



Altorra PowerShield Whitelist User Guide

April 2024 – v1.2

Table of Contents

1. Introduction	4
2. Installation	4
3. Upgrading	4
4. PowerShell Whitelist Menu	5
5. How it works	6
6. Setting up the PowerShell Whitelist application	7
6.1 Configuration Page	7
<i>Enable email filtering</i>	8
<i>Whitelisted external email addresses</i>	8
<i>Whitelisted Gmail addresses</i>	8
<i>Send when no recipients found</i>	9
<i>Log Messages</i>	9
<i>Keep logs for # days</i>	10
6.2 Whitelist Group	11
7. Using the PowerShell Whitelist	12
8. Logs	13
9. Support	13

1. Introduction

The Altorra PowerShield Whitelist application offers better control of email notifications in your sub-production instances, preventing unintended spam to users that exist in both sub-production and production instances. Over and above what ServiceNow base functionality is capable of, the PowerShield Whitelist allows selecting who receives email notifications through group membership and for external email addresses.

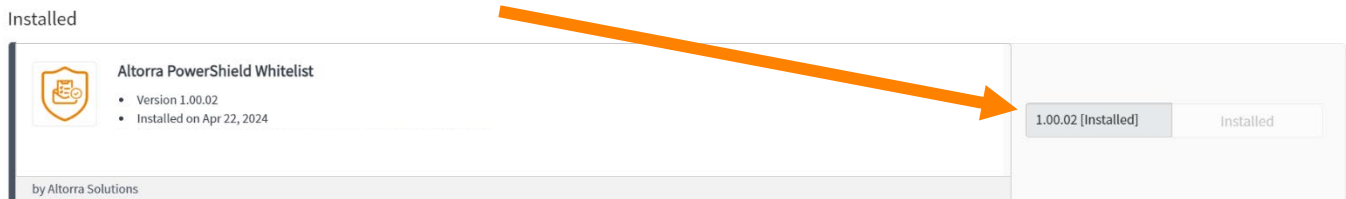
2. Installation

IMPORTANT NOTE: Although the application can be installed in production instances for clone-back purposes in advance of instance upgrades, it should typically be “enabled” (see configuration in section 6.1) in sub-production instances.

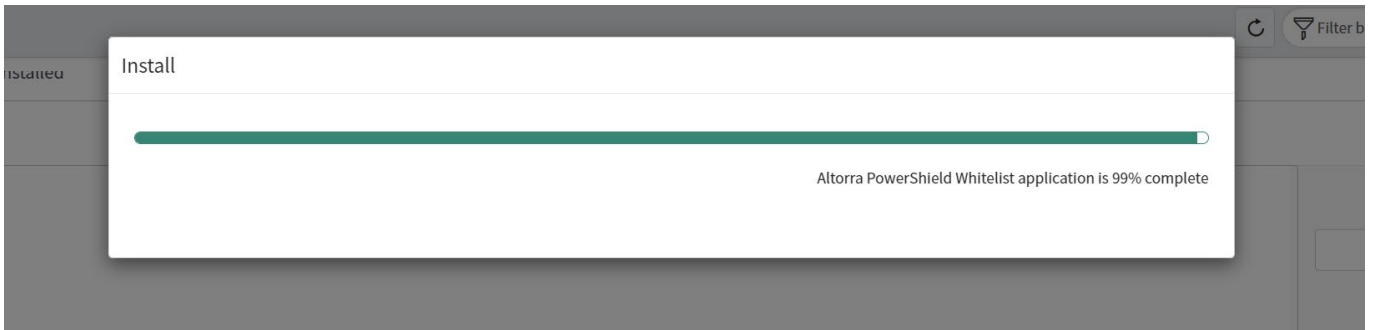
3. Upgrading

Altorra will release updates to the tool as required. They can be accessed via **All->System Applications->All Available Applications->All**

The installed version will be displayed. If there is an update available, a dropdown menu will show options. Once selected, the dialog box next to the version will change from **Installed** to an **Update** button. Click on the Update button. A pop up will appear. Click on the **Install** button on the pop up.

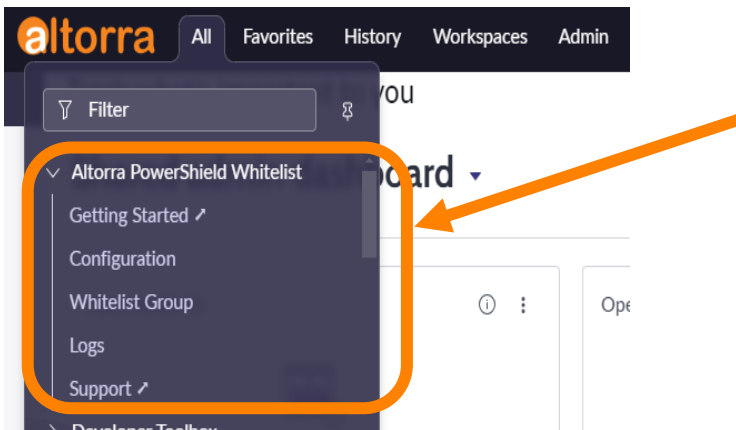


A progress bar will appear during installation/upgrade. After a few minutes, a Success status will be displayed if the installation was successful. Please note, the progress bar may pause at certain percentage numbers – this is normal. Please allow time for the installation to complete and for the Success message to appear.



4. PowerShield Whitelist Menu

Once installed, the PowerShield Whitelist application will appear in the **All -> Altorra PowerShield Whitelist** menu.



The PowerShield Whitelist application menu contains the following menu pages:

Getting Started: This is an external link to the PowerShield Whitelist product page on the Altorra website. You will find this document and other helpful information about the application.

Configuration: This will open the system properties page for the PowerShield Whitelist. You can turn the application on/off and configure the settings.

Whitelist Group: This will open the group used for the PowerShield Whitelist. Users added to this group will be added to the email whitelist list thus allowing email notifications to be sent to them.

Logs: All actions taken by the PowerShield Whitelist application will be logged here.

Support: This is an external link to the PowerShield Whitelist support page on the Altorra website. You will find this document, other helpful resources, and the ability to contact us for support.

IMPORTANT NOTE: All changes must be Saved before navigating between menu pages.

5. How it works

The PowerShield Whitelist application allows you to configure email addresses that will be able to receive emails on the instance(s) it is installed and enabled on. Emails will not be sent to Users/email addresses that have not been whitelisted.

IMPORTANT NOTE: The PowerShield Whitelist should be used on Sub-Production instances only.

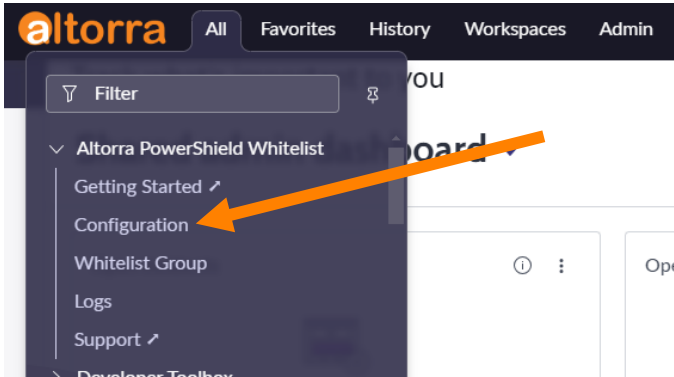
When an email is generated, the PowerShield Whitelist application will intercept and strip out email addresses not specified in the whitelist.

The whitelist is comprised of 4 sets of email addresses:

1. The Whitelist group – Controlled by group membership, where system users are added to the group. This is specified in the **All -> Altorra PowerShield Whitelist -> Whitelist group** module.
2. External email addresses – A list of external email addresses specified in the configuration page of the application. Located in the **All -> Altorra PowerShield Whitelist -> Configuration** module.
3. Gmail addresses - A list of Gmail email addresses specified in the configuration page of the application. Located in the **All -> Altorra PowerShield Whitelist -> Configuration** module.
4. Users with the admin role.

6. Setting up the PowerShell Whitelist application

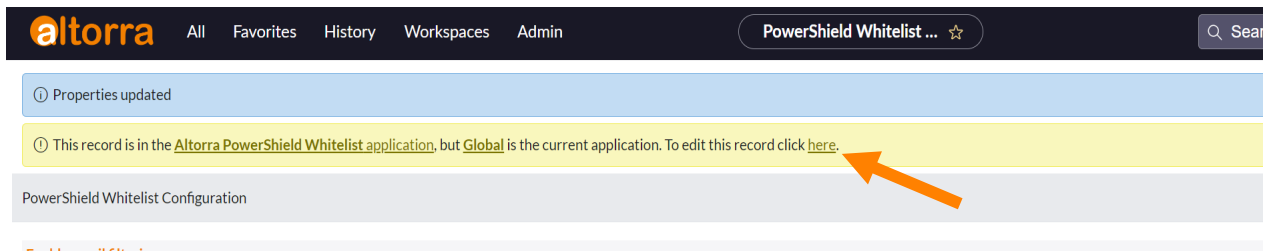
6.1 Configuration Page



From the **All -> Altorra PowerShell Whitelist** menu, navigate to the Configuration screen. This is where the application's settings can be found.

IMPORTANT NOTE: Upon installation, the PowerShell Whitelist application is ***disabled*** by default.

If not already in the "Altorra PowerShell Whitelist" Application Scope, you will be presented with a yellow informational notice at the top of the Configuration page, reminding users that they must be in that scope in order to make changes to edit the record. As a convenience, a quick link is made available. Click on the link to unlock the fields and edit the record.



In order for any changes to take effect, you must click Save.

Note: Once a System Property has been modified and saved, the message will be displayed again, and you must click on the link to be able to edit the record again.

Here are the settings available on the Configuration page:

Enable email filtering (Options: Yes/No – Default: No)

When checked (Yes), the PowerShield Whitelist application is Active (i.e. turned ON)

Whitelisted external email addresses

Enter external email addresses you want to allow emails to be sent to from this instance. As opposed to the Whitelist Group (see section below), this setting allows for manually adding one or more external addresses without the need to create user(s) on the instance.


When entering more than one external email address, enter in a comma-separated format.


When testing and an action triggers an email notification destined to an email in this list, it will be allowed to be sent.

Whitelisted external email addresses:

A comma-separated list of email addresses that will be allowed to receive emails.

Useful for including external testers.

Saves you from creating User records then adding them to the Whitelist Group just to allow the emails to go out. 

tester@example.com, alerts@example.com 

Whitelisted Gmail addresses

Enter Gmail addresses you want to allow emails to be sent to, from this instance.

Important Note: Enter only the Gmail username, without the **@gmail.com**

Again, as opposed to the Whitelist Group (see section below), this setting allows for manually adding one or more Gmail addresses without the need to create user(s) on the instance.

When entering more than one Gmail email address, enter in a comma-separated format.

When testing and an action triggers an email notification destined to an email in this list, it will be allowed to be sent.

Great Testing Feature – This configuration item supports Gmail Plus addressing, allowing an unlimited number of email addresses to be sent to a single Gmail inbox.

Here's how it works:

If you have the Gmail email address: **AcmeTestList@gmail.com**, you can send to any email in the following format: **AcmeTestList+XXXX@gmail.com**, where XXXX can be almost anything you wish. (visit <https://gmail.googleblog.com/2008/03/2-hidden-ways-to-get-more-from-your.html> for more information)

For example: **AcmeTestList+one@gmail.com** or **AcmeTestList+superhero@gmail.com** or **AcmeTestList+service@gmail.com**, and they will all be delivered to **AcmeTestList@gmail.com**

This gives testers a powerful means to create many email addresses without the need to create many Gmail test accounts.

If you are using Gmail Plus addressing, you only need to enter your base Gmail username into the **Whitelisted Gmail addresses** configuration item, and the application will automatically add all email addresses that follow the pattern to the whitelist.

Whitelisted Gmail addresses:

A comma-separated list of Gmail usernames, without "@gmail.com".


This allows you to whitelist infinite Gmail email addresses by leveraging the Gmail Plus Addressing feature.


To use, simply add the the username part of the email address here. To include multiple accounts, separate with a comma.


*** Do NOT include "@gmail.com".

Examples:

some.user

some.user, first.last, testaccount 

JohnTestList, AcmeTestAccount 



Send when no recipients found (Options: Yes/No – Default: Yes)


In situations where an email is created, but no recipients were found in the whitelist (i.e. no emails would have been sent), you can elect to **send** the email to the user whose actions caused the email notification to be triggered.

This feature is useful for testers to see what the intended recipients would have normally received.

Send when no recipients found:

When no whitelisted recipients are found, send the email to the person who caused it to be triggered.

Perfect for testers to see what the intended recipients would have received.

Default is "checked" or "true". 

Yes | No 

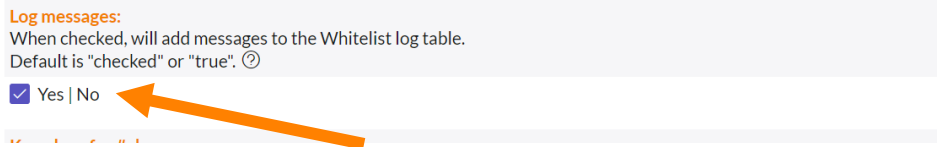


Log Messages (Options: Yes/No – Default: Yes)

This gives you the option to log actions of the PowerShield Whitelist tool.

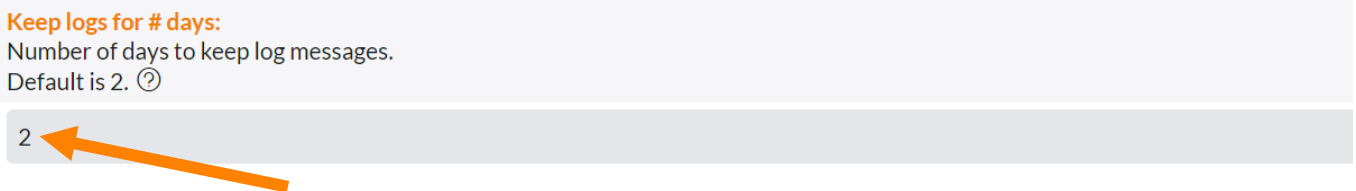
Logs are stored in the **All -> Altorra PowerShield Whitelist -> Logs** module.

This is helpful to troubleshoot or to observe what the criteria used for decision-making of the PowerShield Whitelist application.



Keep logs for # days (Default: 2)

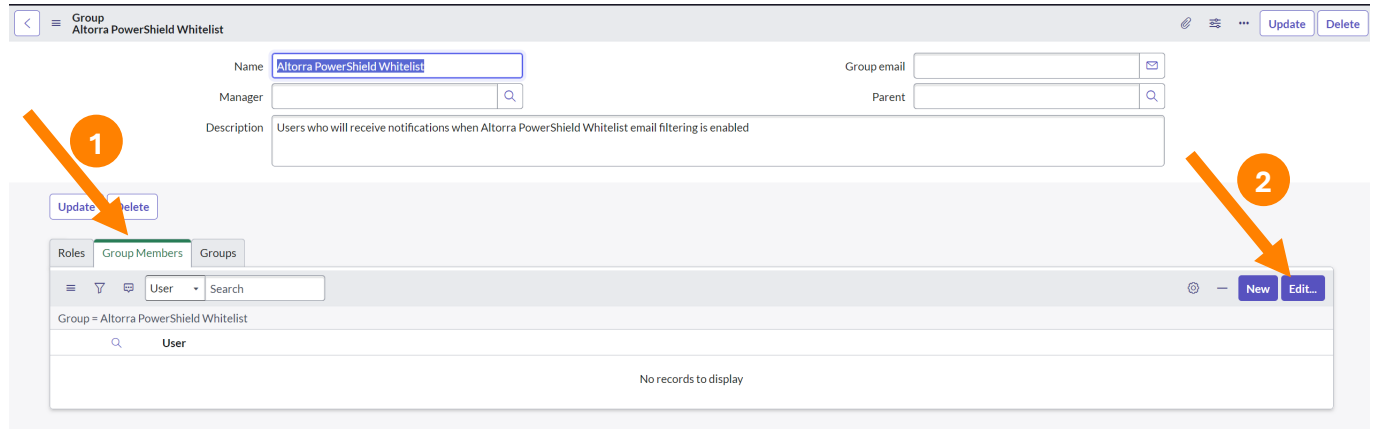
This gives you the ability to specify the number of days worth of logs to keep.



6.2 Whitelist Group

In section 6.1, the configuration page, including the external email addresses and Gmail addresses were explained. In addition to manually specifying email addresses, you can control the whitelist using Group membership.

The Whitelist Group can be found in the **All -> Altorra PowerShield Whitelist -> Whitelist Group** module.

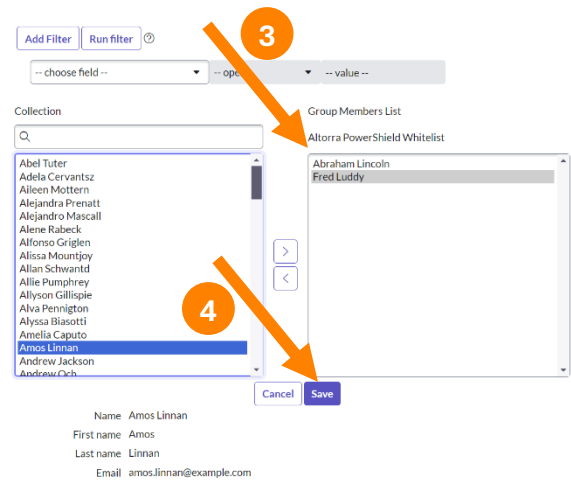


1 – Select Group Members Tab.

2 – Select Edit

3 – Select Members and move into the Whitelist

4 – Click Save



7. Using the PowerShield Whitelist

The PowerShield Whitelist is disabled by default (after initial installation). Ensure to enable the application on the Configuration page (see section 6.1) and save the change prior to use.

When an email notification is triggered, the PowerShield Whitelist intercepts the email and removes any recipient addresses that don't match the email addresses specified in:

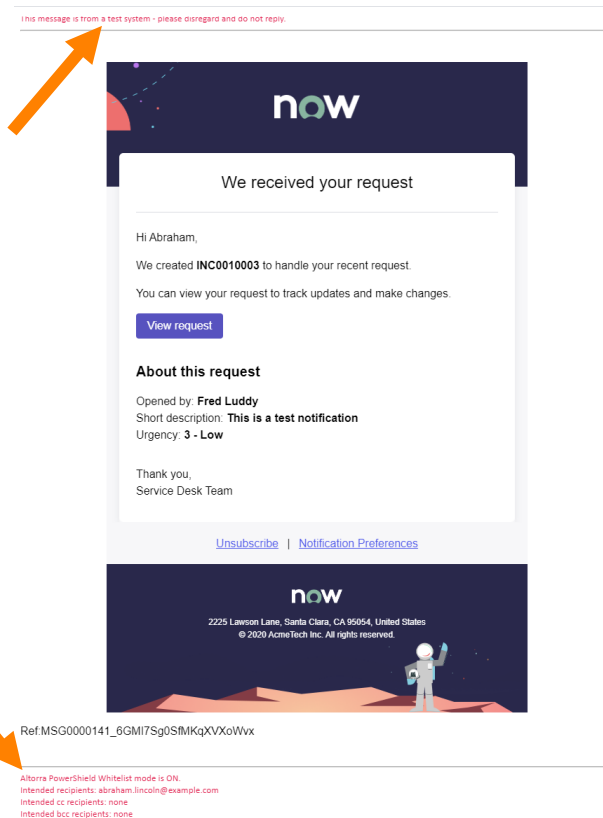
- The Whitelist Group
- The list of specified External addresses.
- All email addresses destined for the specified Gmail account(s), using the Gmail Plus addressing logic, allowing an unlimited number of email addresses to be used, while only using a single Gmail Inbox. (i.e. XXXX+YYYY@gmail.com, where XXXX is the Gmail username, and YYYY is any supported characters).

In situations where, after applying the Whitelist and the result is having no recipients for the notification email, you can select to have the email sent to the user that triggered the notification, by enabling the **Send when no recipients found** setting on the Configuration page (see section 6.1)

The PowerShield Whitelist application will also add a header and footer to the email that is sent out to the resulting recipient list. The header and footer will appear in red.

The footer will list the **Intended recipients**: i.e. The email addresses that would have received the email notification if the PowerShield Whitelist was disabled or not installed.

This information is helpful to troubleshoot the notification recipients for a given event.



8. Logs

As described in section 6.1, when the **Log Messages** setting is turned on, the PowerShield Whitelist application will log every time the application is triggered. Logs will be kept for the duration specified in the **Keep logs for # days** configuration setting (found on the Configuration page – see section 6.1).

Logs are stored in a custom table, and are visible in the **All -> Altorra PowerShield Whitelist -> Logs** module.

The logs will show the logic used to filter the email recipients.

The screenshot displays a log entry in a web interface. At the top, there are fields for 'Whitelist tool' (Email), 'Status' (Info), 'Email' (Email: Incident INCO010003 was creat), 'Created' (2024-04-22 20:34:32), 'Source record' (Incident: INCO010003), and 'Created by' (system). Below this is a 'Message' section with several expandable items:

- Current Email Whitelist Configuration:**
 - Whitelist group name = Altorra PowerShield Whitelist
 - External email addresses = support@altorra.com
 - # of external email addresses = 1
 - Gmail usernames = altorrasupport
 - # of Gmail usernames = 1
 - Send to last updated user = true
- Intended Recipient Addresses:**
 - 1 recipient(s) = abraham.lincoln@example.com
 - 0 cc =
 - 0 bcc =
- Validating against Gmail Usernames...**
 - abraham.lincoln@example.com **DOES NOT** match Gmail username altorrasupport
- All Whitelisted Addresses:**
 - abraham.lincoln@example.com
 - admin@example.com
 - fred.ludley@example.com
 - support@altorra.com
- Valid Recipient Addresses:**
 - 1 recipient(s) = abraham.lincoln@example.com
 - 0 cc =
 - 0 bcc =

The log shows helpful information to troubleshoot the recipient list and to better understand the logic used in determining which addresses the email will be sent to.

9. Support

If you require further support, have comments or even have a feature request, please contact us by visiting us at <https://www.altorra.com/support> or by emailing us at support@altorra.com.

Thank you for your interest in Altorra Solutions products and services.