Check Website Certificate Expiry



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."
 Actions + Add Check S Add Check Group ↓[↑] Sort Check Groups By Name S Export Check History
- Select "Start Fresh," and click "Start."

Create Check	⊗
The new check wizard will guide you through the process of adding a new check to CheckCentral.	
• Start fresh	
Ocopy settings from existing check:	
Altaro Hyper-V - SERVER05 Nightly	•
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 Select 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. <u>Halo Integration (asset ID)</u>.)

• Leave the Asset ID blank.



Your Check so far will look something like this:

Identification	Schedule	Matching	Stat
Name	Website Certificate Expiry C	heck	
Assign to Group	Misc	▼ SAdd Check Group	
Label	Certificate Expiry		- 🗙
Description	Checking SSL cert expiratio	n	
Asset ID			

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.

Identification	Schedule	Matching		
Frequency	Ounscheduled			
	• Scheduled			
Expected Interval	1 Day(s) •			
Set as Overdue	Je After 30 Minutes			
	Use Custom Schedule			

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.



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

Identification	Schedule	Matching	Stat	atus Notifications	Notifications are simply how you want to be informed of Check
Notifications Failure and Warning Notifica	tions			Notifications Configure how failures, warnings, and status ch communicated for this check. Failure and Warning Notifications	Status changes.
C Email SMS Push Push Pushover Notification Channels				Users will be sent Failure and Warning notificati personal notification settings. Notification Channels (optional) Configure which organization notifications Cher to when updating this check's status. Add notification channels on your organization External Ticketing Systems (optional) Configure which external Ticketing systems Che update based on this check's status. Configure external ticketing systems on your ex- systems page. Notify authorized users when this check is rest failure or warning Users will be notification settings. In order to r must have the appropriate notifi + Send notifications for messages processed ou Time Window Uncheck to have CheckCentral only send notific Arrival Time Window. The window can be config advanced schedule. If this option is enabled, Cf Notify on Repeated Alerts Configure notification behaviour for consecutiv set to failure or warning multiple times without	Email, push, chat and other softward can be integrated as well as ticketin systems, allowing for automatic ticket creation and management. Further configuration is required for each to function and is done via the
 ▲ Asana ▲ Bugzilla ▲ External Emails ▲ External Emails ▲ Microsoft Teams (webf ▲ Microsoft Teams (webf ▲ Rocket.Chat (webhook) 	× Sustom Webhook × th Dis GitHub × → GitLab × → Googl Jira Software (webhook) × () nook) × √ Microsoft To Do List × Slack × ‡ Slack (webho	cord (webhook) e Chat (webhook) vattermost (webhook) vattermos			
External Ticketing Systems	× È Bugzilla ×♥ ConnectWiss ×♥ HaloPSA ×♥ Jira Service seya BMS ×♥ Microsoft To Do desk	Manage × Freshdesk Management List × Redmine			Notifications tab in the main menu. They can be configured before or after Check creation.
Options Notify authorized users wh Send notifications for mes	en this check is restored to succes sages processed outside of the Ar	is from failure or warning rival Time Window		between, CheckCentral will use this + Notification Grace Period If there is a grace period set, CheckCentral will 1 notifications for each failure activity received. If to success before an activity's grace p +	
Notify on Repeated Alerts Notify on every failure or war Notification Grace Period	ning v				
No Grace Period	•				

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: <u>CheckWebsiteCertExpiry.zip</u>.



- 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.

Recent Activity			
Date	Title		
🔵 39s ago	External website certificate check status: (SUCCESS)		
2m ago	Check Created		
	View Activity History		

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.cc

About Binary Fortress Software

Binary Fortress has spent 18 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.

Copyright © 2007-2025 Binary Fortress Software, all rights reserved. The Binary Fortress logo is a trademark of Binary Fortress Software. The CheckCentral logo is a trademark of Binary Fortress Software.

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