# Work instruction: group membership check

This document describes the work instruction of the daily check “Group Membership Check”. The goal of this work instruction is to check if all Active Directory administration groups have the correct members, validating that only authorized personnel has access to the environment.

# Involved servers

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

# Steps

|  |  |
| --- | --- |
| Step | Screenshot |
| Step 1:  Open a RDP session to the Admin server |  |
| Step 2:  Open Active Directory Users and Computers mmc |  |
| Step 3:  Browse to <OU> and open the Administration groups | X  Y  Z |
| Step 4:  Check if the correct accounts are a member of the correct group.  If this isn’t the case: Create an incident to have this investigated. | X - a,b,c  Y - d,e,f |
| Step 5:  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 the group membership isn’t the way it is supposed to be, determine how this is possible. This can result in two conclusions:

1. The change is not legitimate and the group membership(s) need to be corrected.
2. The change is legitimate, the specification needs to be updated.
   1. When this is checked using the script: The configuration files of the script need to be updated as well.