



CyberArk SAP Scanner

Copyright © 1999-2018 CyberArk Software Ltd. All rights reserved.

This document contains information and ideas, which are proprietary to CyberArk Software Ltd. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, without the prior written permission of CyberArk Software Ltd.

11/05/2018

Table of Contents

Introduction and Overview	3
Install CyberArk SAP Scanner	4
System Requirements.....	5
Scan SAP Systems.....	6



Introduction and Overview

CyberArk SAP Scanner is a discovery tool that assists organizations to scan for privileged accounts in their various SAP NetWeaver environments. The tool streamlines and simplifies the on-boarding process of SAP environments managed by the CyberArk Privileged Access Security solution.



Install CyberArk SAP Scanner

This section describes how to install CyberArk SAP Scanner. It contains the following topics:

- System Requirements
- Installation Notes

System Requirements

Minimum system requirements for running CyberArk SAP Scanner

- Operating System – Windows Server 2012 R2 or higher
- Disk space – At least 1GB free disk space
- Install .Net Framework 4.6.1

Prerequisites

- Install SAP .NET Connector (NCo) 3.0
- TCP/IP port 3301 is opened to the SAP NetWeaver server

Supported SAP NetWeaver

CyberArk SAP Scanner can perform scans on the following SAP NetWeaver versions:

- 7.x

Installation Notes

1. Download the CyberArk SAP Scanner package.
2. Extract the CyberArk SAP Scanner package to the local drive.



Scan SAP Systems

Start the Scan

Launch the following command to initiate the scan:

```
> CyberArk.SAPScanner.exe <systems_file> <user_permissions_file>
```

System File

Create a CSV file that contains the following details:

Parameter	Description
SID	System ID Usually composed of three letters
Host Name	Target system IP address
System Number	System number in two digits
User Name	User that has sufficient privileges to retrieve the list of users
Password	User name password
Client	Client number in three digits

Example:

SID	HostName	SystemNumber	UserName	Password	Client
ABC	192.168.1.1	00	DDIC	Password1	001

Note: You can add multiple systems. Each system is listed in a separate row. You can use the template provided with the scanner. Example file is attached in the package.

User Permissions File

Create a text file that contains a list of all permissions that you consider as privileged permissions (i.e. SAP_ALL).

Each permission in a separate line.

Example:

SAP_ALL
S_A.SYSTEM

Note: You can add multiple systems. Each system is listed in a separate row. You can use the template provided with the scanner. Example file is attached in the package.

Output Files

The output files are created in the same directory where the CyberArk SAP Scanner executable is located.

There are two output files generated by the CyberArk SAP Scanner, one in a CSV format and the other in a JSON format.

CSV File

The list of all detected users in a format that can be used to onboard all accounts via the Account Onboard Utility (AOU). You can find the AOU in the following link <https://github.com/cyberark/epv-api-scripts>.

JSON File

This file contains the full details of the users that are scanned by the CyberArk SAP Scanner utility. The account permissions are described in details in the Profiles parameters.



JSON file example:

```
{
  "UserName": "BWDEVELOPER",
  "FirstName": "John",
  "LastName": "Doe",
  "LogonData": {
    "ValidFrom": "1900-01-01T00:00:00",
    "ValidTo": "1900-01-01T00:00:00",
    "Type": "A",
    "UserGroup": "SUPER"
  },
  "AccountStatus": {
    "WrongLogon": "U",
    "LocalLocked": "U",
    "GlobalLocked": "U",
    "NoPassword": "U"
  },
  "LastModified": {
    "DateTime": "2016-01-20T13:23:20",
    "Modifier": null
  },
  "Profiles": [
    {
      "Profile": "SAP_ALL",
      "Description": "All SAP System authorizations"
    },
    {
      "Profile": "S_A.SYSTEM",
      "Description": "System administrator (Superuser)"
    }
  ]
}
```

