# Work instruction: SSL Certificate Check

This document describes the work instruction of the monthly check “SSL Certificate Check”. The goal of this work instruction is to check if any certificate in the environment is expiring in the next two months.

# Involved servers

|  |  |  |
| --- | --- | --- |
| Acceptance | Production | Disaster Recovery |
|  |  |  |

# Steps

|  |  |
| --- | --- |
| Step | Screenshot |
| **Important: These steps need to be performed on all servers in the environment.** | |
| Step 1:  Open a RDP session to the server |  |
| Step 2:  Start the mmc.exe, add the “Certificates” snap-in and select “Computer account”. |  |
| Stap 3:  Open the folder “Personal > Certificates”. Check if the “Expiration Date” is longer than two months.  If this isn’t the case: Create an incident to have this investigated. |  |
| Step 4:  If the server is a SharePoint server (if not, go to step 8):  Open the Central Administration site |  |
| Step 5:  Click “Security” and under “General Security” click “Manage trust” |  |
| Step 6:  Select every trust and click “Edit” in the Ribbon. |  |
| Stap 7:  Check if the “Certificate Expiration Date” is longer than two months.  If this isn’t the case: Create an incident to have this investigated. |  |
| Step 8:  Record your findings in the “Registration list Periodic Checks” |  |

# Automatic check

This check is part of the Periodic Checks script, which means the above checks do not have to be performed manually. Analysis will take place by reviewing the generated e-mail and taking actions if issues are reported.

# resolution

Create a change to renew the certificate.