Service Overview: CA ecoGovernance On Demand

Revision date: September 14th, 2012

An Introduction to the CA ecoGovernance On Demand Service

Contents

Chapter 1: Introduction

The content contained herein is current as of the date it was published. Check support.ca.com to obtain the most current version of this document.

CA ecoGovernance On Demand is a web-based service that provides subscribers with access to the energy and sustainability management offering from CA. It is comprised of two core components: the CA ecoGovernance On Demand application, which is the main focus of this document, and a front-end portal (CA On Demand Portal) used for authenticating to the application and other CA Technologies On Demand applications.

Chapter 2: Service Overview

Architecture

The CA ecoGovernance application is a J2EE application and has the following architectural details:

- The underlying J2EE application server controls Web, integration, business logic and persistence services providing common application functions such as caching, security, globalization, configuration and workflow
- The application server connects to Oracle through DataDirect JDBC drivers. The CA ecoGovernance service is accessed through a web interface on both Linux & Windows servers.
- Customers are deployed in a stateless application environment connected to an Oracle database. With failover at the application tier, the data model is designed to guarantee data integrity. Data transactions are modeled into transaction units that are saved (or committed) to the database in one batch. In the event a database instance goes offline, the pending transactions resume once the database is restored.
- The application limits the amount of network resources consumed by compressing the data sent to the browser from the server using Java compression functionality. The browser can then uncompress the data stream using built-in gzip functionality. This results in an average page size of 7–25 KB going over the network. As a stateless application, end-user sessions are allowed to failover seamlessly with no disruption in productivity.
- To ensure high-performance and availability, the application runs on Apache Tomcat application servers connecting to Oracle back-end databases, and utilizes load balancing between a minimum of two application servers using SSL acceleration and F5 BIG-IPs.

Certification and Compliance

The components of CA ecoGovernance On Demand are certified or compliant to various standards as follows:

- **SSAE 16 compliant**: The CA ecoGovernance service is subject to an annual SSAE 16 attestation. SSAE 16 (formally known as Statement on Standards for Attestation Engagements no. 16), is an attestation standard issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). The attestation includes the auditor's opinion on the fairness of the presentation of the CA Technologies description of controls that have been placed in operation and the suitability of the design of the controls to achieve the specified control objectives, and the auditor's opinion on whether the specific controls were operating effectively during the period under review.
- **Section 508**: The nature and extent to which the CA ecoGovernance application enables compliance with the requirements of Section 508 of the Rehabilitation Act of 1973 is detailed in our Voluntary Product Accessibility Template, available upon request.
- **Languages**: The CA ecoGovernance On Demand service currently supports ten languages (English, French, Spanish, German, Japanese, Brazilian Portuguese, Italian, Dutch, traditional Chinese and simplified Chinese) and over 100 regional settings for date, time, and number formatting.

Version and Release Management

Upgrades to the ecoGovernance On Demand are included as part of the base service. CA Technologies notifies customers when the CA ecoGovernance On Demand service will be upgraded and will work with clients to accommodate their business needs in regard to scheduling upgrades. New versions are released two to three times per year. When practical, CA Technologies schedules updates during non business hours and provides a minimum of five days notice. For emergency updates, we provide a minimum 24 hours notice when practical.

Approved security patches are applied quarterly, with critical security patches applied earlier on a case-by-case basis.

Standard Maintenance

On Demand Maintenance falls into three categories:

- Monthly: Our monthly maintenance windows are scheduled at least 3 months in advance and occur one Saturday each month. Maintenance windows are scheduled during local non-business hours. There is limited client input over these scheduled windows as the infrastructure maintenance performed during these windows may impact multiple or all clients. A reminder notification will be sent 7-10 days prior to these maintenance windows.
- Critical Scheduled: Periodically, a critical scheduled maintenance involving security or system stability may be required. A 72 hour notice will be provided to customers for these activities. In many cases this maintenance can be more flexibly timed as it is generally for individual client systems. CA will provide reasonable accommodations to these types of maintenance periods where possible.
- Unplanned: Unplanned downtime is any loss of production system availability that is not does not have at least 72 hours advance notice to clients. These downtimes are generally system fault type issues but can also be proactive, emergency maintenance performed to prevent a system failure from occurring. Notices of service interruption will be sent as soon as the maintenance is scheduled or monitoring has determined a client's system is unavailable. These types of downtime count against the client's uptime SLA and, therefore, are infrequent.

Standard Support

The ecoGovernance On Demand service includes standard 24x7x365 support which is defined in the following documents:

- **CA On Demand Service Standard Maintenance**: details the scope and other terms and conditions of the maintenance agreement. Available at: CA.com

- **CA On Demand Service - Maintenance Policy and Terms**: defines the maintenance support policy, detailing service level objectives and supported services. Available at support.ca.com under Contact and Resources, CA Support Policies.

Client Access

Customers can access the CA ecoGovernance On Demand service using a supported web browser as noted in current the Product Architecture Stack. Depending on processing requirements, there are additional client technologies that customers can use:

- **XML Open Gateway (XOG)**: A CA ecoGovernance Web service used for data import and export between external systems and the CA ecoGovernance service. Direct WSDL calls may also be initiated to service using a client developed SOAP call.
- **Data Accelerators**: CA ecoGovernance On Demand allows for data to be uploaded from spreadsheets via SFTP access to a secure drop-off/pickup location. The spreadsheets need to be in a pre-defined format and have to be saved as a comma-separated value (CSV) file for uploading.

Direct access to On Demand environment servers using a VPN, remote desktop, or other connection method is not permitted. Limited, read-only database access may be granted to support development of custom report content.

Chapter 3: Customizations

CA Technologies' on demand solutions are delivered as a standardized service. This standardization allows CA Technologies to deliver high quality services in a repeatable and cost effective manner. To achieve this standardization certain design principles are enforced to limit customizations that may cause instabilities in the delivery of the service. Allowing for only supported configurations ensures the security, stability, and maintainability of the service for all clients.

Application Customizations

Customization of the CA ecoGovernance application layer or alterations/insertions of any files on the application servers are not compatible with the ecoGovernance On Demand service. CA ecoGovernance On Demand leverages a uniform code base and, therefore, cannot support application customizations. Customizations under this policy include, but are not limited to, the following:

- Custom Java code
- Alterations to the base ecoGovernance code set including XSL and JAVA files
- Placement of a parameter or any other file into the directory structure of a server. Note an SFTP directory is available at the application level for file uploads.

Database Customizations

Direct alteration of the database schema is not permitted. However, the CA ecoGovernance On Demand solution allows and supports all configurations done through CA ecoGovernance Studio. Customizations under this policy include, but are not limited to, the following:

- Triggers
- Stored procedures
- Custom tables or schemas
- Functions

Supportability and upgradeability are the primary concerns that govern the CA ecoGovernance On Demand customization policies. The Global Delivery team (GD) can be engaged to design, build, and support custom components to conform to On Demand support policies. GD reviews requirements and works directly with CA Services and the On Demand team to design supportable components that can be deployed to on demand environments.

Chapter 4: Security

Security Framework

CA Technologies continuously improves the security framework by doing the following:

1. Risk management drives policy creation
2. Policy shapes architecture
3. Architecture drives engineering solutions
4. Solutions are sustained by operations and administration.
5. Operations and administration efforts are monitored for performance and compliance (depending on risk)
6. Performance/compliance test results drive policy improvements

Architectural Security

The CA ecoGovernance On Demand service security architecture is comprised of SSAE 16 Type II controls and security measures across facility, network, and server infrastructure. CA Technologies security suite, including threat management, provides server security. In addition, “stateful” inspection firewalls are in place; these firewalls stop all incoming traffic, analyze it, and prevent standard internet attacks.

Application servers are located in a demilitarized zone (DMZ), which is separated from the service database servers by a firewall. Only the necessary ports are opened between the DMZ and the internal trusted network. In addition, all web traffic is protected by 128–bit SSL encryption.

The CA ecoGovernance application is set up to run under SSL in encrypting the user session. The application handles illegal SQL injections by enforcing content-validation rules and Web use prepared statements exclusive to the application itself almost exclusively in the ecoGovernance application.

A federated single sign-on (SSO) authentication option is available; refer to the Integration section for more details.

Within the CA ecoGovernance On Demand application, over 150 individual rights/roles/groups can be used to secure application functionality and data records. Additionally, standard audit trail functionality can be configured for most objects and attributes to capture creation, edits, and deletions of selected data records or attributes.

Third Party Security Scans

CA Technologies contracts with an independent, third party vendor to evaluate and validate the security of our service on an ongoing basis. High risks are identified, validated, and remediated before production systems are made available. Medium risks are evaluated and resolved on a priority basis. Ongoing scans are performed to ensure that no new risks have been introduced. Two types of scans are performed:

- **Vulnerability Scans:** Vulnerability tests are performed weekly
- **Penetration Scans:** Penetration test are performed on a quarterly basis

Application Security and User Management

- **Data integrity**: CA ecoGovernance On Demand customers are deployed in a stateless application environment connected to Oracle database instances. With failover at the application tier, the application data model is designed to guarantee data integrity by modeling data transactions into transaction units that are saved (committed) to the database in one batch. In the event a database instance goes offline, the pending transactions resume once the database is restored.
- **Data segregation**: Customer data is segregated in separate logical databases that may reside on the same physical Oracle database server. All customer configurations and customer data are stored in the database.
- **User authentication**: Users can authenticate to the CA ecoGovernance On Demand service by using a username and password combination. In addition to internal authentication, CA Technologies also provides the option to use Federated SSO for user authentication. Some non web browser client applications, such as Microsoft Project, can be accessed from within the application and do not require additional logon. Where these applications are accessed from outside the application, username and password are required.

  For customers that do not have Federated SSO implemented, a login to the on demand environment is required to manage passwords. CA Technologies does not currently support direct LDAP integration because exposing client directory data outside the firewall exposes clients to an unacceptable security risks and the establishment of a business to business VPN tunnel to ship directory data exposes the ecoGovernance On Demand service and its clients to unacceptable security risks. Users of the CA ecoGovernance On Demand service can be added, deactivated, or modified through the user interface on the CA On Demand Portal or via a WSDL based interface. New users can optionally receive an email notification with instructions for how to log on to the CA ecoGovernance service.

  User passwords are managed either in the CA On Demand Portal, the ecoGovernance application or in the customer's environment if the customer is using Federated SSO.
- **Permissions**: Additional application security is provided through role-based and OBS-based permissions. Using these permission schemes, the CA ecoGovernance application can be configured to allow or deny access to features and data in accordance with any business need. CA Technologies also implements best practices in guarding from outside threats. Each customer's data and configurations are stored in a dedicated database schema with security rights restricted at the database level. Currently, Web services are not shared between clients.

Session Management

The CA ecoGovernance service uses a session-based cookie that carries a token for accessing the session data that is transient in the cache (for a single application environment), or in the database (for a clustered environment). The application session cookie is transient. The only data that is kept in the cookie is the authentication token, which is a value in the database. Session data that is keyed off the cookie includes the user's profile (username, language choice, locale choice, and time zone), global access rights of the user, and other shopping cart-like data.

Data Center Security

CA Technologies' data centers have multiple levels of security to protect customer information. This protection includes physical and logical security measures.

PHYSICAL SECURITY

All data centers have highly restricted access and use the following physical security measures:

- **Physical Access**: All areas of each data center are monitored using CCTV, and all access points are controlled. The center is staffed with security officers around the clock to augment physical security features.
- **Visitors Access**: No public visitor access to the data centers without prior knowledge and approval of the On Demand infrastructure team is permitted. Approved visitors are required to present a government issued picture ID upon entry to verify their identity and access privileges. They are then escorted to the appropriate locations within the data center by security staff. Access history is recorded for audit.
- **CA Security Personnel**: CA Technologies maintains a department of security engineers. New security employees and contractors are all subjected to background checks. Security policies and data retention and destruction policies are in place and published.

LOGICAL SECURITY

Logical security is provided by commercial Anti Virus software, and by stateful inspection firewalls. Application servers are located in a demilitarized zone (DMZ), which is separated from the database servers by a firewall. Only the necessary ports are opened between the DMZ and the internal trust network. In addition, all web traffic is protected by 128-bit SSL encryption. SSL certificates are provided by Entrust®.

The following security methods are employed:

- **Hacker Monitoring**: The systems are monitored 24 x 7 by CA Technologies products (CA Cohesion ACM). Audit logs are sent to a centralized CA Audit system and are reviewed daily to ensure that there is no unusual activity.

- **Virus Protection**: All CA Technologies servers are protected by commercial Anti Virus software. The environment undergoes regular vulnerability scans to protect against both internal and external network threats. Files being uploaded to the service are scanned for threats before being saved.
- **Ports**: Only specific ports are opened for data traffic. Application data, including interface data, is directed through port 443. Ports 80 and 8080 are utilized for reporting functionality.
- **Application Security**: During the development and QA stages, the application undergoes security review and testing.
- **Server Hardening**: All servers are hardened in accordance with industry best practices. By running only the necessary services, CA Technologies reduces its exposure to operating-system-level security issues. Servers undergo weekly vulnerabilities scans and standard quarterly maintenance.
- **Server Patching**: Security patches are applied as needed and emergency patches are applied as quickly as possible.
- **Segregated Customer Data**: Data is currently segregated with customers having their own schema instance and security is enforced at the database level so that no cross schema access is available. Also, customers do not have logical access to the database servers.
- **Protection Controls**: Unauthorized access to servers and changes to the operating system are monitored. CA Cohesion© is used to manage changes to the configuration of the application.
- **Data Sanitization**: Data storage and tape media are sanitized when a CA ecoGovernance service contract has expired, hardware breaks, or customers ask for sanitization to be performed. Note, customer data is only stored on network data storage, so there is no process necessary for other media (for example, tape, USB, CD, DVD). A low-level format is performed on the media when they are no longer in use.

Chapter 5: Data Backup and Recovery

CA Technologies performs regular server backups of all customer data and maintains a disaster recovery plan.

Data Backup

Customer data is backed up as follows:

- **Daily server backups**: A full backup is performed weekly along with daily incremental backups. These backups are replicated off-site daily as part of the business continuity plan.
- **30 day retention time**: Backups are retained for 30 days. Backups reside only on network storage that is replicated to a remote site. Backup data is never stored outside of a CA Technologies hosting facility.
- **Customer backup requests**: Customers may request manual backups or may request a restore from any snapshot within the retention period. All restore requests are processed as a complete environmental restore. When a customer requests a recovery, the restored system may be unavailable for a predetermined amount of time, which will be communicated to the customer.

  CA Technologies limits the number of times manual restores can be requested each quarter; please see the document Specific Program Documentation - CA On Demand Service Standard Maintenance for details.

Disaster Recovery

In a disaster, CA Technologies recovers from the most recent backup. For most disaster recovery scenarios, minimal or no customer action is required. Data backups are replicated each evening to an alternate data center that acts as a recovery site for the primary data center.

Recoveries are usually performed in the following scenarios:

- **Hardware/software failure**: Because of high availability and redundancy there should be zero loss of data, but in rare cases, the maximum amount of data lost could be from the previous 24 hours. CA Technologies will use all commercially reasonable efforts to recover from any system failures with the objective of restoring system availability within four hours.
- **Force majeure event (disaster)**: Depending on the time of the event, the maximum amount of data lost could be from the previous 24 hours. CA Technologies will use all commercially reasonable efforts to recover from any force majeure event with the objective of restoring system availability within 72 hours.

Disaster to the CA Technologies corporate network in New York will not affect customers' service. Secondary services, such as email notification and domain name services will be routed through the secondary CA Technologies network in Illinois.

Chapter 6: Integration

The CA Technologies approach to integration is through the supply of an integration toolkit that enables field integrations to be performed easily. This toolkit consists of the XOG XML Web Services interface and GEL Scripting capabilities of the process management functionality. Clients may build integrations themselves or engage CA Services to build integrations for them; the work to build integrations is not part of the ecoGovernance Service subscription.

The CA ecoGovernance application also has some out-of-the-box integrations and, even though the application is based on J2EE, it runs seamlessly under the .NET framework with any integrations utilizing .NET's native XML/SOAP layer. The following are the different integration methodologies provided:

- XML Open Gateway (XOG)
- SFTP Drop-off combined with GEL (Generic Execution Language) enabled processes
- Simple Object Access Protocol (SOAP)
- Federated single sign-on

XML Open Gateway (XOG)

XOG is the CA ecoGovernance application's Web service interface, available on the same HTTPS port as the CA ecoGovernance service HTML Web browser interface. XOG uses SOAP, an open-standard, human-readable, XML-based protocol for communication. Using XOG, it is possible to read and write data objects from the application, execute queries, and execute other server-side actions. XOG includes a full Web Service Description Language (WSDL) file that is downloadable from the CA ecoGovernance application. The WSDL describes where and how to invoke it, the URL to use, and available messages (complete with full XML schema).

CA Technologies recommends customers use the import/export functionality in XOG for promoting changes between Development, Test, and Production environments. Customers are responsible for promoting the changes themselves.

XOG is safe in the CA ecoGovernance service environment for the following reasons:

- **Web service**: Because XOG communicates over HTTP/HTTPS using a Web service, there are no extra ports or sockets to secure.
- **Authentication**: XOG must use an authenticated CA ecoGovernance application user to access the application.
- **Access rights**: The application user must have access to the data in the CA ecoGovernance service exactly like the user would have inside of the CA ecoGovernance application.

SFTP Access

SFTP access provides customers an asynchronous and scheduled way to integrate with their applications. The CA ecoGovernance service allows for SFTP access to a secure drop-off/pickup location. This method allows customers to deliver to or receive files (for example, XOG files or GEL scripts) from their CA ecoGovernance application.

SOAP

Custom SOAP integrations can be set up between the service and a customer's third-party solutions. Third-party SOAP integration toolkits include Apache AXIS and Microsoft Visual Studio (.NET Framework) for Windows. Direct SOAP integration with a client is possible by using the XOG API over standard HTTPS port.

Federated Single Sign-On

The federated single sign-on (SSO) integration allows customers to create a trusted relationship with the CA ecoGovernance service. This relationship has the following benefits:

- **Seamless integration between networks and environments**: Users can move easily between their intranet and the various production, development, and test CA ecoGovernance service environments.
- **Simplified password management**: Customers do not have to manage their users' passwords separately for the CA ecoGovernance service because they are handled by their existing SSO solution.

CA Technologies uses CA SiteMinder® for SSO federation.

If the customer is using federated SSO, their password management is centralized within their environment. All password construction, change intervals, and so on, are controlled on the customer side. The customer might not even have passwords if they are using a different form of authentication.

The federated SSO only works if the customer also has a federated SSO solution installed on their network. In this scenario, the customer must manage the following tasks themselves (or engage CA Services):

- Maintain an identity management solution, such as CA SiteMinder, capable of producing a SAML 2.0 assertion.
- Add and configure internal applications inside their SSO environment.
- Configure a trusted relationship with the CA ecoGovernance service.
- Optionally, create links on their intranet to the CA ecoGovernance service.

Federated SSO is safe in the CA ecoGovernance On Demand environment for the following reasons:

- **SAML**: Security Assertion Markup Language (SAML) is a proven secure protocol for handling SSO.
- **Password Management**: Passwords do not need to be managed in the CA ecoGovernance service and this means fewer places for security breaches.

Chapter 7: Reporting

In addition to real-time reporting using the CA ecoGovernance application, CA Technologies also provides business intelligence through Business Objects. Business Objects runs against both the live application database and the supplied CA ecoGovernance Business Objects Universe by serving reports as DHTML pages to the client.

For more information about how Business Objects components are configured to work with CA On Demand environments, see the *On Demand Business Objects Connectivity Technical Overview* available on request.

The CA ecoGovernance application comes with standard reporting features as follows:

- InfoView
- Webi
- Xcelsius
- VPN Read-Only Database Access
- BO Designer Tool Access (edit and create BO Universes)
- Crystal Reports Access

Webi and Infoview

Once the client has access to the database they may utilize Webi and Infoview to generate and upload custom reports in a self service manner. Both Webi and Infoview are available to the client as part of their CA ecoGovernance On Demand service. The types of reports created by these tools are generally simple in nature.

Xcelsius

Xcelsius enabled portlets can be created and uploaded in ecoGovernance Studio to provide interactive analytics and dashboards. The Xcelsius designer tool is provided for download within the ecoGovernance On Demand application.

Database Access for Report/Universe/Generation

The CA ecoGovernance On Demand service allows for the creation of a limited number of read-only database accounts for the client. To grant this access, a read-only database user is created along with a VPN connection to the database server.

Crystal Reports

Customers who wish to create more sophisticated reports can use the Crystal Reports tool. The customer can download a copy of the Crystal Reports Designer client which is provided as part of the CA ecoGovernance On Demand service. Note that CA Technologies does not provide any training or functional support for the usage of Crystal Reports; all support for this tool is provided directly from SAP.

While CA Technologies provides access to create reports using the Crystal Reports tool, it cannot provide the access required to create custom database components (such as, methods, views, and functions). Only reports that can be packaged for Infoview deployment can be uploaded to a CA ecoGovernance On Demand system by the client. CA Technologies does not support or deploy any custom reports created with the Crystal Reports tool unless provided for under a statement of work with CA Services.

Universe Creation

Clients can also alter and create universes with BO Designer. The BO Designer tool is available to a client as part of the CA ecoGovernance On Demand service upon request via a support ticket. CA Technologies does not support or deploy any custom universes created with the BO Designer tool unless provided for under a statement of work with CA Services.

Chapter 8: Application

Configuration with CA ecoGovernance Studio

To become more productive, users need a single place to obtain personalized content and a standard, easy-to-use interface that helps them do their jobs effectively. Portal technology is targeted squarely at this need, delivering customized information from across the enterprise to the user's desktop.

The key to unlocking the power of this technology is CA ecoGovernance Studio, a point-and-click configuration module in the CA ecoGovernance application. CA ecoGovernance Studio empowers organizations to create and deploy personalized portals, pages, menus, and business objects that adapt the software to the business process—not the other way around.

CA ecoGovernance Studio allows you to tailor business objects, such as facilities, projects, resources, and ideas, without programming or customization. Your system administrators can accomplish a wide array of configurations, including adding user-defined fields and objects and rearranging pages and forms, all through a point-and-click Web interface. In addition, the CA ecoGovernance application supports multiple local configurations in a single instance through System Partitions. System Partitions support the local management of fields, forms, processes, methodologies, and branding even as they enable the global governance and oversight of a single system.

Email Notifications

The CA ecoGovernance service has the capability of sending email notifications for events such as user addition, addition to project teams, and so on.

This functionality is turned off for sandbox systems but can be enabled using a support ticket request.

Search Capabilities

Customers can search across all structured and unstructured data in the CA ecoGovernance application.

To learn more about the architecture and technology powering CA ecoGovernance On Demand, visit CA Technologies online or contact your CA representative

Data Integrity and Management

Data between the client and database may be interrupted when an application server fails and the session is lost. Transactions complete if they are submitted before the application server goes down. If the database goes offline, the transactions complete once the database is restarted.

The CA ecoGovernance application data model was designed to guarantee data integrity by modeling data transactions into transaction units that are saved (committed) to the database in one batch. Inside of PL/SQL stored procedures and the CA Technologies JDBC-based application code, this happens using the TRANSACTION/COMMIT Oracle constructs/commands. All jobs and tasks that were cut off during the failure resume once the servers are activated.