

Project Monitor – Security of Information

Project Monitor provides a web-enabled collaborative project planning and project execution environment that can be accessed and shared by users from multiple organizations. It is a single source for project information that can be accessed and shared by company staff, partners, suppliers, and contractors.

Security is a vital concern in such an open collaborative environment, especially security of information. Therefore Project Monitor provides a multi-layer security model with four principal components:

- ▶ Administrative Security
- ▶ Project Access Security
- ▶ Project Information Management Security
- ▶ Information Transmission Security



Administrative Security

Project Monitor contains three levels of administrative security: Project Administrator, Company Administrator, and System Administrator.

Project Administrator: A Project Administrator can administer Project and Program information. A Project Administrator may Add a Project or Program, Modify Project and Program parameters, Manage Program lists and Program/Project assignments, and Manage Project Status information.

Company Administrator: Each Company using Project Monitor has a Company Administrator. A Company Administrator has access to an extended Administration Menu that allows the modification of company-specific parameters such as Functional Areas, Description Types, Status Types, Program Types, Budget Categories, and Company Types. A Company Administrator is also able to administer Company Users and configure Dashboards. A Company Administrator may act as a Project Administrator for any Project in the Company.

System Administrator*: A System Administrator may modify Project Monitor parameters that affect all organizations using the Project Monitor installation. A System Administrator may change Company "branding" parameters and files, and may assign any individual Project Monitor User access to multiple Project Monitor Companies. A System Administrator may also act as a Company Administrator for any Project Monitor Company.

*This level of Administrative privilege is only available to Project Monitor clients using a local or private installation of Project Monitor.

Project Access Security

Project Access Security controls how a Project (and its information content) is made visible or invisible to Users of Project Monitor.

Secure Access: By default, all Company Projects are non-Secure. In a non-Secure Project, the Project Name is visible to all Company Users, and the project information content is available for viewing by all Company Users. In a Secure Project, the Project Name is only visible to Project Team members, and the Project information content is only available for viewing by Project Team members.

Houston, TX
+1 713-956-2165
+1 877-9PETRIS

Toulouse, France
+33 581 330 020

London, UK
+44 20 8202 2433

www.petris.com

Assignment Access: Project Monitor users are classified as Employees or Contractors. To a Contractor, all Company Projects appear as "Secure," so Project Names are only visible to Contractors who are Project Team members, and Project information content is only available for viewing by Contractors who are Project Team members.

Document Access Security: By default, all documents for Projects in Project Monitor are "non-Secure," so documents are visible to all Project Monitor Users, and document content is available for viewing by all Project Monitor Users. If Project Documents need to be kept confidential, they can be marked as "Secure," so they are only visible and accessible to Project Team members.

Project Information Management Security

Used at the Project level, Project Information Management Security allows the Project Manager to define which Team Members may view, add, modify, or delete specific elements of Project information content.

The Project Manager may restrict the viewing and updating of budgets and evaluations to a subset of Project Team members, and may also limit the ability to "post" (or upload) documents. Conversely, the Project Manager may extend to any number of Project Team members the ability to modify all Issues, Meetings, and Tasks.

Document Storage Security

Used at the Project level, Document Storage Security provides the Project Manager and Project Team control over how Project Documents are stored in Project Monitor.

Document Upload: A Project Document may be "uploaded" to the Project Monitor Server and stored in the Secure Document Repository for that Project. This action copies the Document to the Document Repository on the Project Monitor Server, and allows other Project Team Members to view or download the Document as required. Project Monitor will not allow the upload of high-risk document types, such files with the .com, .dll, .exe, or .vbs extensions.

Document Links: A Document Reference may be created in the Project Document Repository using a "Document Link." This action creates a Reference to that Document using the file path location of the Document and an optional Document location description. References may be created, deleted, or moved just like any other Project Document. Referenced Documents are only accessible to browsers configured to recognize the Project Monitor Server as a "Trusted Site."

Information Transmission Security

Project Monitor employs a digital certificate to encrypt information that is exchanged between the User client and the Project Monitor server. Digital certificates provide data encryption using "Secure Socket Layer (SSL)" technology, an accepted, industry-standard method for protecting client-server exchanges. The SSL security protocol also provides server authentication, message integrity, and optional client authentication for TCP/IP connections.

Upon login, Project Monitor establishes a secure "Session" with an authenticated User. If this Session remains idle for more than 20 minutes, Project Monitor will automatically terminate the Session. Project Monitor will deny all further client-server exchanges until the User establishes a new Session with Project Monitor.

www.petris.com

© Copyright 2006 Petris Technology, Inc. All rights reserved.

PetrisWINDS is a trademark of Petris Technology, Inc. in the United States and other countries. Other parties' trademarks and service marks are the property of their respective owners, and should be treated as such. Information in this document is subject to change without notice, and does not represent a commitment on the part of Petris Technology, Inc.

Ver 090606