VOYAGE2007

MONTEREY
OSISOFT USER CONFERENCE 2007
CALIFORNIA

PI Server Security Best Practice Guide

Bryan Owen
Cyber Security Manager
OSIsoft

OSIsoft

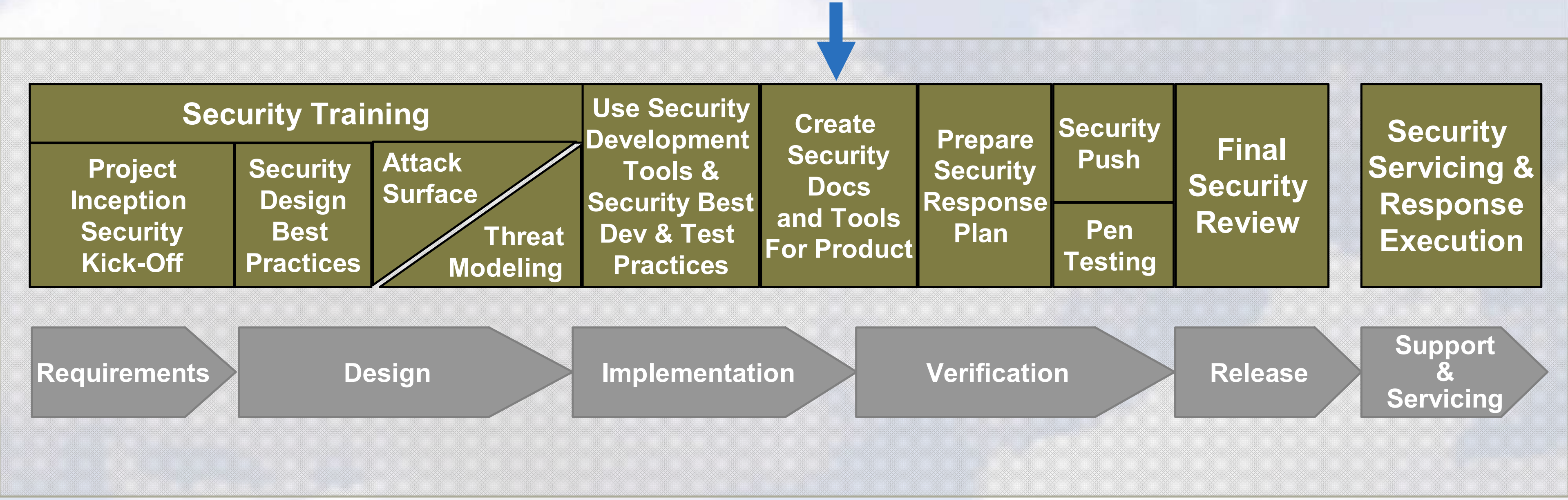
VALUE NOW, VALUE OVER TIME

Agenda

- Security Development Lifecycle Initiative
- Using PI to Protect Critical Infrastructure
- Hardening Advice for the PI System
- Tools: Security Configuration Wizard
- Security Work In Progress

What is the Security Development Lifecycle?

“A Process for Developing Demonstrably More Secure Software”



Security Training

Project Inception Security Kick-Off

Security Design Best Practices

Attack Surface

Threat Modeling

Use Security Development Tools & Security Best Dev & Test Practices

Create Security Docs and Tools For Product

Prepare Security Response Plan

Security Push

Pen Testing

Final Security Review

Security Servicing & Response Execution

Requirements

Design

Implementation

Verification

Release

Support & Servicing

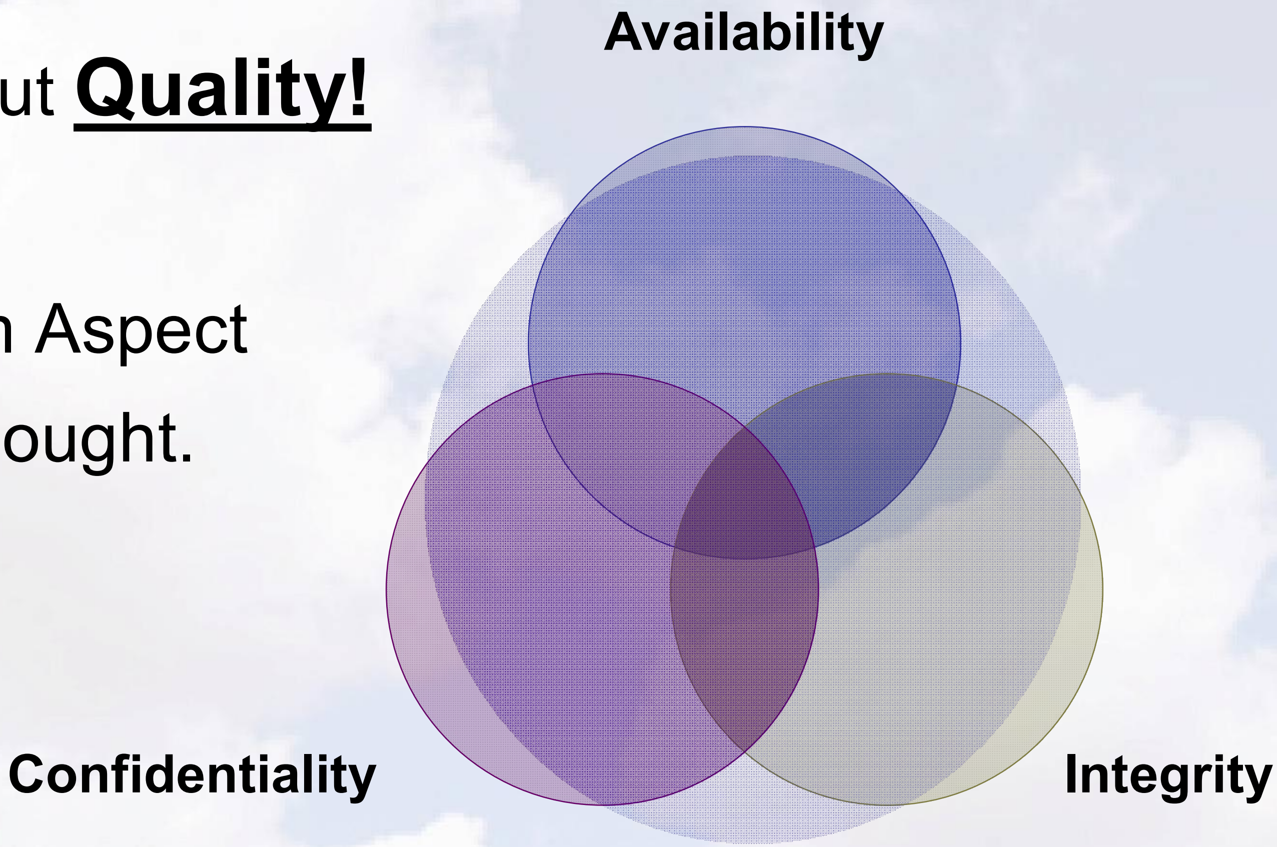
Microsoft Press Best Practice Series:
“The Security Development Lifecycle” by Michael Howard and Steve Lipner

The C.I.A. Security Model for PI

- It’s really about **Quality!**

- Core Platform Aspect

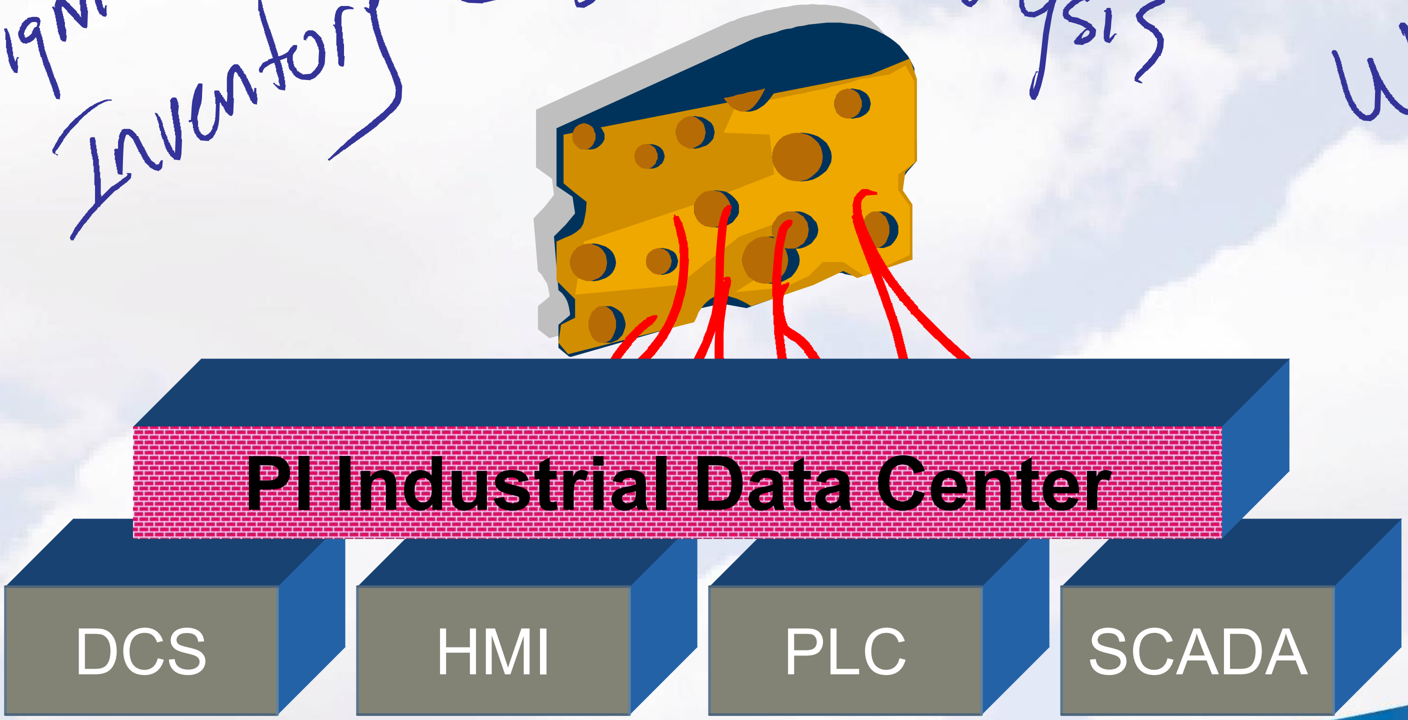
...not an after thought.



Using PI for
Critical Infrastructure Protection

$ Scheduling Optimization Orders www

Six Sigma JIT Inventory CBM Analysis MES Wifi



PI Industrial Data Center

DCS

HMI

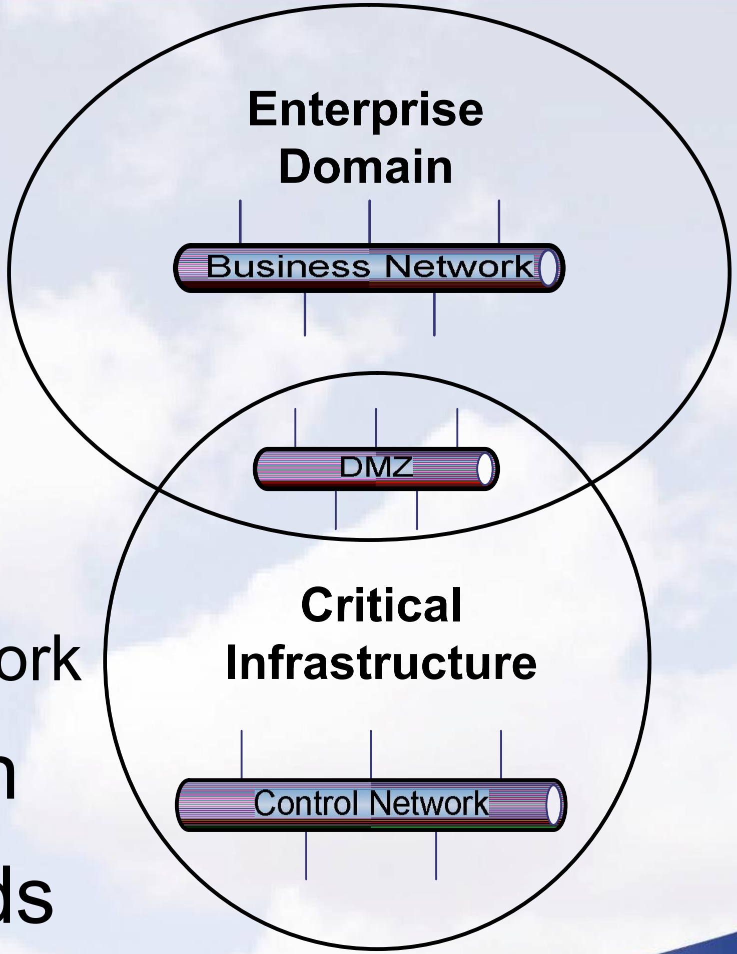
PLC

SCADA

OSIsoft®

PI Industrial Data Center

- Defense in Depth
- Reduce Surface Area
- Network DMZ Concept
  - ALL Terminations in DMZ
  - Boundary Security
  - Allow PI Data from Control Network
- IT Monitoring and Notification
- Aligns with Industry Standards

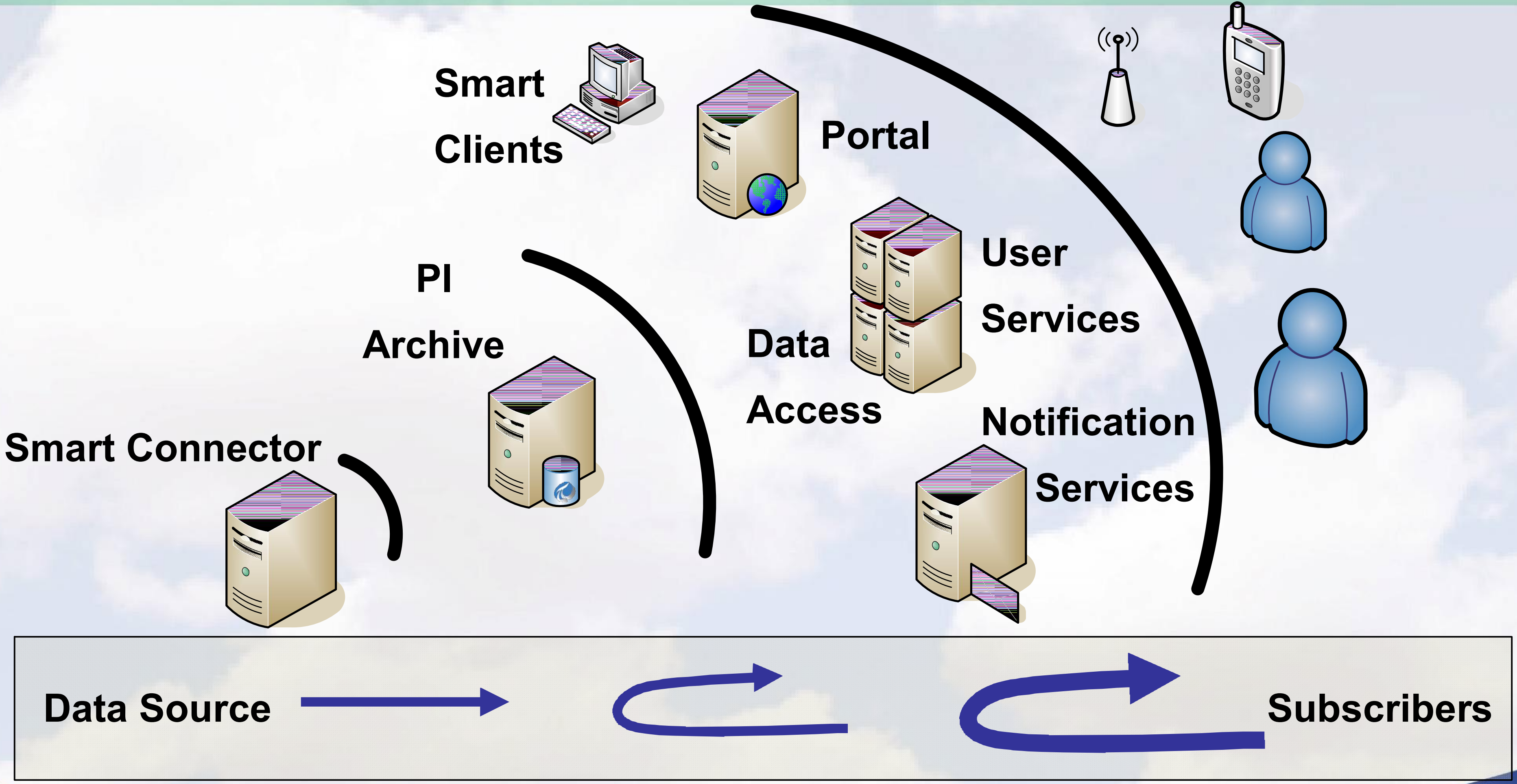


OSIsoft

How to Protect PI ...Same Principles!

- Adopt Mid-Tier Secure Service Layer
  - Authentication by Infrastructure Provider
  - Minimize Connections to PI Server
- Distribute PI Roles for Optimum Security
  - Interface and IT Monitoring per Zone
  - Consider PI Server per Zone (Use HA Collective)
  - User Services/Data Access
  - Avoid IIS on PI Server

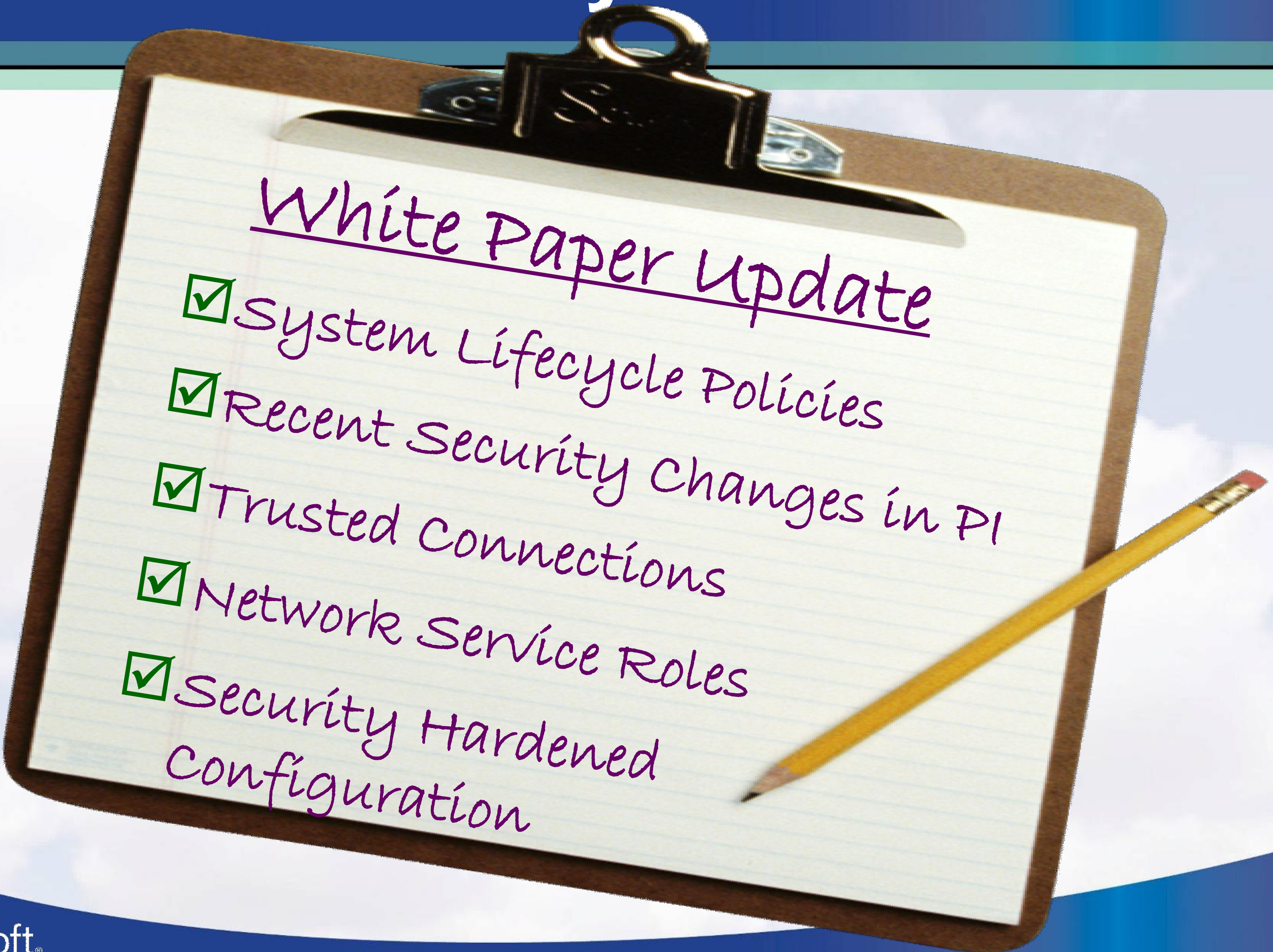
PI System Security Boundaries



OSIsoft®

VALUE NOW, VALUE OVER TIME

PI Server Security Best Practices

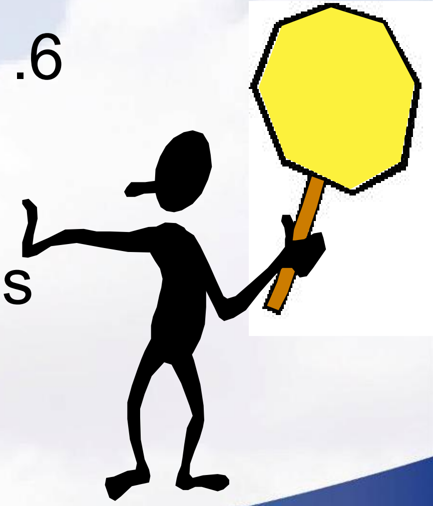


White Paper Update

- ☑ System Lifecycle Policies
- ☑ Recent Security Changes in PI
- ☑ Trusted Connections
- ☑ Network Service Roles
- ☑ Security Hardened Configuration

Infrastructure Lifecycle

- Server Platform Minimum Security Baseline
  - Windows 2003 SP1 with Firewall Enabled
  - Hardware NX Support
  - PR1 Server 3.4.375.x
    - Applications & Interfaces: SDK 1.3.5 / API 1.6
- Security for W2K / NT4 ?
  - Move Direct Client Access to Mid-Tier Services
  - External Firewall



Patch Management

- Windows Update
- PI Software Update Service
- Anti-Virus Signatures

Potential Issue: Automatic Hot Patching

- **High Availability Solution Recommended!**

Quality of Service Monitoring

- Managed PI Subsystem
  - PI Server Check Utility
- Windows Perfmon Templates
  - PI Server
  - Exchange, IIS, SQL, …
- SNMP Agent Templates
  - Network Devices
  - Unix O/S Support

PI Server Overview for server rtpmpi
SNAPSHOT
QUEUE
COMPRESS
OVERFLOWS
CACHE
PI-CLIENT APPLICATIONS
ON-LINE ARCHIVES
PI Server Health for RTPMPI
Interface Node Health for Arbiter-Node

Recent Security Changes in PI

- DBSecurity Roles
- PI Trust Attributes
  - Host name
  - Application name
- PI Module
  - Permission Inheritance
- Interfaces
  - New Buffer Subsystem
  - Disconnected Startup

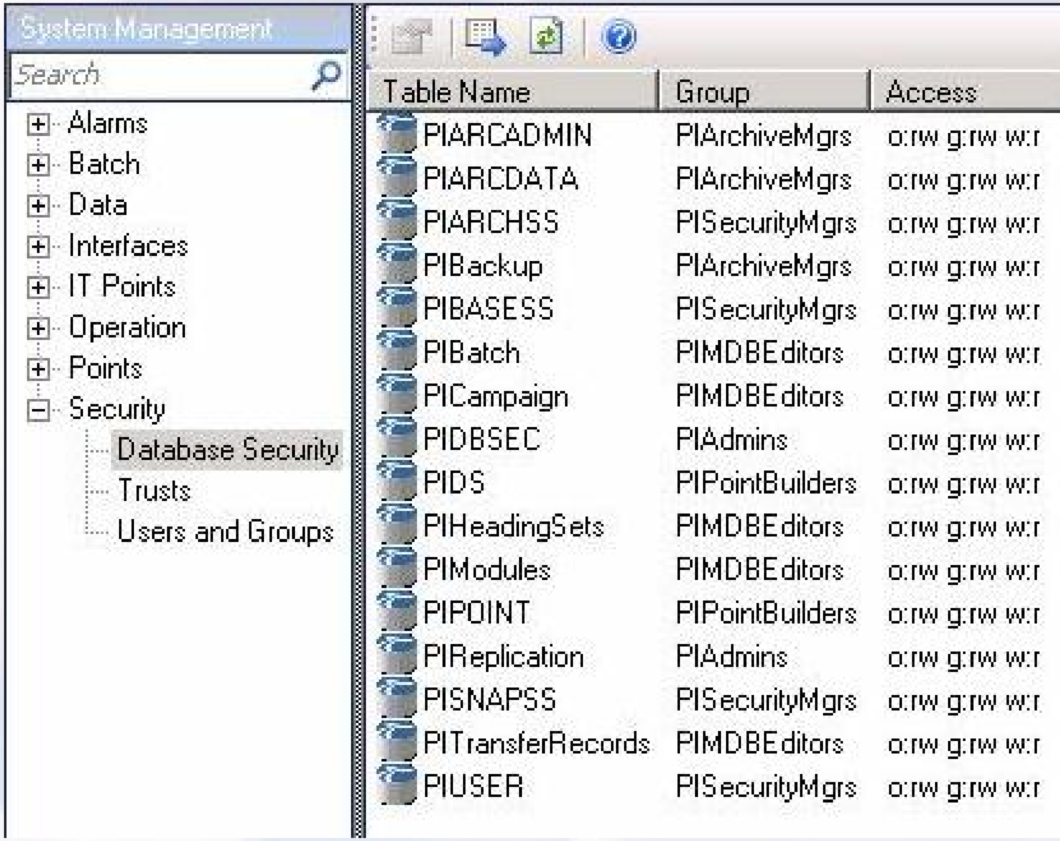
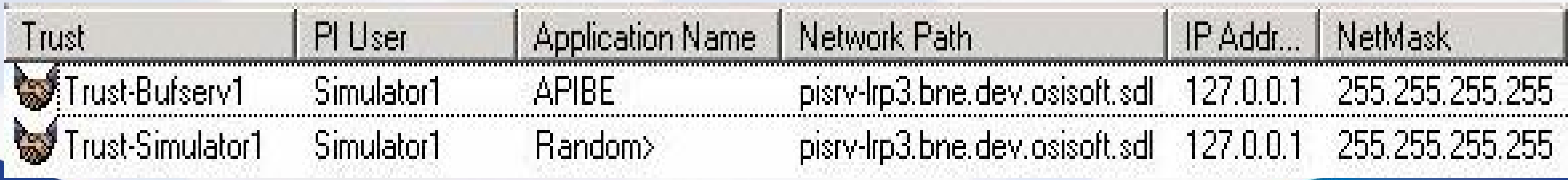


Table Name	Group	Access
PIARCADMIN	PIArchiveMgrs	o:rw g:rw w:r
PIARCDATA	PIArchiveMgrs	o:rw g:rw w:r
PIARCHSS	PISecurityMgrs	o:rw g:rw w:r
PIBackup	PIArchiveMgrs	o:rw g:rw w:r
PIBASESS	PISecurityMgrs	o:rw g:rw w:r
PIBatch	PIMDBEditors	o:rw g:rw w:r
PICampaign	PIMDBEditors	o:rw g:rw w:r
PIDBSEC	PIAdmins	o:rw g:rw w:r
PIDS	PIPointBuilders	o:rw g:rw w:r
PIHeadingSets	PIMDBEditors	o:rw g:rw w:r
PIModules	PIMDBEditors	o:rw g:rw w:r
PIPOINT	PIPointBuilders	o:rw g:rw w:r
PIReplication	PIAdmins	o:rw g:rw w:r
PISNAPSS	PISecurityMgrs	o:rw g:rw w:r
PITransferRecords	PIMDBEditors	o:rw g:rw w:r
PIUSER	PISecurityMgrs	o:rw g:rw w:r

Use Case: Interface Trust

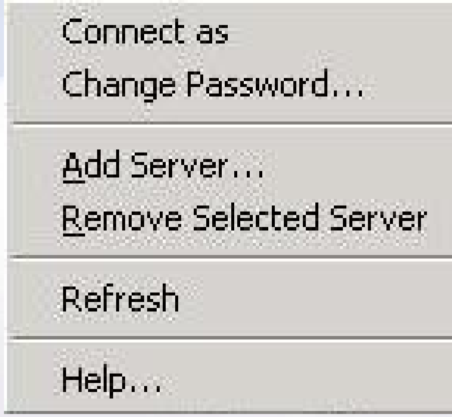
- Trust PI User is “Owner” of Points and Data
  - Change owner of root module for interface configuration
- Set Trust Entries with at Least 2 Credentials
  - a) Masked IP Address
  - b) FQDN for Network Path
  - c) Application Name
    - Specific syntax rules for PI-API applications



Trust	PI User	Application Name	Network Path	IP Addr...	NetMask
Trust-Bufserv1	Simulator1	APIBE	pisrv-lrp3.bne.dev.osisoft.sdl	127.0.0.1	255.255.255.255
Trust-Simulator1	Simulator1	Random>	pisrv-lrp3.bne.dev.osisoft.sdl	127.0.0.1	255.255.255.255

PI Trusts for Windows Users

- To Trust or Not to Trust?
  - Extra password challenge is desirable in some cases
    - Special purpose domain, Network access control
    - Use Windows “Run As” or PI-SDK “Connect As”
- Domain User Trust Guidelines
  - Map user trusts to least privilege PI accounts
  - Consider User + Application Name + Subnet
  - Reserve *“piadmin”* trust for console use



OSIsoft

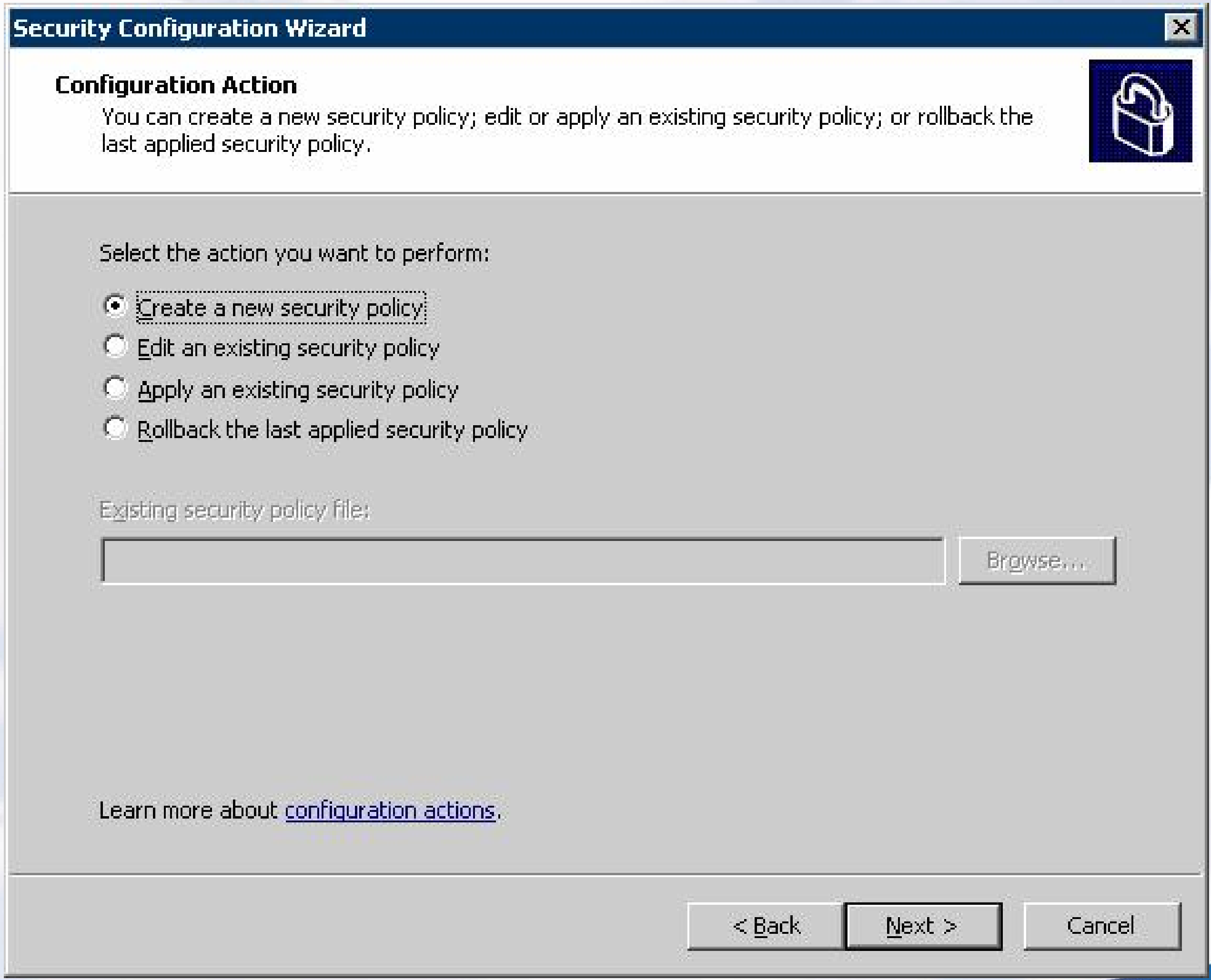
PI Network Service Roles

- PI Network Manager
- Advanced Computing Engine 2.x (Web Services)
- AF 1.x and AF 2.x
- Analysis and Notification
- OPC HDA/DA Server
- Process Template Monitor

Security Configuration Wizard

- Part of Windows 2003 SP1 and greater
  - Register PI SCW Extension
  - Set Roles and Optional Features
  - Disable Unused Services
  - Apply Best Practice Security Policy Templates
- Demo
- Verify Baseline MBSA
  - Functional Testing

Security Configuration Wizard



Security Configuration Wizard

Configuration Action

You can create a new security policy; edit or apply an existing security policy; or rollback the last applied security policy.

Select the action you want to perform:

● Create a new security policy

○ Edit an existing security policy

○ Apply an existing security policy

○ Rollback the last applied security policy

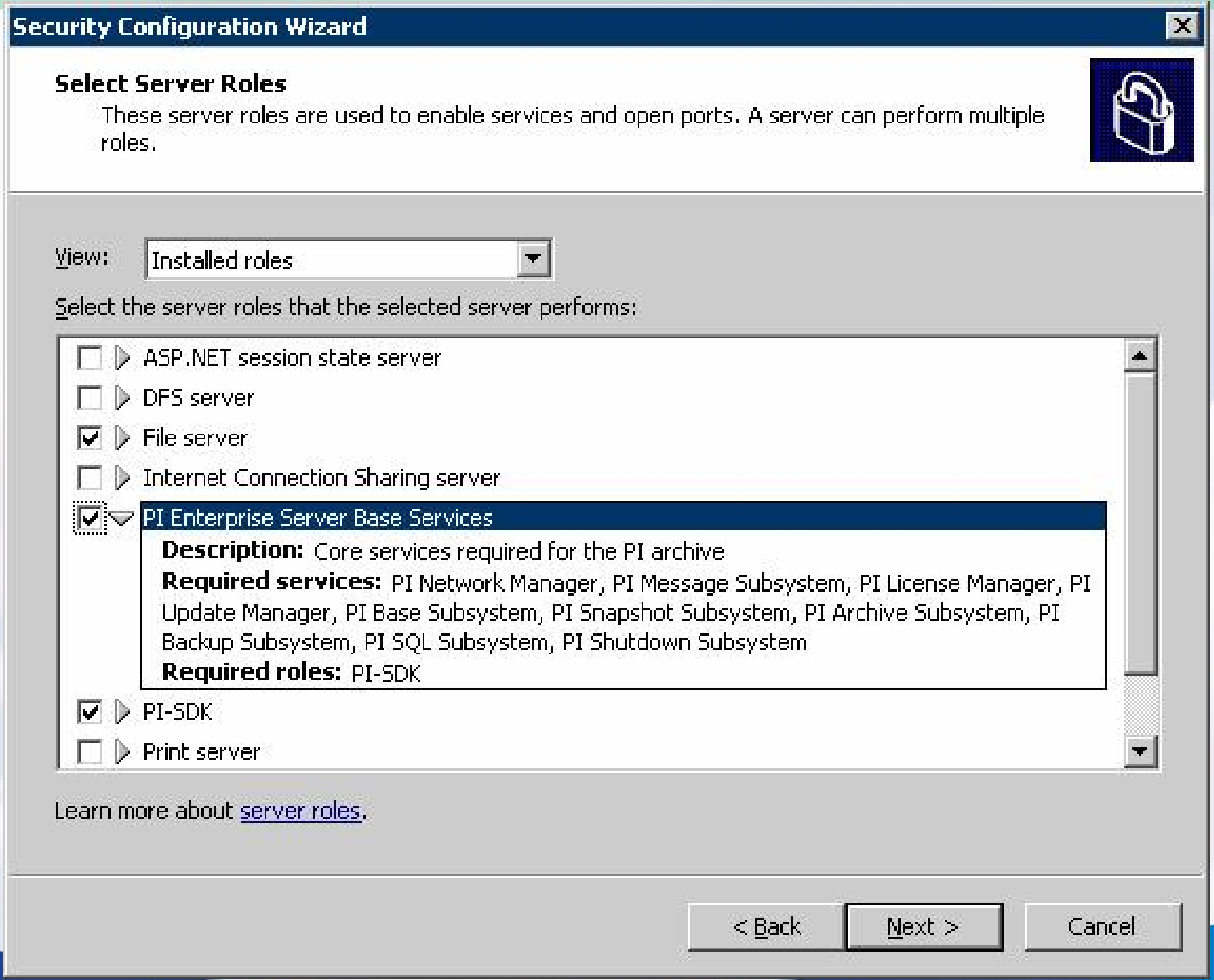
Existing security policy file:

Learn more about configuration actions.

OSIsoft®

VALUE NOW, VALUE OVER TIME

Security Configuration Wizard



Security Configuration Wizard

Select Server Roles

These server roles are used to enable services and open ports. A server can perform multiple roles.

View: Installed roles

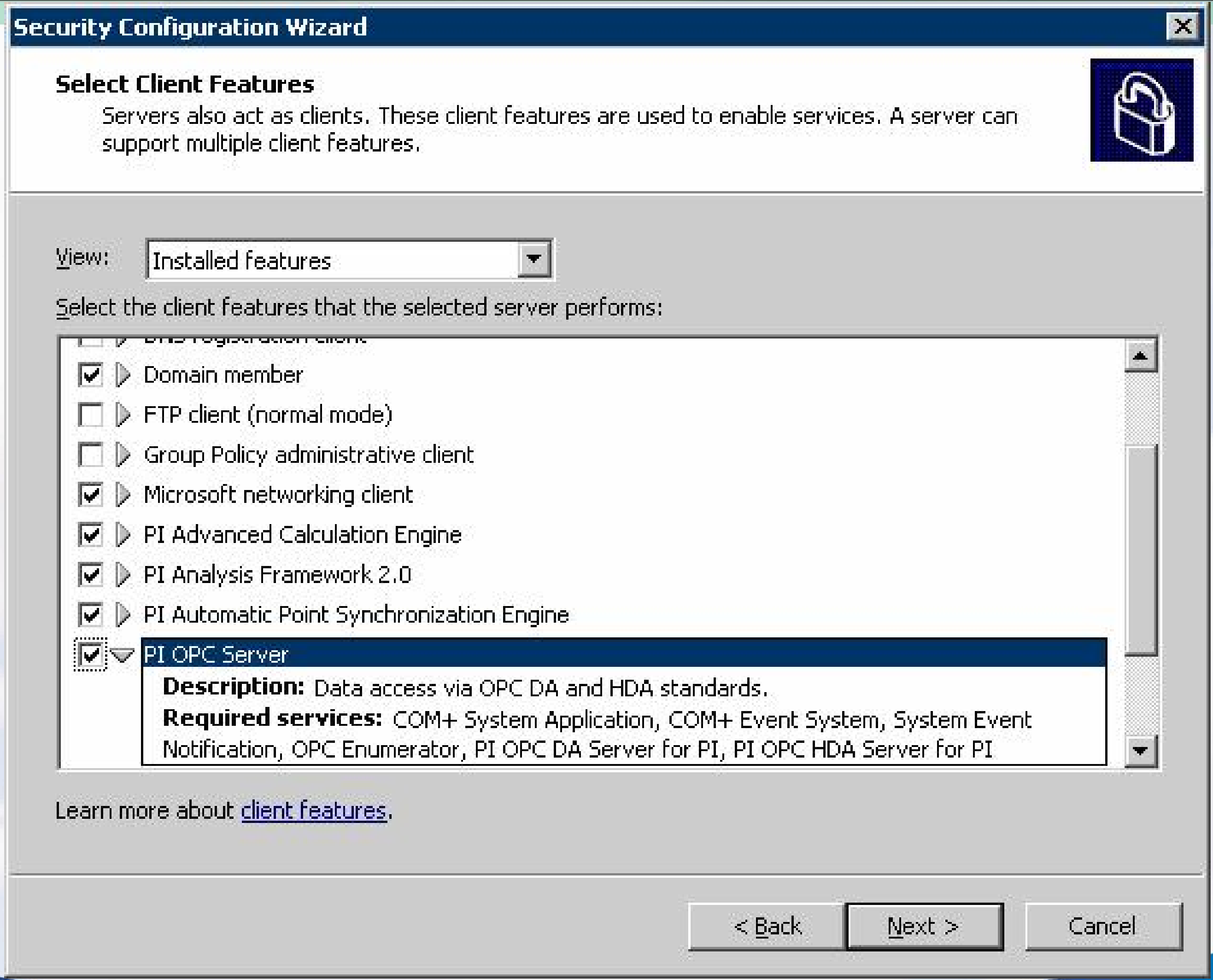
Select the server roles that the selected server performs:

- □ ASP.NET session state server
- □ DFS server
- ☑ File server
- □ Internet Connection Sharing server
- ☑ PI Enterprise Server Base Services
  - **Description:** Core services required for the PI archive
  - **Required services:** PI Network Manager, PI Message Subsystem, PI License Manager, PI Update Manager, PI Base Subsystem, PI Snapshot Subsystem, PI Archive Subsystem, PI Backup Subsystem, PI SQL Subsystem, PI Shutdown Subsystem
  - **Required roles:** PI-SDK
- ☑ PI-SDK
- □ Print server

Learn more about server roles.

VALUE NOW, VALUE OVER TIME

Security Configuration Wizard



Security Configuration Wizard

Select Client Features

Servers also act as clients. These client features are used to enable services. A server can support multiple client features.

View: Installed features

Select the client features that the selected server performs:

- □ DNS registration client
- ☑ Domain member
- □ FTP client (normal mode)
- □ Group Policy administrative client
- ☑ Microsoft networking client
- ☑ PI Advanced Calculation Engine
- ☑ PI Analysis Framework 2.0
- ☑ PI Automatic Point Synchronization Engine
- ☑ PI OPC Server

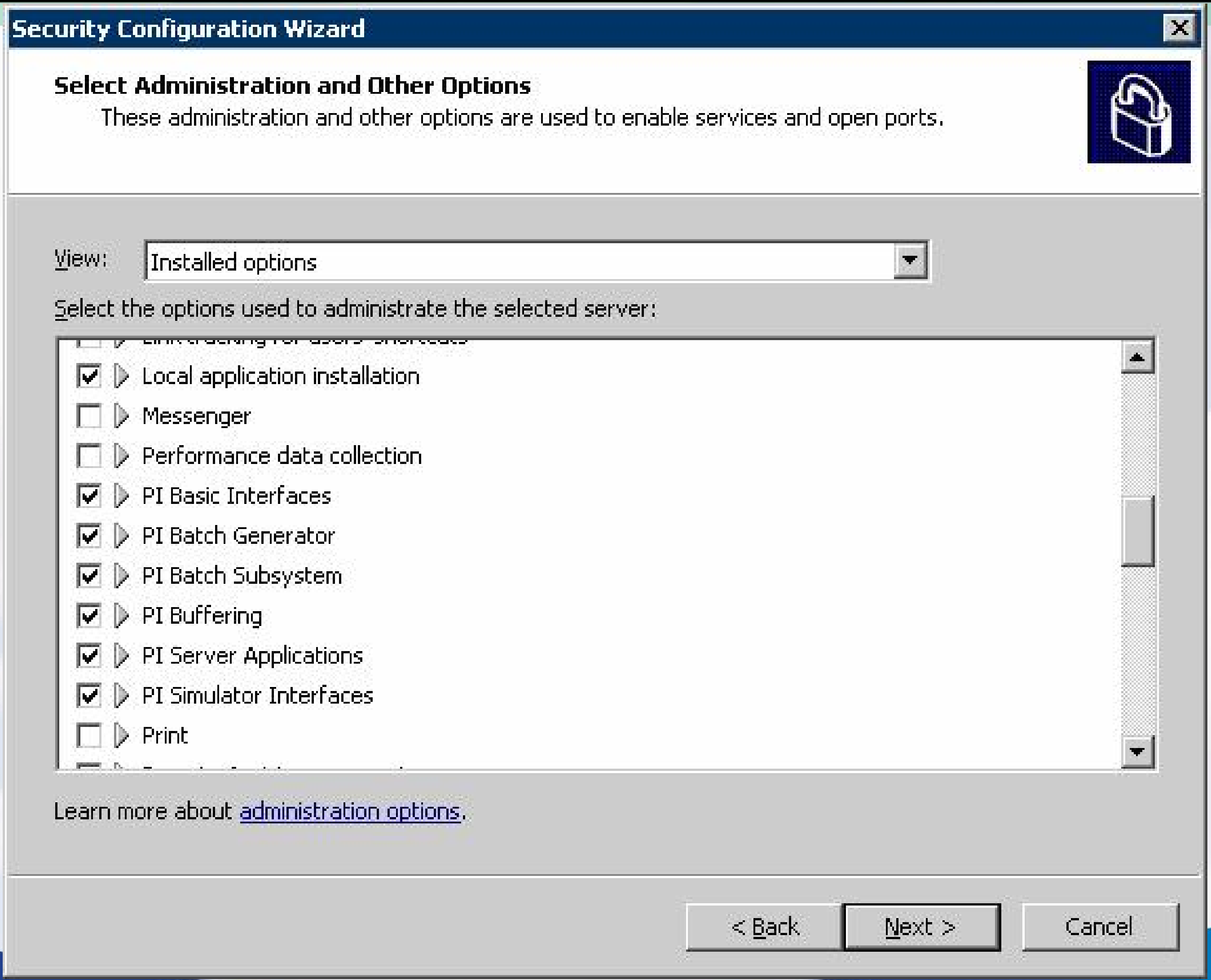
Description: Data access via OPC DA and HDA standards.

Required services: COM+ System Application, COM+ Event System, System Event Notification, OPC Enumerator, PI OPC DA Server for PI, PI OPC HDA Server for PI

Learn more about client features.

OSIsoft

Security Configuration Wizard



Security Configuration Wizard

Select Administration and Other Options

These administration and other options are used to enable services and open ports.

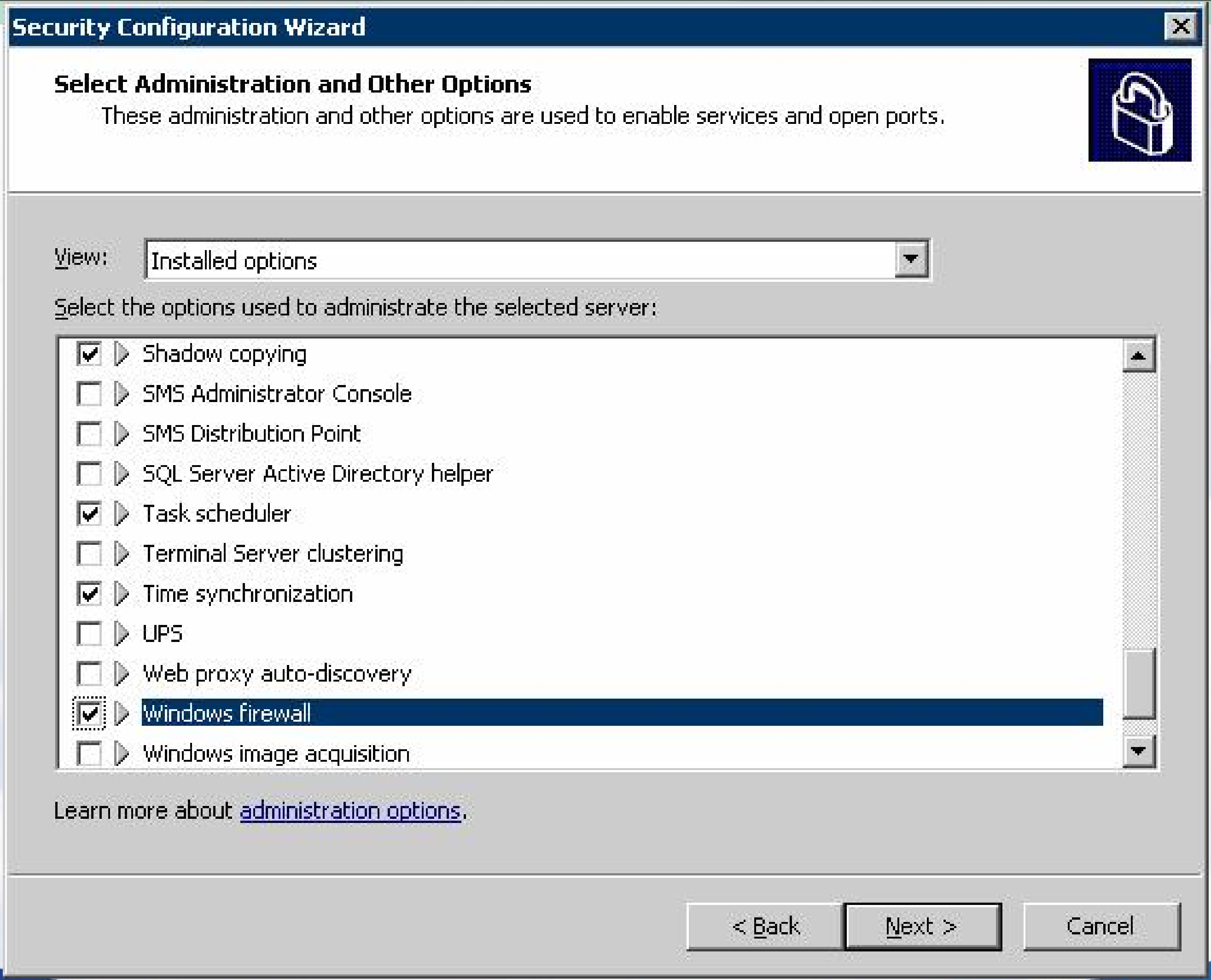
View: Installed options

Select the options used to administrate the selected server:

- □ Link tracking for users' shortcuts
- ☑ Local application installation
- □ Messenger
- □ Performance data collection
- ☑ PI Basic Interfaces
- ☑ PI Batch Generator
- ☑ PI Batch Subsystem
- ☑ PI Buffering
- ☑ PI Server Applications
- ☑ PI Simulator Interfaces
- □ Print

Learn more about administration options.

Security Configuration Wizard



Security Configuration Wizard

Select Administration and Other Options

These administration and other options are used to enable services and open ports.

View: Installed options

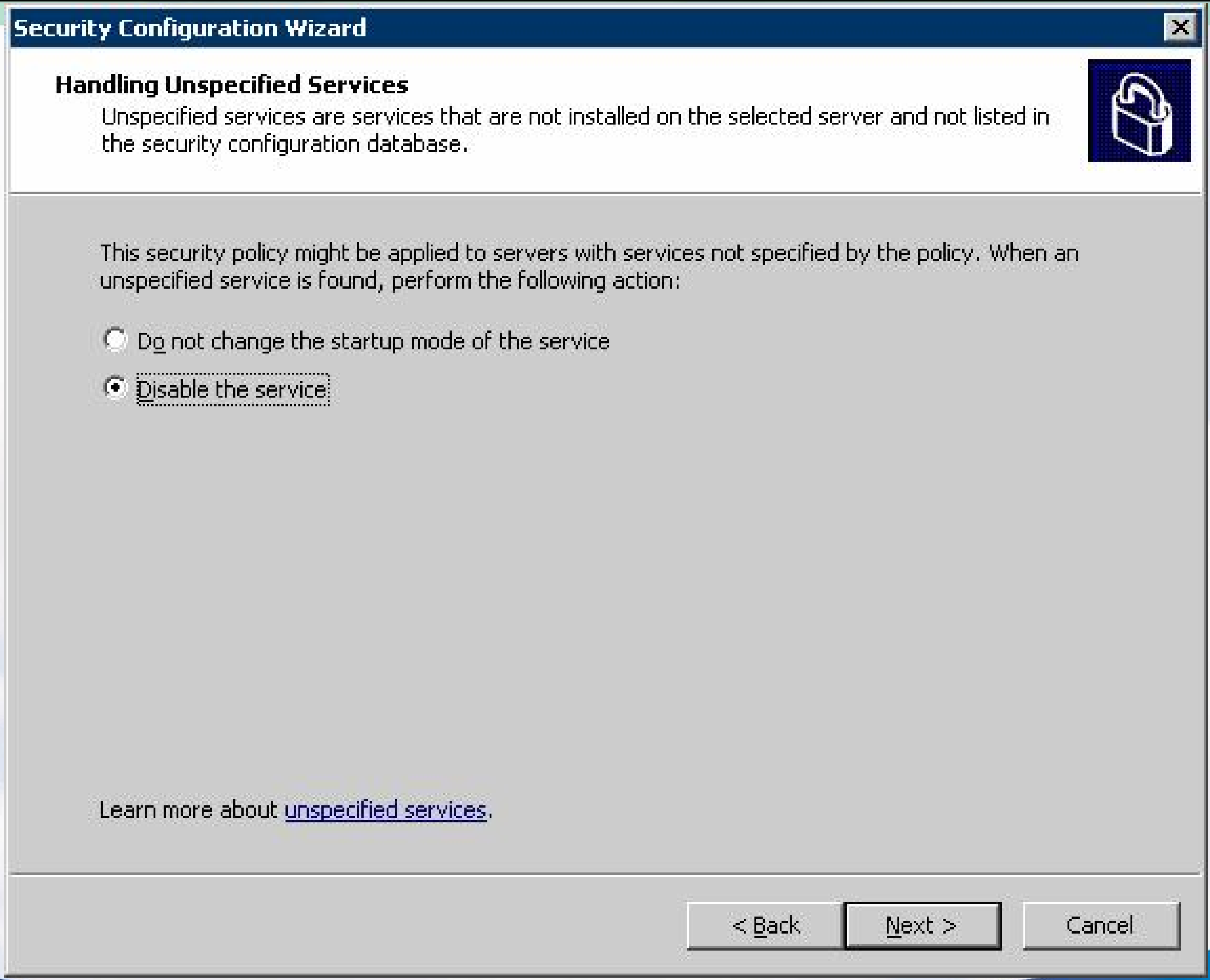
Select the options used to administrate the selected server:

- ☑ Shadow copying
- □ SMS Administrator Console
- □ SMS Distribution Point
- □ SQL Server Active Directory helper
- ☑ Task scheduler
- □ Terminal Server clustering
- ☑ Time synchronization
- □ UPS
- □ Web proxy auto-discovery
- ☑ Windows firewall
- □ Windows image acquisition

Learn more about administration options.

OSIsoft

Security Configuration Wizard



Handling Unspecified Services

Unspecified services are services that are not installed on the selected server and not listed in the security configuration database.

This security policy might be applied to servers with services not specified by the policy. When an unspecified service is found, perform the following action:

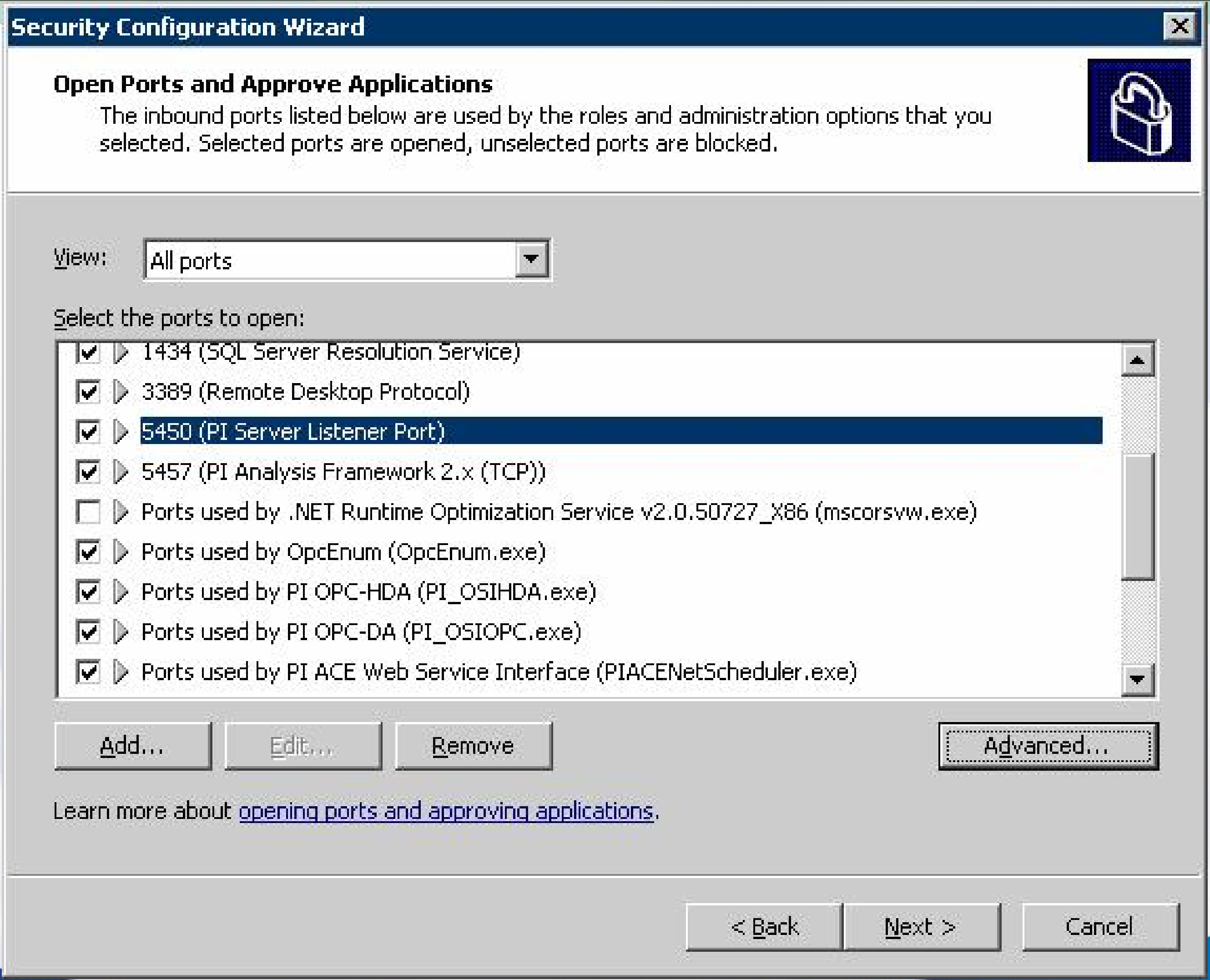
○ Do not change the startup mode of the service

● Disable the service

Learn more about unspecified services.

VALUE NOW, VALUE OVER TIME

Security Configuration Wizard



Security Configuration Wizard

Open Ports and Approve Applications

The inbound ports listed below are used by the roles and administration options that you selected. Selected ports are opened, unselected ports are blocked.

View: All ports

Select the ports to open:

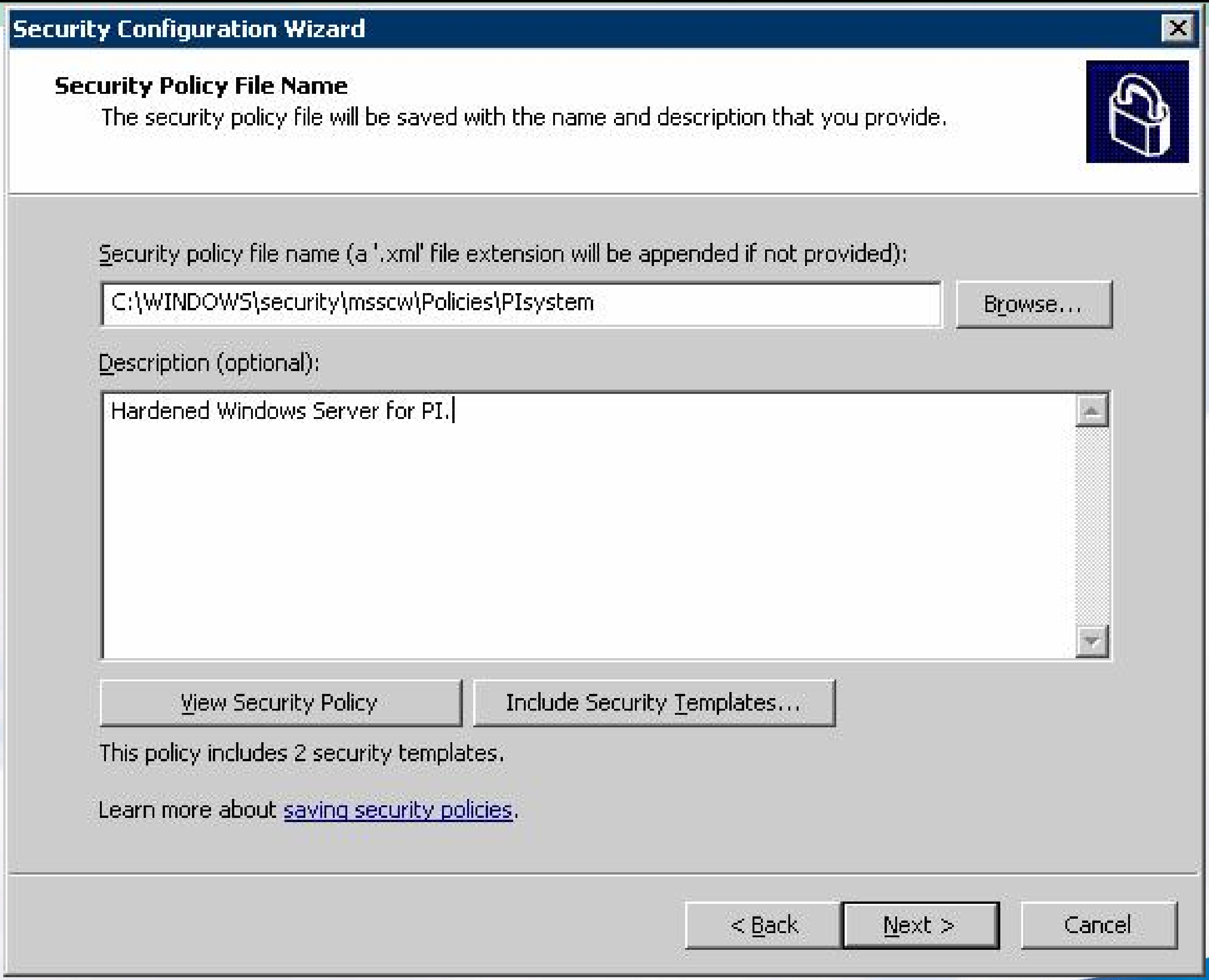
- ☑ 1434 (SQL Server Resolution Service)
- ☑ 3389 (Remote Desktop Protocol)
- ☑ 5450 (PI Server Listener Port)
- ☑ 5457 (PI Analysis Framework 2.x (TCP))
- □ Ports used by .NET Runtime Optimization Service v2.0.50727_X86 (mscorsvw.exe)
- ☑ Ports used by OpcEnum (OpcEnum.exe)
- ☑ Ports used by PI OPC-HDA (PI_OSIHDA.exe)
- ☑ Ports used by PI OPC-DA (PI_OSIOPC.exe)
- ☑ Ports used by PI ACE Web Service Interface (PIACENetScheduler.exe)

Learn more about opening ports and approving applications.

OSIsoft®

VALUE NOW, VALUE OVER TIME

Security Configuration Wizard



Security Configuration Wizard

Security Policy File Name

The security policy file will be saved with the name and description that you provide.

Security policy file name (a '.xml' file extension will be appended if not provided):

C:\WINDOWS\security\msscw\Policies\PIsystem

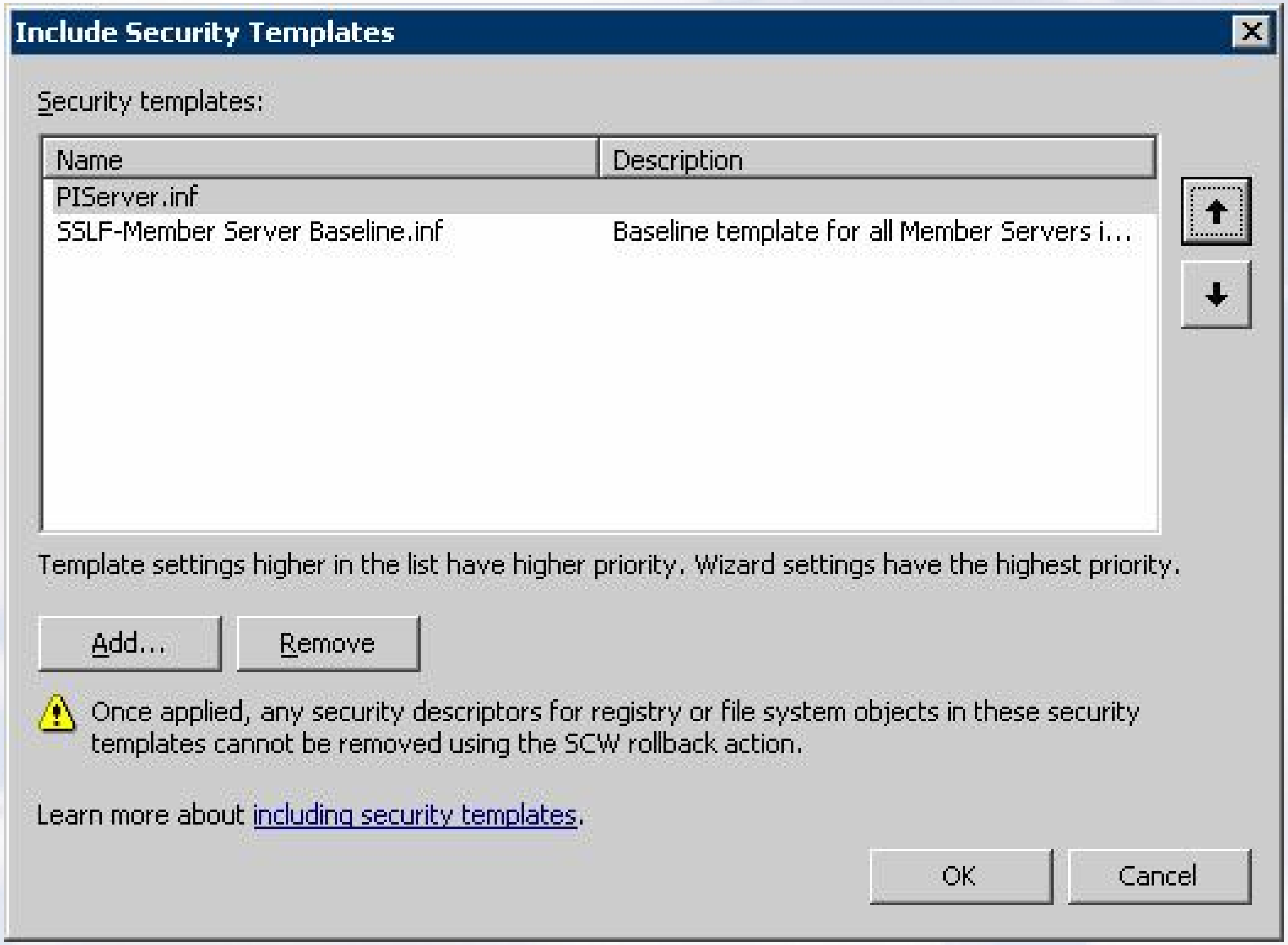
Description (optional):

Hardened Windows Server for PI.

This policy includes 2 security templates.

Learn more about saving security policies.

Security Configuration Wizard



Include Security Templates

Security templates:

Name	Description
PIServer.inf	
SSLF-Member Server Baseline.inf	Baseline template for all Member Servers i...

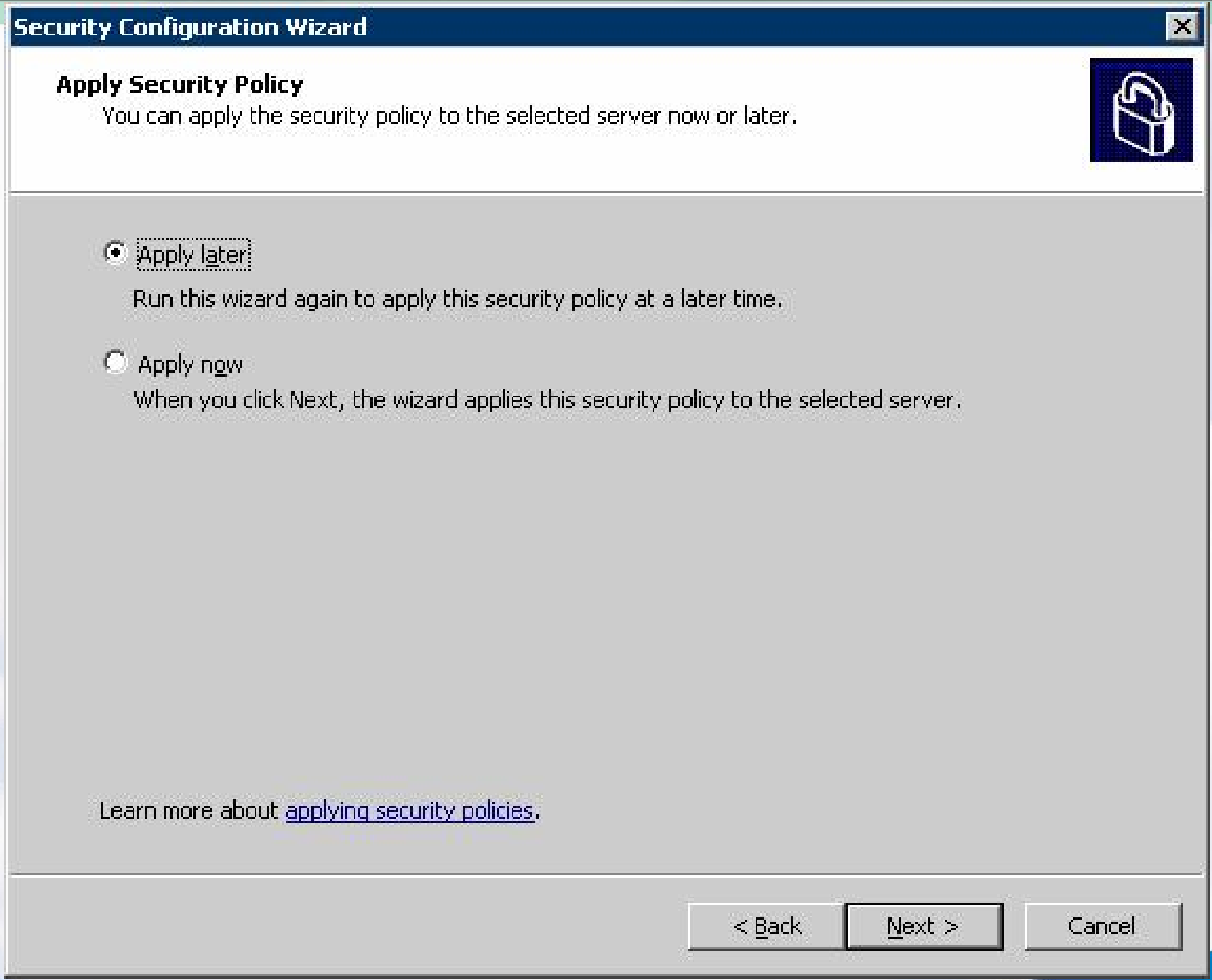
Template settings higher in the list have higher priority. Wizard settings have the highest priority.

⚠ Once applied, any security descriptors for registry or file system objects in these security templates cannot be removed using the SCW rollback action.

Learn more about including security templates.

OSIsoft®

Security Configuration Wizard



Apply Security Policy

You can apply the security policy to the selected server now or later.

● Apply later

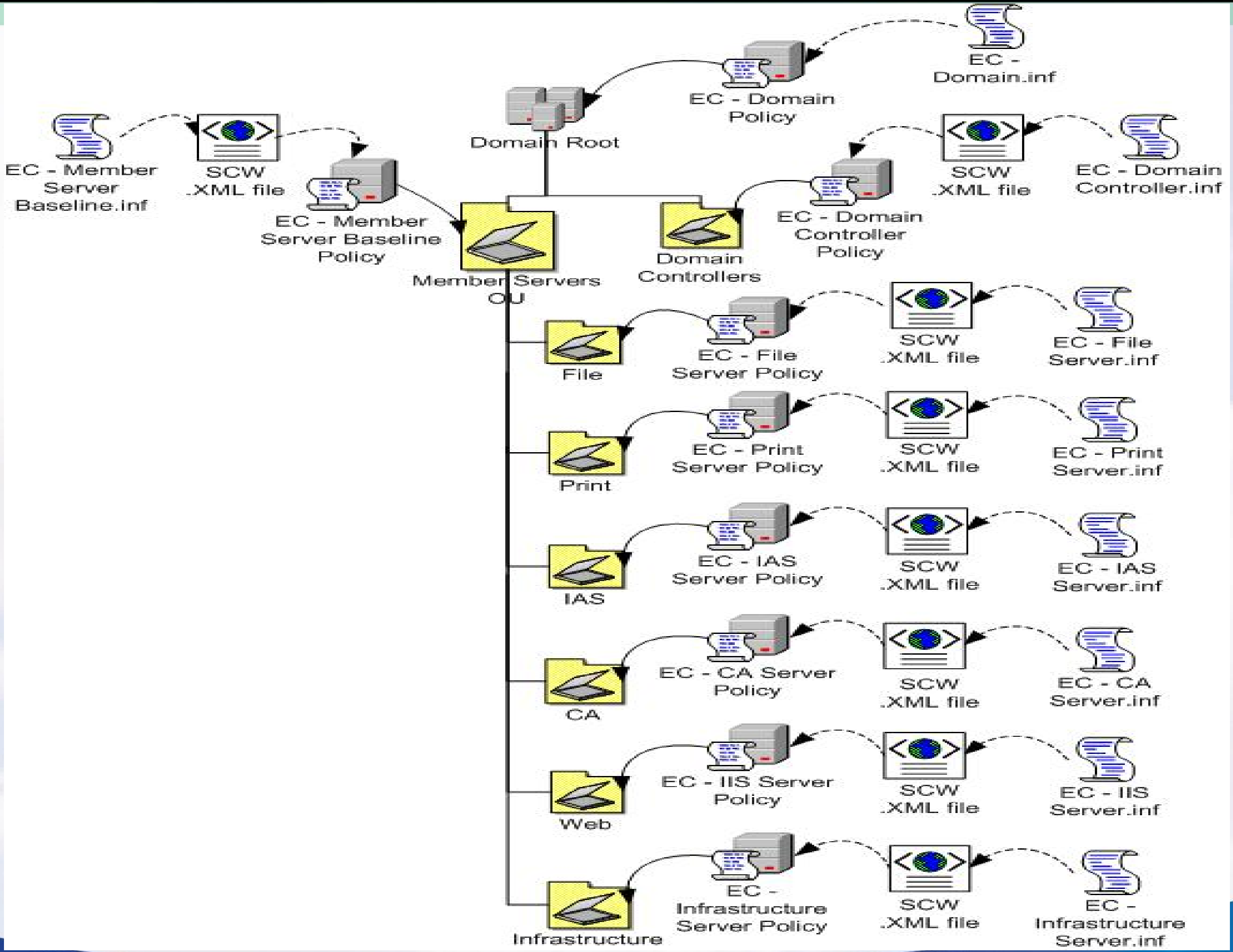
Run this wizard again to apply this security policy at a later time.

○ Apply now

When you click Next, the wizard applies this security policy to the selected server.

Learn more about applying security policies.

Security Configuration Wizard



EC - Domain.inf

EC - Domain Policy

Domain Root

EC - Member Server Baseline.inf

SCW .XML file

EC - Member Server Baseline Policy

Member Servers OU

Domain Controllers

EC - Domain Controller Policy

SCW .XML file

EC - Domain Controller.inf

File

EC - File Server Policy

SCW .XML file

EC - File Server.inf

Print

EC - Print Server Policy

SCW .XML file

EC - Print Server.inf

IAS

EC - IAS Server Policy

SCW .XML file

EC - IAS Server.inf

CA

EC - CA Server Policy

SCW .XML file

EC - CA Server.inf

Web

EC - IIS Server Policy

SCW .XML file

EC - IIS Server.inf

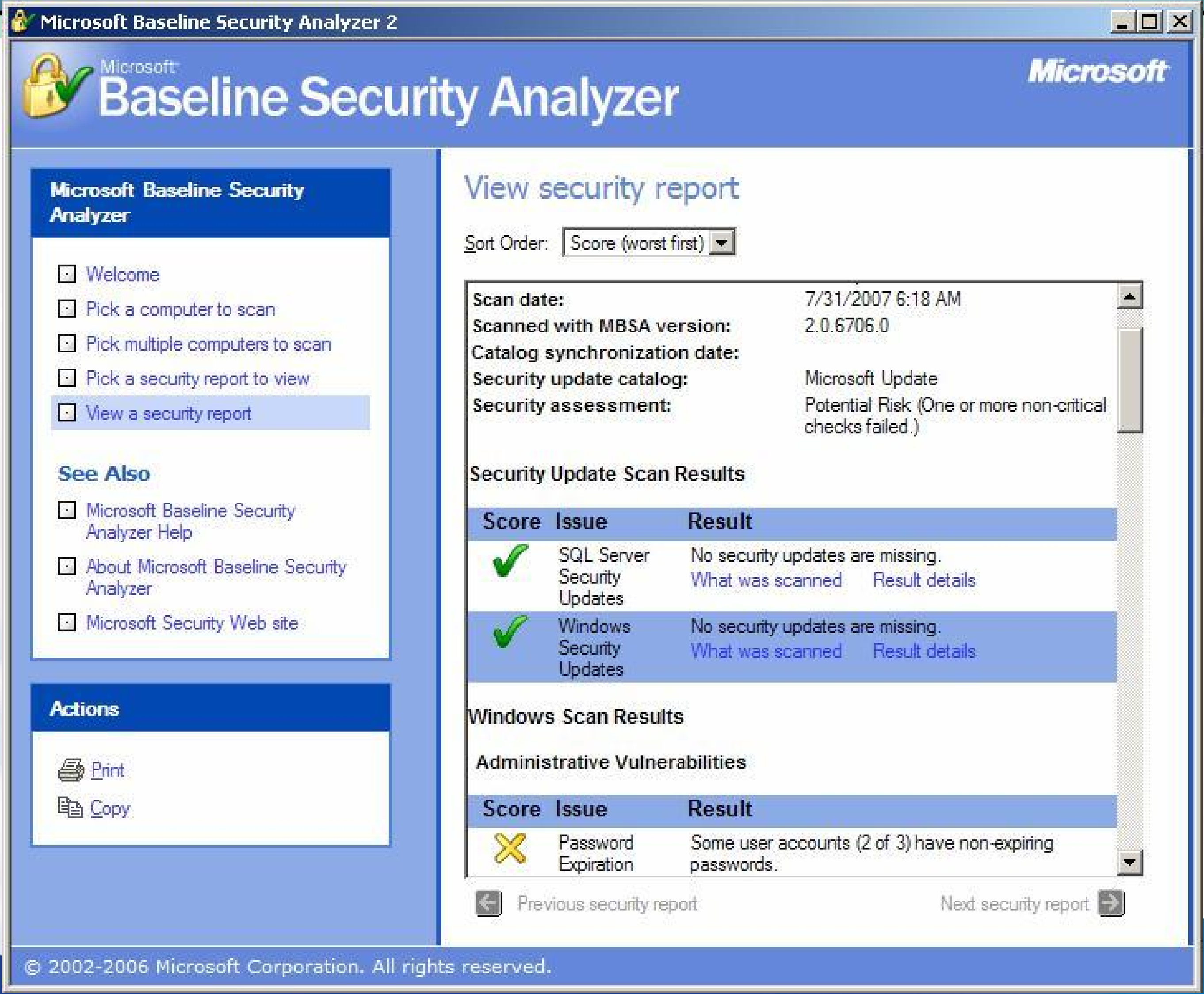
Infrastructure

EC - Infrastructure Server Policy

SCW .XML file

EC - Infrastructure Server.inf

Windows MBSA



Microsoft Baseline Security Analyzer 2

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report

See Also

- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

Actions

- Print
- Copy

View security report

Sort Order: Score (worst first)

Scan date:	7/31/2007 6:18 AM
Scanned with MBSA version:	2.0.6706.0
Catalog synchronization date:	
Security update catalog:	Microsoft Update
Security assessment:	Potential Risk (One or more non-critical checks failed.)

Security Update Scan Results

Score	Issue	Result
✓	SQL Server Security Updates	No security updates are missing. What was scanned Result details
✓	Windows Security Updates	No security updates are missing. What was scanned Result details

Windows Scan Results

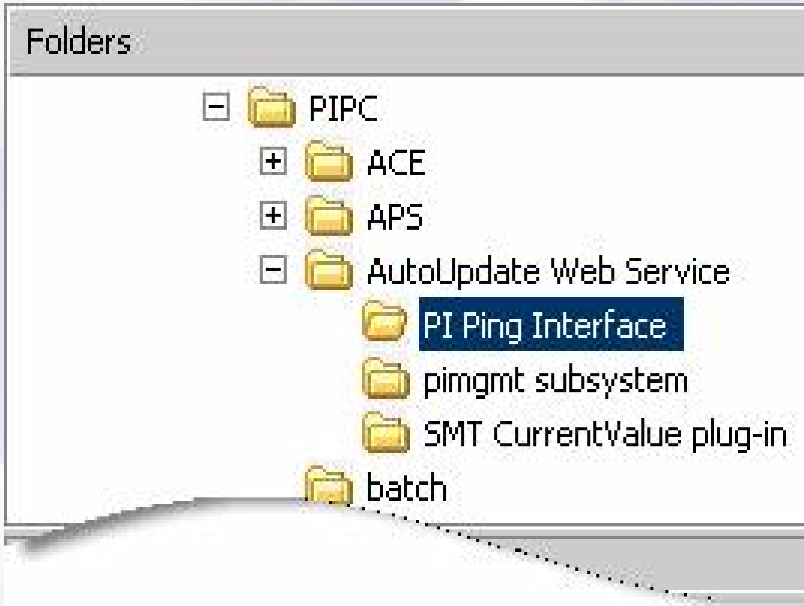
Administrative Vulnerabilities

Score	Issue	Result
✗	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords.

© 2002-2006 Microsoft Corporation. All rights reserved.

Security Related Work In Progress

- SDL Baseline Engineering Practices
  - Require Latest Compiler and Built-In Defenses
  - Security Scrub of Legacy Code and Documentation
  - Threat Models and Countermeasures
  - Least Required Privilege
- Product Highlights
  - Windows Integrated Security
  - User Service / Access Layer
  - PI Software Update Service



OSIsoft

VALUE NOW, VALUE OVER TIME

Security Summary

- It’s really all about **Quality!**
  - Starts in Design and Secure Coding Practices
  - Secure Infrastructure and Deployment Architecture
  - Good Advice and Configuration Tools
  - Quality of Service Monitoring and Support
- Call to Action
  - Get: PI Security Best Practices Whitepaper
  - Visit: Data Center Monitoring Demo Pod

VOYAGE2007

MONTEREY

OSISOFT USER CONFERENCE 2007

CALIFORNIA

Thank You

OSIsoft

VALUE NOW, VALUE OVER TIME