|  |
| --- |
| **JDN Standards – Configured users** |

Introduction 1

Domain integrated users 1

Non-domain users 2

Overview 2

Accounts per device 2

# Introduction

This document describes the credentials used across standard JDN deployments in 2015.

Passwords chosen should be different for each ship or site, and as such should be diligently registered in RDM for each ship or site.

# Domain integrated users

For local standalone domains:

* JDN administrator users:
  + SE use the SE domain admin: adm\_se
  + SA use the SA domain admin: adm\_sa
  + TSE use the TSE administrator: adl\_tse
  + SSE use the limited SSE administrator: adl\_sse
  + Note: The normal “administrator” is left unused for normal operation.
* JDN development users (should be disabled unless needed for 3rd line support):
  + Architecture: USR\_ICT\_ARC\_GEN
  + Administration: USR\_ICT\_DEV\_ADM
  + Finance: USR\_ICT\_DEV\_FIN
  + Logistics: USR\_ICT\_DEV\_LOG
  + Production: USR\_ICT\_DEV\_PRO
* Local administrator users (can be disabled at the captain’s request):
  + Captain: adl\_captain
  + Chief: adl\_chief
  + Elec: adl\_elec
* Local users (modified to fit the needs of the site or ship):
  + Crew: CAPTAIN, CHIEF, ELEC, ECR, BRIDGE, OFFICE, COOK, SURVEY, TD, AMOS,...
* Service accounts:
  + Comm-E: srv\_comme
  + Backup (Veeam): srv\_backup
  + Tasks (deployment): srv\_altirisns
  + Antivirus: srv\_nod32
  + Scheduled tasks: srv\_schedtask

Refer to the domain scripts & AD domain to verify user rights of these users.

For a jandenul.com member domain:

These use the pre-existing conventions. Consult SA/SE for more information.

# Non-domain users

## Overview

Various equipment used in the JDN standards will not be AD integrated. For this equipment the following users should be created where they are not already created through scripts:

The “**root**”, “**administrator**” & “**admin**” user accounts & passwords are reserved for installation and SA/SE usage. Which of the three user names is used can depend on the system in question. They should never be communicated to the crew (even the Captain).

A separate “**adl\_tse**” user (with the same user rights) will be created for TSE usage. This will enable TSE to always use the same login on all devices. Ideally, TSE should never use the “root”, “administrator” & “admin” passwords after the installation has been concluded and the normal support cycle has started.

A separate “**adl\_local**” user will be created to be communicated to the Captain (and potentially ELEC). Depending on the device in question, only restricted rights will be granted to the adl\_local user.

Note: Some of these devices utilize case sensitive usernames. To keep things simple, you should use lower case usernames for all devices.

## Accounts per device

**Virtualization infrastructure:**

* VRTX CMC:
  + root (administrator)
  + adl\_tse (administrator)
  + adl\_local (super user)
* iDRAC 1, 2 & 3:
  + root (administrator)
  + adl\_tse (administrator)
  + adl\_local (super user)
* iLO:
  + root (administrator)
  + adl\_tse (administrator)
  + adl\_local (super user)

**VMWare vCenter:**

* root / root@localos (administrator, should not be used)
* administrator / administrator@vsphere.local (SSO administrator used for initial setup and by SA/SE)
* adl\_tse / adl\_tse@vsphere.local (TSE administrator)
* adl\_local / adl\_local@vsphere.local (local user with restricted users)
* srv\_ups / srv\_ups@vsphere.local (APC PowerChute admin)
* srv\_backup / srv\_backup@vsphere.local (Veeam administrator)
* Note: @vsphere.local should have been set as the default log on domain in the vCenter. If this is the case, added @vsphere.local to the username is not needed. By default however the default log on domain is @localos.

**Local OS (virtual machine deployed from template):**

* Virtual machine:
  + administrator (note that the password can be set by the customization wizard)

**Synology (standalone or cluster):**

* Web administration:
  + admin (administrator)
  + adl\_tse (administrator)
  + adl\_local (administrator)
* Service accounts for share access:
  + srv\_backup (Veeam)
  + srv\_wyse (Dell Wyse WTOS)
  + srv\_juniper (FW & SW)

**Artica proxy:**

* Web interface:
  + manager (administrator)
  + adl\_tse (administrator)
  + adl\_local (administrator)
  + statadmin (statistics access only)
* SSH:
  + root

**Commbox:**

* Web interface:
  + admin (administrator)
  + adl\_tse (administrator)
  + captain (mail account & administrator)
  + *crew accounts* (various users: webmail access only)

**Meinberg time server:**

* Web interface:
  + root (super-user)
  + adl\_tse (super-user)
  + adl\_local (admin-user)

**Juniper firewalls & switches:**

* root
* ald\_tse
* securelink
* space
* srv\_iris

**APC UPS with network management module:**

* Web interface:
  + root (administrator)
  + apc (superadmin, should not be used except for initial config & PowerChute)
  + adl\_tse (administrator)
  + adl\_local (read-only)

**PowerChute virtual appliance:**

* Web interface:
  + apc