ALSID FOR ACTIVE DIRECTORY

UPDATE PROCEDURE

1. Document contributors:

<table>
<thead>
<tr>
<th>Author</th>
<th>Qualification</th>
<th>Contact address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALSID</td>
<td>DevOpsteam</td>
<td><a href="mailto:support@alsid.com">support@alsid.com</a></td>
</tr>
</tbody>
</table>

2. Document history:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date (dd/mm/yyyy)</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4.0</td>
<td>12/07/2019</td>
<td>ALSID</td>
<td>Initial document</td>
</tr>
<tr>
<td>2.5.0</td>
<td>23/10/2019</td>
<td>ALSID</td>
<td>Update for 2.5.0</td>
</tr>
<tr>
<td>2.5.3</td>
<td>16/12/2019</td>
<td>ALSID</td>
<td>Use InitDbSize</td>
</tr>
<tr>
<td>2.6.0</td>
<td>21/02/2020</td>
<td>ALSID</td>
<td>Update for 2.6.0</td>
</tr>
<tr>
<td>2.6.1</td>
<td>05/03/2020</td>
<td>ALSID</td>
<td>Update for 2.6.1</td>
</tr>
<tr>
<td>2.6.3</td>
<td>04/04/2020</td>
<td>ALSID</td>
<td>Update for 2.6.3</td>
</tr>
<tr>
<td>2.7.0</td>
<td>06/06/2020</td>
<td>ALSID</td>
<td>Update for 2.7.0</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

I. **Introduction** .................................................................................................................. 3
   1. Document objectives ....................................................................................................... 3
   2. Abbreviations .................................................................................................................. 3
   3. Infrastructure presentation ............................................................................................. 3
      3.1. Network Overview .................................................................................................. 3
      3.2. Recommended architectures ..................................................................................... 6
      3.3. Meta-Kapteyn architecture (optional) ....................................................................... 8
      3.4. Installation log file ................................................................................................... 8
   4. Prerequisites .................................................................................................................... 8
      4.1. Minimal configuration .............................................................................................. 8
      4.2. Supported context ..................................................................................................... 9
      4.3. Binaries .................................................................................................................... 9
      4.4. Special note for Kapteyn update from v2.5.X .......................................................... 10

II. **Update** .......................................................................................................................... 11
   1. Update Directory Listener .............................................................................................. 11
   2. Update Security Engine Nodes ....................................................................................... 13
      2.1. One machine ............................................................................................................. 13
      2.2. Multiple machines ................................................................................................... 15
      2.3. Meta-Kapteyn (optional) ........................................................................................ 15
   3. Update Storage Manager ............................................................................................... 16
   4. Restart machines ........................................................................................................... 18
      4.1. Start Security Engine Nodes services ...................................................................... 18
      4.2. Start Directory Listeners services .......................................................................... 18

III. **Annexes** ....................................................................................................................... 19
   1. How to change IIS certificate for AlsidForAD Web Application .................................. 19
   2. How to back up Storage Manager .................................................................................. 24
      2.1. InfluxDB ................................................................................................................ 24
      2.2. MSSQL ................................................................................................................... 24
   3. Expert Mode for Directory Listener .............................................................................. 25
      3.1. Additional subnets for Ceti ..................................................................................... 25
1. INTRODUCTION

1. Document objectives

This document is intended to help you perform a clean installation of ALSID’s on-premise solution. Each component is made of one server:

- A Directory Listener targeting audited domains,
- A Security Engine Node also acting as a Control Plane,
- A Storage Manager hosting all data, based on MSSQL and InfluxDB.

Note: For many examples, the “E” partition letter will be used by default for data partition.

2. Abbreviations

The following table lists the abbreviations used in this documentation:

<table>
<thead>
<tr>
<th>Abbr.</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DL / DLxx</td>
<td>Directory Listener</td>
</tr>
<tr>
<td>SEN / SENxx</td>
<td>Security Engine Node</td>
</tr>
<tr>
<td>DB / DBxx</td>
<td>Storage Manager</td>
</tr>
<tr>
<td>WI / Wlxx</td>
<td>Web interface, or any application offering a website</td>
</tr>
<tr>
<td>PC / PCxx</td>
<td>Personal Computer, or devices used as a computer</td>
</tr>
<tr>
<td>CP / CPxx</td>
<td>Control Plane (also referred as Web Interface)</td>
</tr>
<tr>
<td>IoE / IoExx</td>
<td>Indicator of Exposure</td>
</tr>
<tr>
<td>DC / DCxx</td>
<td>Domain Controller</td>
</tr>
</tbody>
</table>

3. Infrastructure presentation

The following information is provided as a referral for this document. The infrastructure presented here must be considered as a supported architecture.

3.1. Network Overview

The network is spliced across three areas. The following schema shows an overview of the network communication:

![Figure 1: Network overview](image-url)
To go further, please read the following schema and its associated network matrix. They describe each required protocol and port used by Alsid’s platform:

![Network flow matrix](image)

*Figure 2: Network flow matrix*

The following network matrix describes each required protocol and port used by Alsid’s platform.

<table>
<thead>
<tr>
<th>Network flows (From -&gt; To)</th>
<th>Alsid’s usage</th>
<th>Type of traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User and Computer Authentication, Forest Level Trusts</td>
<td>Kerberos</td>
<td>TCP/88, TCP/464 and UDP/464</td>
</tr>
<tr>
<td></td>
<td>User and Computer Authentication, Name Resolution, Trusts</td>
<td>DNS</td>
<td>UDP/53 and TCP/53</td>
</tr>
<tr>
<td></td>
<td>Replication, User and Computer</td>
<td>RPC, DCOM, EPM, DRSUAPI</td>
<td>TCP Dynamic (&gt; 1024)</td>
</tr>
<tr>
<td>Network flows  (From -&gt; To)</td>
<td>Alsid’s usage</td>
<td>Type of traffic</td>
<td>Protocol and Port</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| 2                           | Alsid’s Directory Listeners  
Alsid’s Security engine nodes                                                  | Alsid’s communication bus  
Advanced Message Queuing Protocol  
Alsid’s internal API flows  
(Optional)  
TL/HTTP               | TCP/5671 and TCP/5672                 | TCP/443                      |
| 3                           | End-users  
Alsid’s Security engine nodes                                                  | Alsid’s end-user services  
(Web portal, REST API, etc.)  
TLS/HTTP               | TCP/443                      |
| 4                           | Alsid’s platform  
Support services                                                                | Time synchronization  
Update infrastructure  
(e.g., WSUS or SCCM)  
PKI infrastructure  
Identity provider SAML server  
Identity provider LDAP  
Identity provider OAuth  
NTP  
HTTP/HTTPS  
HTTP/HTTPS  
TLS/HTTP  
TLS/HTTP  
TCP/80 or TCP/443  
TCP/80 or TCP/443  
TCP/443               | UDP/123  
TCP/80 or TCP/443  
TCP/389 and TCP/636  
TCP/443           |
In addition to the Active Directory protocols, some additional flows may be required depending on Alsid’s platform configuration. These protocols and ports need to be opened between Alsid’s platform and the targeted service.

<table>
<thead>
<tr>
<th>Network flows</th>
<th>Alsid’s usage (optional)</th>
<th>Type of traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5</strong> Alsid’s Security engine nodes &lt;-&gt; Cybersecurity services</td>
<td>Alsid Web Application</td>
<td>HTTP/TLS</td>
<td>TCP/443</td>
</tr>
<tr>
<td></td>
<td>Email notifications</td>
<td>SMTP</td>
<td>TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025 (depending on the SMTP server’s configuration)</td>
</tr>
<tr>
<td></td>
<td>Syslog notifications</td>
<td>Syslog</td>
<td>TCP/601, TCP/6515, UDP/514 (depending on the event log server’s configuration)</td>
</tr>
<tr>
<td>6</td>
<td>Alsid REST API</td>
<td>HTTP/TLS</td>
<td>TCP/443</td>
</tr>
<tr>
<td>Alsid’s Security engine nodes &lt;-&gt; Alsid’s Storage Manager</td>
<td>MSSQL Server database access</td>
<td>MSSQL queries</td>
<td>TCP/1433</td>
</tr>
<tr>
<td></td>
<td>InfluxDB Server access</td>
<td>InfluxDB queries over HTTP</td>
<td>TCP/8086</td>
</tr>
</tbody>
</table>

### 3.2. Recommended architectures

The application runs through many engines that are divided across multiple machines. The power we need depends on the AD activity traffic, which is hard to estimate before deploying. Most of the time, it can be correlated with the number of active users in the AD.

Under 300,000 active users, we recommend using a three-server architecture. Each server has one or more services, and each server must be considered as an independent entity.
If there are more than 300,000 active users, these three servers will be overloaded, and performance will be insufficient. Security Engine Node needs to be split into four machines.

For more information about the hardware specification, please refer to Start Security Engine Nodes services on page 18.
3.3. Meta-Kapteyn architecture (optional)

For example, let’s consider a group which is in Europe and has a subsidiary in North America. They are not directly connected and there is no trust relationship between their Active Directory domains. Meta-Kapteyn can be used as a consolidation platform to display both dashboards of Europe and North America instances on a single page.

This feature is optional and is not required for the analysis.

For more information, please refer to appropriate install documentation.

3.4. Installation log file

If the installer cannot update Alsid for AD on a machine, please forward us the log file to our support address (support@alsid.com). This file is in your %temp% folder and its name is always starting with “MSI” followed by random numbers. For example: MSI65931.LOG.

4. Prerequisites

4.1. Minimal configuration

The Alsid_for_AD_On-Premise_technical_prerequisites_vX.X document describes the sizing requirements to run the solution. Running AlsidForAD on a configuration thinner than these prerequisites is not supported.

<table>
<thead>
<tr>
<th>Directory Listeners - Sizing Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active AD users</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>1 – 25 000</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
</tr>
<tr>
<td>50 001 – 75 000</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Engine Nodes - Sizing Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active AD users</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>1 – 25 000</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
</tr>
<tr>
<td>50 001 – 75 000</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

(Gold Performance)
### 4.2. Supported context

- AlsiforAD works with Windows Server 2016 with the latest available update.
- AlsiforAD installer requires Local Administrator rights on Windows Server 2016. If the account used for the installation is not the built-in one, make sure that this account can run programs without restrictions.
- AlsiforAD services require Local Administrator rights to run local services on the machine.
- AlsiforAD requires a dedicated data partition. AlsiforAD must not be run on the OS partition to prevent system freeze if the partition is full.
- AlsiforAD SQL instance requires the virtual accounts usage feature.
- AlsiforAD works on a three-tier model. One or two VMs are not supported. At least three VMs and eventually more than one DL are supported. **Exception:** Ceti-TLS mode requires only one VM from a customer point-of-view.
- AlsiforAD must be considered as a black-box: Each machine must be considered as dedicated to the product and must not be shared for another purpose.
- AlsiforAD can create any folder starting with ‘Alsid’ prefix on the data partition. Therefore, do not create folders starting with ‘Alsid’ on the data partition.
- Erlang known issues: the HOMEDRIVE environment variable must not be modified. The PATHTEXT environment variable must contains the .EXE and .BAT file extensions.

### 4.3. Binaries

AlsiforActive Directory installer binary is available on its release portal [https://release.alsid.app](https://release.alsid.app):

- AlsiforAD_v2.X.X.exe

This package contains the files required to perform installation/uninstallation/update and to reconfigure the solution with different IP addresses (if needed).
◊ **Windows Server (Desktop Experience)**

The installer binary must be placed in a valid location on each server to be set up. In the following example, on the Storage Manager machine, we put it on the Desktop:

<table>
<thead>
<tr>
<th>Binaries location</th>
<th>Binaries content</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Users\Administrator\Desktop\</td>
<td><img src="image" alt="Desktop Folder" /></td>
</tr>
</tbody>
</table>

- Extended debug logging can be activated with the following command (replace the first path by your installer file location, and the second by your log file path):

  ```
  "C:\Users\Administrator\Desktop\AlsidForAD_2.X.X.exe" Ai_DEBUGLOG=1 /L*v "E:\example.log"
  ```

◊ **Windows Server Core**

The installer GUI can be displayed on a Server Core. Type this command to start the installation:

- Run the following command (replace the path by your exe file location):

  ```
  C:\Users\Administrator\Desktop\AlsidForAD_2.X.X.exe
  ```

### 4.4. Special note for Kapteyn update from v2.5.X

As we are switching from a PowerShell installer to an executable installer, the **IIS configuration will be reset**. Therefore, you will have to re-select manually your trusted certificate as explained in **How to change IIS certificate for AlsidForAD Web Application** on page 19 after the update.
II. UPDATE

1. Update Directory Listener

During this step, the process will update the following applications:

- Alsid component
  - Ceti

In a specific context, it can be useful to deploy more than one DL within the same infrastructure. For example, if two forests are registered in the solution but those two are on different networks because of legal restrictions, you can deploy one DL in the first subnet and another DL in the second subnet.

**IMPORTANT NOTICE:**

If you are updating AlsidForAD from a PowerShell installation, please refer to the version 2.6.0 for a complete explanation of the migration process.

---

Expert Mode:
This configuration requires to check the "Expert mode" box on the first installer window to display advanced installation options. For more details, please refer to Expert Mode for Directory Listener on page 25.

---

The update mechanism is fully automated through an installer file. To perform the update, execute "AlsidForAD_v2.X.X.exe" with full Local Administrator privileges and click on the "Next" button.

![Welcome dialog on Directory Listener](image)

*Figure 5: Welcome dialog on Directory Listener*

On the next dialog, features and location are automatically preselected based on the previous installation. As mentioned just before, here you can see that only the **DirectoryListener** feature must be selected. Click on the "Next" button.
RabbitMQ's IP address is automatically filled based on the previous version. You can check if this is consistent, then click on the “Next” button and update Alsid for AD.

At the end of the installation, WAIT until the server asks for a reboot. Don’t reboot it now! Leave it like this for the moment and go to the next page. We will reboot it later.
2. Update Security Engine Nodes

During this step, the process will update the following applications:

- Alsid nodes
  - Cancri
  - Caroli
  - Cephei
  - Ceti-Bridge
  - Corvi
  - Corvi2
  - Cygni
  - Electra
  - Enif
  - Equuleus
  - Eridanis
  - Kapteyn
  - IIS
  - RabbitMQ

The SEN machine can be split into different machines to improve performance on huge infrastructures.

2.1. One machine

The update mechanism is fully automated through an installer file. To perform the update, execute "AlsidForAD_v2.X.X.exe" with full Local Administrator privileges and click on the "Next" button.

![Welcome dialog on Security Engine Node](image)

Figure 8: Welcome dialog on Security Engine Node

On the next dialog, features and location are automatically preselected based on the previous installation. As mentioned before, here you can see that only the **SecurityEngineNode** feature must be selected. Click on the "Next" button.
All required fields are automatically filled based on the previous version. You can check if this is consistent, then click on the "Next" button.

The same thing applies to the next window. Then, click on the "Next" button and update Alsid for AD.
At the end of the installation, **WAIT** until the server asks for a reboot. *Don’t reboot it now!* Leave it like this for the moment and go to the next page. We will reboot it **later**.

### 2.2. Multiple machines

Follow the instructions above, but in the following order on the machines which are running those services:

1. Cygni
2. Cancri
3. Caroli
4. Others (Eridanis, Kapteyn, etc.)
5. RabbitMQ

### 2.3. Meta-Kapteyn (optional)

To update Meta-Kapteyn, as it’s just a component without data, please refer to appropriate Uninstall and Install guides.

1. Uninstall Meta-Kapteyn using the uninstall script for Security Engine Nodes (follow the uninstall procedure).
2. As asked by the script, reboot
3. Install Meta-Kapteyn using the dedicated install script (follow the install procedure).
3. Update Storage Manager

During this step, the process will update the following applications:

- InfluxDB (Alsid database)
- MSSQL (Alsid database)

The update mechanism is fully automated through an installer file.

If you are looking for a procedure to back up the databases before running the update, please refer to How to back up Storage Manager on page 24.

The update mechanism is fully automated through an installer file. To perform the update, execute “AlsidForAD_v2.X.X.exe” with full Local Administrator privileges and click on the “Next” button.

![Figure 12: Welcome dialog on Storage Manager](image)

On the next dialog, features and location are automatically preselected based on the previous installation. As mentioned before, here you can see that only the StorageManager feature must be selected. Click on the “Next” button.
All required fields are automatically filled based on the previous version. You can check if this is consistent, then click on the "Next" button and update Alsid for AD.

Wait for the end of the installation and click on YES to reboot the server.
4. Restart machines

4.1. Start Security Engine Nodes services

Databases must be running before starting SEN services. So now the SEN machine can be restarted by clicking on the “Yes” button.

![Image of Installer Information window](image)

Figure 15: Reboot message after update message box on SEN

If you have more than one SEN machine, please follow this reboot order:

1. RabbitMQ
2. Others (Eridanis, Kapteyn, etc.)
3. Cancri
4. Caroli
5. Cygni

4.2. Start Directory Listeners services

Databases and SEN must be running before starting DL services. So now the DL machine can be restarted by clicking on the “Yes” button.

![Image of Installer Information window](image)

Figure 16: Reboot message after update message box on DL
III. ANNEXES

1. How to change IIS certificate for AlsidForAD Web Application

When the AlsidForAD SEN module is installed, a self-signed certificate is created and binds to the AlsidForAD web application.

The certificate name is chosen during the installation, and is equal to webAppHostName. Let’s assume that the chosen name is the IP address of the SEN server where the IIS role is installed, since this is the most common scenario.

If, by assumption, the IP address of the SEN server is 10.0.48.55, after installation, the web application can be accessed via https://10.0.48.55.

![Figure 17: Login page of AlsidForAD](image)

There are two important pieces involved here so you can access the web application via HTTPS:

- Self-signed certificate
- Web App binding

During installation, a self-signed certificate is created and placed in the IIS Server Certificate store.

To access this certificate, go to Windows Start > Windows Administrative Tools > Internet Information Services (IIS) Manager, and click on Server Name on the left (Connections) pane followed by a double-click on ‘Server Certificates’.
During installation, IIS Site Binding is created by using the HTTPS port (443 by default) and the self-signed certificate.

To explore this binding, go to **Windows Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager** and expand the ‘Sites’ menu on the left pane. Right-click on your site (Default Web Site, in this example) and choose ‘Edit Bindings’. A new window ‘Site Bindings’ will pop up, and from there you can select ‘https’ binding and click on ‘Edit’.

On the ‘Edit Site Binding’ window that will appear, you can find installed IIS certificates in the drop-down menu at the bottom of the dialog.
To use your certificate for the AlsidForAD web application, you must:

- Install your certificate in IIS.
- Edit site binding to use your installed certificate.

To install the IIS Certificate, go to Windows Start > Windows Administrative Tools > Internet Information Services (IIS) Manager and click on Server Name on the left (Connections) pane followed by a double-click on ‘Server Certificates’. From there, choose ‘Import’ on the right pane menu and import your certificate.
You can also choose any other way to install the IIS certificate. The end goal is to have your certificate appear on the IIS Server Certificates list.

To edit binding, navigate to 'Edit Site Binding' as described above, and choose your newly installed certificate from the SSL certificate dropdown menu at the bottom of the dialog:
Figure 22: Select new certificate in IIS Manager

Right-click on the website on the left pane and restart to take effect.

Figure 23: Restart IIS Manager service
2. How to back up Storage Manager

2.1. InfluxDB

◊ Backup

To perform a remote backup, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to D:\Alsidi\AlsidiForAD\AfadInfluxDB\influxdb
- Run the following command (replace the yellow part by the real expected value):

```
influx backup -portable -host <host:port> <path-to-backup>
```

To perform a local backup, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to D:\Alsidi\AlsidiForAD\AfadInfluxDB\influxdb
- Run the following command (replace the yellow part by the real expected value):

```
influx backup -portable <path-to-backup>
```

◊ Restore

To perform a remote restoration, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to D:\Alsidi\AlsidiForAD\AfadInfluxDB\influxdb
- Run the following command (replace the yellow part by the real expected value):

```
influx restore -portable -host <host:port> <path-to-backup-files>
```

To perform a local restoration, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to D:\Alsidi\AlsidiForAD\AfadInfluxDB\influxdb
- Run the following command (replace the yellow part by the real expected value):

```
influx restore -portable <path-to-backup-files>
```

⚠️ The backup is a folder, not a file.

Source: [https://docs.influxdata.com/influxdb/v1.7/administration/backup_and_restore/](https://docs.influxdata.com/influxdb/v1.7/administration/backup_and_restore/)

2.2. MSSQL

Please follow the official documentation to perform MSSQL backup or restoration:

The database name is "dsc" prior to version 2.6.0, and "alsiforad" for ulterior versions.
3. Expert Mode for Directory Listener

Expert Mode: The following options are only available when this mode is switched on.

3.1. Additional subnets for Ceti

You can specify the subnet(s) you want to use for Ceti. If you want to add more than one subnet, use a comma as a separator between the CIDR subnets you will use. For example, 10.0.0.1/32, 192.168.0.0/24.

All required fields are automatically filled based on the previous version. You can check if this is consistent (in the following screenshot, we are only using one subnet). Then, click on the “Next” button and update Alsid for AD.

![Figure 24: DirectoryListener settings dialog with Expert Mode](image)

At the end of the installation, **WAIT** until the server asks for a reboot. **Don’t reboot it now!** Leave it like this for the moment and go to **Update Security Engine Nodes** on page 13. We will reboot it **later**.