Packaged Work Product Catalog for Security Solutions

Packaged Work Products (PWP) from CA Services extends the value of your CA Technologies solutions.

Developed, implemented and supported* by the Global Delivery team within CA Services, these offerings provide a range of benefits, including:

- Delivering new integrations
- Enhancing functionality that provides value to additional audiences
- Providing industry-specific configurations and

**Implementation services and supplementary support services are available separately.*

About Packaged Work Products

Packaged Work Products include software binaries and documentation. These pre-built components from CA Services can be deployed and adopted quickly with little disruption to your IT operations and staff. Additionally, CA Services can provide tailored (built-to-specification) packaged work products to meet unique customer requirements.

Packaged Work Products add further depth of functionality to the built-in features of core Security products and require minimum effort to configure and deploy. The Packaged Work Products support industry standard processes and represent best practices across CA customers. With Packaged Work Products for Security solutions, you can:

- Extract additional value for business and IT stakeholders
- Accelerate and broaden solution adoption
- Provide additional integrations and functionality to your implementations to deliver greater business agility

The portfolio of Packaged Work Products available from Global Delivery is always growing. View a brief description of PWPs available for Security solutions in the table below.

CA SINGLE SIGN-ON	
SmWalker for CA Single Sign-On	SmWalker for CA Single Sign-On is a general purpose scripting language that with the appropriate user written scripts can perform many useful functions that involve searching, reading and writing user store data from an LDAP directory. It can be used as Active Response, Active Rule and active Policy. SmWalker for CA Single Sign-On can also be used as an Authentication Scheme wedge that is inserted between the CA SSO Authentication service and an out-of-the-box authentication scheme.
Advanced Certificate Authentication for CA Single Sign-On	Advanced Certificate Authentication for CA Single Sign-On enables customers to specify LDAP search filters to map data from their certificates to data in their user store in order to determine which account in the user store to associate with the session being authenticated.
Impersonation for CA Single Sign-On	Impersonation for CA Single Sign-On extends the functionality of CA Single Sign-On to enable one set of users to 'impersonate' another set of users (Customer Service Rep use case, CSR), or to enable a user who has multiple accounts to switch between accounts, without having to re-submit authentication credentials (Persona use case).
Limit Concurrent Login for CA Single Sign-On	CA Single Sign-On customers may need the ability to limit the number of times that a single user can be "logged into" the system. This prevents a single user from authenticating and accessing their site from two or more different browser instances simultaneously. Since web sessions are connectionless, the session is not necessarily maintained between the browser and web server at all times. This makes it extremely difficult to determine when a session ends and thus to track or limit multiple simultaneous sessions by the same user. Limit Concurrent Login for CA Single Sign-On meets this requirement.
Integration for CA Single Sign-On with NGiNX	Integration for CA Single Sign-On with NGiNX is designed to secure resources that are front-ended or deployed on NGiNX. This PWP 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 the NGiNX servers.
User Session Monitor for CA Single Sign-On	User Session Monitor for CA Single Sign-On extends CA SSO's capabilities by providing a user session monitoring interface for both the end user and administrator. For users, it provides the capability to view their current active sessions from different IP addresses. For administrators, it provides the capability to view users' current active sessions from different IP addresses and terminate sessions from different IP addresses and the capability to remotely terminate a session for a selected IP address or for a selected user DN.

Integration for CA Single Sign-On with Tomcat	Integration for CA Single Sign-On for Tomcat is designed to provide CA Single Sign-On security features for the Apache Tomcat Servlet container. Unlike other CA SSO Application Server Agents, this Agent provides standard CA SSO Web Agent functionality such as: Single Sign-On URL-Based Authorization and Session Management
XauthRADIUS Integration for CA Single Sign-On	In a typical deployment of CA Single Sign-On for use in an extranet or consumer portal, users have a single login based on a single entry in a centralized user directory, typically LDAP. To aid in the deployment of CA SSO and simplify the development of custom authentication schemes, the XauthRADIUS Integration for CA SSO provides an authentication scheme that can be used to authenticate through other products via the RADIUS protocol.
Dynamic Assertion Generator Plugin for CA Single Sign-On	Dynamic Assertion Generator Plugin for CA Single Sign-On allows designated sites to send user information along with a request for a SAML assertion. The information is used to dynamically modify the SAML assertion, specifically Name ID and Attributes.
Google reCAPTCHA Integration for CA Single Sign-On	Growing security threats due to automated software attacks led to the evolution of CAPTCHA. Integration of Google reCAPTCHA with CA SSO helps prevent automated software attacks by using a CAPTCHA while letting valid users pass through with ease. This solution enhances CA SSO capabilities and adds an additional layer of security.
Lightweight SSO Ticket Authentication for CA Single Sign-On	The Lightweight SSO Ticket Authentication for CA Single Sign-On seamlessly logs on a user to a Single Sign-On environment when they already have an authenticated session from a “trusted”non-CA SSO environment.
Extended NTLM Authentication for CA Single Sign-On	While CA Single Sign-On has a built-in Windows auth scheme, the scheme expects that user login IDs are unique across all Active Directory (AD) domains that are represented as CA SSO User Directories. If a user’s login ID is not unique then it will be unable to successfully authenticate that user since the disambiguation phase will not map to a single User Directory object. This Packaged Work Product can be used to successfully authenticate users in this use case because it can be configured with a mapping of domain names versus User Directories, and given the user’s domain and login ID as input that can uniquely locate the user’s LDAP entry.
Integration for CA Single Sign-On with Microsoft Windows Web Server Identity	Integration for CA Single Sign-On with Microsoft Windows Web Server Identity (WWSI) enables Integrated Windows Authentication (IWA) based applications to be protected by CA SSO and utilize its single sign on capabilities while using the applications’ existing security model.
SSO Filter for CA Access Gateway	When CA Single Sign-On is normally integrated with customer web applications, the applications own authentication system (legacy) is disabled and it relies on CA SSO to authenticate the user and establish an identity for the application to pick up. There are

	situations where customers are unable to disable the application's native authentication method. In such cases, in order to establish a user session for that application, credentials must be submitted to the application. This PWP enables that capability.
DATA PROTECTION	
Hierarchy Sync for CA Data Protection	Hierarchy Sync for CA Data Protection is a tool for importing data from multiple data sources, applying basic logic and building a CA Data Protection hierarchies XML file. Hierarchy is critical to making the CA Data Protection product function on both a management and policy perspective. This tool was designed to give clients an ability to gather data from multiple sources (beyond the LDAP and XML supported by CA Data Protection) and join into a single data file.
CA IDENTITY MANAGER	
Offsite Forgotten Password Reset for CA Identity Manager	When a user forgets the domain password used to login to a Windows computer, the Credential Provider of CA Identity Manager allows the user to reset the password using the Forgotten Password Reset self-service at Windows logon screen. However, this is only available if the computer has access to the self-service web application which is often protected inside a corporate network. The Offsite Forgotten Password Reset for CA Identity Manager PWP enhances the Credential Provider of CA Identity Manager with the ability to reset forgotten passwords from outside of a corporate network by establishing a secured connection to the corporate network at the Windows logon screen.
CA Advanced Authentication	
IIS ISAPI Filter for CA Advanced Authentication	This Packaged Work Product integrates CA Advanced Authentication with IIS via an ISAPI filter residing on the IIS Web Server. The filter redirects the web browser to the configured CA Advanced Authentication Flow Manager URL and facilitates Advanced Authentication.

Additional Resources from Global Delivery

Catalogs for Packaged Work Product Catalogs from Global Delivery

- Project & Portfolio Management
- Service Assurance
- Virtualization and Service Automation