Directory Services and Your Enterprise RtPM

Presented by:

John Matranga
CTO, Omicron Consulting

OMICRON
imagine. develop. evolve.

Omicron Consulting
1500 Market Street
Philadelphia, PA 19102

Abstract

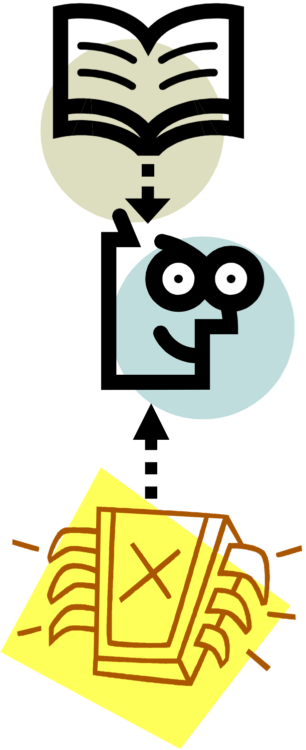
- Your company is rolling out Active Directory (AD), Novell Directory Services (NDS) or SunOne Directory Service or IBM SecureWay Directory.
  - What are directory services? What is AD and NDS? How do directory services fit with your PI Server and Portal infrastructure?
  - These are the types of questions that John will cover as he outlines Directory Services and what role they play in moving your PI Server to an Enterprise Level RtPM Infrastructure.
- DISCLAIMER:
  - This talk is designed to be a primer, there will be some OSIsoft specifics for what is today. Also there will be some forward looking, non- OSIsoft endorsed ideas that will be used as examples.

Agenda

- Directory Services
  - General Overview
  - Uses
  - Examples
- LDAP
  - History
  - Use
- PI and Security - A few notes
- RtPortal and Directory Services
  - SPS Overview
  - RtPortal Issues
- Q/A & Resources

Directories

- Non-electronic Directories
  - Phone Book
  - Healthcare Providers
  - Parts Catalog
- Electronic Directories
  - Users
  - Web Sites (Yahoo List)
  - Printer Resources



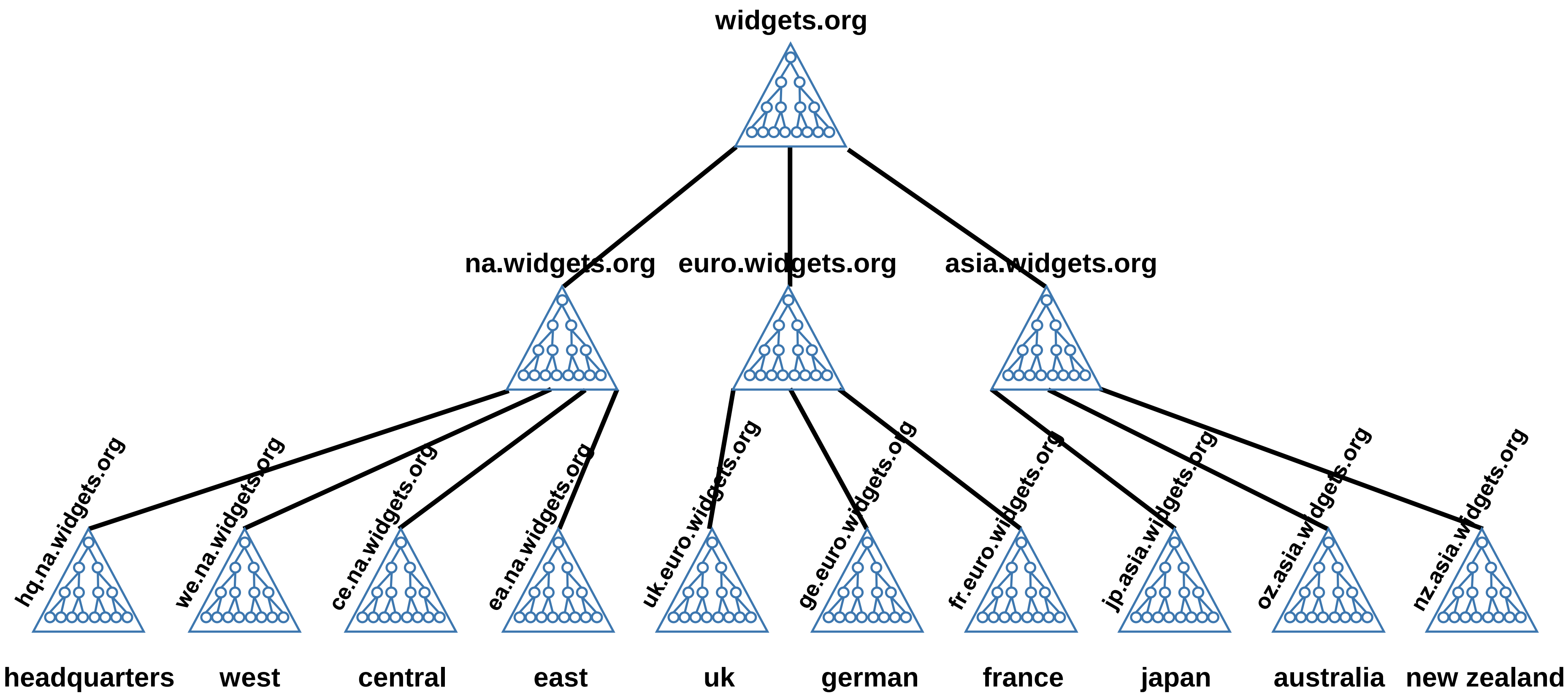
Directory Service Attributes

- Special Purpose Database – Resource Lookup
- Not Just a Normal Database, But Optimized
  - Write Few, Read Many Times
  - Often Contain Certain Types of Data
    - Servers, Printers, File Systems, Applications, Users, Profiles, Etc..
  - Not Designed For Complex Queries
  - Hierarchically Organized
  - Standard Namespace
  - Remote Access - LDAP

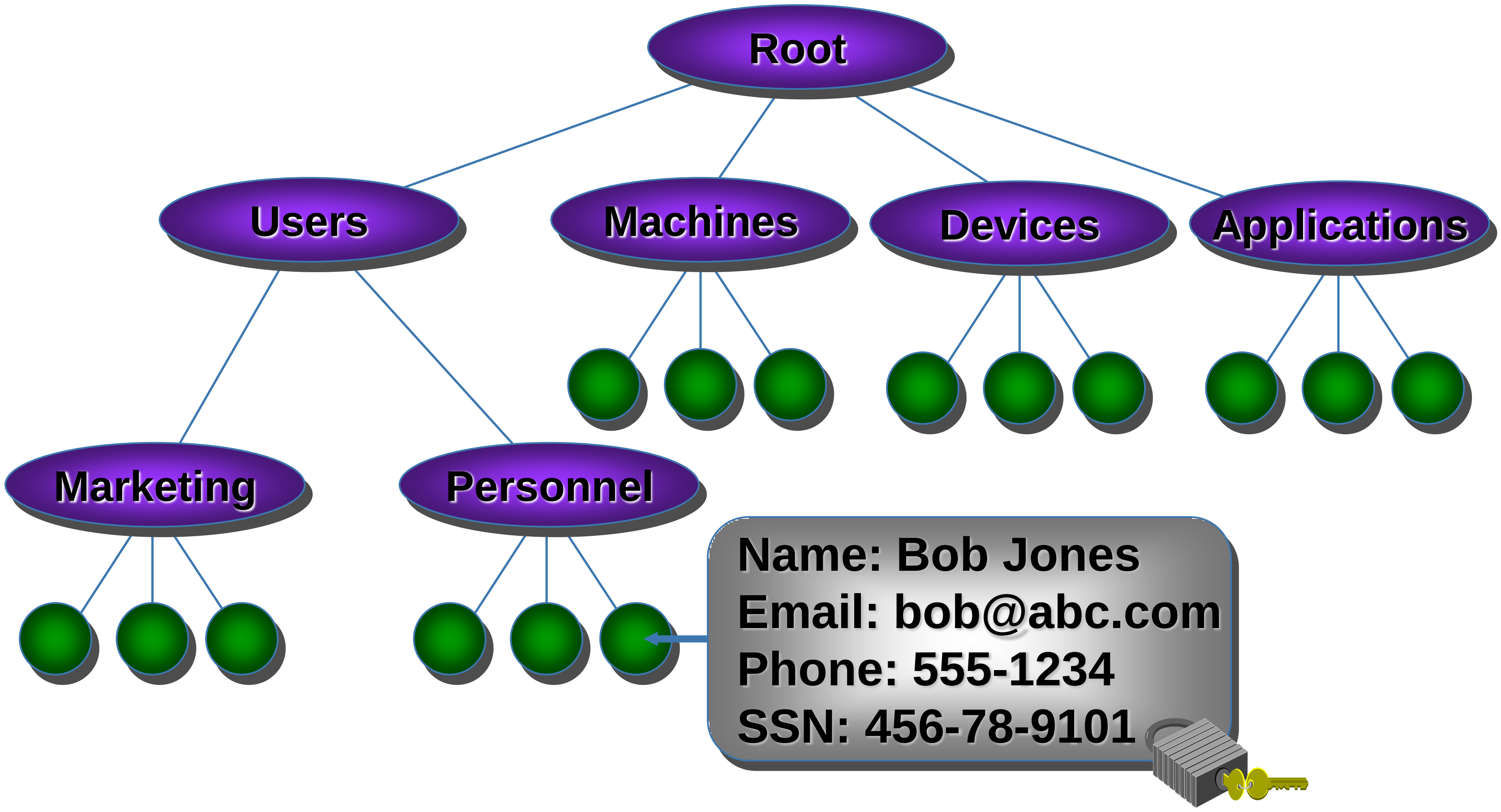
Drivers for a Directory

- Single Unified Security
  - THE Security Service (“The C/S” Subsystem)
- Single Source of Users
- Single Source of Role Based Profiles
- Authorization & Authentication
  - What & Who
- Dynamic Indirection
  - List Based Management – eg. Mail Lists
  - Role Based Solutions
- Costs
  - Multiple Create/Update/Delete Lists
  - No Need for Specific Security DBAs
- Integration

Domain Name System (DNS)



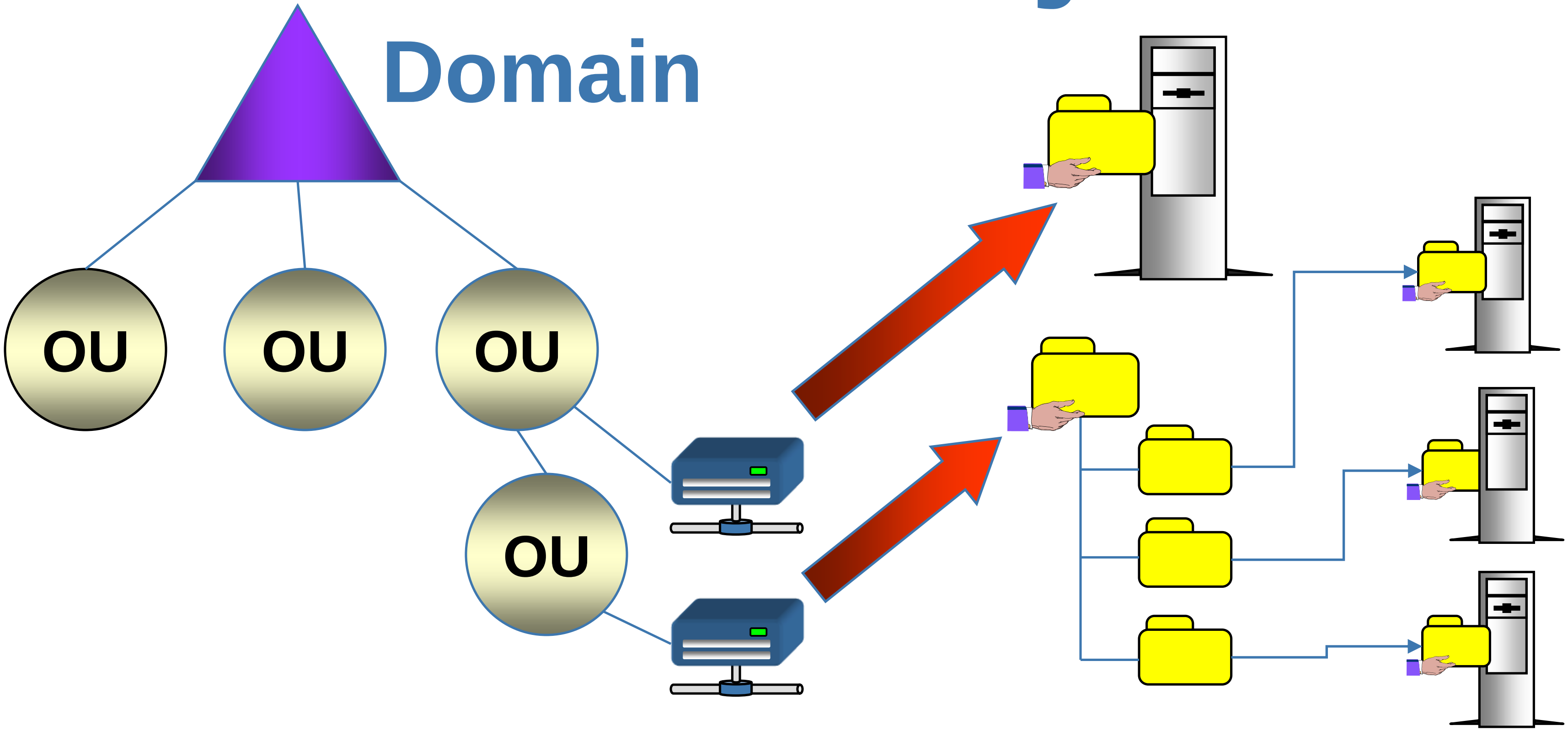
Directory Architecture



Name: Bob Jones
Email: bob@abc.com
Phone: 555-1234
SSN: 456-78-9101

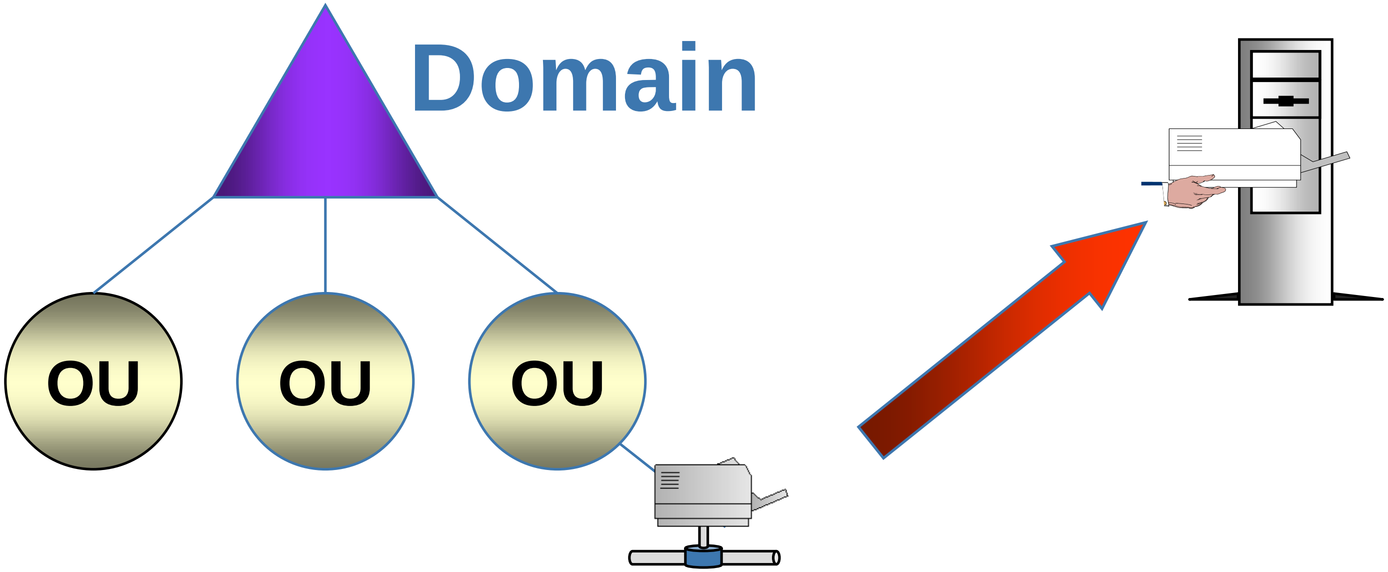
- Directory objects have attributes
- Object and attributes are protected by ACLs

Shared Folder Objects



- A shared folder directory object abstracts a shared folder or Dfs volume
  - A UNC path points to the resource

Printer Objects

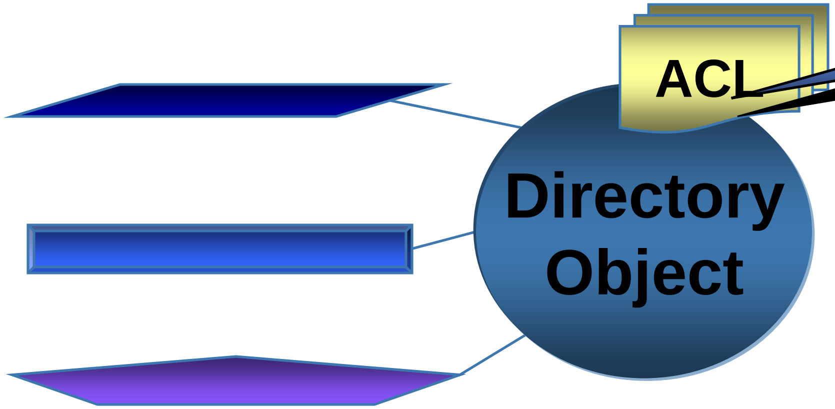


- A printer directory object abstracts a shared printer
  - The printer object attributes include:
    - The printer's UNC path
    - Printer model and capabilities

John Matranga
jmatranga@omicron.com

Omicron Consulting
1500 Market Street
Philadelphia, PA 19102

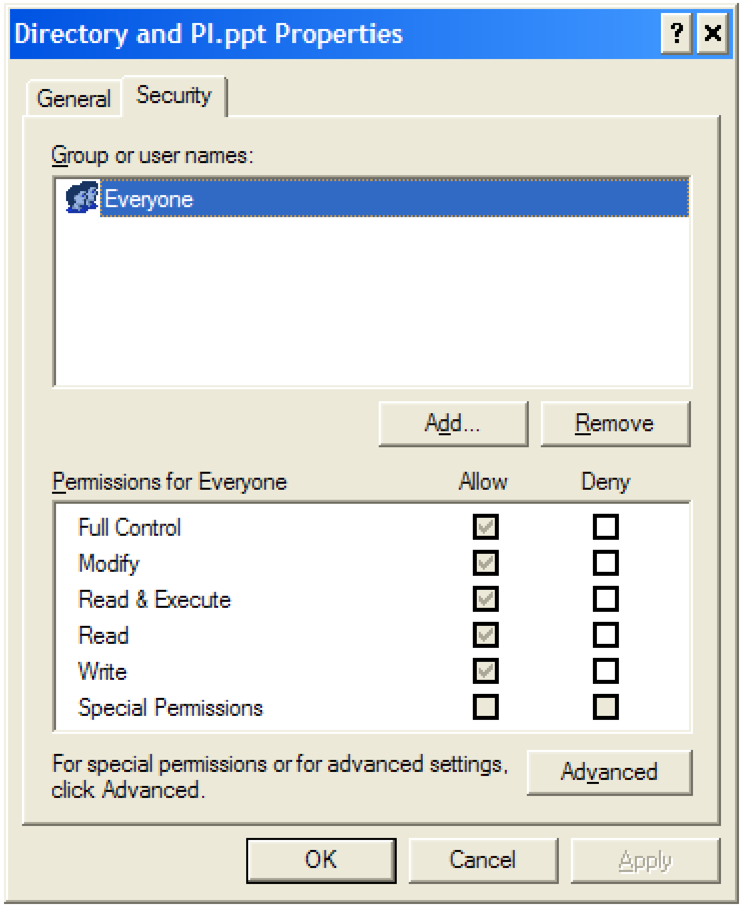
Object Access



Sales Managers

read access

- Access to directory objects is controlled via Access Control Lists (ACLs)
- Why is this important?



Group or user names:

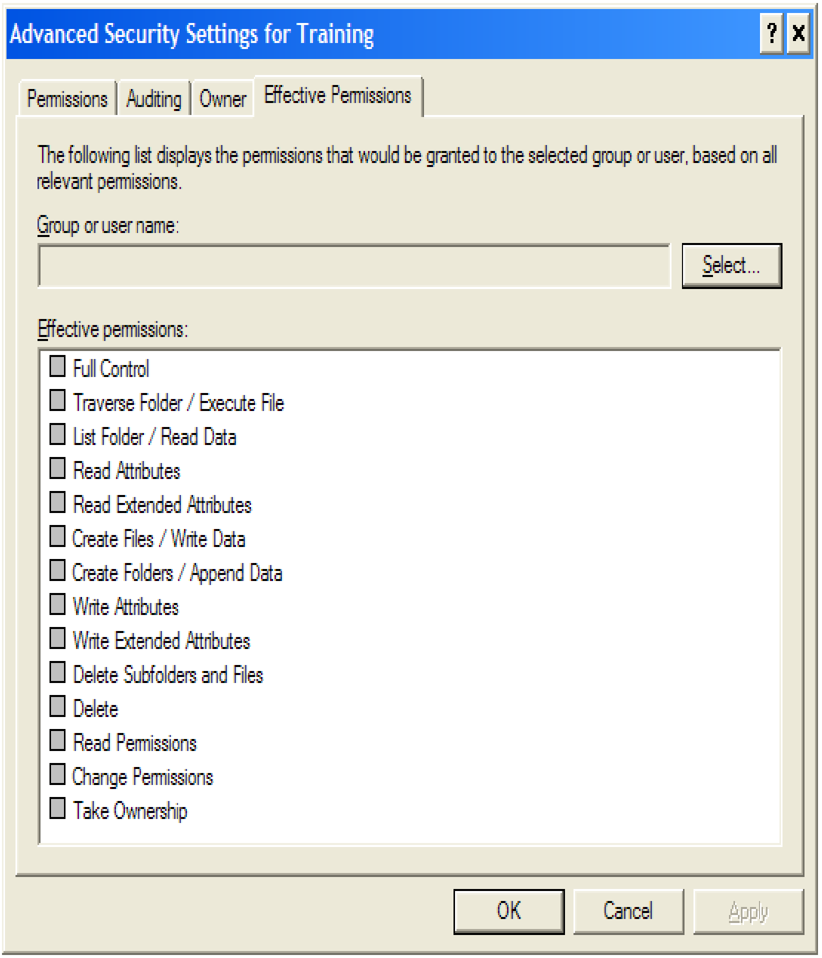
Everyone

Permissions for Everyone	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

ACLs

- Access Control Lists
  - Access – What can be done?
  - Control – Who can do it?
  - Lists – One to many
- Role Based or User Based
  - Any number of Groups
    - Groups, Groups of what?
      - Roles, Users, Points,Etc.
- Central Management
- Standard Management
- SO?
  - Gets OSIsoft 'out of the business'



Advanced Security Settings for Training

The following list displays the permissions that would be granted to the selected group or user, based on all relevant permissions.

Group or user name:

Effective permissions:

□ Full Control
□ Traverse Folder / Execute File
□ List Folder / Read Data
□ Read Attributes
□ Read Extended Attributes
□ Create Files / Write Data
□ Create Folders / Append Data
□ Write Attributes
□ Write Extended Attributes
□ Delete Subfolders and Files
□ Delete
□ Read Permissions
□ Change Permissions
□ Take Ownership

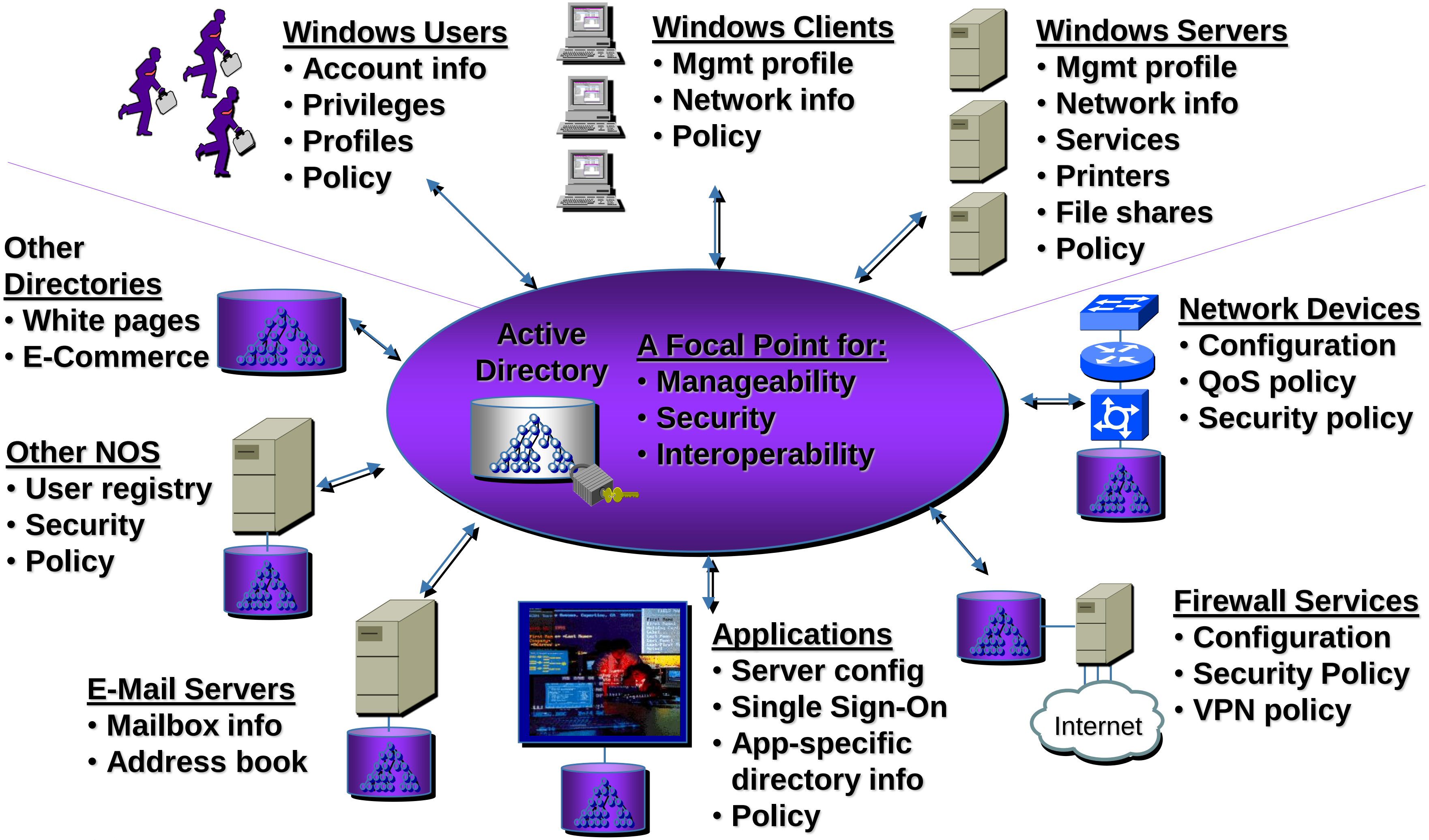
Example Object Classes

- User
  - Given-Name, Address, Picture …
- Print-Queue
  - Print-Language, Print-Status …
- Computer
  - Operating-System …
- Organizational-Unit
  - Organizational-Unit-Name …
- Forward Looking OSIsoft
  - Points, Point Classes, Digital States, Calculations, etc.

What is Active Directory?

- *Microsoft's Network Resource Platform*
- *Active Directory is an integral part of Windows 2000 Server that delivers essential network operating system services:*
  - **Focal point for management of network elements (users, applications, devices, etc.)**
  - **Trusted repository of security data for authentication and authorization**
  - **Open platform for application development and integration with other systems**

Windows 2000 Active Directory



Windows Users
- Account info
- Privileges
- Profiles
- Policy

Windows Clients
- Mgmt profile
- Network info
- Policy

Windows Servers
- Mgmt profile
- Network info
- Services
- Printers
- File shares
- Policy

Other Directories
- White pages
- E-Commerce

Active Directory

A Focal Point for:
- Manageability
- Security
- Interoperability

Network Devices
- Configuration
- QoS policy
- Security policy

Other NOS
- User registry
- Security
- Policy

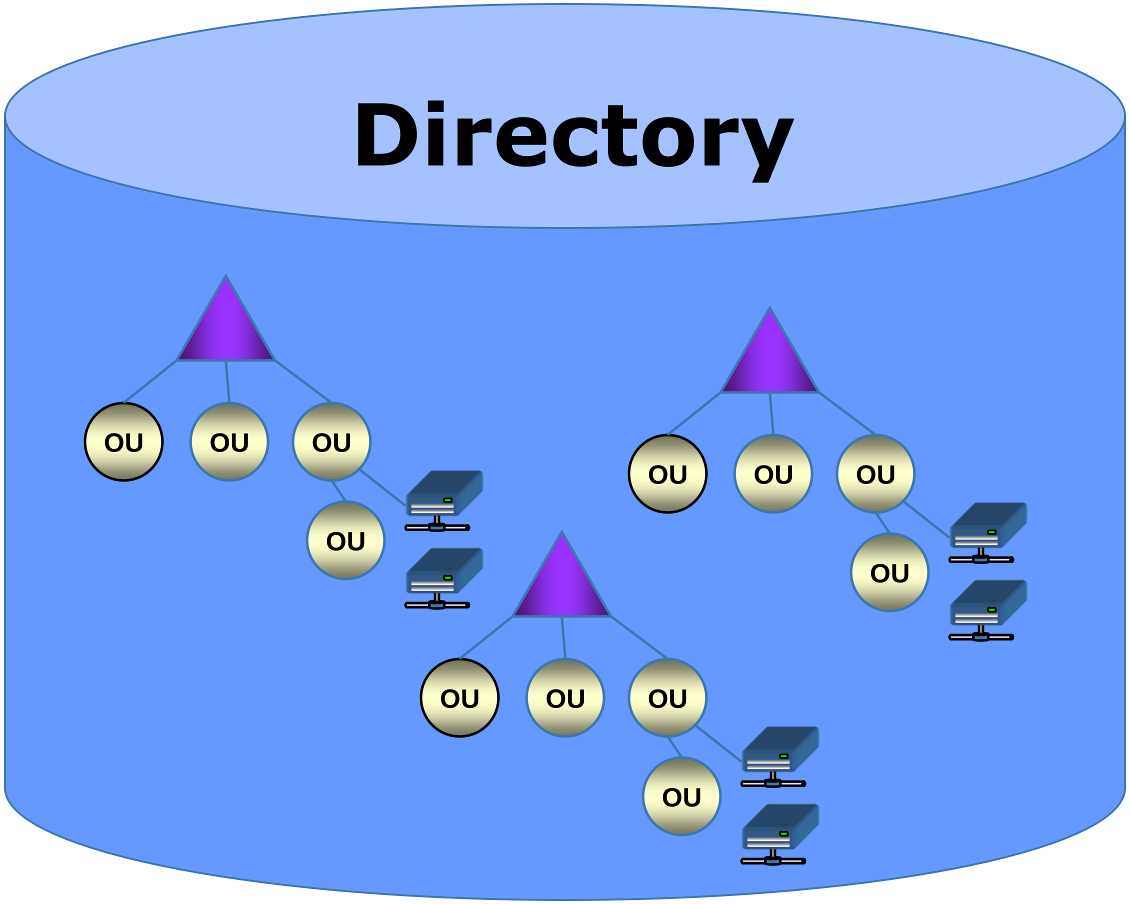
E-Mail Servers
- Mailbox info
- Address book

Applications
- Server config
- Single Sign-On
- App-specific directory info
- Policy

Firewall Services
- Configuration
- Security Policy
- VPN policy

Active Directory provides a focal point for management, security and interoperability

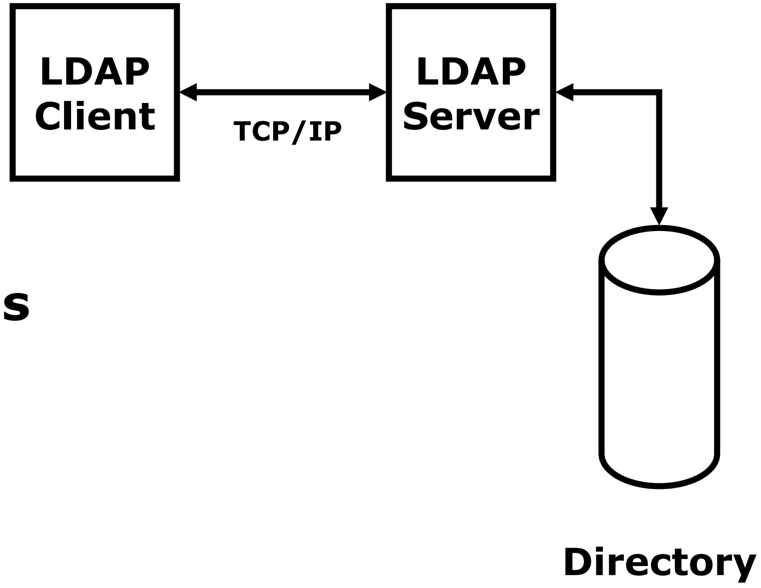
So Now We Have A Directory



- **Now what?**

Directory Access - LDAP

- Open Standard, Originally Defacto by Major Network Players
  - Came From X.500:
    - 1990 - CCITT
    - ISO 9594, Data Communications Network Directory, Recommendations X.500-X.521
    - DAP, then add "L"
- Lightweight Directory Access Protocol



LDAP ‘Models’

- Information
  - Describes the structure of information stored in an LDAP directory.
- Naming
  - Describes how information in an LDAP directory is organized and identified.
- Functional
  - Describes what operations can be performed on the information stored in an LDAP directory.
- Security
  - Describes how the information in an LDAP directory can be protected from unauthorized access.

PI Security Document

1. Overview
2. Computer System Security
   - 2.1 Physical Security
   - 2.2 File System
   - 2.3 Auditing
   - 2.4 User Database
3. PI Server Security
   - 3.1 Concepts
   - 3.2 Firewall Table
   - 3.3 Trust Table
   - 3.4 Users and Groups
   - 3.5 Backing Up the PI Server
4. Procedures
   - 4.1 Enabling Auditing
   - 4.2 Configuring the Windows Event Log
   - 4.3 Establishing Minimum Audit Settings
   - 4.4 Secure Boot Settings
   - 4.5 Password Management
   - 4.6 Requiring Login for Piconfig at the Console
   - 4.7 Disabling the PI Default User
   - 4.8 Users and Groups

http://support.osisoft.com/PIServer/WhitePapers/PI Security Best Practices.doc

RtPortal and Directories

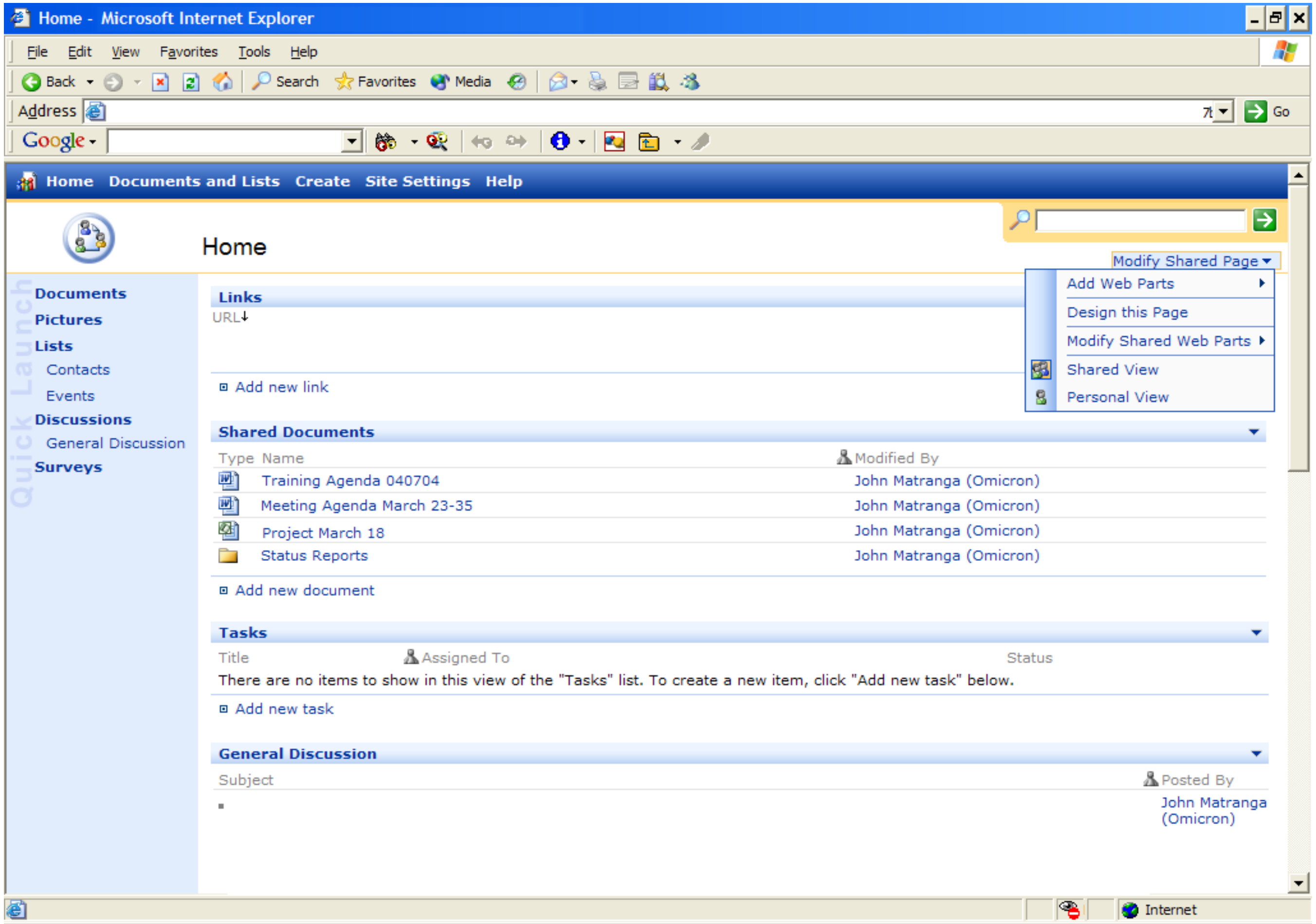
OMICRON
imagine. develop. evolve.

Omicron Consulting
1500 Market Street
Philadelphia, PA 19102

Overview

- RtWebParts Is Built Upon
  - Windows SharePoint Services
    - Windows Server 2003
    - IIS
- RtWebParts Fits In
  - Office SharePoint Portal Server 2003
    - Windows Server 2003
    - IIS
- Windows Server 2003
  - File Access
  - User Authorization For Files & Resources
- IIS
  - Basic Authentication Over HTTPS
  - Windows Authentication – Internal
- AD for Roles etc
- SPS Details
  - AD Tree Import and Synchronization tree
  - Rules For Targeting

SPS Overview


Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Google
Home Documents and Lists Create Site Settings Help
Modify Shared Page
Add Web Parts
Design this Page
Modify Shared Web Parts
Shared View
Personal View
Quick Launch
Internet

Home

Documents
Pictures
Lists
Contacts
Events
Discussions
General Discussion
Surveys

Links

URL

Add new link

Shared Documents

Type	Name	Modified By
	Training Agenda 040704	John Matranga (Omicron)
	Meeting Agenda March 23-35	John Matranga (Omicron)
	Project March 18	John Matranga (Omicron)
	Status Reports	John Matranga (Omicron)

Add new document

Tasks

Title	Assigned To	Status

There are no items to show in this view of the "Tasks" list. To create a new item, click "Add new task" below.

Add new task

General Discussion

Subject	Posted By
▪	John Matranga (Omicron)

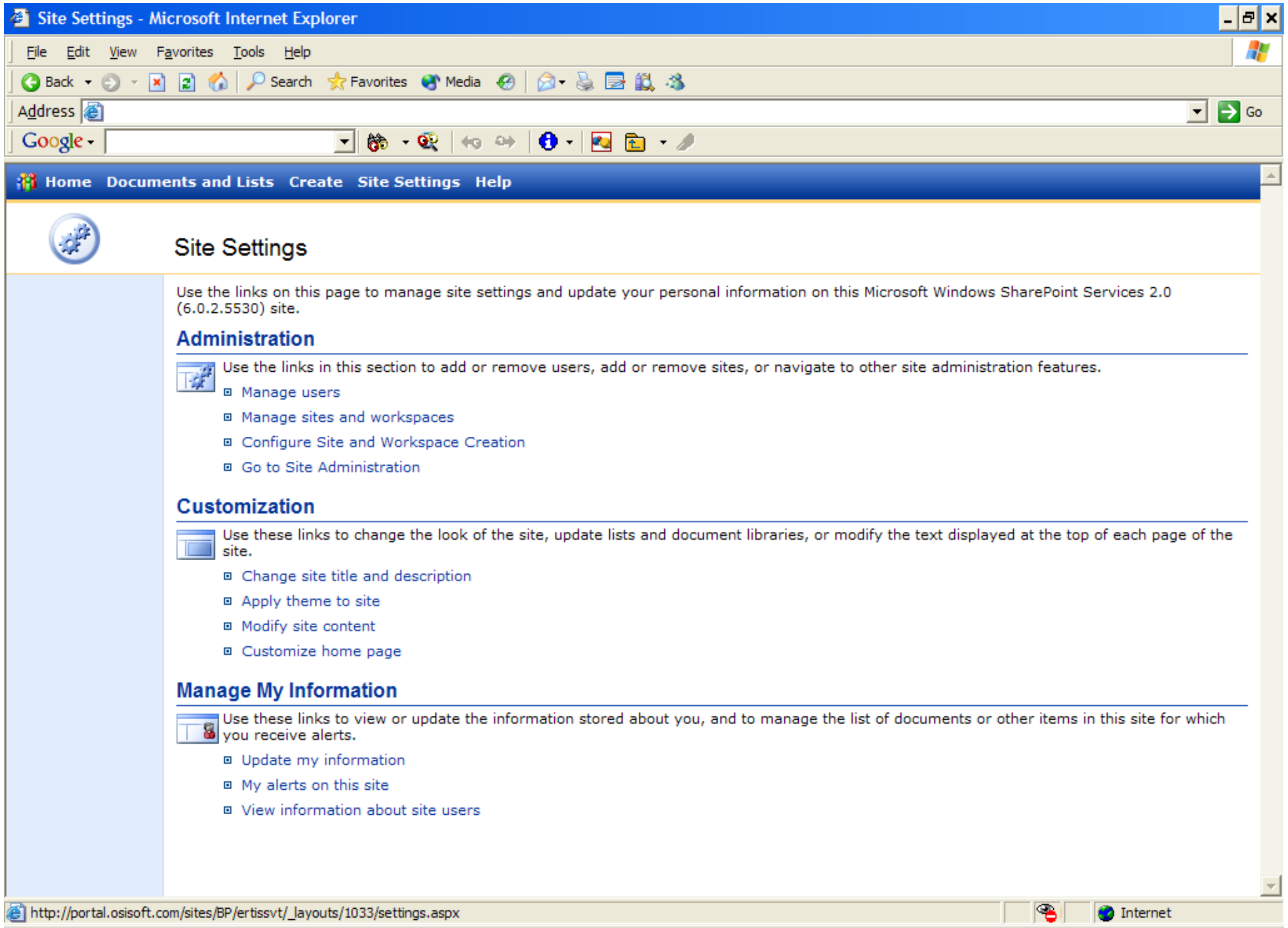
- **User or Role Based**
- **Today**
  - **File Dirs**
  - **Files**
- **Portal**
  - **Sites/ Areas**
  - **Pages**
- **Rights To Change Page**
  - **Design**
  - **Modify**
  - **Public View**
  - **Personal View**

OMICRON
imagine. develop. evolve.

John Matranga
jmatranga@omicron.com

Omicron Consulting
1500 Market Street
Philadelphia, PA 19102

SPS Site Settings


Site Settings - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Google
Home Documents and Lists Create Site Settings Help
http://portal.osisoft.com/sites/BP/ertissvt/_layouts/1033/settings.aspx
Internet

Site Settings

Use the links on this page to manage site settings and update your personal information on this Microsoft Windows SharePoint Services 2.0 (6.0.2.5530) site.

Administration

Use the links in this section to add or remove users, add or remove sites, or navigate to other site administration features.

- Manage users
- Manage sites and workspaces
- Configure Site and Workspace Creation
- Go to Site Administration

Customization

Use these links to change the look of the site, update lists and document libraries, or modify the text displayed at the top of each page of the site.

- Change site title and description
- Apply theme to site
- Modify site content
- Customize home page

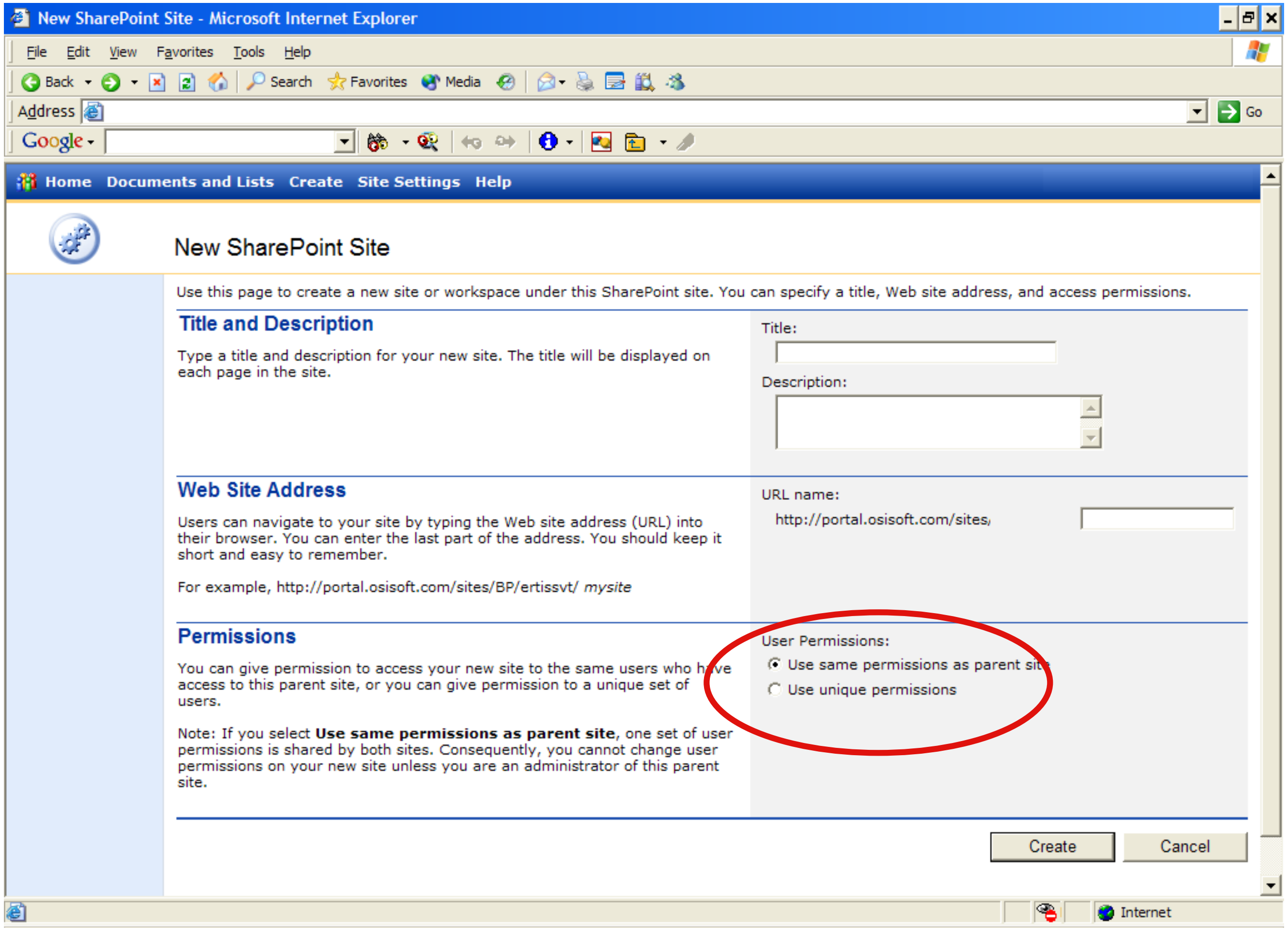
Manage My Information

Use these links to view or update the information stored about you, and to manage the list of documents or other items in this site for which you receive alerts.

- Update my information
- My alerts on this site
- View information about site users

- **Users and ACL Rights**
- **Same As For Files**

New Site


New SharePoint Site - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Google
Home Documents and Lists Create Site Settings Help
Internet

New SharePoint Site

Use this page to create a new site or workspace under this SharePoint site. You can specify a title, Web site address, and access permissions.

Title and Description

Type a title and description for your new site. The title will be displayed on each page in the site.

Title:

Description:

Web Site Address

Users can navigate to your site by typing the Web site address (URL) into their browser. You can enter the last part of the address. You should keep it short and easy to remember.

For example, http://portal.osisoft.com/sites/BP/ertissvt/ *mysite*

URL name:

http://portal.osisoft.com/sites/

Permissions

You can give permission to access your new site to the same users who have access to this parent site, or you can give permission to a unique set of users.

Note: If you select **Use same permissions as parent site**, one set of user permissions is shared by both sites. Consequently, you cannot change user permissions on your new site unless you are an administrator of this parent site.

User Permissions:

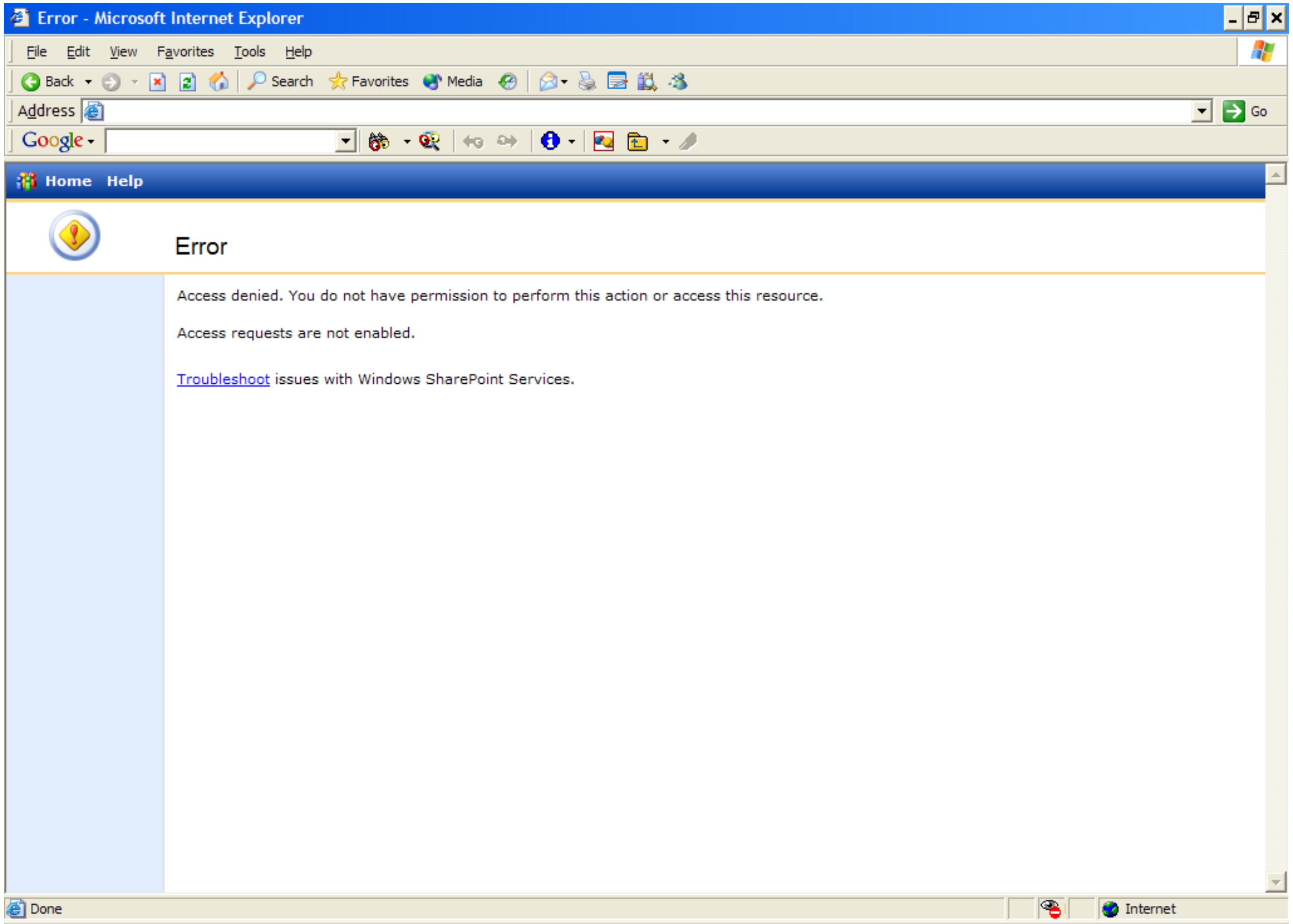
● Use same permissions as parent site
○ Use unique permissions

Create Cancel

John Matranga
jmatranga@omicron.com

Omicron Consulting
1500 Market Street
Philadelphia, PA 19102

Security On The Security


Error - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Google
Home Help
Done
Internet

Error

Access denied. You do not have permission to perform this action or access this resource.

Access requests are not enabled.

Troubleshoot issues with Windows SharePoint Services.

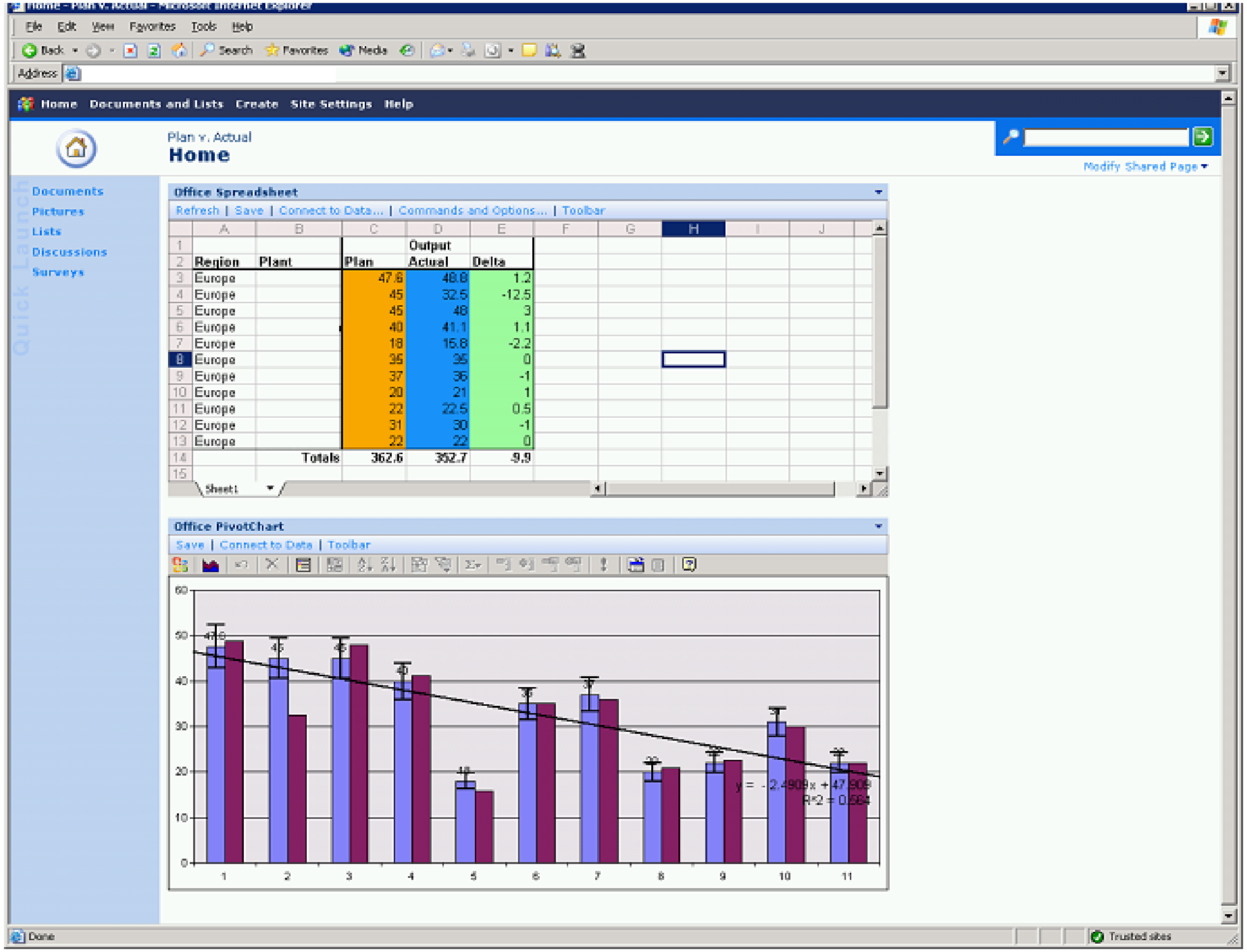
- **As One Would Expect**

OMICRON imagine. develop. evolve.

John Matranga
jmatranga@omicron.com

Omicron Consulting
1500 Market Street
Philadelphia, PA 19102

Excel Integration


Home - Plan v. Actual - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Home Documents and Lists Create Site Settings Help
Plan v. Actual
Home
Modify Shared Page
Quick Launch
Documents
Pictures
Lists
Discussions
Surveys
Office Spreadsheet
Refresh | Save | Connect to Data... | Commands and Options... | Toolbar
Sheet1
Office PivotChart
Save | Connect to Data | Toolbar
60
50
40
30
20
10
0
1
2
3
4
5
6
7
8
9
10
11
47.6
45
45
40
18
35
37
20
22
31
22
y = -2.4909x + 47.909
R^2 = 0.564
Done
Trusted sites

	A	B	C	D	E
1				Output	
2	Region	Plant	Plan	Actual	Delta
3	Europe		47.6	48.8	1.2
4	Europe		45	32.5	-12.5
5	Europe		45	48	3
6	Europe		40	41.1	1.1
7	Europe		18	15.8	-2.2
8	Europe		35	35	0
9	Europe		37	36	-1
10	Europe		20	21	1
11	Europe		22	22.5	0.5
12	Europe		31	30	-1
13	Europe		22	22	0
14		Totals	362.6	352.7	-9.9
15					

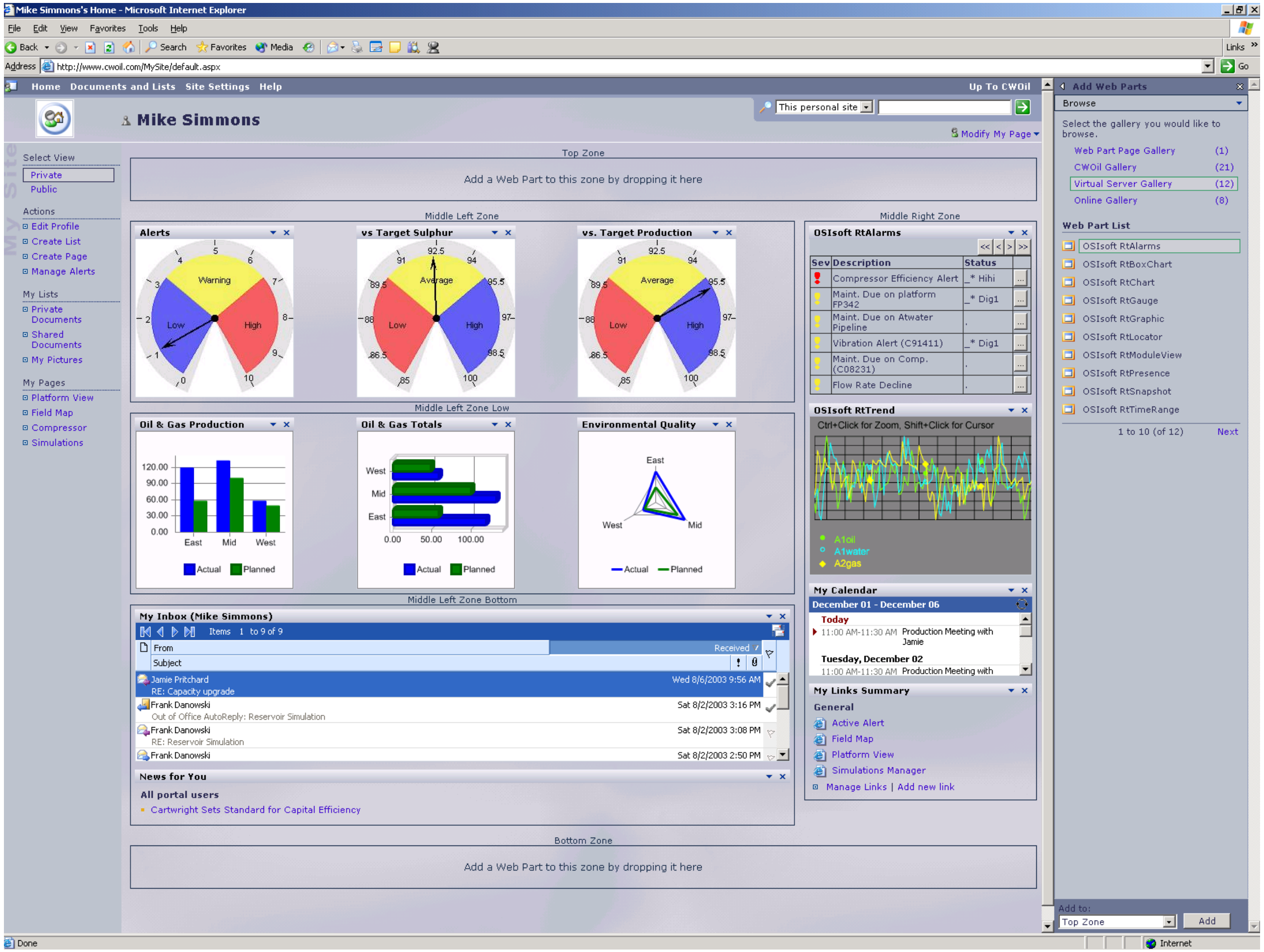
- **Embed Actual Excel Spreadsheets Into The Portal**
- **Have Excel Drive Other Items On The Page (Trend Below)**
- **Allows For Direct, Secure Editing Of Spreadsheet (With Rights)**
- **Can Be Used For What-if An Analysis**

OMICRON
imagine. develop. evolve.

John Matranga
jmatranga@omicron.com

Omicron Consulting
1500 Market Street
Philadelphia, PA 19102

Sample Portal Page



Add a Web Part to this zone by dropping it here

Sev	Description	Status
!	Compressor Efficiency Alert	_* Hihi
!	Maint. Due on platform FP342	_* Dig1
!	Maint. Due on Atwater Pipeline	.
!	Vibration Alert (C91411)	_* Dig1
!	Maint. Due on Comp. (C08231)	.
!	Flow Rate Decline	.

Ctrl+Click for Zoom, Shift+Click for Cursor

Today

11:00 AM-11:30 AM Production Meeting with Jamie

Tuesday, December 02

11:00 AM-11:30 AM Production Meeting with

My Inbox (Mike Simmons)

Items 1 to 9 of 9

From / Subject	Received
Jamie Pritchard RE: Capacity upgrade	Wed 8/6/2003 9:56 AM
Frank Danowski Out of Office AutoReply: Reservoir Simulation	Sat 8/2/2003 3:16 PM
Frank Danowski RE: Reservoir Simulation	Sat 8/2/2003 3:08 PM
Frank Danowski	Sat 8/2/2003 2:50 PM

Add a Web Part to this zone by dropping it here

Select the gallery you would like to browse.

Gallery	
Web Part Page Gallery	(1)
CWOil Gallery	(21)
Virtual Server Gallery	(12)
Online Gallery	(8)

- OSIsoft RtAlarms
- OSIsoft RtBoxChart
- OSIsoft RtChart
- OSIsoft RtGauge
- OSIsoft RtGraphic
- OSIsoft RtLocator
- OSIsoft RtModuleView
- OSIsoft RtPresence
- OSIsoft RtSnapshot
- OSIsoft RtTimeRange

1 to 10 (of 12)

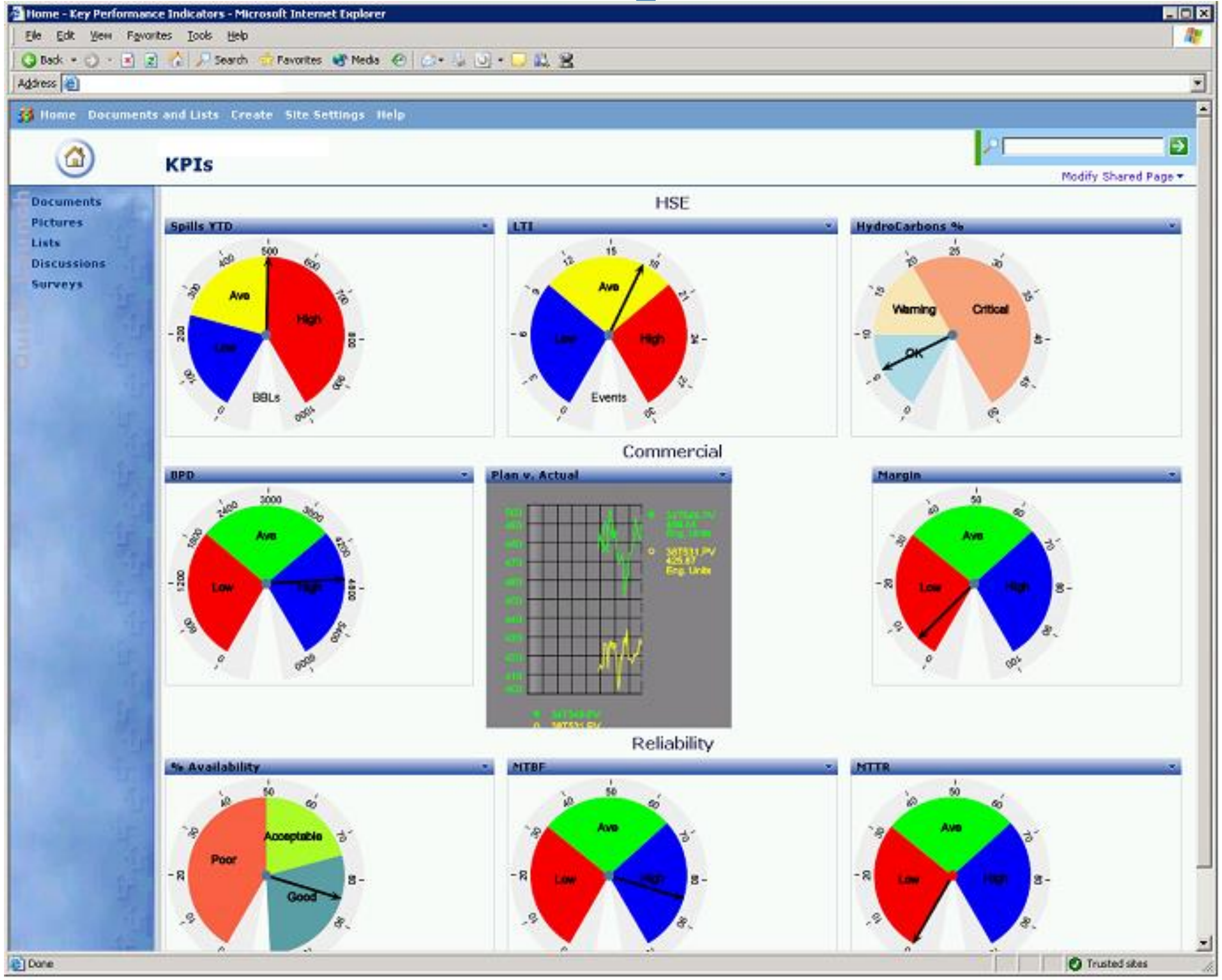
- **Personalized Page Access**
- **Resource Access**
- **PI Data Access**

OMICRON
imagine. develop. evolve.

John Matranga
jmatranga@omicron.com

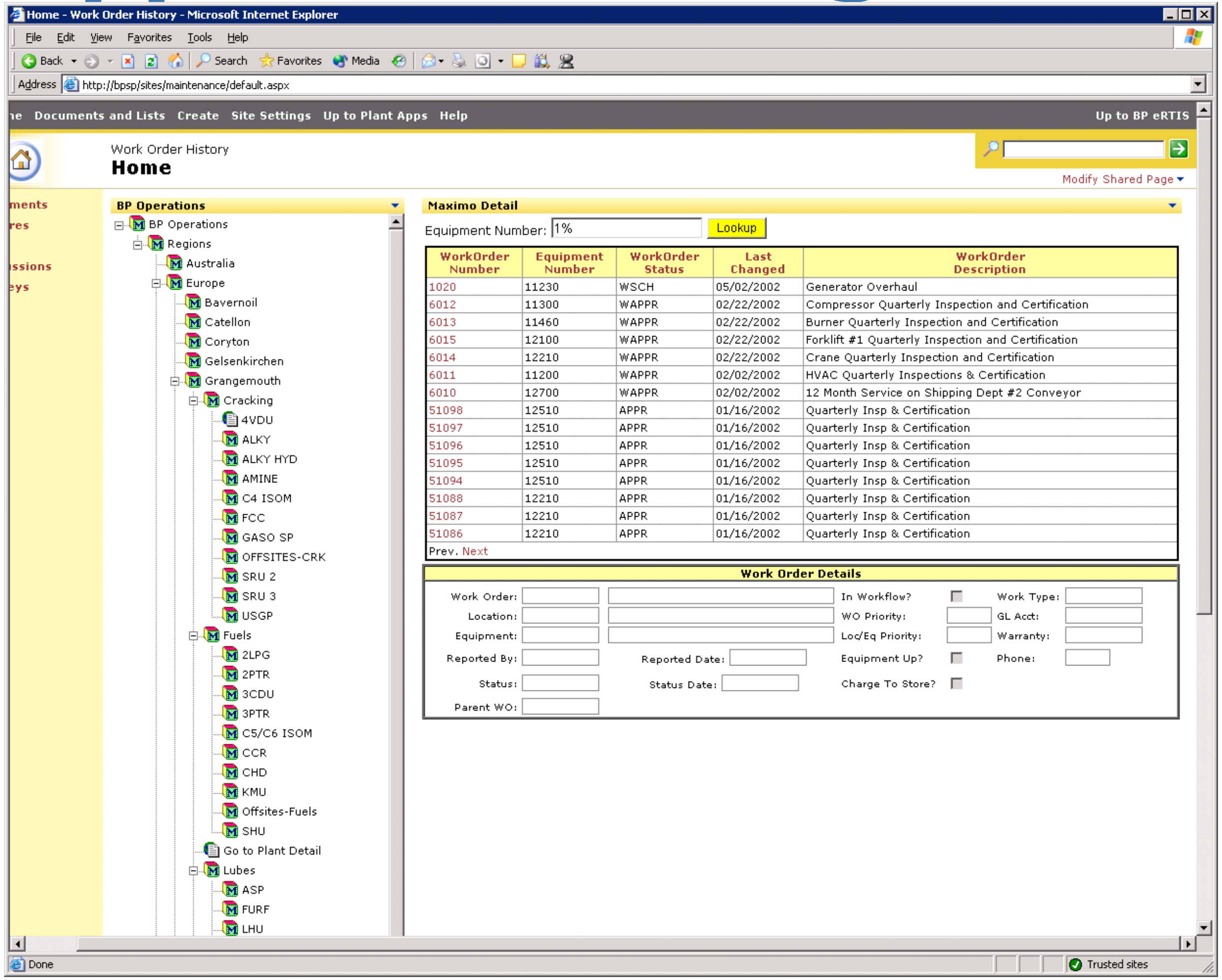
Omicron Consulting
1500 Market Street
Philadelphia, PA 19102

KPI Example



- Parts Can Be Driven From PI, Relational, Web Services Sources Of Data
- Can Keep User "ID" OR Share

Application Integration Example



Maximo Detail

Equipment Number: 1% Lookup

WorkOrder Number	Equipment Number	WorkOrder Status	Last Changed	WorkOrder Description
1020	11230	WSCH	05/02/2002	Generator Overhaul
6012	11300	WAPPR	02/22/2002	Compressor Quarterly Inspection and Certification
6013	11460	WAPPR	02/22/2002	Burner Quarterly Inspection and Certification
6015	12100	WAPPR	02/22/2002	Forklift #1 Quarterly Inspection and Certification
6014	12210	WAPPR	02/22/2002	Crane Quarterly Inspection and Certification
6011	11200	WAPPR	02/02/2002	HVAC Quarterly Inspections & Certification
6010	12700	WAPPR	02/02/2002	12 Month Service on Shipping Dept #2 Conveyor
51098	12510	APPR	01/16/2002	Quarterly Insp & Certification
51097	12510	APPR	01/16/2002	Quarterly Insp & Certification
51096	12510	APPR	01/16/2002	Quarterly Insp & Certification
51095	12510	APPR	01/16/2002	Quarterly Insp & Certification
51094	12510	APPR	01/16/2002	Quarterly Insp & Certification
51088	12210	APPR	01/16/2002	Quarterly Insp & Certification
51087	12210	APPR	01/16/2002	Quarterly Insp & Certification
51086	12210	APPR	01/16/2002	Quarterly Insp & Certification

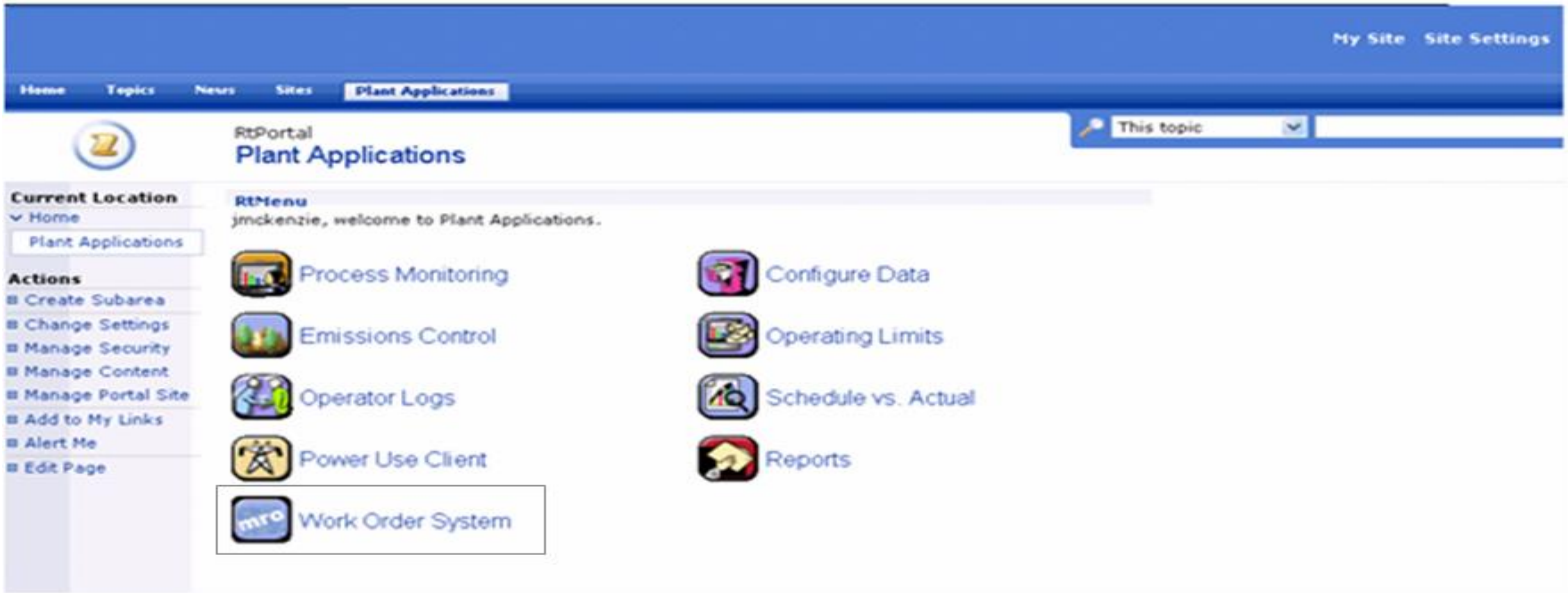
Prev. Next

Work Order Details

Work Order: In Workflow? □ Work Type:
Location: WO Priority: GL Acct:
Equipment: Loc/Eq Priority: Warranty:
Reported By: Reported Date: Equipment Up? □ Phone:
Status: Status Date: Charge To Store? □
Parent WO:

- **Data Access (User Context)**
- **Custom WebParts Can Be Driven From The Portal**

Applications Page



My Site Site Settings

Home Topics News Sites Plant Applications

RtPortal

Plant Applications

This topic

Current Location

Home

Plant Applications

Actions

- Create Subarea
- Change Settings
- Manage Security
- Manage Content
- Manage Portal Site
- Add to My Links
- Alert Me
- Edit Page

RtMenu

jmckenzie, welcome to Plant Applications.

- Integrated Security To THE Network Directory
- Plant Applications Menu – See What You Get
- Role Based Application Access
- ADAM
- No Need For Extra Administration

Questions and Information

- John Matranga
  - CTO Omicron Consulting
  - 215-854-3485
  - jmatranga@omicron.com
- Other References
  - PI Security Whitepaper
    - http://support.osisoft.com/PIServer/WhitePapers/PI Security Best Practices.doc
  - Microsoft
    - http://www.microsoft.com/AD
  - LDAP (Open Standard, IBM Site for Good Overview)
    - http://www.redbooks.ibm.com/redbooks/SG244986.html
  - SharePoint
    - SharePoint Portal Server Administrator's Guide (Online)