# Work instruction: Access check

This document describes the work instruction of the weekly check “Access Check”. The goal of this work instruction is to check if who has logged onto the servers in the environment in the last week and if these accounts are supposed to log onto the environment.

# Involved servers

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

# Steps

|  |  |
| --- | --- |
| Step | Screenshot |
| **Important: Perform these steps on all servers** | |
| Step 1:  Open a RDP session to the server |  |
| Step 2:  Check which accounts have logged onto the server in the last 7 days.  Check who these accounts belong to and if they have a reason to log onto the server.  If this isn’t the case: Create an incident to have this investigated. | Event ID: 4624 and 4625 |
| Step 3:  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

When accounts log onto the servers which do not have any business on the servers, an investigation needs to be started. Create an overview of the logon times and contact the owner of the account. If there is a valid explanation the person logged onto the environment, there is no issue. In all other cases, actions to prevent this from happening again must be taken.