

CA Clarity PPM On Demand Technical Overview

Table of Contents

SECTION 1: INTRODUCTION AND ARCHITECTURE

Introduction and Architecture	1
Web Browser and Client Access	1
Interactive Graphs & Portlets	2
Data Integrity & Management	2
Version and Release Management	2
Certification & Compliance	2

SECTION 2: SECURITY

Framework	3
Architectural Security	4
Vulnerability	4
Application Security & User Management	4
Session Management	5
Data Center Security	5

SECTION 3: DATA CENTERS

Data Center Overview	7
Power Management, HVAC Environmental	7
Control and Disaster Prevention	7
Site Access	7

SECTION 4: DATA BACKUP AND RECOVERY

Data Backup	7
Disaster Recovery	8

SECTION 5: INTEGRATION

Integration Overview	8
XML Open Gateway (XOG)	9
FTP Access	9
SOAP	9
Open Workbench	9
Microsoft Project	10
Microsoft SharePoint	10
Federated Single Sign-On	11

SECTION 6: APPLICATION

Configuration with CA Clarity PPM Studio	11
Reporting	12
Email Notifications	12
Search Capabilities	12

SECTION 7: APPENDIX

CA Clarity Service Product Architecture Stack (PAS)	12
---	----

Introduction and Architecture

Please make sure that you have the most current version of this Technical Overview by checking with your CA Sales representative. The content contained herein is current provided it represents the latest current version number. Please check the On Demand portal or Support. CA.com to obtain the most current version (Version 1.3) of this document.

CA Clarity PPM On Demand is a web-based service (“Clarity Service”) that provides subscribers with access to the market-leading project and portfolio management system. The Clarity Service comprises two core components - the CA PPM Clarity application (“Clarity Application”), about which most of this document is focused, and a front-end portal (“On Demand Portal”) used for accessing the Clarity Application and other CA On Demand applications.

- The Clarity Application is a J2EE application. It’s 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 via DataDirect Type 4 JDBC drivers. The Clarity Service is accessed through a web interface on both Linux & Windows servers.
- Customers are deployed in a stateless application environment connected to an Oracle RAC database. With fail-over at the application tier, the data model is designed to guarantee data integrity by modeling data transactions 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 will resume once restored.
- The Clarity Application limits the amount of network resources being consumed by compressing the data being 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. The Clarity Application is stateless, allowing end user sessions to fail-over seamlessly with no disruption in productivity.
- To ensure high-performance and availability, the Clarity 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-IP’s. The On Demand Portal is built on a 3rd party portal product running on the Apache Tomcat application server which connects to an Oracle database.

Web Browser and Client Access

Customers can access the Clarity Service using a supported Web browser as noted in the Product Architecture Stack. There are also other client technologies that customers can use depending on processing requirements.

- **Clarity XML Open Gateway (XOG):** Used for data import and export between external systems and the Clarity Service.
- **Open Workbench and Microsoft Project:** These are scheduling tools that allow project plans to be created and updated from within the Clarity Application or the scheduling tools. Open Workbench was made open source in June 2004 by CA.



Interactive Graphs and Portlets

Chart and graphs are provided standard as JPEG renditions. To view these graphs and charts interactively, the Adobe SVG viewer (which is supported natively in some browsers) is required. The viewer can be downloaded from the Clarity Application or pushed out through a tool like SMS.

Data Integrity and Management

Data between the client and database may be interrupted when an application server fails and the session is lost. Transactions will complete if submitted prior to the application server going down. If the database crashes, the transaction will complete once the database is restarted. The Clarity 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, as well as CA's JDBC-based application code, this happens using the TRANSACTION/COMMIT Oracle constructs/commands. All jobs and tasks that were cut off during the failure will resume once the servers are activated.

Version and Release Management

CA will notify customers when new versions of the Clarity Service are available. Maintenance upgrades are typically released once per quarter. When practical, CA will schedule updates during non-business hours and provide a minimum of five days notice. For emergency updates, CA will provide a minimum twenty-four hours notice when practical.

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

Certification and Compliance

- **Languages:** The Clarity Application currently supports 15 languages, as well as a total of 100+ regional settings for date, time, and number formatting. For more information, please consult the Product Architecture Stack.
- **SAS-70 Type II:** The Clarity Service has been subject to a SAS 70 Type II audit for North America as of May 31, 2009. SAS-70 Type II, formally known as Statement on Auditing Standards No. 70: Service Organizations, is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). The statement includes the auditor's opinion on the fairness of the presentation of CA's description of controls that have been placed in operation and the suitability of the design of the controls to achieve the specified control objectives, as well as the auditor's opinion on whether the specific controls were operating effectively during the period under review. No exceptions were identified in the report.
- **Section 508:** The Clarity Application conforms to the Federal Rehabilitation Act, Section 508 (now referred to as the Voluntary Product Accessibility Template).

Framework




CA continuously improves the security framework by doing the following:

- 1) Use Risk Management to drive Policy creation
- 2) Use Policy to shape Architecture
- 3) Use Architecture to Engineer Solutions
- 4) These Solutions are sustained by Operations and Administration.
- 5) Operations and Administration efforts are monitored for performance and/or compliance (depending on risk).

Performance/Compliance test results drive policy improvements.

Architectural Security

The Clarity Service security architecture is comprised of SAS70 Type II controls and security measures across facility, network and server infrastructure. Server security is provided by CA's security suite including threat management and intruder detection. In addition, stateful inspection firewalls are in place. ("Stateful inspection firewall" means that the firewall stops all incoming traffic, analyzes it, and prevents standard Internet attacks.) Application servers are located in a demilitarized zone (DMZ), which is separated from the Clarity 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 Clarity Application is setup to run under SSL in encrypting the user session. It handles illegal SQL Injections by enforcing content-validation rules and web use prepared statements almost exclusively in the Clarity Application.

A federated SSO option is available - please refer to the integration section for more details. Within the Clarity Application, there are over 150+ individual rights/roles/groups that can be used to secure application functionality and keep data confidential as well as an audit trail function that can be setup for most objects and attributes.

Vulnerability

Vulnerability tests are performed weekly by DDI (Digital Defense, Inc.), a 3rd party vendor, as external penetration and internal vulnerability scans


Application Security and User Management

- **Languages:** The Clarity Application currently supports 15 languages, as well as a total of 100+ regional settings for date, time, and number formatting. For more Data Integrity: Clarity Service customers are deployed in a stateless application environment connected to Oracle RAC database instances. With fail-over at the application tier, the Clarity Application data model is designed to guarantee data integrity by modeling data transactions 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 will resume once restored.
- **Data Segregation:** Customer data is segregated in separate logical databases that may reside on the same physical Oracle database server. The Clarity Application is shared across customers. All customer configurations and customer data are stored in the database.
- **Log in and SSO:** Users can access the Clarity Service by using a username and password combination. In addition to internal authentication, CA also provides the option to use Federated SSO for web browser authentication. Some non-web browser client applications e.g. Microsoft Project can be accessed from within the Clarity Application and will not require additional logon. Where these are accessed from outside the Clarity Application, e.g. username and password will be required.

For customers that do not have Federated SSO, they log into the On Demand environment to manage passwords. Alternatively, the passwords can be managed using Web Services in the On Demand Portal. CA does not currently support direct LDAP integration since customers have not expressed any interest in exposing such directory outside the firewall; this is true even when access is provided over a SSL socket or using StartTLS. User integration can be built using our user import Web Service.

Users of the Clarity Service can be added, deleted or modified through the user interface on the On Demand Portal. Whenever a new user is created, the user will receive an email notification with instructions for how to log onto the Clarity Service. Customers can also perform a mass creation of users via a User Management tool located on the On Demand Portal or through a direct Web Service.

User passwords will be managed either in the CA On Demand environment or in the customer’s environment, depending on whether the customer is using Federated SSO. If a customer has users with non-web-browser clients, those users will need to manage their passwords in the CA On Demand Portal.

- 
- **Permissions:** Additional application security is provided through role-based and OBS-based permissions. Using these permission schemes, the Clarity Application can be configured to allow or deny access to features and/or data in accordance with any business need. CA also implements best practices in guarding from outside threats. Each customer's data and configurations are currently 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 Clarity Service uses a session-based cookie that carries a token for accessing the session data that is transient in the cache (for a single app 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, time zone), global access rights the user has, and other shopping cart-like data.

Data Center Security

CA data centers have multiple levels of security to protect customer information. This includes physical as well as data security measures operating systems on a single hardware platform.

Physical Security


All data centers have very limited access:

- **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:** There is no public visitor access to the data centers without prior knowledge and approval of the On Demand Infrastructure team. 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 maintains a security department of security engineers. New security employees and contractors are all subjected to background checks. Security policies along with data retention and destruction policies are in place and published.

Logical Security

Logical security is provided by eTrust Antivirus, as well as by stateful inspection firewalls. "Stateful inspection firewall" means that the firewall stops all incoming traffic, analyzes it, and prevents standard Internet attacks and denial of service attacks. Application servers are located in a demilitarized zone (DMZ), which is separated from CA's 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.

- **Penetration Tests:** Tests are performed weekly by a 3rd party vendor, Digital Defense, Inc.
- **Medium/High Risks:** Medium/high risks are identified and remediated before production systems are made available. Ongoing scans are performed to ensure no new risks have been introduced and are resolved if found.
- **Hacker Monitoring:** The systems are monitored 24x7 by CA products (CA Audit and CA Cohesion). Audit logs are sent to centralized CA Audit system and are reviewed daily to ensure there is no unusual activity.

- 
- **Virus Protection:** All CA servers are protected by CA eTrust Threat Management Antivirus product. The environment undergoes regular vulnerability scan from internal and external network.
 - **Application Security:** During the development and QA stages, the application undergoes security review and testing.
 - **Asset Management:** CA Asset Management is being used to optimize asset utilization by centralizing, managing, and tracking assets as well as enforcing software compliance.
 - **Server Hardening:** All servers are hardened in accordance with CA Global Enterprise standards. By running only the necessary services, CA 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. All security patches are tested and approved by CA Global Enterprise Security prior to installation.
 - **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:** CA Audit is used to detect unauthorized access to the server and manages changes to the operating system. CA Cohesion is used to manage changes to the configuration of the application.
 - **Data Sanitization:** Data storage and tape media are sanitized when a Clarity Service contract has expired, hardware breaks, or customers ask for sanitization to be performed. Note, customer data is only stored on data storage and tape media, so there is no process necessary for other media (e.g. USB, CD, DVD). A low level format is performed on the media when they are no longer in use. Tapes used for backup are formatted and recycled in the pool.

SECTION 3: DATA CENTERS

Data Center Overview

CA On Demand solutions are operated, maintained, and managed by highly skilled IT staff in multiple locations around the world. To optimize performance, all data centers are located near core Internet hubs.

The hardware and data are currently located in three data centers as below and various others are being considered based on demand:

- Somerset, New Jersey: managed by DataPipe
- San Jose, California: managed by DataPipe
- Munich, Germany: managed by Equinix

All three data centers are network neutral, which generally allows for uninterrupted service should an Internet Service Provider, other than the customer's own, experience outages.

Power Management, HVAC Environmental Controls, and Disaster Prevention

All datacenters employ extremely modern power management, HVAC, and disaster prevention systems. The most current details on these can be found at:

http://www.datapipe.com/Data_Centers.aspx

<http://www.equinix.com/solutions/colocation>

Site Access

All data centers have very limited access, in order to prevent any compromise of customer information. Please see Security above for details.

SECTION 4: DATA BACKUP AND RECOVERY

Data Backup

The process for backing up and recovering customer data is as follows:

- Server backups occur daily. A full backup is performed on Friday, and differential backups are performed Saturday through Thursday. These daily backups are replicated offsite.
- Backup retention time is thirty days and all backup data is encrypted. For the first 7 days backed up data is stored on disk, and thereafter moved to tape. Backup tapes do not leave the premises.
- Customers may request manual backups or may request a restore from any snapshot within the retention period. This restore is a complete environmental backup restore (database, filestore and reports), which could be from backup or from another server. 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. If only selective data needs to be restored, customers should contact CA Professional Services.
- In case of a disaster, CA will recover from the most recent backup. Minimal or no action is required by the customer in most disaster recovery scenarios.

Disaster Recovery

The two North America datacenters serve as disaster recovery sites for each other, and for EMEA. 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. Also, during recovery, the system may be unavailable for 4 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.

Disaster to the CA 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 network in Illinois.

Integration Overview

CA's 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. The work to build integrations is not part of the Clarity Service subscription, but CA Professional Services can be engaged to assist or customers can build these themselves.

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

- XML Open Gateway (XOG)
- FTP Drop-off combined with GEL (Generic Execution Language) enabled processes
- SOAP
- Open Workbench
- Microsoft Project integrated with CA Clarity PPM
- CA Clarity PPM Connector for Microsoft SharePoint
- Federated Single-Sign-On

XML Open Gateway (XOG)

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


CA 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 Clarity 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 that need to be secured.
- **Authentication:** XOG must use an authenticated Clarity Application user to access the application.
- **Access Rights:** The Clarity Application user must have access to the data in the Clarity Service exactly like the user would have inside of the Clarity Application.

FTP Access

FTP access provides customers an asynchronous and scheduled way to integrate with their applications. The Clarity Service allows for FTP access to a secure drop-off/pickup location.



This allows customers to deliver to or receive files from (e.g. XOG files and/or GEL scripts) their Clarity Application.

SOAP

Custom SOAP integrations can be setup between the Clarity Service and a customer's third party solutions. Third party SOAP integration toolkits include Apache AXIS 1.3 and MS Visual Studio 2005 (.NET Framework 2.0) for Windows. Direct SOAP integration with a client is possible by using the XOG API over standard HTTPS port.

Open Workbench

The Clarity Application includes a free comprehensive client scheduling tool called Open Workbench (OWB). Users can download this tool from the Clarity Application and can launch OWB from the Clarity Application without providing credentials.

Since the Open Workbench is an optional client for the Clarity Service, the customer must install the Open Workbench client to their users' machines, and configure the Open Workbench with username, password, and URL. Open Workbench is safe in the Clarity Service environment for the following reasons:

- **Web Service:** Because OWB communicates over HTTPS using a specialized Web Service, there are no extra ports or sockets that need to be secured.
- **Authentication:** OWB must use an authenticated Clarity Service user to access the application.
- **Access Rights:** The Clarity Application user must have access to the data in the Clarity Service exactly like the user would have inside of the Clarity Application.

Microsoft Project


The Clarity Application provides bi-directional, real-time integration with Microsoft Project and allows users to create, view and modify detailed project plans in Microsoft Project. The Clarity Application Microsoft Project macro transports raw data from Microsoft Project from/to the Clarity Application over HTTPS connections. Users can open a plan in Microsoft Project through a link on the Clarity Application project overview page. Clicking on this link invokes Microsoft Project and loads the project from the Clarity Application. User credentials are not required for this activity.

Once updates are complete, the user saves the project back to the Clarity Application from within Microsoft Project. While the project is open in Microsoft Project, it is locked within the Clarity Application, allowing other users to view but not revise the plan. It should be noted that detailed project scheduling could also be done directly in the Clarity Application via the browser, eliminating the requirement for Microsoft Project if preferred.

Because Microsoft Project is a client for the Clarity Application, the customer must install the Microsoft Project client to their users' machines, and configure Microsoft Project with username, password, and URL.

Microsoft Project is safe in the CA On Demand environment for the following reasons:

- **Web Service:** Because Microsoft Project communicates over HTTP/HTTPS using a specialized Web Service, there are no extra ports or sockets that need to be secured.

- 
- **Authentication:** Microsoft Project must use an authenticated Clarity Service user to access the application.
 - **Access Rights:** Access Rights: The Clarity Application user must have access to the data in the Clarity Service exactly like the user would have inside of the Clarity Application.

Microsoft SharePoint

The Clarity Service provides a connector for Microsoft SharePoint (SP Connector). This SP Connector provides the ability to have a read-only view of the Clarity Application project data in from within an existing SharePoint installation by using SharePoint Web Parts.

The Connector integrates with the Clarity Application through a Web Service over HTTPS, and therefore no special ports or sockets need to be exposed to pull Clarity Application data into an existing SharePoint deployment.

The Connector can be thought of as another client for the Clarity Service. Because of this, the customer must manage the installation and configuration of SharePoint and the connectivity to the Clarity Service.

The Connector is safe in the Clarity Service environment for the following reasons:

- **Web Service:** The Connector communicates over HTTPS using a Web Service and there are no extra ports or sockets that need to be secured.
- **Read Only:** The Connector is a read only client, so there is no way for Clarity Service data to be modified.
- **Authentication:** The Connector must use an authenticated Clarity Service proxy User to access the application.
- **Access Rights:** The Clarity Service proxy user must have access to the project data in the Clarity Application exactly like the user would have inside of the Clarity Application.
- **Single Project:** The Web Parts access data from a single project. With the scope limited to one project, there are fewer concerns about unwanted data being exposed.
- **Encrypted Passwords:** The Clarity Service proxy user's password is an encrypted (Triple DES) property in SharePoint.

Federated Single-Sign-On (SSO)

The Federated Single-Sign-On integration allows customers to create a trusted relationship with the Clarity Service and this has the following benefits:

- **Seamless integration between networks and environments:** Users can move easily between their intranet, and the various production, development, and test Clarity Service environments.
- **Simplified password management:** Customers do not have to manage their users' passwords separately for the Clarity Service since these will be handled by their existing SSO solution.



CA uses eTrust SiteMinder for this SSO federation.

If the customer is using Federated SSO, their password management will be centralized within their environment. All password construction, change intervals, etc. will be controlled on the customer side. The customer might not even have passwords if they are using a non-username/password means of authentication.

The Federated SSO only works if the customer also has a Federated SSO solution installed on their network. Because of this, the customer must manage the following tasks themselves or engage CA Professional Services:

- Install the Federated SSO Assertion Producer. This does not need to be CA SiteMinder because SAML is an open standard. Most standard SAML 2.0 or 1.x solutions should work with the Clarity Service. .
- Add and Configure internal applications inside their SSO environment.
- Configure a trusted relationship with the Clarity Service.
- Optionally, create links on its intranet to the Clarity Service.

Federated SSO is safe in the CA 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 Clarity Service and this means fewer places for security breaches.

SECTION 6: APPLICATION

Configuration with CA Clarity PPM 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 Clarity PPM Studio, a point-and-click configuration module in the Clarity Application, that 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 Clarity PPM Studio allows you to easily tailor business objects, such as portfolios, 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 Clarity 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.

Reporting

In addition to real-time reporting using the clarity application, CA also provides business intelligence via Business Objects. Business Objects runs against both the live application database, as well as the supplied Business Objects Universe by serving reports as DHTML pages to the client. Using Business Objects, reports can be scheduled or immediately executed from within the Clarity application. Reports can be saved as PDF files or exported to Microsoft Excel or RTF format.

Email Notifications

The Clarity Service has the capability of sending email notifications for events such as user addition, addition to project teams etc.

Search Capabilities

Customers can search across all structured and unstructured data in the Clarity Application. As documents are added, each word in every document is indexed. The Clarity Application search engine provides a full file content search for:

- Microsoft Office: Word, Excel and PowerPoint
- Microsoft Project
- Microsoft Visio
- Text and RTF (Rich Text Format)
- PDF
- HTML or XML
- ZIP

To learn more about the architecture and technology powering CA Clarity PPM On Demand, visit ca.com/ondemand or contact your CA representative.

APPENDIX: CA Clarity Service Product Architecture Stack

Clarity Internationalization and Localization

The Clarity Application is internationalized and currently supports 15 languages (see table below), as well as many regional settings for date, time, and number formatting.

Supported Languages			
English	Spanish	Dutch	Korean
French	Brazilian Portuguese	Swedish	Simplified Chinese
German	Italian	Czech	Traditional Chinese
Japanese	Danish	Finnish	

Note: Not all languages are supported in client applications referred to elsewhere in this Technical Overview.

Client Components	Microsoft Windows	Apple Mac OS	Desktop Linux
Client Operating System	Microsoft Windows XP Professional: Service Pack 2 or higher Microsoft Windows	Mac OS X: release 10.3 or higher	Any vendor or version with support for browsers listed below.
Client Browser	Internet Explorer 6.0 SP1, version 6.0.2800 or higher Internet Explorer 7.0 Firefox: version 3.0 or higher	Safari: version 2.0.1 or higher Firefox: version 3.0 or higher	Firefox: version 3.0 or higher
Federated Identity Providers	CA SiteMinder Federation Security Services (CA FSS) CA Federation Manager Any SAML 1.1, SAML 2.0 or WS Fed Provider		
SharePoint Server Integration	Integration requires Windows SharePoint Services 3.0 (WSS 3.0) or greater with Microsoft Office Web Components. Both Microsoft Office SharePoint Portal Server 2003 and Microsoft Office SharePoint Server 2007 are supported if you use them with WSS 3.0.		
Client Applications	Microsoft Excel 2002-2007, all editions. Note: Excel 2002 or higher is required for Export to Excel functionality. Microsoft Project 2002-2007, all editions Java 5 Runtime Environment	Microsoft Office Excel. Mac OS Preview PDF viewer (for reading Clarity installation guides, technical manuals and user guides) No MS Project support	Acrobat Reader 7.0 or higher (for reading Clarity installation guides, technical manuals, user guides, and offline reports) No Excel Export support No MS Project support
Third-party SOAP Integration Toolkits	MS Visual Studio 2005 (.NET Framework 2.0) Apache AXIS 1.3	Apache AXIS 1.3	Apache AXIS 1.3
Configuration	1 GHz Pentium III 512 MB (power users) 1 GHz Pentium III 256 MB (all other users)	Macintosh with G3 or Intel processor 256 MB	1 GHz Pentium III 256 MB



Required Network Setup	
Web Access	SSL port 443 for the application service access SSL port 8080 for the reporting service access
Mail Server	mail.ca.com needs to be on the exception list

IDENTITY AND ACCESS MANAGEMENT COMPONENTS	
Single Sign On (On Demand Portal only)	CA Siteminder R6 SP5 CR26
Federated Single Sign On	CA SiteMinder Federation Security Services (CA FSS) r6.0 SP5 CR26
LDAP	CA Directory Server R12SP1



CA, one of the world's largest information technology (IT) management software companies, unifies and simplifies the management of enterprise-wide IT for greater business results. Our vision, tools and expertise help customers manage risk, improve service, manage costs and align their IT investments with their business needs.