October 1, 2015

To: CA Single Sign-On Customers

From: The CA Technologies CA Single Sign-On Product Team

Subject: Availability of a technology preview of CA SSO as a software appliance

The CA Single Sign-On team is happy to announce the availability of a technology preview of CA SSO as a software appliance in a Docker container format (<https://www.docker.com/whatisdocker>) for members of the community to test. Simplifying the installation, deployment, and upgrade of CA SSO is an element of the product strategy and providing the solution in an appliance form factor is one of the threads of that strategy.

We encourage you or members of your team to take advantage of this opportunity to download the containers and test. From download to login you can be up and running in 30 minutes!

**Here are the details:**

The base solution made up of the Policy Server, Administration UI, and Access Gateway (previously called Secure Proxy Server) and CA Directory is available today. A ForwardInc sample solution for CA Single Sign-On will be provided in due course.  When that ForwardInc sample is available a message will be published to all that have registered to test the appliance.

To access the appliance you start by registering for the validation program – go to [validate.ca.com](https://validate.ca.com) and register for “ca Securecenter Virtual Appliance”. In response you will receive an email confirming your ability to access the appliance.  No further commitment is required, just download an appliance, click the “Deploy” button for the “CA Single Sign-On 12.52.01.ga” solution and see how easy it is.

The following details will be needed to access the administrative user interfaces:

**CA Single Sign-On Admin user interface**

* Use siteminder/test123 and set server to "policy-server"

**CA Access Gateway Admin user interface**

* There is a need to create a /etc/hosts entry in your browser machine to map your cluster machine IP address to "access-gateway-admin.ca.local". If you hit enter on your master machine console window, you will see the IPv4 address of the machine to add to the /etc/hosts file.
* The Access Gateway Admin user interface, by default, does not have any credentials for the Base configuration. Create a user directory by logging in to the Single Sign-On Admin user interface and add the user directory to the proxyui domain. After this, any users in the user directory should be able to login to the Access Gateway Admin user interface. Please refer to the CA Access Gateway (previously called Secure Proxy Server) product documentation for specific instructions.

**Helpful Links**

* Subscribe to our [YouTube channel](https://www.youtube.com/channel/UCrCjhdhuAMYu6lxIb8RhZ6w) to get access to other helpful video clips.
* Found an issue? Log a [defect report](https://validate.ca.com/project/feedback/view.html?cap=13BF137CB219472F9B10FF2EBCA3575D&f=%7BD57016FC-8761-4AD6-89FC-92CB08BB9501%7D).
* Got an idea to make this better? Log a [suggestion](https://validate.ca.com/project/feedback/view.html?cap=13BF137CB219472F9B10FF2EBCA3575D&f=%7B2FF04D98-51FD-480B-81C6-45B8F69535D3%7D).
* See the ca Securecenter Virtual Appliance [draft documentation](https://wiki.ca.com/scva).
* CA SSO technical information can be found [here](https://wiki.ca.com/dashboard.action).

Take advantage of this great opportunity to become familiar with this appliance format and encourage your team members to do the same. We look forward to your feedback.