SYXSENSE UPDATES Q4 2022

New version of Syxsense is shipping.

KEY FEATURES

- **Zero Trust:** Syxsense evaluates DEVICES for trusted status, protecting you from breaches by blocking at risk users from accessing corporate assets. Syxsense is first to automatically remediate security risks on devices and bring them into a trusted state so employees can safely continue to be productive
- **Local Time Zone Support:** Create a single maintenance window and Syxsense Cortex will automatically start the window in the devices local time zone (Syxsense Secure and Enterprise)
- **Patch Staging:** IT managers can now separate download and deployment actions in both tasks and cortex workflows. At deployment, Payload files will already be available on client devices

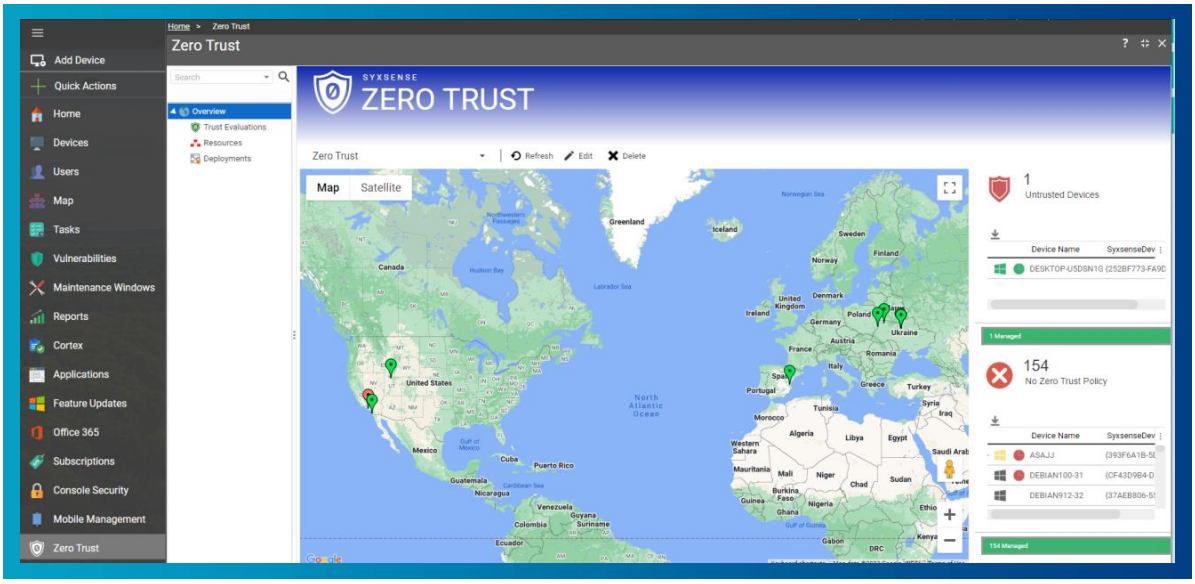
SYXSENSE ZERO TRUST SOLUTION

Syxsense makes it easy to implement a Zero Trust strategy for organizations starting from scratch or for those looking to consolidate into a single solution. Zero Trust assumes that all devices are untrusted and will be denied access to corporate assets until they meet a defined set of criteria. By blocking users on these untrusted devices, Syxsense protects you from breaches. With this end-to-end solution, Syxsense manages

- Creation of the trust criteria, known as a Security Posture
- Evaluation of trusted status on each managed device
- Triggering of appropriate actions or blocks based on trusted/untrusted status

Zero Trust Dashboard Overview

Shows a global map of the trusted status of each device, lists any devices in an untrusted state and any windows devices without an established Zero Trust Policy.



 |

TRUST EVALUATION

Each time an endpoint attempts to access a resource on your network, Syxsense Zero Trust validates the health of your endpoints by checking the Security Posture. Security Postures are built by dragging and dropping the elements you want to check into a Trust Evaluation Workflow. Check for missing patch updates, specific versions of software, installed and up to date antivirus software, configuration settings and more.

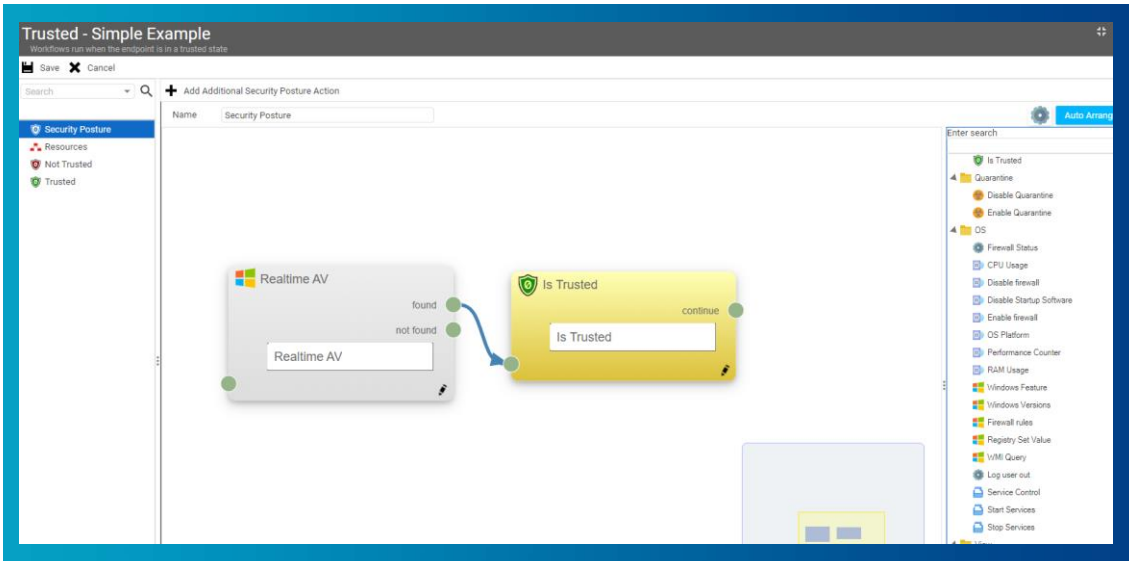
Trust Evaluations run on the client and include:

1. **Security Posture:** The list of requirements for device to be trusted.
2. **Resources:** Specific resources that are blocked/allowed if a device is not trusted/trusted
3. **Not Trusted:** Actions to take if the current device evaluates to not trusted
4. **Trusted:** Actions to take if the device is trusted

To Create A Security Posture

- Click Zero Trust
- Trust Evaluations
- Create
- Enter a name
- Drag and drop the information you want evaluated on each device
- NOTE: the final step of any Security Posture must be “Is trusted”

For a simple example you can check for the existence of specific software and if found, mark the device as trusted.



For more information on working with Zero Trust, refer to Chapter 11 of the Users Guide.

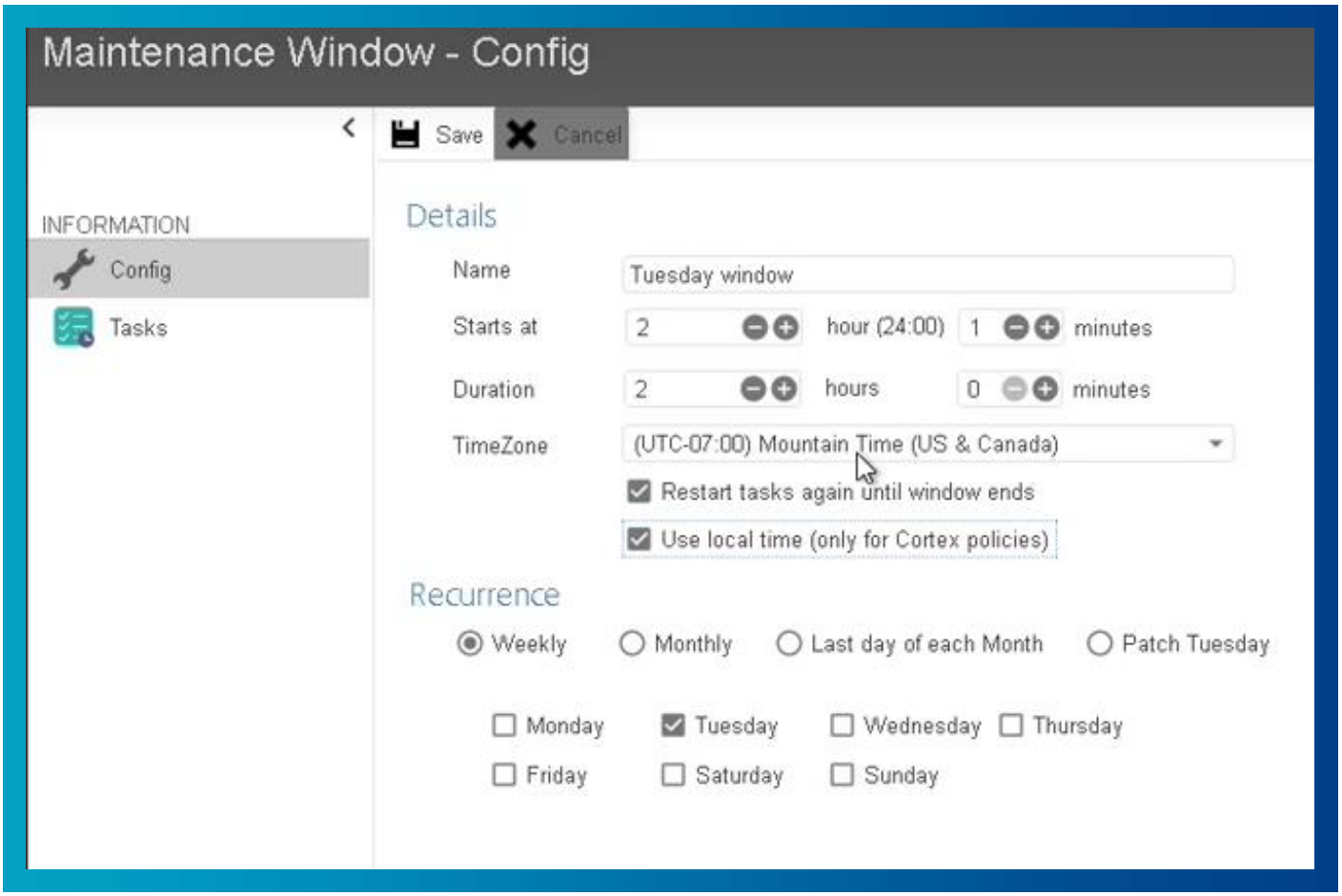
LOCAL TIME ZONE SUPPORT

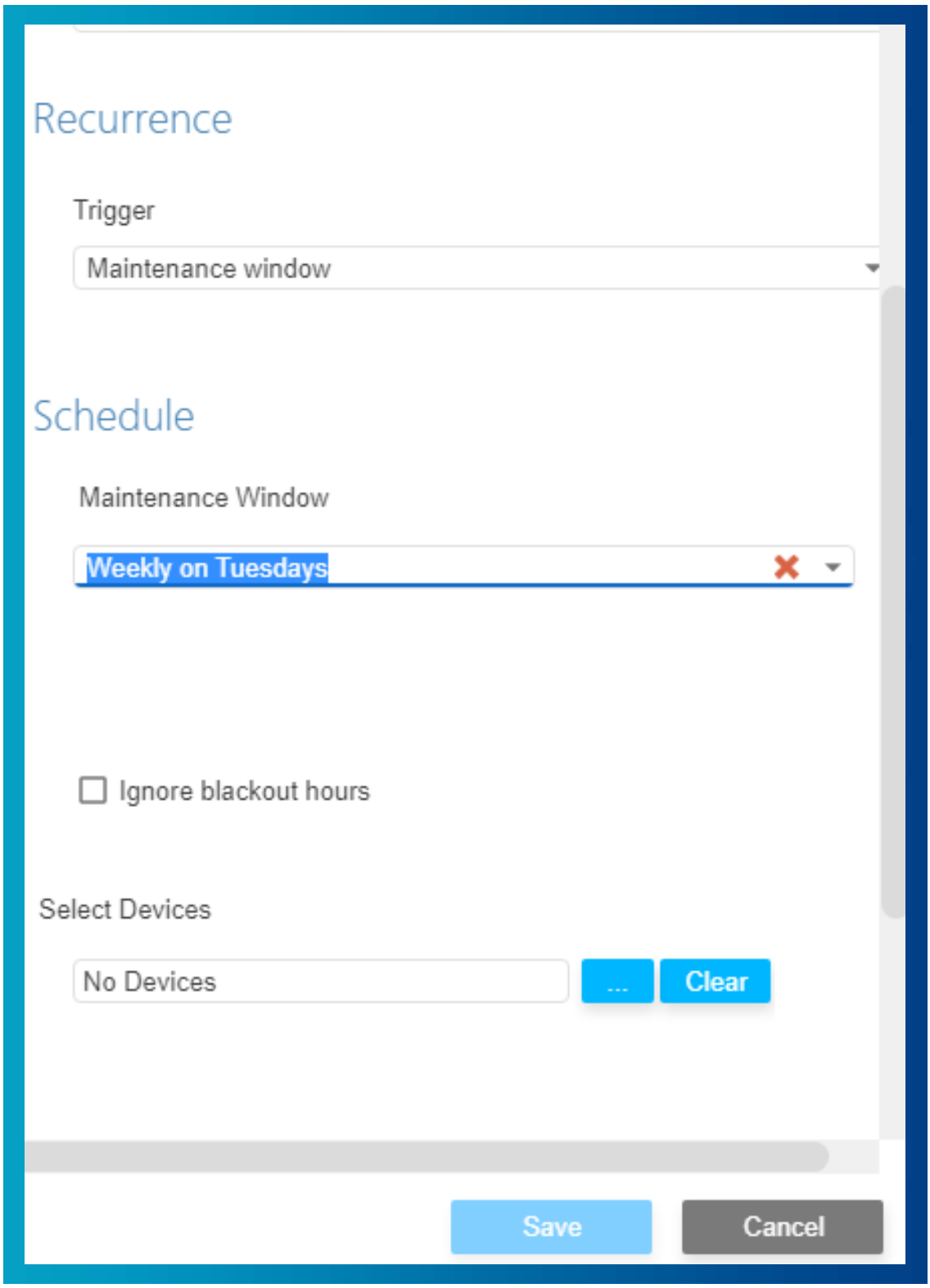
Geographically disbursed organization save time by setting a single maintenance window to the start time, Syxsense translates the time to the devices local time zone.

You can now set a Cortex Trigger to run on a maintenance window. This change is a major benefit for offline devices. Because the policy is stored locally, devices that come online at any point during the Maintenance Window will start the workflow. Previously only devices online at the start of a maintenance window would run the task

Building a Localized Maintenance Window

- Select a cortex policy
- Select publish
- Under Recurrence Policy select Maintenance Window



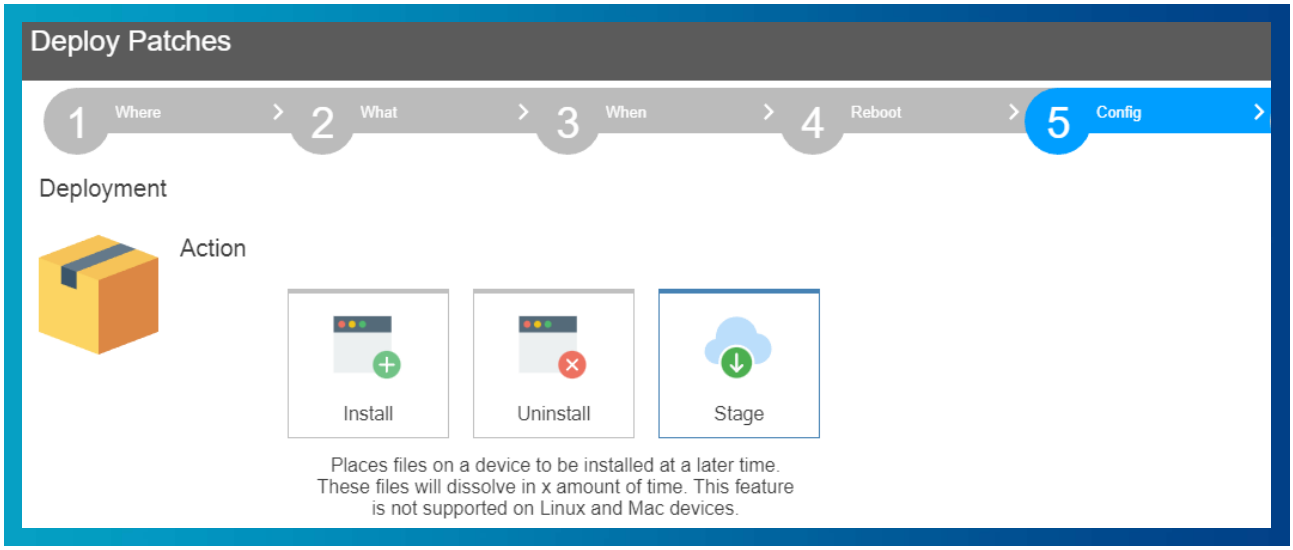


PATCH STAGING

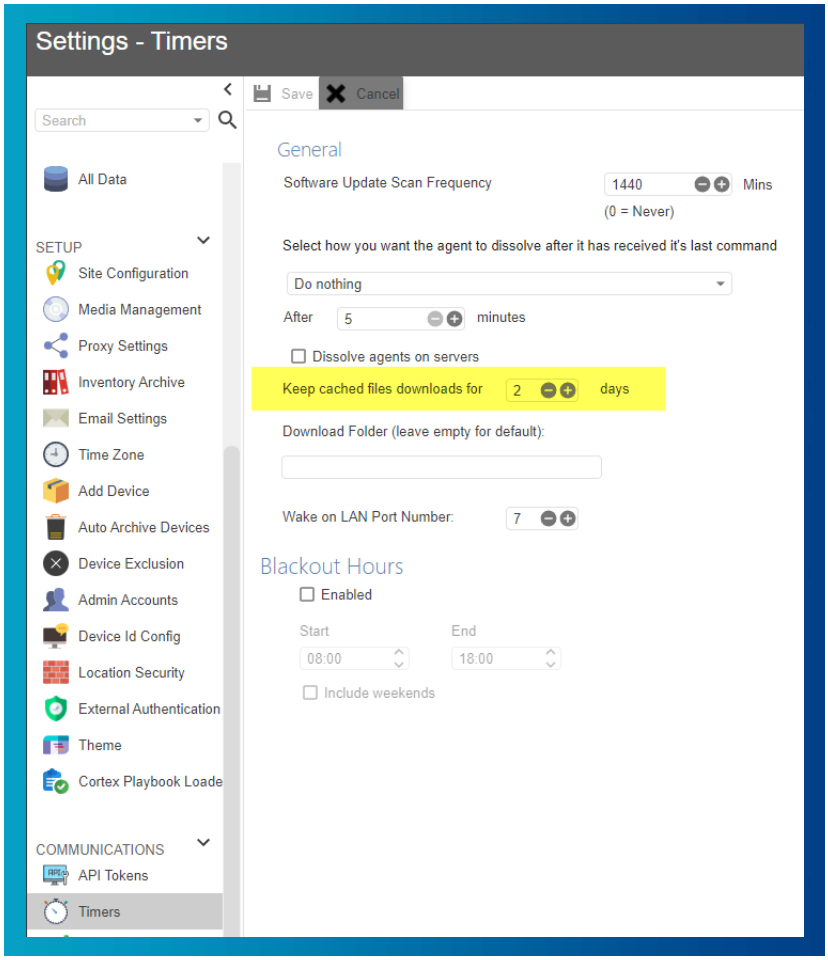
IT managers can now separate download and deployment actions in both tasks and cortex workflows. At deployment, Payload files will already be available on client devices, reducing the time needed for tasks to complete.

To Stage Patch Files from Tasks

- Create a patch deploy task
- On Step 5 Config, select Stage



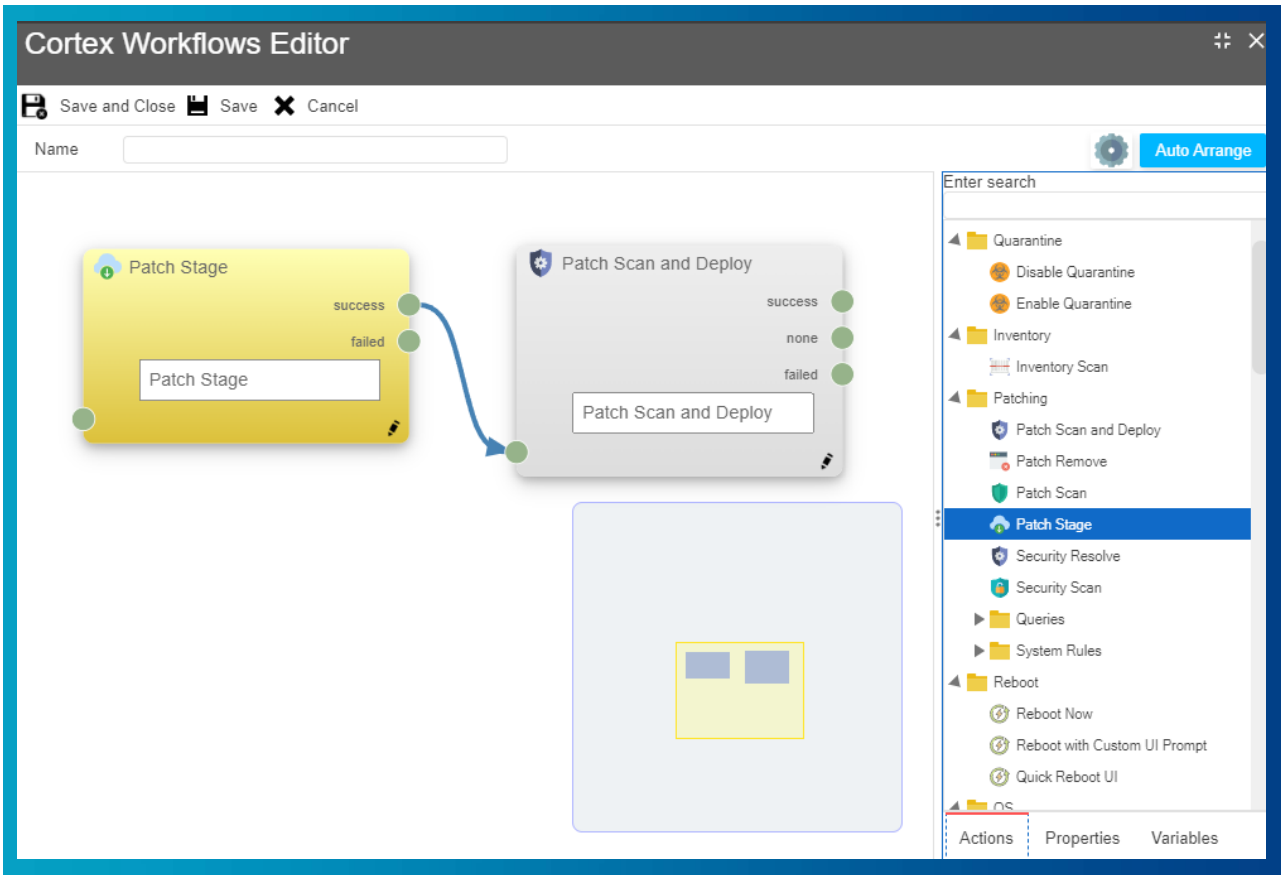
- Files will be downloaded to C:\$VCMSTEMP$\DownloadFolder
- Files dissolve after x days, x is configurable under Settings | Communications | Timers | Keep cached files for



 |

To Stage Patch Files in a Cortex Workflow

- Create or edit an existing Cortex workflow
- Drag and Drop “Patch Stage”



- The subsequent Patch Scan and Deploy task automatically looks for staged patch files for deployment. If none are found it will redownload and continue.