TENABLE.AD
UNINSTALL PROCEDURE

1. Document contributors:

Author	Qualification	Contact address
TENABLE	DevOps team	support@alsid.com

2. Document history:

Version	Date (dd/mm/yyyy)	Author	Comments
2.4.0	12/07/2019	ALSID	Initial document
2.4.1	19/07/2019	ALSID	Update for 2.4.1
2.4.2	02/08/2019	ALSID	Update for 2.4.2
2.5.0	23/10/2019	ALSID	Update for 2.5.0
2.6.0	19/02/2020	ALSID	Update for 2.6.0
2.6.3	04/04/2020	ALSID	Update for 2.6.3
2.7.0	06/06/2020	ALSID	Review for 2.7.0
3.0.0.	01/12/2020	TENABLE	Update for 3.0.0

TABLE OF CONTENTS

I. INTRODUCTION

1. Document objectives

This document is intended to help you uninstall TENABLE's on-premises solution. Each component is made of one server:

- A Directory Listener targeting the audited domains,
- A Security Engine Node where the security analysis is performed and the web interface served,
- 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 list abbreviations used within this documentation

Abbr.	Definition
DL / DLxx	Directory Listener
SEN / SENxx	Security Engine Node
DB / DBxx	Storage Manager
WI / WIxx	Web Interface, or any application offering a website
PC / PCxx	Personal Computer, or devices used as a computer
IoE / IoExx	Indicator of Exposure
DC / DCxx	Domain Controller

3. Installation log file

If the installer cannot uninstall Tenable.ad on a machine, please forward us the log file to our support address (support@alsid.com). This file is in your `%tmp%` folder and its name is always starting with "*MSI*" followed by random numbers. For example: `MSI65931.LOG`.

II. UNINSTALL TENABLE PACKAGES

During this step, the process will remove all the components of Tenable.ad.

The uninstallation mechanism is fully automated through the control panel. To perform the uninstallation, select "*Alsid for Active Directory*" or "*Tenable.ad*" and click on the "*Uninstall*" button.
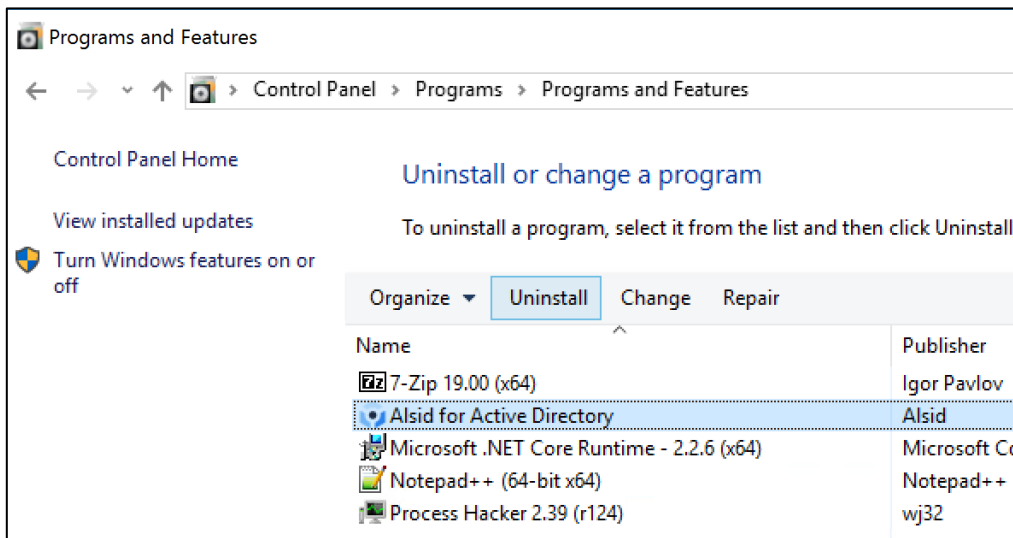

Figure 1: Control Panel Programs and Features view

The next dialog will ask you to confirm, click on the "*Yes*" button.
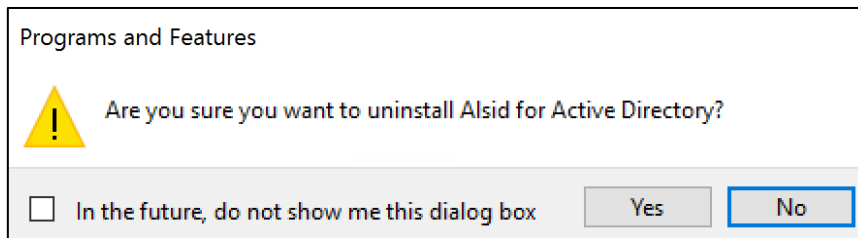

Figure 2: Uninstall Tenable.ad

Wait for the main uninstall operation to complete, the dialog will then disappear.

The uninstall process includes a second stage as indicated by the system tray icon status on the right:

Figure 3: Prerequisites uninstall

This icon disappears from the system tray when the uninstall process is fully achieved.

III.   UNINSTALL TENABLE'S INDICATORS-OF-ATTACKS

In case of an uninstallation of Tenable's product, the configuration can be rolled back using the **Tenable's deployment script**.

To uninstall the audit policies, WMI filters and initial GPO, simply run the following command:

Command line
`Register-TenableIOA.ps1 -Uninstall`

This command creates a new GPO, named "`Tenable.ad cleaning`" by default, that will be used to clean the previously installed GPO's. The previous GPO and its SYSVOL files, including the registry setting the advanced logging policy, and the WMI filters will be cleaned.

If you had changed the initial GPO's name, e.g. to comply to your naming conventions, you will have to pass it to the uninstall step too for the script to know which GPO to uninstall.

This new GPO also needs to be replicated over the entire domain, and the GPO refresh interval passed, for the uninstall process to be complete. Tenable recommends letting it run for a week, then simply **manually removing this cleaning GPO**.