Check Website Certificate Expiry

CHECKCENTRAL

BINARYFORTRESS

Checking Website Certificate Expiry Dates with CheckCentral

We've recently released a Direct Integration built for checking SSL/TLS certificate expiry dates. The script for this guide will still work, but we would highly recommend using the built-in integration for it. You can get started with the Direct Integration by navigating to your CheckCentral dashboard and clicking Services > Direct Integrations in the top menu.

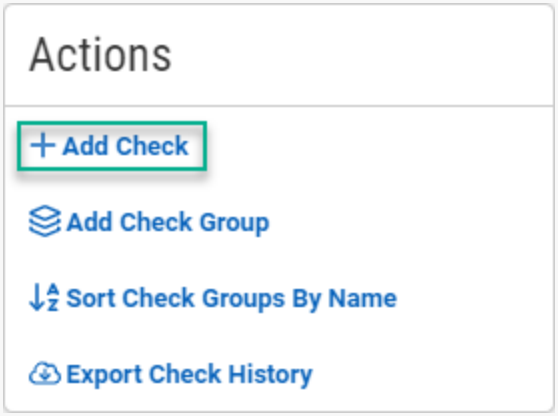
If you have websites for which you maintain the SSL certificates, this PowerShell script will help more efficiently monitor the expiration status of those certificates. The script can be run from anywhere, as it connects to the public URL for the website, and it will email the results wherever you like. This help guide shows how to configure the script to email the results to CheckCentral and create a companion Check to automate the status parsing.

Configure the Check

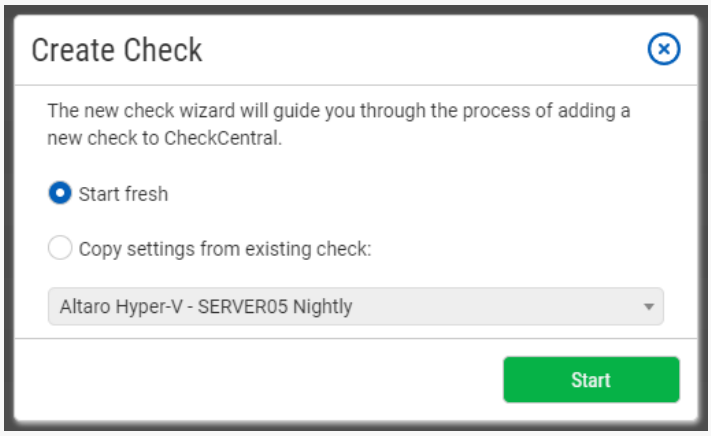
Create and Identify

Checks can be added from various locations in the CheckCentral interface, from the Dashboard, Checks page, Activity page, and the Check Group details page.

- Begin by clicking "+ Add Check."



- Select "Start Fresh," and click "Start."

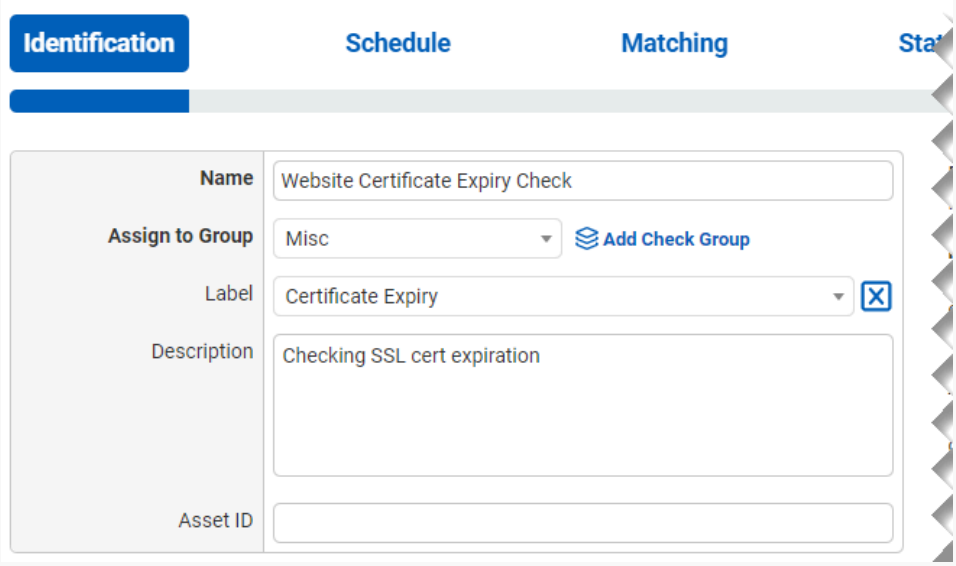


- Name the Check. It can be whatever you like, for example `Website Certificate Expiry Check`.
- Select an existing Check Group or create a new one by clicking Add Check Group.
- Select an existing Label or create a new one by typing the name in the text field of the dropdown. (optional)
- Add a description (optional).

The Asset ID is used exclusively with certain ticketing systems and is not required for Checks. Asset ID details and ticketing systems are more fully covered by other documents (e.g. **Halo Integration (asset ID)**.)

- Leave the Asset ID blank.

Your Check so far will look something like this:



Navigate to the next step in CheckCentral by clicking the "Next" button or the tab name.

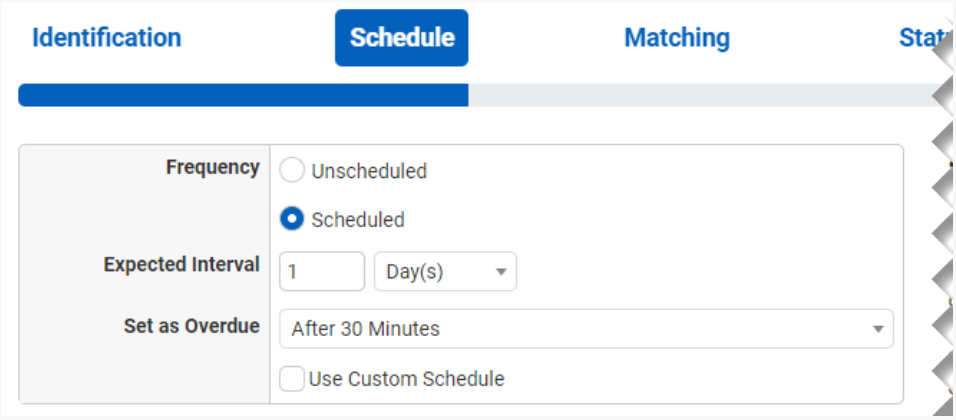
Schedule

- Leave "Scheduled" selected as we will be running the script regularly.
- Assuming you'll run the script daily, leave the Expected Interval on "1" "Day(s)." If you plan to run the script on another interval, adjust accordingly.

> The initial expectation time is set by the first email message that is received and processed by its Check. (For example, if a notification email arrives at noon and its Check is set for every half hour, it will expect another notification email at 12:30.)

- Leave the Set as Overdue setting at "After 30 Minutes." If the script notification email is not received after this amount of time has been exceeded, the Check will be marked as a failure.

Leave Custom Schedule de-selected.



Matching

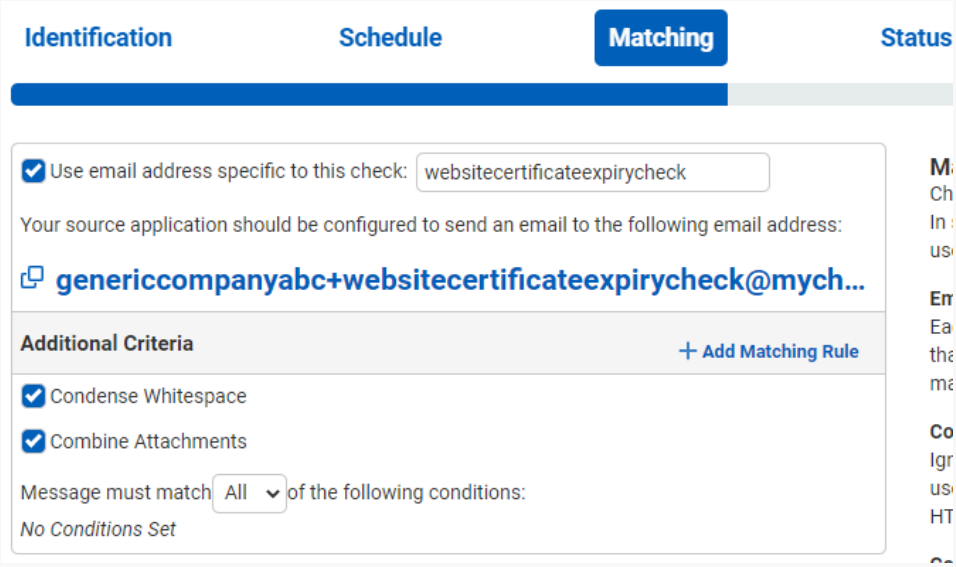
The Matching step is what matches a notification email to its specific Check. It's also where you'll set the notification's CheckCentral destination email. For CheckCentral to parse notification emails, they must be sent to a "mycheckcentral.cc" address. By default, the email address is [your organization name]@mycheckcentral.cc.

A more unique email address is created using the name given to the Check (with white spaces removed).

- Leave the default selections enabled.

- Copy the unique email address for later use by clicking on the Copy icon .

Do not add any matching rules. The unique email address is sufficient.



The email address will appear different based on your organization name and the name you specified for your check.

Status

The previous Matching step identifies the incoming email to the Check. The Status step looks for indicators of what *type* of notification you're receiving (e.g. The job was successfully run, it failed, or there were some issues.) The configuration options you choose can vary considerably, but the approach is the same.

The Default Status is what is set when the other Rules in this step don't match. Criteria for the remaining statuses then need to be defined, requiring their own unique one-to-one matches.

- Leave the Default Status on "Failure."

The "Success Criteria" section is where you'll set the criteria that will mark an activity as successful.

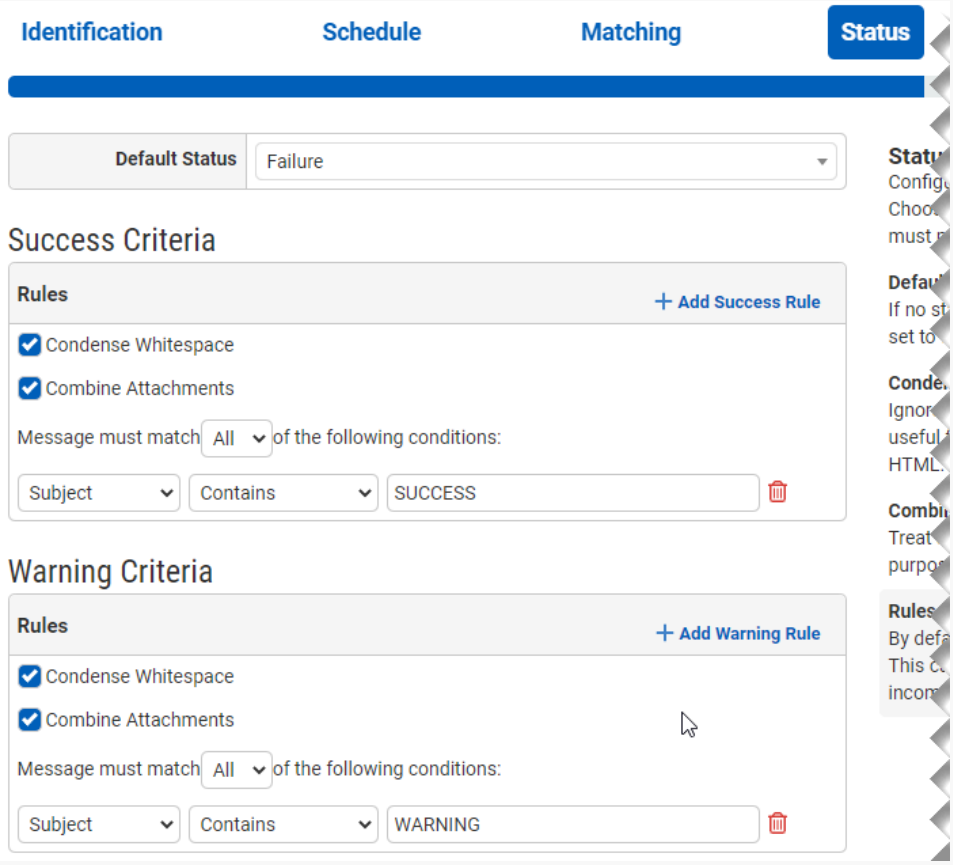
- Click + Add Success Rule.

A successful run (no certificates expired or expiring soon) of the script will have the word "SUCCESS" in the email Subject.

- Set the rule to "Subject contains SUCCESS" by leaving the default dropdown selections and typing `SUCCESS` (all caps) in the empty text field.

The "Warning Criteria" section is where you'll set the criteria that will mark an activity with a warning.

- Click + Add Warning Rule.

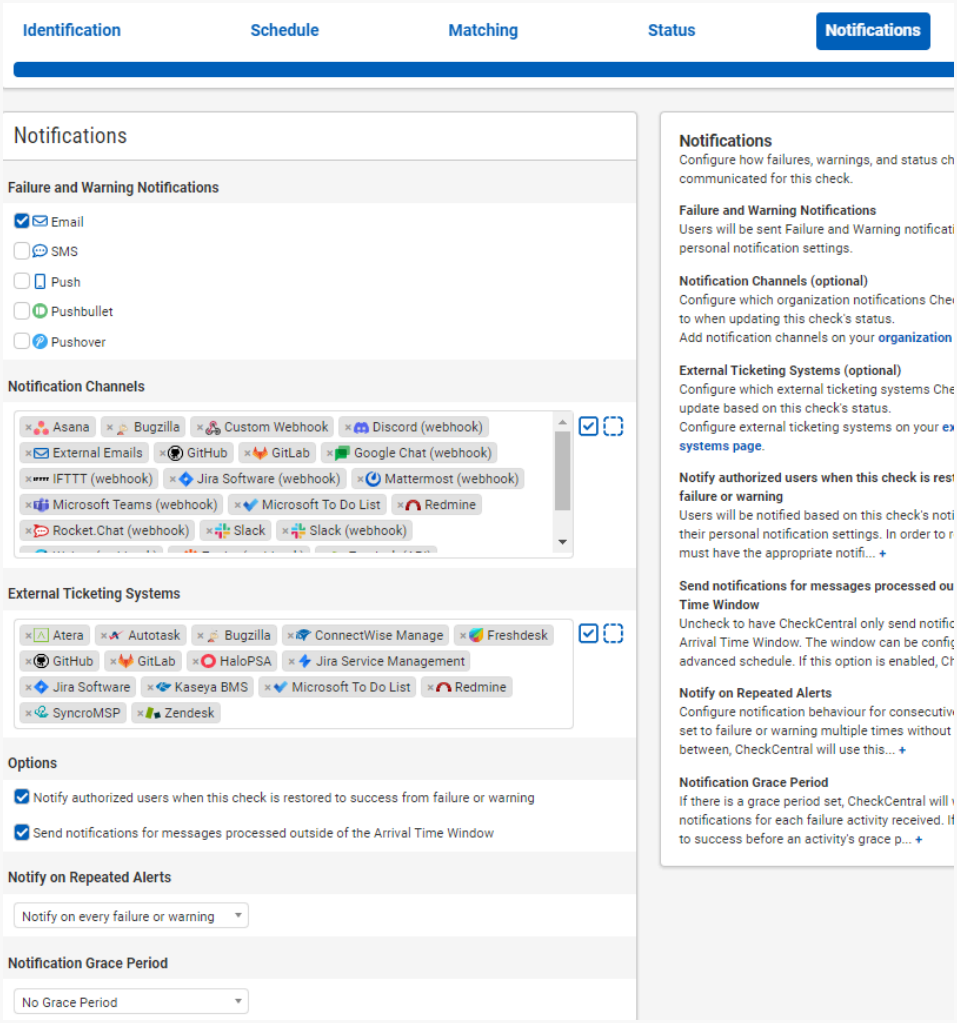


A warning result (certificate(s) expiring soon) from the script will have the word "WARN" in the email Subject.

- Set the rule to "Subject contains WARN" by leaving the default dropdown selections and typing `WARN` (all caps) in the empty text field.

Leave the Condense Whitespace and Combine Attachments checkboxes enabled.

Notifications



Notifications are simply how you want to be informed of Check Failures, Warnings, and some other Status changes.

Email, push, chat and other software can be integrated as well as ticketing systems, allowing for automatic ticket creation and management.

> Further configuration is required for each to function and is done via the Notifications tab in the main menu. They can be configured before or after Check creation.

For more understanding of Notification setup, see the **CheckCentral Beginner's Guide (Notifications)**.

- Select the desired means of Notification. If in doubt of the selections here, leave the defaults.

Save

- From the Save tab, click the "Save Check" button.

Setting Up the Script

Installation

With the Check configured in CheckCentral, you need to install the script onto a machine (where it will regularly run).

- Download the script: **CheckWebsiteCertExpiry.zip**.

- Extract it somewhere on the computer (e.g. C:\Scripts). There will be three files: CheckWebsiteCertificateExpiry.ps1, createScheduledTask.ps1, and websites.txt
- Edit the websites.txt file to contain the list of websites you want the script to check. Save it. **Make sure to put one URL on each line.**
- Open a PowerShell console and run the script to make sure it works. For example:

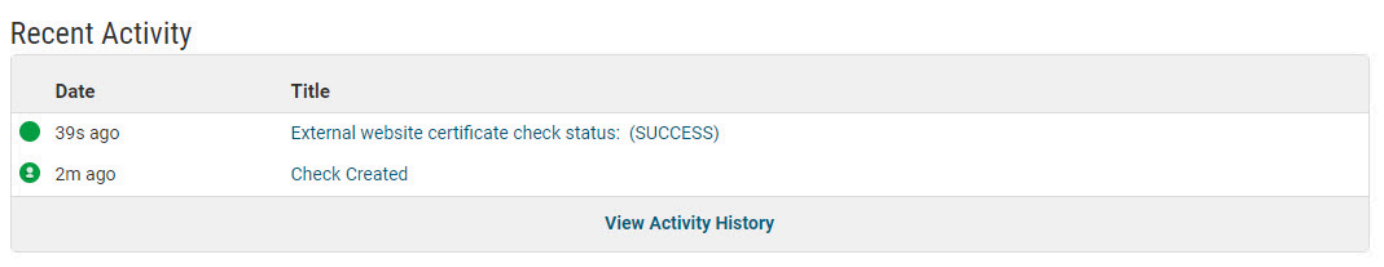
```
.\CheckWebsiteCertExpiry.ps1 -Websites (Get-Content websites.txt) -
EmailFromAddress {Email From Address} -
EmailToAddress {Check Email Address}
```

- Refresh the Check page or Dashboard to see the new Activity for your Check.

Scheduling

You're ready to set up the Windows Scheduled Task so the script will automatically run each day.

- First, edit the parameters at the top of the CreateScheduledTask.ps1 script and save the changes.
- You'll see the new Scheduled Task in the Windows Task Scheduler. Run it and verify that a second Activity shows up in the CheckCentral Check.



For more detail on Check creation and best practices, see our **Check Creation Guide**.

For other guides and support contact information, see **CheckCentral Support**

About CheckCentral

CheckCentral Monitoring consolidates and simplifies backup, system, and software email updates into a clean, graphical dashboard, bringing peace of mind to IT administrators of SMBs, Enterprises, and MSPs.

To learn more about CheckCentral, visit: **https://www.checkcentral.com**

About Binary Fortress Software

Binary Fortress has spent 19 years in pursuit of one goal: create software to make life easier. Our software ranges from display management and system enhancement utilities to monitoring tools and digital signage. IT administrators, professional gamers, coffee-shop owners, and MSPs all rely on Binary Fortress to make their days better, and their lives easier.

Binary Fortress Software
1000 Innovation Drive, Suite 500
Kanata, Ontario, Canada
K2K3E7
https://www.binaryfortress.com