Safeguard for Privileged Passwords Package

Readme

Version 1.1

27/04/2021

Table of Contents

1. Introduction

This document contains all essential information for the user to make full use of this A2019 Safeguard for Privileged Passwords package. It includes a description of the functions and capabilities and step-by-step procedures for setup & configuration of the Safeguard for Privileged Passwords package.

1.1 Overview

This package allows a robot to obtain a credential managed by Safeguard for Privileged Passwords, to be used by the Automation Anywhere bot at runtime.

1.2 Use cases

The key use cases include:

- Where a bot is required to use a credential, under management of the Safeguard for Privileged Passwords vault, this package makes action steps available for the robot to be configured to retrieve credentials at runtime.
  - The action step uses a certificate to authenticate to the Safeguard for privileged passwords API
  - An API key is then obtained from Safeguard for Privileged Passwords
  - The API is then used to retrieve the credential that is allocated for that bot, according to policies held within Safeguard for Privileged Passwords.
  - The credential provided is made available to the bot as a variable, which can be used to authenticate using the corresponding privileged account.

2. Requirements & Prerequisites

2.1 System Requirements

Enterprise A2019 (Cloud deployed) and Community Edition device requirements.

Review the machine hardware specifications, operating system versions, and browser types supported by Automation Anywhere Enterprise for creating and running bots and command packages as an Enterprise A2019 (Cloud deployed) or Community Edition user on your local machine.

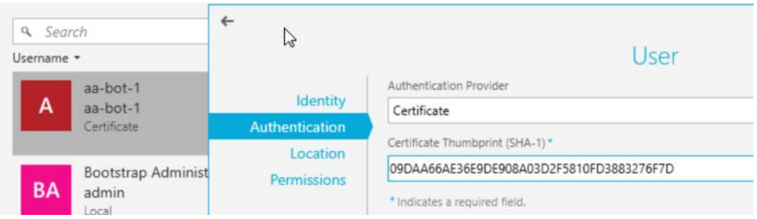
2.2 Prerequisites

- Automation Anywhere (AA) A2019 is installed.
- Safeguard for Privileged Passwords (SPP) is installed. For version compatibility, see **Changelog** at the end of the document.
- Bot device users have a certificate that will be used to authenticate to Safeguard.

3. Getting Started

3.1 Configuration of Safeguard for Privileged Passwords

1. Create a certificate user for the bot which is going to obtain passwords from SPP, for example aa-bot-1.

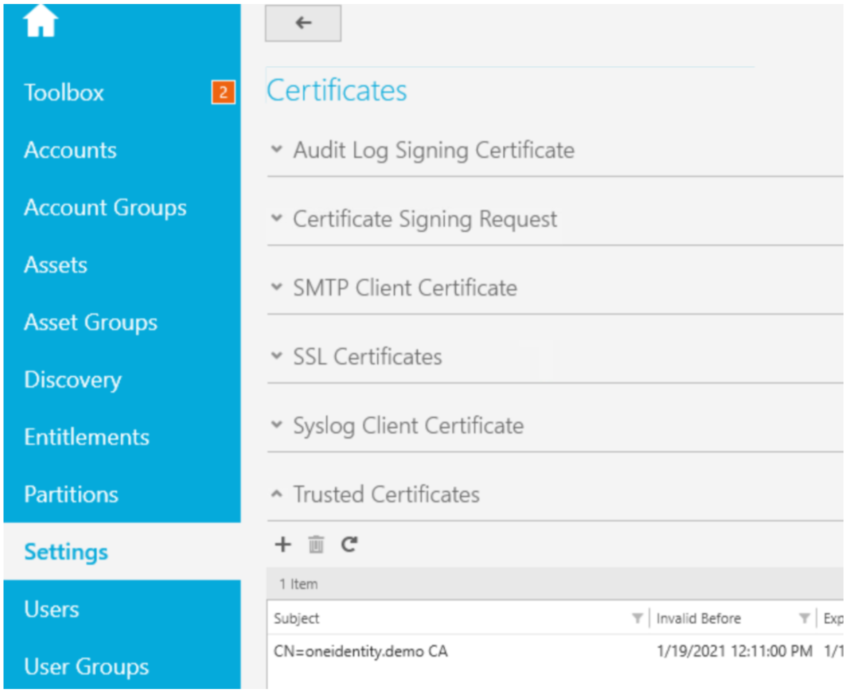


Authentication Provider
Certificate

Certificate Thumbprint (SHA-1) *
09DAA66AE36E9DE908A03D2F5810FD3883276F7D

* Indicates a required field.

   a. Make sure the signing CA of the user's certificate is trusted

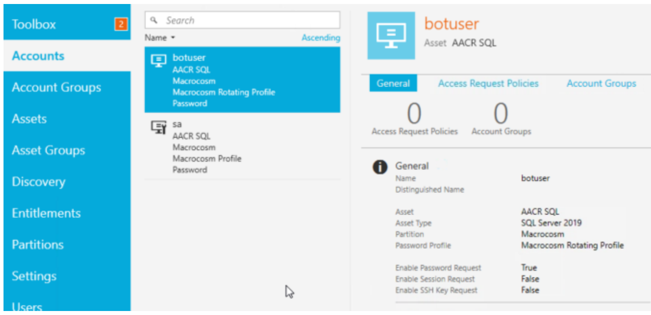


1 Item

Subject	Invalid Before	Exp
CN=oneidentity.demo CA	1/19/2021 12:11:00 PM	1/1

2. Configure the Assets and Accounts which will be used by the AA bot.

    a. Do not configure an Access Request Policy.



botuser
AACR SQL
Macrocosm
Macrocosm Rotating Profile
Password

sa
AACR SQL
Macrocosm
Macrocosm Profile
Password

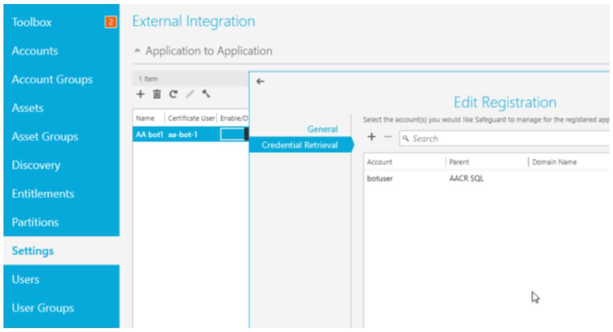
botuser
Asset AACR SQL

General

Name	botuser
Distinguished Name	
Asset	AACR SQL
Asset Type	SQL Server 2019
Partition	Macrocosm
Password Profile	Macrocosm Rotating Profile
Enable Password Request	True
Enable Session Request	False
Enable SSH Key Request	False

3. Enable the Application to Application (A2A) service.

4. Configure Application to Application access for the bot certificate user (e.g. the aa-bot-1) and assign the above created account to it for Credential Retrieval.

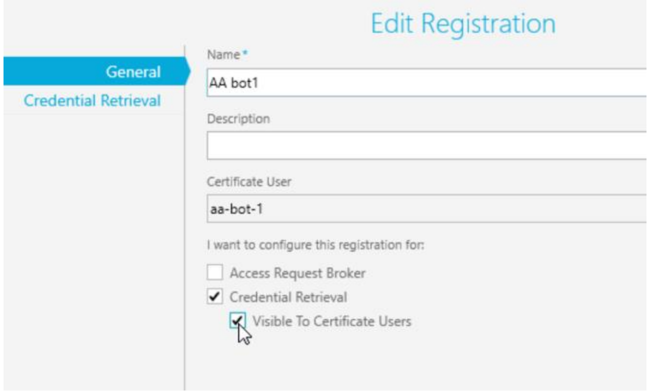


Name	Certificate User	Enable/D
AA bot1	aa-bot-1	

Select the account(s) you would like Safeguard to manage for the registered app

Account	Parent	Domain Name
botuser	AACR SQL	

    a. Make sure the 'Visible to Certificate Users' function is enabled.



Name *
AA bot1

Description

Certificate User
aa-bot-1

I want to configure this registration for:

☐ Access Request Broker
☑ Credential Retrieval
☑ Visible To Certificate Users

3.2 Configuration of Bot Runner

1. Define a device user which will be used to login to the bot devices and will be used as the bot's execution context. Login with that user to the machine which you will run the bot on.

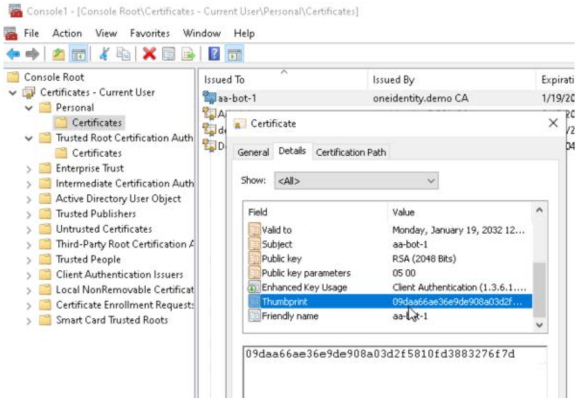
2. Obtain the following PFX certificates:

    a. The certificate of the Safeguard user configured for A2A access.

    b. The CA certificate signed by the user's certificate.

3. Import the certificates to the *Current User* certificate store of this user on the executing device machine (e.g. a Windows client):

    a. The user's PFX certificate into the *Personal* certificate store:

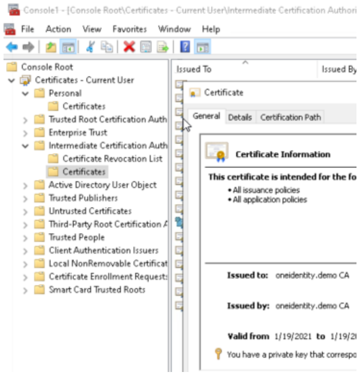

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Auth
Certificates
Enterprise Trust
Intermediate Certification Auth
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification A
Trusted People
Client Authentication Issuers
Local NonRemovable Certificat
Certificate Enrollment Requests
Smart Card Trusted Roots
Certificate
General
Details
Certification Path
Show:
<All>

Issued To	Issued By	Expirati
aa-bot-1	oneidentity.demo CA	1/19/20

Field	Value
Valid to	Monday, January 19, 2032 12...
Subject	aa-bot-1
Public key	RSA (2048 Bits)
Public key parameters	05 00
Enhanced Key Usage	Client Authentication (1.3.6.1....
Thumbprint	09daa66ae36e9de908a03d2f...
Friendly name	aa-bot-1

```
09daa66ae36e9de908a03d2f5810fd3883276f7d
```

    b. The PFX CA of the user's certificate into the *Intermediate Certification Authorities*:


Console1 - [Console Root\Certificates - Current User\Intermediate Certification Authori
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Auth
Enterprise Trust
Intermediate Certification Auth
Certificate Revocation List
Certificates
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification A
Trusted People
Client Authentication Issuers
Local NonRemovable Certificat
Certificate Enrollment Requests
Smart Card Trusted Roots
Issued To
Issued By
Certificate
General
Details
Certification Path

Certificate Information

This certificate is intended for the fo

- All issuance policies
- All application policies

Issued to: oneidentity.demo CA

Issued by: oneidentity.demo CA

Valid from 1/19/2021 **to** 1/19/2

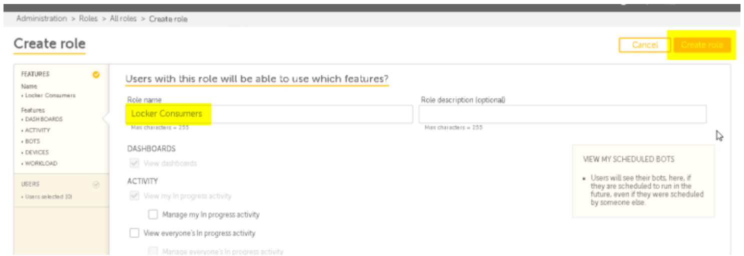
You have a private key that correspo

3.3 Configuration of Automation Anywhere control center

In case you already have a bot developer user with a device configured to run bots, you may skip this chapter.

1. Login to the Control Room with an administrator account.

2. Navigate to *Administration* > *Roles* and create a new *Locker Consumers* role so the bot developer will be able to consume the credentials required to integrate with Safeguard. Name it and create the role with the default selected features.



Create role

FEATURES
Name
- Locker Consumers
Features
- DASHBOARDS
- ACTIVITY
- BOTS
- DEVICES
- WORKLOAD

USERS
- Users selected (0)

Users with this role will be able to use which features?

Role name: Locker Consumers (Max characters = 255)

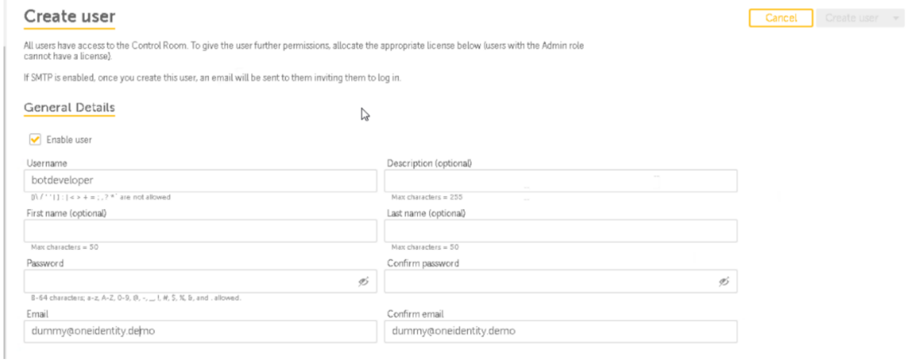
Role description (optional): (Max characters = 255)

DASHBOARDS
☑ View dashboards

ACTIVITY
☑ View my in progress activity
☐ Manage my In progress activity
☐ View everyone's In progress activity
☐ Manage everyone's In progress activity

VIEW MY SCHEDULED BOTS
- Users will see their bots, here, if they are scheduled to run in the future, even if they were scheduled by someone else.

3. Navigate to *Administration* > *Users* and create a new *botdeveloper* user.



Create user

All users have access to the Control Room. To give the user further permissions, allocate the appropriate license below (users with the Admin role cannot have a license).

If SMTP is enabled, once you create this user, an email will be sent to them inviting them to log in.

General Details

☑ Enable user

Username: botdeveloper
[]\ / ' ' [ ] : | < > + = ; , ? * ` are not allowed

Description (optional):
Max characters = 255

First name (optional):
Max characters = 50

Last name (optional):
Max characters = 50

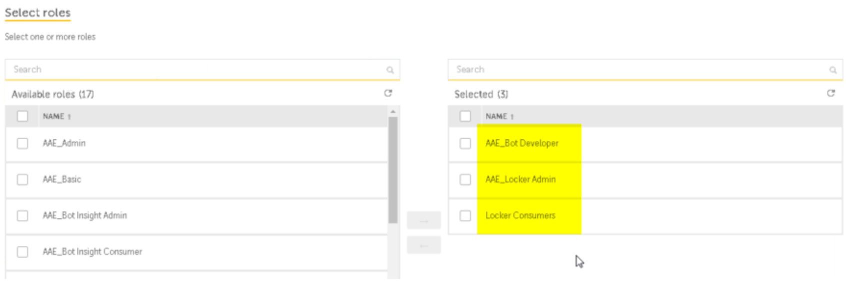
Password:
8-64 characters; a-z, A-Z, 0-9, @, -, _, !, #, $, %, &, and . allowed.

Confirm password:

Email: dummy@oneidentity.demo

Confirm email: dummy@oneidentity.demo

a. Select the following roles:



Select roles

Select one or more roles

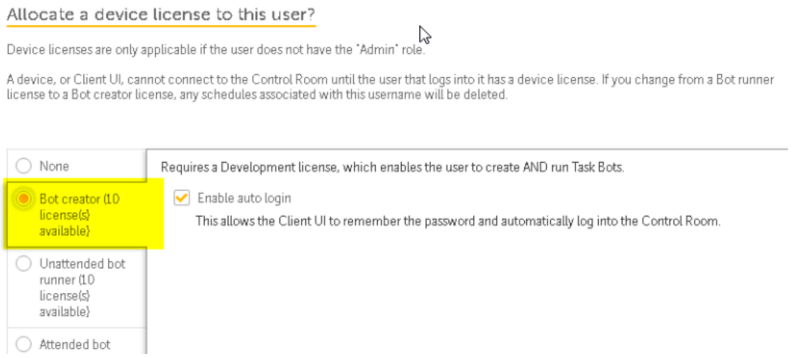
Available roles (17)

☐	NAME ↑
☐	AAE_Admin
☐	AAE_Basic
☐	AAE_Bot Insight Admin
☐	AAE_Bot Insight Consumer

Selected (3)

☐	NAME ↑
☐	AAE_Bot Developer
☐	AAE_Locker Admin
☐	Locker Consumers

b. Allocate a *Bot creator* license to the user.



Allocate a device license to this user?

Device licenses are only applicable if the user does not have the "Admin" role.

A device, or Client UI, cannot connect to the Control Room until the user that logs into it has a device license. If you change from a Bot runner license to a Bot creator license, any schedules associated with this username will be deleted.

○ None

● Bot creator (10 license(s) available)

○ Unattended bot runner (10 license(s) available)

○ Attended bot

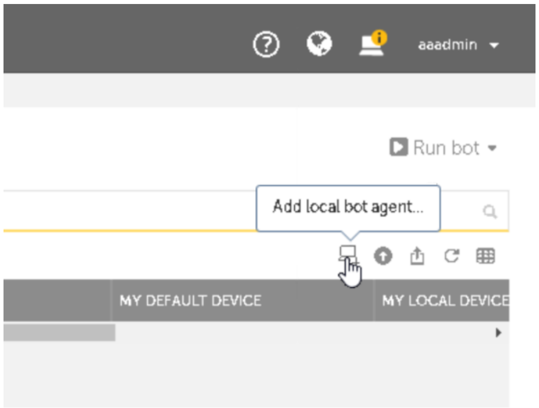
Requires a Development license, which enables the user to create AND run Task Bots.

☑ Enable auto login

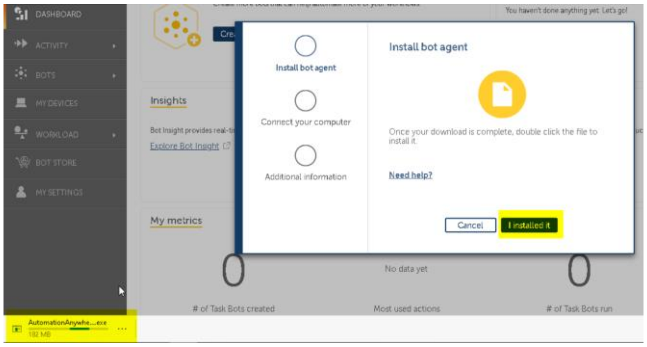
This allows the Client UI to remember the password and automatically log into the Control Room.

4. In case you're not logged in through a browser running on the but execution device, logout and login from that machine.

5. Navigate to *My devices* and click *Add local bot agent..*



a. Click *Connect to my computer* then install the bot agent, then click '*I installed it'.*



Install bot agent

Connect your computer

Additional information

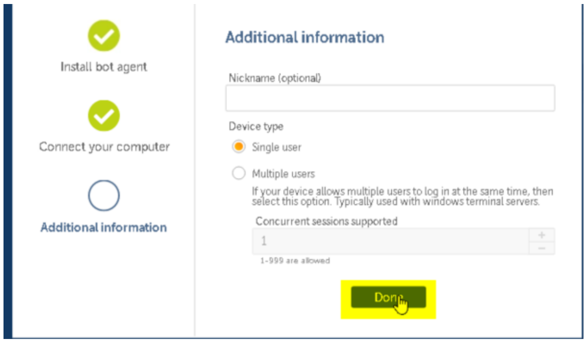
Install bot agent

Once your download is complete, double click the file to install it.

Need help?

Cancel | I installed it

b. When connected, click Done.



Install bot agent

Connect your computer

Additional information

Additional information

Nickname (optional)

Device type

● Single user

○ Multiple users

If your device allows multiple users to log in at the same time, then select this option. Typically used with windows terminal servers.

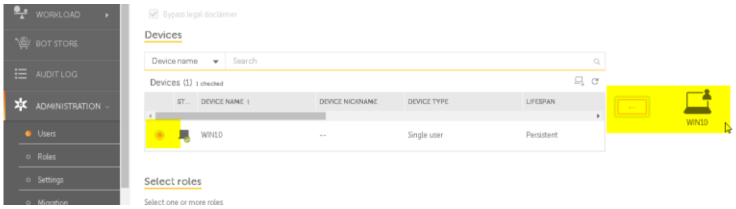
Concurrent sessions supported

1

1-999 are allowed

Done

6. Navigate to *Administration* > *Users* and look into the details of our *botdeveloper* user. Assign the new device to our botdeveloper user.



☑ Bypass legal disclaimer

Devices

Device name ▾ Search

Devices (1) 1 checked

	ST...	DEVICE NAME ↑	DEVICE NICKNAME	DEVICE TYPE	LIFESPAN
●		WIN10	--	Single user	Persistent

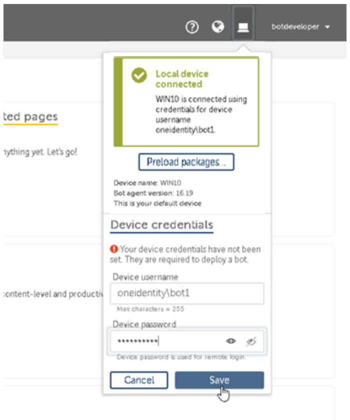
WIN10

Select roles

Select one or more roles

7. Logout with the AA administrator and login with our *botdeveloper* to the Control Center. Make sure you do it on a browser running on the device client machine the bot will be executed on.

8. Configure the device credentials.



Local device connected

WIN10 is connected using credentials for device username oneidentity\bot1.

Preload packages...

Device name: WIN10
Bot agent version: 16.19
This is your default device

Device credentials

Your device credentials have not been set. They are required to deploy a bot.

Device username

oneidentity\bot1

Max characters = 255

Device password

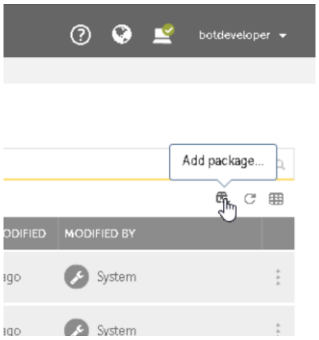
••••••••••

Device password is used for remote login.

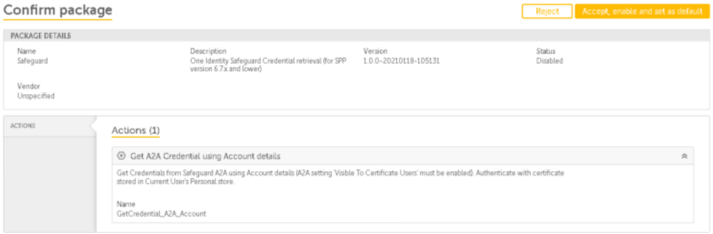
Cancel Save

3.4 Installation and Usage of the Safeguard Package

1. Navigate to *Bots > Packages* and click *Add package.*



   a. Upload the package, then click *Accept, enable, and set as default.*



Confirm package

PACKAGE DETAILS

Name
Safeguard

Description
One Identity Safeguard Credential retrieval (for SPP version 6.7.x and lower)

Version
1.0.0-20210118-105131

Status
Disabled

Vendor
Unspecified

ACTIONS

Actions (1)

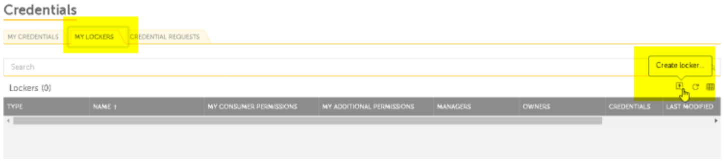
Get A2A Credential using Account details

Get Credentials from Safeguard A2A using Account details (A2A setting 'Visible To Certificate Users' must be enabled). Authenticate with certificate stored in Current User's Personal store.

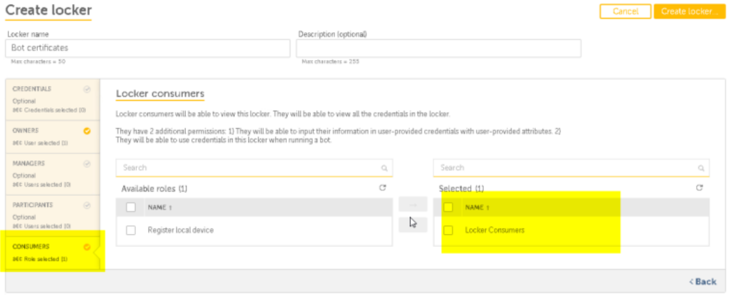
Name
GetCredential_A2A_Account

2. Put the certificate thumbprint into a locker.

   a. Navigate to *Bots > Credentials* and click *Create locker.*



   b. Make sure you add the previously created *Locker Consumer* role to the *Consumers.*



Create locker

Locker name
Bot certificates
Max characters = 50

Description (optional)
Max characters = 255

Credentials selected (0)

User selected (1)

Users selected (0)

Users selected (0)

Role selected (1)

Locker consumers

Locker consumers will be able to view this locker. They will be able to view all the credentials in the locker.

They have 2 additional permissions: 1) They will be able to input their information in user-provided credentials with user-provided attributes. 2) They will be able to use credentials in this locker when running a bot.

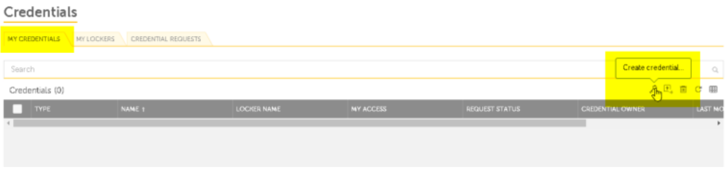
Available roles (1)

□ Register local device

Selected (1)

□ Locker Consumers

c. Create a new Credential.

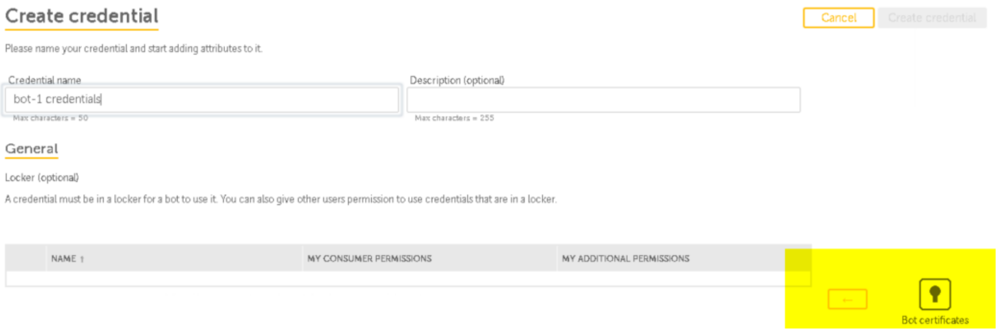


Credentials

Credentials (0)

☐	TYPE	NAME ↑	LOCKER NAME	MY ACCESS	REQUEST STATUS	CREDENTIAL OWNER	LAST MO

d. Add the credential to the previously created locker.



Create credential

Please name your credential and start adding attributes to it.

Credential name: bot-1 credentials
Max characters = 50

Description (optional):
Max characters = 255

General

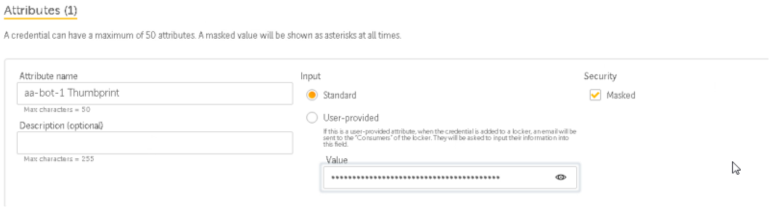
Locker (optional)

A credential must be in a locker for a bot to use it. You can also give other users permission to use credentials that are in a locker.

NAME ↑	MY CONSUMER PERMISSIONS	MY ADDITIONAL PERMISSIONS

In this example we organized credentials per device user. Feel free to organize the credentials per preference. The only credential required by the Safeguard package, is the thumbprint of the certificate which will be used by the bot to authenticate to Safeguard. This is the certificate which is stored in the Personal certificate store of the device user.

e. Save the credential as User-provided or Standard per preference, in this example it is saved as Standard with masked ticked.



Attributes (1)

A credential can have a maximum of 50 attributes. A masked value will be shown as asterisks at all times.

Attribute name: aa-bot-1 Thumbprint
Max characters = 50

Description (optional):
Max characters = 255

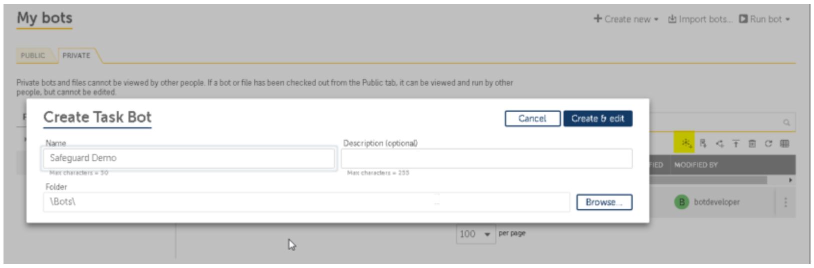
Input
● Standard
○ User-provided
If this is a user-provided attribute, when the credential is added to a locker, an email will be sent to the "Consumers" of the locker. They will be asked to input their information into this field.

Value: ••

Security
☑ Masked

3. Configure the Safeguard package

   a. Navigate to *Bots* > *My* bots and create a sample bot.



Private bots and files cannot be viewed by other people. If a bot or file has been checked out from the Public tab, it can be viewed and run by other people, but cannot be edited.

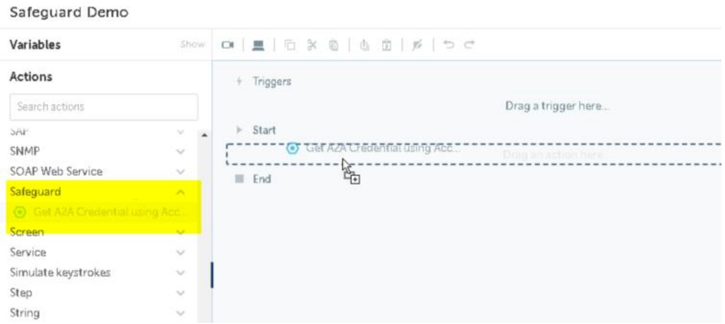
Create Task Bot

Name: Safeguard Demo (Max characters = 50)

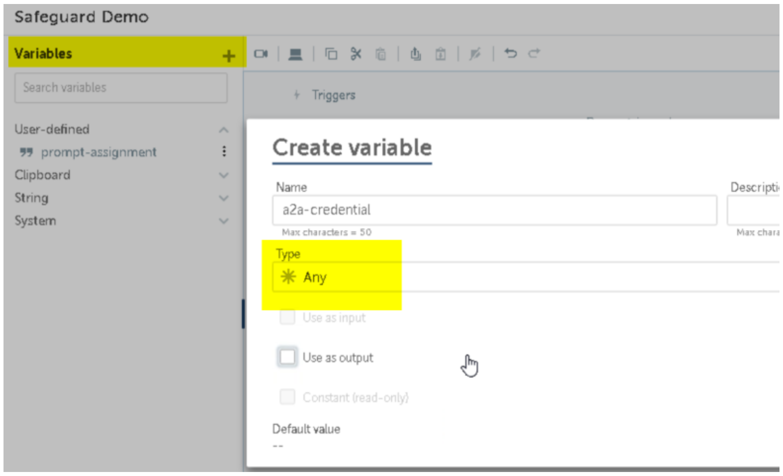
Description (optional): (Max characters = 255)

Folder: \Bots\

   b. Drag & Drop the *Get A2A Credential using Account details* action to the bot.



   c. The Safeguard package saves the obtained password into a secure variable, which then can be used as a Credential input when connecting to remote system. Create a variable with type 'Any'.



Create variable

Name: a2a-credential (Max characters = 50)

Descripti (Max chara

Type: Any

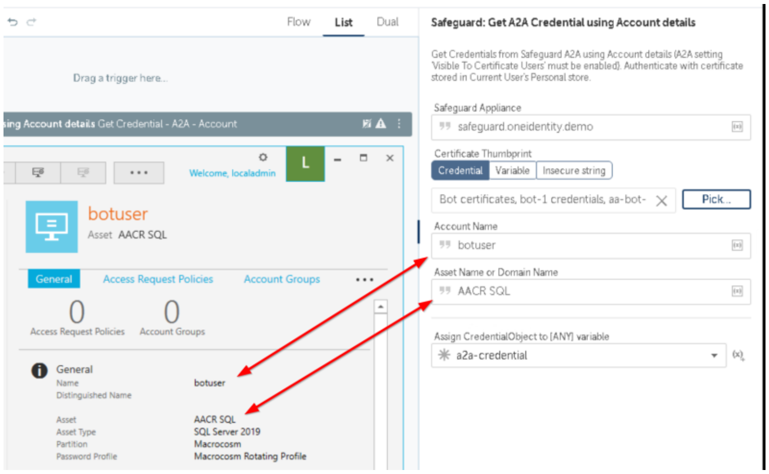
□ Use as input

□ Use as output

□ Constant (read-only)

Default value: --

d. Configure the input parameters of the action, the account name and asst/domain name are as defined for the managed account within Safeguard.



botuser
Asset AACR SQL

0 Access Request Policies
0 Account Groups

General
Name botuser
Distinguished Name
Asset AACR SQL
Asset Type SQL Server 2019
Partition Macrocosm
Password Profile Macrocosm Rotating Profile

Safeguard: Get A2A Credential using Account details

Get Credentials from Safeguard A2A using Account details (A2A setting 'Visible To Certificate Users' must be enabled). Authenticate with certificate stored in Current User's Personal store.

Safeguard Appliance: safeguard.oneidentity.demo

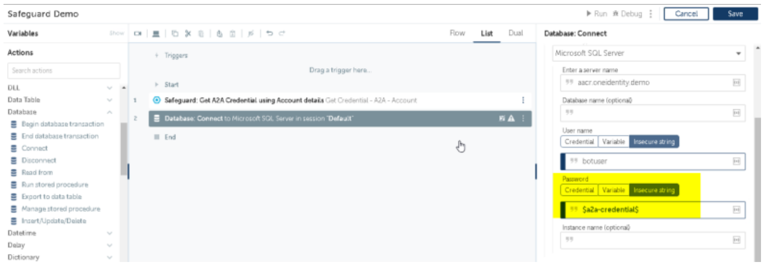
Certificate Thumbprint: Credential | Variable | Insecure string — Bot certificates, bot-1 credentials, aa-bot-

Account Name: botuser

Asset Name or Domain Name: AACR SQL

Assign CredentialObject to [ANY] variable: a2a-credential

e. Add a remote connection action to the bot, matching the account that is managed by Safeguard. Use the type 'Any' variable as an insecure string for the Password input.



1 Safeguard: Get A2A Credential using Account details Get Credential - A2A - Account

2 Database: Connect to Microsoft SQL Server in session "Default"

Database: Connect

Microsoft SQL Server

Enter a server name: aacr.oneidentity.demo

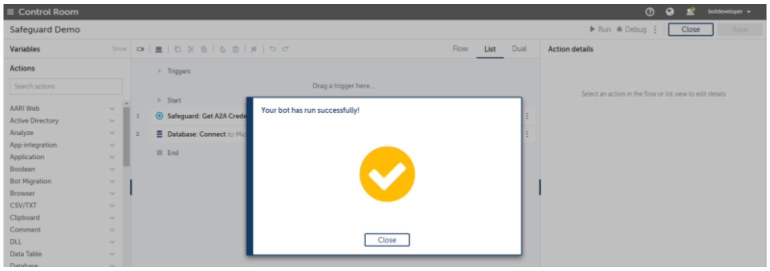
Database name (optional):

User name: Credential | Variable | Insecure string — botuser

Password: Credential | Variable | Insecure string — $a2a-credential$

Instance name (optional):

f. You may add further actions to execute on the targeted system, but for testing you can run the bot as it is.



Your bot has run successfully!

Close

4. Support & FAQs

4.1 Support

Free bots are not officially supported. You can get access to Community Support through the following channels:

- You can get access to Community Support, connecting with other Automation Anywhere customers and developers on APeople – the Bot Building Forum, the Bot Store Support Forum, or the Developers Everywhere Group.
- Automation Anywhere also provides a Product Documentation portal which can be accessed for more information about our products and guidance on Enterprise A2019.

4.2 FAQs

In case of any problems, the action will return an empty credential object, which may be caused by any of the following scenarios;

- The action input parameters are incorrect.
- The certificates are not imported to the proper certificate store or in the proper PFX format.
- The A2A service is disabled.

Further steps for logging and troubleshooting authentication can be found here.

Manual cross-check can be performed using the safeguard-ps module. It should provide the same result when A2A commands are executed by the device user on the device machine.

For questions relating to Enterprise A2019: See the Enterprise A2019 FAQs.

Appendix A: Record of Changes

No.	Version Number	Date of Change	Author	Notes
1	*1.1*	*27/04/2021*	*Viktor Varga, Alan Radford*	*Initial release*

Appendix B: References

No.	Topic	Reference Link
1	Overview of Enterprise A2019	Click here
2	Guidance: Building basic A2019 bots	Click here
3	Guidance: Building A2019 action packages	Click here
4	APeople Community Forum	Click here
5	Automation Anywhere University	Click here