

# SafeNet Trusted Access

## Customer Qualification Guidelines

### Audience

This document can be used by Gemalto Sales Representatives to engage with current SAS customers to qualify them for the upcoming release of SafeNet Trusted Access.

### Purpose

Initially, SafeNet Trusted Access will be offered to existing SAS customers. Our goal is to target customers who:

- ✖ Are using cloud apps, and planning expanding their use
- ✖ Have not implemented an IDaaS / Web SSO solution
- ✖ Are looking to complement their enterprise SSO solution with a Cloud SSO solution

Use the guidelines below to qualify your current SAS customer base for upgrade to SafeNet Trusted Access.

### Qualifying questions:

Organizations who planning to use cloud apps, or that are already using several cloud apps will be the most likely customers for STA. The purpose of the questions below is to help us understand where our customer is in terms of cloud adoption. The first thing to verify is whether the customer already is using an IDaaS solution. Those that are not, will more likely be potential customers for STA.

- ✖ **Customers who are NOT using a web SSO or IDaaS solution:**
  - ✖ How many cloud apps are deployed in your organization?
  - ✖ How is your company approaching cloud adoption and how are you defining security best practices?
  - ✖ What kind of are your users facing when having to manage multiple passwords for the various apps? How do you handle that currently?
  - ✖ What other applications does SAS protect besides the VPN?
  - ✖ How do you plan to apply 2FA and SSO to other cloud apps?
- ✖ **Customers who ARE already using an IDaaS / password vault / federation solution:**
  - ✖ What are you using today?
  - ✖ How does it allow you to set policies per application and per user?
  - ✖ What type of 2FA methods can you use?
  - ✖ What additional features would you like to see in your current solution that are not available?
  - ✖ What types of other solutions are you looking into at this time?