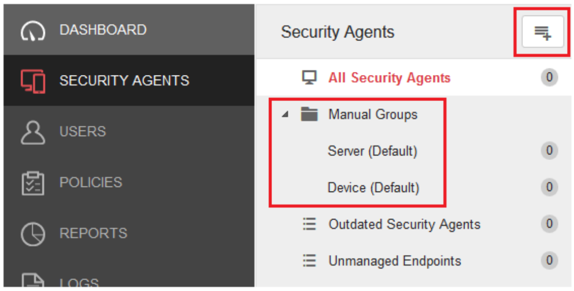
This section of the getting started guide covers endpoint management including manual groups, filter groups, global policies, policies assigned to manual groups, and the policy settings you should review and configure to manage your endpoints based on your organizational requirements.

Manual Groups

Security Agents > Manual Groups

Manual Groups are custom groups that you create to categorize your endpoints and apply custom policies. Each group has its own set of policy settings, and the policy settings can be copied/replicated to other groups. **To create new groups**, click the Add icon in the top-right of the Security Agents area.

> **Note**: The groups cannot be nested, and they are sorted alphabetically.

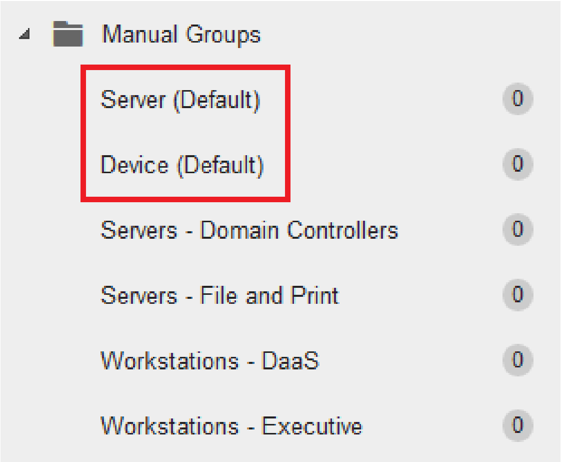


Default Manual Groups

The default groups are the permanent, out-of-the-box groups used to apply policies against endpoints that have not been assigned to a custom group or a domain group if AD sync is enabled. Both of the default groups have their own set of policies.

The **Server (Default)** group is for endpoints running Windows Server. The **Device (Default)** group is for endpoints running Windows client operating systems, Mac OS, Android, and iOS.

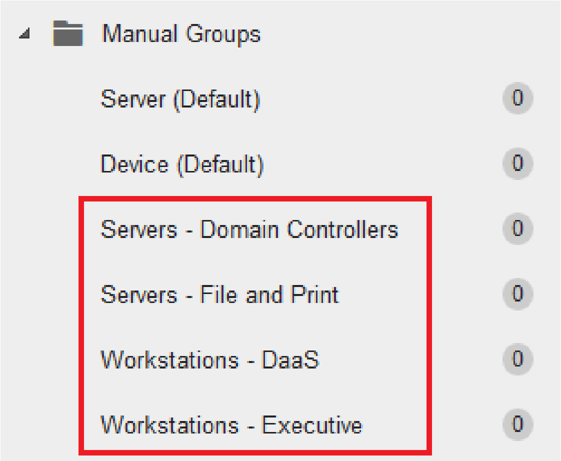
> **NOTE**
>
> **Evolve IP** can define the default policy settings to get you started. However, we strongly suggest you take the time to become familiar with all of the policy settings, and make changes based on your requirements.



Manual Groups	
Server (Default)	0
Device (Default)	0
Servers - Domain Controllers	0
Servers - File and Print	0
Workstations - DaaS	0
Workstations - Executive	0

Manual Group Naming Suggestions

Here are some suggestions when creating manual groups for your endpoints.



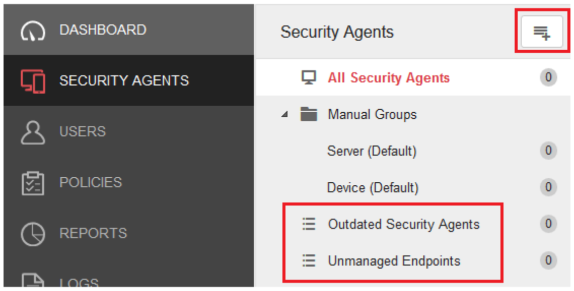
Manual Groups	
Server (Default)	0
Device (Default)	0
Servers - Domain Controllers	0
Servers - File and Print	0
Workstations - DaaS	0
Workstations - Executive	0

Filter Groups

Manage endpoints based on specific criteria, such as an IP address range or operating system. There are two default, out-of-the-box filter groups to start with. **To create new filters**, click the Add icon in the top-right of the Security Agents area.

Filter criteria include:

- Endpoint Name
- Endpoint Type
- Operating System
- Manual Groups or Domain Groups
- Label
- IP Address
- Last Connected Time



Global Policies

One might think you go to the **POLICIES** section to manage all polices within Worry Free. However, this is not the case. Instead, you go here to manage **global policy settings**.

Global Policy settings apply to all managed endpoints in your Worry Free tenant. This includes:

- Global scan settings
- Locking down the agent installations and checking agent status
- Agent uninstallation restrictions
- Application Control Rules
- Exception Lists
  - Web Reputation / URL Filtering
  - Malware Scan Exclusions (Applies to Real-Time, Behavior & Machine Learning)*
  - Device Control

***IMPORTANT**

The Global Malware Scan Exclusions **do not allow wildcard characters**, and you cannot exclude folders. Each exclusion must be a full path to the file being excluded (EXE, PS1, PST, ZIP, etc.).

However, policies configured against manual groups or a domain group (AD synced OU), **do accept the wildcard * character** for folders and files.

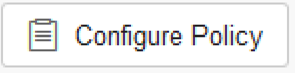
NOTE

Where applicable, the global exception lists can be overridden by policy settings configured against a manual group or a domain group (AD synced OU).

Policy Groups

Policies Applied to Manual Groups

Each **Manual Group** in Worry Free has its own set of policy settings. To access a group's policy settings, select the group, and click the **Configure Policy** button.

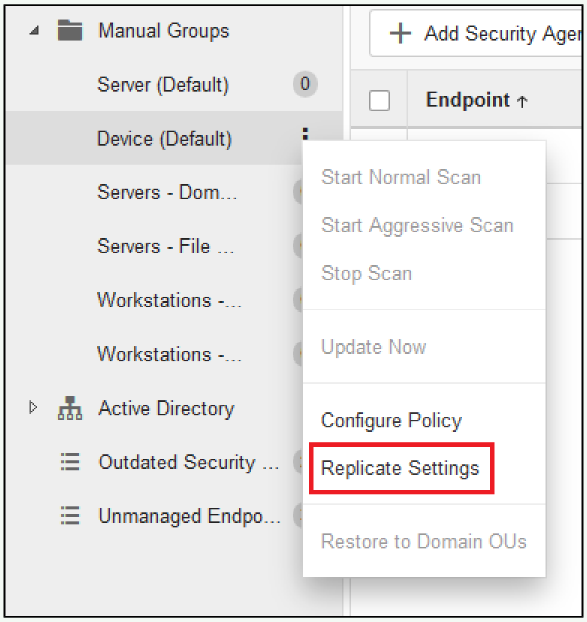


TIP

The policy settings for a manual group can be copied/replicated to another group.

In larger deployments, we recommend creating some empty groups and pre-configure them with certain settings that can be replicated to new groups in the future. For example, you could create a few groups with the word TEMPLATE in their name. Each template group would have a different set of policies settings, which you can replicate to new groups as a starting point.

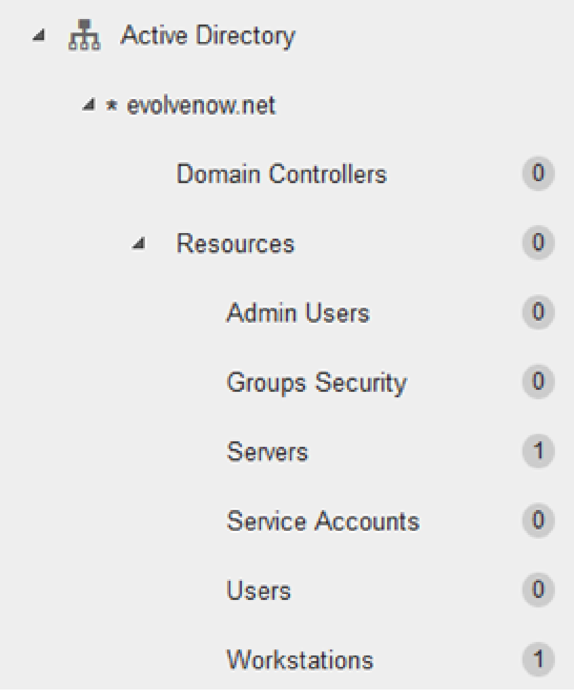
Here's a screenshot of the menu item to replicate settings from one group to another.



Policies Applied to Domain Groups

Domain groups are created when you **sync your Active Directory (AD)** organizational unit structure to Worry Free. Each OU in your AD is represented as a Domain Group.

When it comes to policy settings, domain groups follow an inheritance architecture with each group inheriting the policy settings of its parent group. If needed, you can break the inheritance.

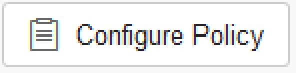


- Active Directory
  - * evolvenow.net
    - Domain Controllers 0
    - Resources 0
      - Admin Users 0
      - Groups Security 0
      - Servers 1
      - Service Accounts 0
      - Users 0
      - Workstations 1

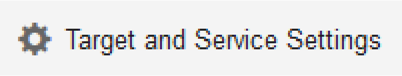
Configure Policy Settings

Policy settings are configurable in all **Manual Groups** and all **Domain Groups** when syncing Active Directory. The settings in a Manual Group can be replicated to another Manual Group. The settings in Domain Groups are inherited from their parent group, but the inheritance can be broken.

For detailed information about each setting, consult the online help from within the **Worry Free management console**.



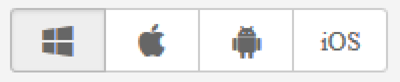
Policy: Target & Service Settings



From here you can do the following:

- Enable the Unauthorized Change Prevention Service on Windows Server and Windows Desktop endpoints (hover over the info icon for more information).
- Check which Manual Group or Domain Group the policy is targeting. If you forget which policy you are editing, check here instead of closing the policy editor.
- If you have configured AD sync, you can restore a broken policy inheritance for a domain group.

Policy: Operating System & Device Type



Choose an operating system to configure in the policy. If needed, turn off all policy modules for the operating systems that will not be configured for the policy. For example, if you're configuring a policy for Mac computers, turn off all of the modules in the Windows operating system.

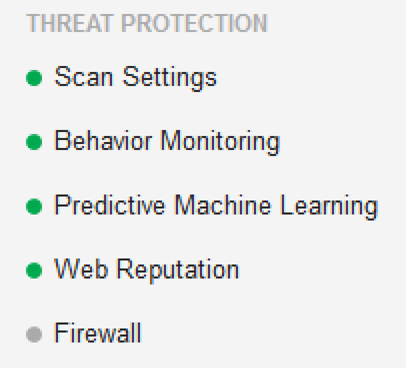
Note that the Windows operating system has the most policy settings. The others are limited in the amount of settings.

Policy: Threat Protection Settings

Select the modules you wish to enable/disable & configure.

NOTES

- Behavior Monitoring & Firewall are only available on the Windows OS.
- For scan settings in a virtual environment (DaaS):
    - Use Trend's IntelliScan feature.
    - Configure real-time scanning for file creation and modifications (writes) only.
    - Do not scan mapped drives or network shares.
    - Do not configure scheduled scans on virtual desktops if you are redirecting folders to a file server or using FSLogix profile redirection.
    - If you choose to configure scheduled scans anyway, make sure the CPU usage setting is set to LOW.
    - Do configure scheduled scans on file servers.



THREAT PROTECTION

🟢 Scan Settings

🟢 Behavior Monitoring

🟢 Predictive Machine Learning

🟢 Web Reputation

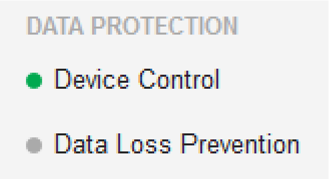
⚪ Firewall

Policy: Data Protection Settings

Select the modules you wish to enable/disable & configure.

NOTE

Device Control is available for the Windows & Mac OS. Data Loss Prevention is only available for the Windows OS.



DATA PROTECTION

🟢 Device Control

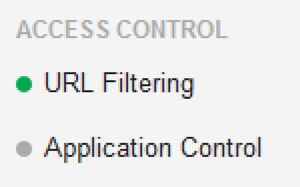
⚪ Data Loss Prevention

Policy: Access Control Settings

Select the modules you wish to enable/disable & configure.

NOTE

The URL Filtering is available for the Windows & Mac OS. Application Control is only available for the Windows OS.



ACCESS CONTROL

● URL Filtering

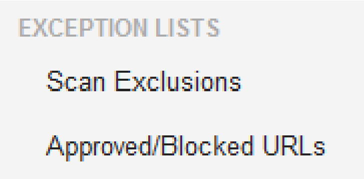
● Application Control

Policy: Exception Lists

These exception lists override the global exception lists. They are not in addition to the global exception lists.

Also, there is no way to copy a global exception list into these exception lists. So, plan accordingly, and consider creating empty group templates as described in the above policy groups section. This will allow you to make changes to the template group, and then copy/replicate the changes to other groups.

> **NOTE**
>
> Blocked URLs are not available on the Mac operating system.



EXCEPTION LISTS

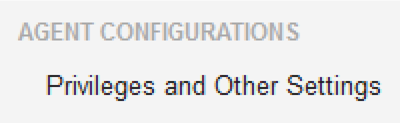
Scan Exclusions

Approved/Blocked URLs

Policy: Agent Configuration Settings

Manage a user's interactions with the agent installed on their endpoint. This includes giving a user the permissions to run a manual scan, view firewall settings, and configure alert settings.

You can also prevent users and other processes from modifying the Trend Micro program files, registries, and processes. Enabling this setting is highly recommended.



AGENT CONFIGURATIONS

Privileges and Other Settings

Ransomware Protection

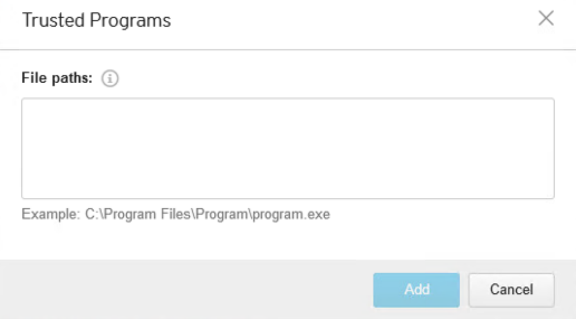
The ransomware protection in Worry Free uses the Behavior Monitoring feature within the agent. Because ransomware is a rapidly moving target, the behavior monitoring feature will likely cause some false positives.

To deal with these false positives, you'll need to exclude certain applications from being watched by behavioral monitoring, which can be done globally or within each individual policy.

Global Exclusions

To exclude apps globally: Policies > Global Exception Lists > Trusted Windows Program List

- The Trusted Program List **does not accept wildcard characters**. It must be a full path to the program.



Trusted Programs

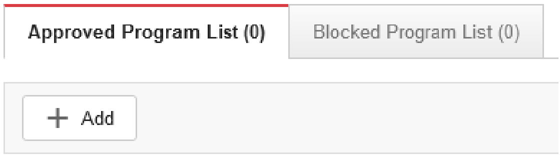
File paths:

Example: C:\Program Files\Program\program.exe

Policy Group Exclusions

To exclude apps in a policy: Windows OS > Exception Lists > Scan Exclusions

- Scroll down to the Behavior Monitoring section, and add your path to the Approved Program List.
- The Approved Program List **does accept the “*” wildcard character**, but you should be careful when excluding entire folder trees.



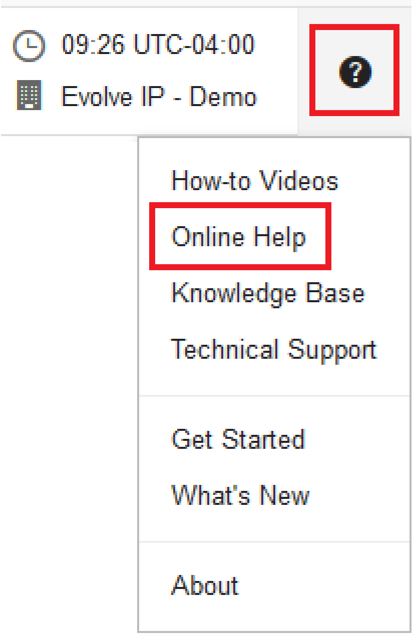
Getting Help

The Worry Free management console has a very robust online help system. For detailed information and step-by-step instructions, you should reference the online help system. If you are new to Worry Free, check out the How-To Videos provided by Trend Micro.

TIP

If you're not signed in to the Worry Free management console, the complete Trend Micro Worry Free Services online help can be referenced in the **Trend Micro Online Help Center**.

If you need further assistance, please submit a ticket via the **Evolve IP Support Page**, or use the information listed in the Worry Free Technical Support page.


09:26 UTC-04:00
Evolve IP - Demo
How-to Videos
Online Help
Knowledge Base
Technical Support
Get Started
What's New
About