



Clear Innovation

White Paper

enPortal Technical Overview

September 2011

Edge Technologies
3702 Pender Drive
Suite 420
Fairfax, VA 22030
T 703.691.7900
F 703.691.4020
888.771.EDGE

Overview

Integration is no longer just a nice-to-have technology – it has become a must-have technology in commercial and government environments around the globe.

For many successful organizations, a portal strategy serves as the foundation for integration. As such, the concept of a portal is maturing rapidly. The original concept of a portal addressed the need to publish information to users via a web page. Enterprises today, however, need a portal that provides more than static displays of back-end applications and information.

Customers today are looking to implement a sophisticated portal that provides data-level integration and secure access to fully interactive applications. Customers expect to be able to share resources and information, in real time, within and between enterprises.

Customers are also demanding that portal implementations provide:

- Single sign-on to a wide variety of applications
- Integration and content customization with little or no coding
- Better security and protection of application servers
- Coordinated interaction between applications

Edge Technologies' enPortal is the industry's only portal focused specifically on network management application integration. enPortal allows organizations to provide secure access to interactive back-end applications, implement consolidated single sign-on, and centrally coordinate interaction between applications – with little or no coding.

At the core of enPortal is Edge's technology engine. This software engine collects and consolidates information from the network's existing tools and applications. enPortal aggregates the information and presents it to the user through a highly customizable dashboard. For even more dashboard flexibility, enPortal can leverage its close integration with Edge's application and dashboard builder, AppBoard.

A distinct advantage of enPortal is rapid deployment, made possible by enPortal's prepackaged Product Integration Modules (PIMs). enPortal PIMs provide plug-and-play integration of products from CA, Hewlett-Packard, InfoVista, IBM Tivoli, EMC, and more.

enPortal reaches well beyond the capabilities of existing portal solutions that focus primarily on document management, indexed searches, and static displays of data. enPortal provides true integration.

"Our clients have mission-critical networks," said Brett Rushton, VP of managed services at Insight, a full-service network integrator and managed service provider. "We needed a strategy to empower our clients ..., [to] provide customized information and develop recommendations on streamlining work processes. Edge's enPortal gives us [that]."

enPortal Architecture

Design Architecture

Edge enPortal is a standards-based, XML-driven portal application. enPortal was developed with Java technologies to provide unparalleled flexibility, scalability, application and content protection, application interaction and complete platform independence. enPortal can be deployed in as a self-contained web application with embedded database or leveraging a multi-tier architectural model. This provides great flexibility for deployment into various network configurations and is the foundation for the redundancy and scalability support.

In a multi-tier deployment architecture, the first tier is typically one or more hardware load-balancers and/or SSL accelerators. These front-end load-balancers pass incoming requests to one or more enPortal servers on tier two, running as Java web applications typically executing under the Tomcat web/application server (referred to as the Servlet/JSP engine). The enPortal configuration database is then resident on tier three, and will often be a redundant database cluster to provide load-balancing and high availability.

All components support maximum platform independence (UNIX or Windows), scalability, and overall system performance.

Software Component Architecture

The primary functions of enPortal are contained within five system components:

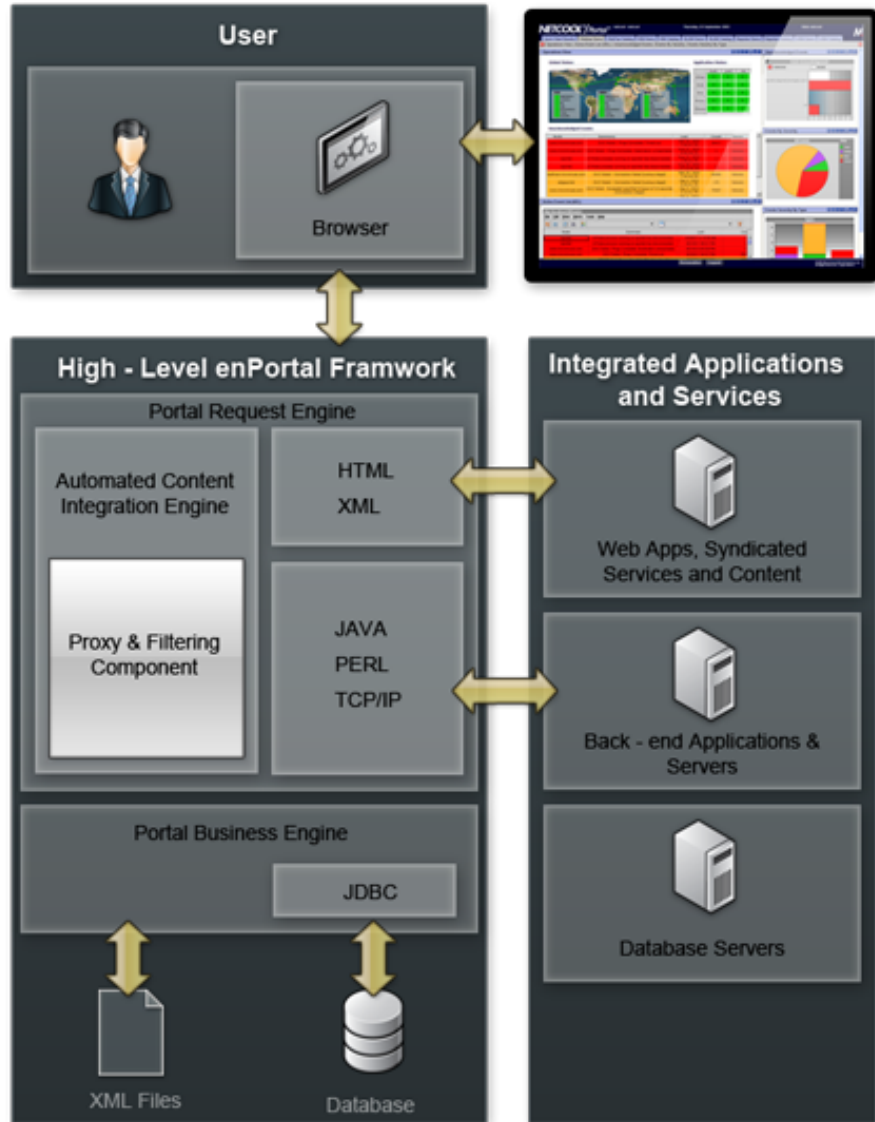
- Portal Request Engine
- Portal Business Logic Engine
- Integration Engine
- Web Resource Proxy and Content Filtering
- Portal Object Database

Portal Request Engine

The Portal Request Engine serves all requests coming from a user via a Web browser.

In fact, all external communications with an enPortal system are requested through the Portal Request Engine. The Portal Request Engine's primary responsibilities are to translate HTTP(S) requests into object requests and to dynamically translate the application-specific results into HTML for transmission to the client Web browser.

The Portal Request Engine executes within a Servlet/JSP engine; Java Servlets and JSPs are the primary components of the Portal Request Engine. The Portal Request Engine also provides an extra level of access security by verifying that the user is logged in to the system before accepting and servicing the request.



Portal Business Logic Engine

The Portal Business Logic Engine is responsible for the overall business logic of the system, enPortal’s security, and the storage of system objects. These responsibilities pertain to users, roles, domains, virtual directory access, content management, and security and system/service objects.

Business Logic manages and stores system objects to a chosen object repository/database.

General access to these objects is provided through the internal enPortal system services.

The Business Logic Engine runs on the same process (Tomcat as the JSP/Servlet Engine) as the Request Engine.

Integration Engine

The Integration Engine allows new content Channels to be created and integrated into an enPortal system at runtime. The Integration Engine consists of a Channel classification model and a set of Request Handlers that are implemented as Java Servlets or JSPs. Request Handlers are the public web interfaces into enPortal Channels that service the Channel requests being made from web browser clients. The Integration Engine provides an external interface through the Portal Request Engine that allows HTTP(S) requests to be sent to any plugged-in visual Channel.

Upon receipt of a request to render a content Channel, the Integration Engine retrieves the specified Channel (if security allows it) from the Portal Server and calls the specified Request Handler to render the Channel content.

Web Application Proxy and Content Filtering

The Web Application Proxy and Content Filtering function facilitates the delivery of and interaction with existing HTTP(S)-based content. It is responsible for applying Single Sign-On (SSO) rules to the retrieval of external HTTP(S) requests, and for manipulating the resulting data streams being returned from an integrated application for control and data customization. The HTTP(S) stream manipulation support within enPortal is both extensive and configurable, and is available as a Proxy Channel. A potential example of the use of this function is the removal of an image from an HTML stream as enPortal delivers the HTTP(S) stream to the browser client.

Portal Object Database

The enPortal Database is a JDBC-compliant RDBMS, and it supports numerous databases, including Microsoft SQL Server and Oracle. For smaller deployments, enPortal ships with an embedded database that provides excellent performance when a redundant, multi-tier solution is not required. The enPortal Database handles mapping between the object-based data model used within enPortal and the relational database model that stores the actual content.

Core Features/Capabilities

The five core software components of enPortal combine to provide advanced capabilities and significant benefits – many of which are unique to enPortal and not possible through other portal offerings.

enPortal offers a vast array of portal-solution features and functions (see "Additional Features" below). The core features/capabilities of enPortal include:

- Content Retrieval and Integration
- Advanced Security
- Single Sign-on
- Proxy Technology
- Dashboard Views

Content Retrieval and Integration

To get the most out of a portal, customers need the ability to integrate new content elements quickly and securely. Customers also need the ability to enable partners and other third parties to organize application services, multi-media streams, and web-based utilities into any number of user views – without complex software development.

To meet the challenge of integrating, controlling, protecting and multiplexing fully interactive back-end applications and content into a virtual portal desktop over private and public networks, Edge developed the Content Retrieval System.

An integral part of enPortal, the CRS detects, modifies, stores, and disseminates information being retrieved from web applications integrated through the enPortal framework. The CRS is designed to incorporate any number of fully interactive dynamic applications into a portal page view. From an administrative perspective, CRS manages user access and control to fully interactive applications and web content based on user, domain, and role.

CRS also provides for the multiplexing of disparate external HTTP(S) communication streams over a single HTTP(S) port to the web browser by:

- Supporting remote access to an unlimited number of fully interactive applications through firewalls and multi-layer DMZ environments utilizing network address translation – regardless of the application's IP address or port number – for transport over public networks
- Supporting the ability to conceal IP addresses and port numbers to applications, web resources and their network elements, thereby protecting the operational network and enterprise applications

Integration – PIMs

Working with the CRS, the enPortal framework also includes a series of integration offerings – called Product Integration Modules (PIMs) – for many popular management applications. Providing out-of-the-box integrations, PIMs offer immediate value to an organization that has made existing investments in these applications.

PIMs are essentially XML definitions that define how enPortal will integrate the third party products and applications into content Channels and Views. To integrate a new application with enPortal using a PIM, an administrator specifies the IP address, web server port, and configuration information for a live application. enPortal then automatically creates content Channels for the third party application for immediate incorporation into a portal page.

The following is a partial list of products for which Edge offers PIMs:

- Alcatel-Lucent VitalSuite
- Arbor Networks (Fluke) Peakflow
- BMC Portal
- CA eHealth
- CA (Nimsoft) SDP
- EMC Ionix Control Center
- EMC Ionix NCM (VoyenceControl)
- EMC Ionix Suite (SMARTS inCharge)
- Frontbridge Email
- Frontbridge Spamshark
- HP BAC (Mercury BAC/Topaz)
- HP OpenView NNM
- IBM Tivoli IT/CAM for ISM
- IBM Tivoli IT/CAM for RTT
- IBM Tivoli IT/CAM for Websphere
- IBM Tivoli Netcool NMIP (ITNM IP, Precision IP)
- IBM Tivoli Netcool Network Manager TN (ITNM TN)
- IBM Tivoli Netcool Performance Manager for Wireline (Proviso)
- IBM Tivoli Netcool Reporter
- IBM Tivoli Netcool TBSM (SLAM, RAD)
- IBM Tivoli Netcool Topoviz
- IBM Tivoli Netcool Webtop/Web GUI
- IBM Tivoli Integrated Portal (included at no charge with TIP-enabled Tivoli-related PIMs)
- InfoVista Portal SE
- InfoVista VistaPortal
- McAfee IntruShield IPS
- NetWitness
- Oracle (Sun) Secure Global Desktop
- Oracle 10g
- Plexier Scrutinizer
- SAP Business Objects InfoView
- SAP Crystal Reports
- SevOne NMS
- SolarWinds NPM (Orion)
- Tripwire
- Viador Biportal
- Websense Explore

The above list continues to expand as Edge generates PIMs for new applications.

Advanced Security

enPortal has a strong security model with powerful features to restrict access to content based on domain, role (group) and/or user. enPortal also provides a combination of firewall infrastructure support, port mapping, content filtering, and a sophisticated security manager.

Enhanced security features include multiple N-Factor authentication methods, secure communications channels, security policies, directory services support, and more (see below).

Additional Security Features

Authentication Mechanisms

enPortal enables authentication through three means:

- via internal enPortal authentication
- via LDAP authentication
 - enPortal can communicate with existing LDAP user directories to synchronize User and Role information, and to authenticate User's login credentials.
 - enPortal maps LDAP people and groups into internal Users and Roles
- through custom-developed authentication mechanisms

Password Management Policies

The security of the system is enhanced by the ability to define password management policies for users' passwords. The following types of policies can be instituted:

- specifying a password lifetime, which forces users to change passwords
- syntax polices, to avoid the use of predictable passwords
- account lockout upon consecutive failed login attempts

Access Control List Rules

enPortal enables Administrators to create "allow" and "deny" rules that can be enforced from the global and/or Channel-specific level. For example, these rules can prevent users from accessing specific URLs.

Streamlined Content Provisioning

enPortal's administrative interface provides a single step assignment of content to users through roles. This process also configures security so that access control lists are automatically managed by enPortal, eliminating the often separated steps of content provisioning and securing, if desired by the administrator.

SSL Communications Support

Communications between enPortal clients and the enPortal server can be secured using HTTPS (HTTP over SSL). This protects the communications streams as they pass through the public Internet. enPortal's Tomcat web server provides the HTTPS support, and the configuration rules to enable this are delivered with the stock configuration files.

The enPortal server can also communicate with external HTTPS web servers. This typically occurs within the Web Resource Proxy (discussed below), and is dictated by the protocol field of the URL that the Proxy has been directed to retrieve.

Single Sign-On

Out of the box, enPortal provides single login to multiple applications. Once a user logs into enPortal, no other credentials are required from that user. This capability is provided with no custom software development or modification to back-end applications.

The enPortal Single Sign-On feature supports the integration of various security and authentication schemes presented by existing applications. This capability is implemented through a component called the Login Proxy Service (LPS) that handles all authentication interactions between the user and third party services.

Web-based single login can be difficult to standardize into a solution that fits in all cases.

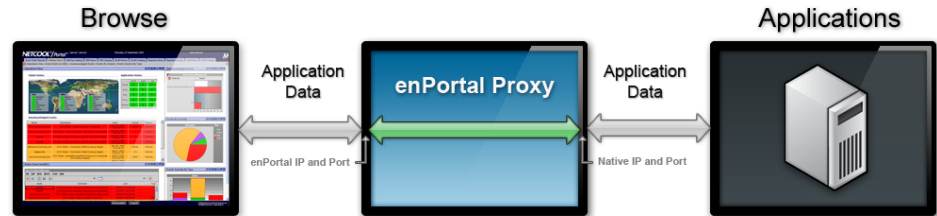
Each single login implementation for an application is a unique integration with its own unique interface. However, while the method of presentation can vary, most methods of authentication still use the HTTP protocol to submit credentials/maintain authentication.

HTTP-based methods of authentication can be automated by the combination of the enPortal CRS and LPS.

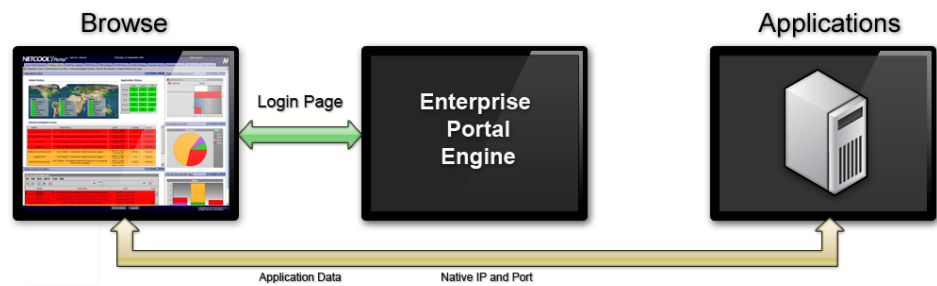
Proxy Technology

A key component, and differentiator, of enPortal is its proxy technology. enPortal proxy technology provides protected access to fully interactive applications over public and private networks. It works by allowing access to specifically identified back-end web applications and content to authorized enPortal users. Of significant importance, enPortal’s web resource proxy does not require installation of additional software on the servers being proxied.

enPortal



Typical Portal



The figure above illustrates two communications methods by which various portal systems interact with, and render, fully interactive applications to the user. The “enPortal” example illustrates data flow between applications and client browsers through the enPortal web resource proxy technology. The “Typical Portal” example illustrates data flow between applications and client browsers within other portal frameworks.

Note that in a typical portal system, direct communication is required between the browser and the external application. In these systems the login page, initial portal page and wrapper-based pages are requested directly from the portal server. However,

when the user begins interacting with an embedded application, the browser begins communicating directly to the external application.

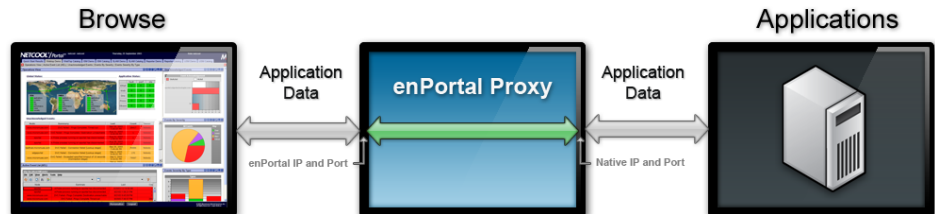
The enPortal system, on the other hand, uses a web resource proxy approach to provide controlled access to fully interactive web applications. The web resource proxy approach allows the web browser to communicate entirely with the enPortal server for all interaction with the external web applications. Moreover, enPortal supports application displays through traditional redirection when the implementation calls for it.

Additional Proxy-based Advantages

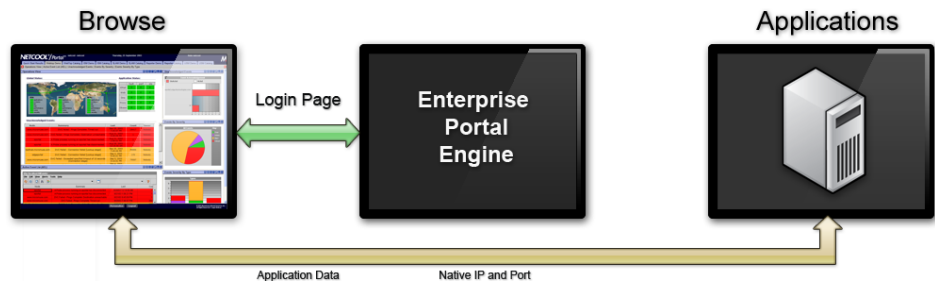
Firewall Support

The enPortal web resource proxy provides users with a single access point (exactly one HTTP(S) port) to all integrated HTTP(S)-based applications. enPortal content retrieval allows all HTTP(S)-based content and applications to be accessed through a single socket connection within a network DMZ, network address translation (NAT) and firewall environment.

enPortal



Typical Portal



Protection of Private Networks and Application Assets

The protection and concealment of back-end applications and network assets are of critical concern to organizations that must provide application access to users and customers over a public network. enPortal allows multiple dynamic HTTP(S)-based resources to be integrated into the enPortal framework, concealed and pushed through a DMZ environment for presentation to external users on a public network. The web resource proxy does not allow clients to directly connect to these resources. Additionally, external entities have no knowledge of applications' addresses, port numbers or operational networks. The enPortal proxy provides an additional layer of protection between internal resources and external users.

Real-time Content Filter and Modification

Real-time content filtering and modification is defined as the ability to detect and modify the contents of HTTP(S)-based character streams as they pass through the enPortal framework. The enPortal web resource proxy allows the system to intercept and manipulate HTTP(S) header requests and message body content. Effectively, enPortal can modify the application presentation and behavior according to each user's needs.

With the enPortal content filtering and modification capability, users can determine which features of an application are dynamically filtered or modified for presentation to the user. Additionally, applications may be modified to "behave properly" within the browser (i.e. remove pop-up windows).

Dashboard Views

One of the challenges of a network administrator's job is to make available a variety of types of information to different types of employees. enPortal's Dashboard View capabilities provide an at-a-glance view of user-centric service health with the ability to drill down for further details.

Specifically, the enPortal Dashboard View:

- Transforms event data to service information
- Transforms component events to service impact
- Integrates data from service-oriented applications
- Provides simple visualization of information derived from disparate data sources

The enPortal Dashboard View also integrates data from multiple management resources, including trouble tickets, events, historical reports, planning resources, and more. With this capability, large enterprise management becomes much less complex – and much more efficient.

For even more dashboard flexibility, enPortal can leverage its close integration with Edge’s application and dashboard builder, AppBoard. The combination of the GUI-based AppBoard Builder, SDK, widgets, and data adapters allow the dashboard builder to rapidly integrate and visualize data.

Additional Features

The CRS, advanced security, single sign-on, proxy technology, and dashboard views make enPortal unique within the portal community. And enPortal offers other, more basic portal features such as:

- The enPortal Administration tool – a web-accessible feature that lets administrators: create/edit domains, roles, and users; set security privileges for enPortal features; create and assign look-and-feels; delegate user accounts, and; manage single sign-on passwords
- Fault tolerance – enPortal was designed to decouple the individual servers from each other, allowing users to be redirected to any running enPortal server without user intervention.

Additional features and benefits of enPortal include:

- Vendor and application-independence
- Distributed, standards-based architecture – Java, JSPs, servlets, XML
- Load balancing
- Online backup
- Consistent look-and-feel
- APIs for customization
- Fail-over support
- Scalability
- Wizard-based tools
- Platform independence: UNIX/Windows support
- Browser independence: IE/Firefox/Chrome browser support
- Personalized portal views
- Read/write/view security privileges by user, role, domain

About Edge Technologies, Inc.

Edge Technologies is an innovative and proven software company specializing in data integration and visualization. Through its core practices in Data Integration, Data Visualization, and Flex Consulting, Edge products and services facilitate faster, more complete data integration; user-centric, customized visualizations; easy, secure information sharing; and enhanced operational awareness across a diverse set of information stakeholders.

Edge has been delivering leading-edge solutions in many of the world's most sophisticated network, intelligence, operational and logistics environments since 1993. Recognized for the ability to identify, adopt and deploy emerging technology platforms, Edge's industry-leading products, such as N-Vision and enPortal, have proven to be ground breaking solutions that stand the test of time.

Edge Technologies' latest innovation, AppBoard, sets a new standard for innovation in real-time data integration and custom visualizations for network and systems management. AppBoard combines a visualization Builder and SDK to fulfill the prerequisites for time-sensitive decision-making in today's dynamic world:

- A vendor-agnostic platform that facilitates simple and seamless integration of all information assets and includes an extensive library of pre-built 3rd party integrations
- The combination of Single Sign-On (SSO) and visualization allowing users to quickly identify and resolve problems.
- The ability to create customized, user-centric, and visually rich dashboards with comprehensive drill-down capabilities
- Real-time data, with real-time interaction

Edge's technological expertise in developing lasting innovation is fortified by the company's value-focused customer and partner relationships. Recognized for meticulous software engineering and a high-touch customer service approach, Edge's success is built on innovative technology driven by experienced, customer-focused personnel.

The Edge Development Methodology first identifies customer challenges, then applies design expertise and innovation to create better solutions and backs it all by the people and technology to ensure the solutions work in the real-world and for the long-haul.

Unlike competitive offerings, Edge's products are designed with both the development

staff and the executive team in mind. Edge software toolkits do the heavy lifting to streamline internal development efforts, accelerate time to market, and empower staff to focus on situational and operational objectives. What's more, Edge's advanced software architecture enables its products to easily scale to handle hundreds of concurrent users.

Edge empowers businesses and government agencies to fulfill the potential of their network and business systems management assets to make better decisions faster. Edge Technologies' clients include Fortune 500 companies, Managed Service Providers, and the United States Federal Government, including the Department of Defense.