# Integration for CA Single Sign On with NGiNX

## What It Does

This packaged work product is designed to secure resources that are front-ended or deployed on NGiNX. Resources can be secured with CA Single Sign-On policies. This agent will allow customers to take advantage of the performance gains provided by the NGiNX server without the need to place a proxy in front of their NGiNX servers.

This Agent is not a full-featured agent but does provide the following core features[1]:

- Check if the requested resource is protected
- Authenticate the end-user[2]
- Check to make sure the user is authorized

[1] For a complete list of functionality supported please refer to the packaged work product documentation.

[2] The packaged work product supports Basic Authentication out of the box but can be configured to work in cooperation with other supported forms of authentication.

## Benefits That Deliver Value

Integration for CA Single Sign-On with NGiNX:

- Check if the requested resource is protected
- Authenticate the end-user
- Check to make sure the user is authorized
- Apply CA Single Sign-On Responses
    - CA Single Sign-On Token (SMSESSION)
        - SMZone Support
        - Persistent Cookie Support
        - Secure Cookie Support
        - Domain Support
        - Path Support
    - HTTP Header Response
    - Cookie Response
    - Redirect Response (OnAuthAcceptRedirect, OnAuthRejectRedirect)

## How It Works

The packaged work product is a Java Ring Handler built to work with NGiNX-Clojure module. It communicates to the CA Single Sign-On Policy Server through an encrypted tunnel. As this is Java-based, the solution can be deployed on multiple platforms as long as the NGiNX-Clojure module is configured to use a supported JRE. The Java based Ring Handler is invoked in the rewrite handler phase, and performs the following tasks:

- Checks to see if the Target Resource is protected
- Checks to see if the user is already authenticated (is CA Single Sign-On Cookie present)
- Authenticates the user
- Checks to see if the user is Authorized to access the Target Resource
- Applies CA Single Sign-On Responses to the browser

During the rewrite handler phase the agent is allowed to:

- Redirect the request
- Add HTTP Headers
- Add Cookies
- Validate an existing Cookie
- Reject the request
- Allow the request to proceed

The use of this handler does not prevent the use of other NGiNX modules although it is crucial that other modules do not circumvent or override the execution and status of the CA Single Sign-On NGiNXRingHandler.

## Technical Prerequisites

A list of technical prerequisites for this packaged work product can be found in **CA Support online**. This is a central repository that will help you identify CA Technologies product compatibility with operating systems, other third-party software products, as well as with certification standards and regulations. **Contact** your CA Services representative for further assistance with purchasing this component.