

**Cookbook for
IBM Tivoli Security Compliance
Manager 5.1.x
Plus
IBM Integrated Security Solution for
Cisco Networks (IISCN)**

I Copyright Notice

© Copyright IBM Corporation 2005. All rights reserved. May only be used pursuant to a Tivoli Systems Software License Agreement, an IBM Software License Agreement, or Addendum for Tivoli Products to IBM Customer or License Agreement. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of IBM Corporation. IBM Corporation grants you limited permission to make hardcopy or other reproductions of any machine-readable documentation for your own use, provided that each such reproduction shall carry the IBM Corporation copyright notice. No other rights under copyright are granted without prior written permission of IBM Corporation. The document is not intended for production and is furnished "as is" without warranty of any kind. **All warranties on this document are hereby disclaimed, including the warranties of merchantability and fitness for a particular purpose.**

U.S. Government Users Restricted Rights—Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corporation.

II Trademarks

IBM, the IBM logo, Tivoli, the Tivoli logo, AIX, Cross-Site, NetView, OS/2, Planet Tivoli, RS/6000, Tivoli Certified, Tivoli Enterprise, Tivoli Enterprise Console, Tivoli Ready, and TME are trademarks or registered trademarks of International Business Machines Corporation or Tivoli Systems Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

III Notices

References in this publication to Tivoli Systems or IBM products, programs, or services do not imply that they will be available in all countries in which Tivoli Systems or IBM operates. Any reference to these products, programs, or services is not intended to imply that only Tivoli Systems or IBM products, programs, or services can be used. Subject to valid intellectual property or other legally protectable right of Tivoli Systems or IBM, any functionally equivalent product, program, or service can be used instead of the referenced product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by Tivoli Systems or IBM, are the responsibility of the user. Tivoli Systems or IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, New York 10504-1785, U.S.A.

I	Copyright Notice	1
II	Trademarks.....	1
III	Notices	1
IV	Document History	6
V	The objective of this document.....	6
VI	Acknowledgements	7
1	Introduction	8
1.1	What is IBM Tivoli Security Compliance Manager?.....	8
1.2	Product Highlights.....	9
1.3	IBM Tivoli Security Compliance Manager Hardware Requirements	10
1.4	IBM Tivoli Security Compliance Manager Software Requirements.....	11
1.5	VMWARE requirements for use is test and demonstration environments	12
2	Installation of the IBM Tivoli Security Compliance Manager on AIX 5.X	14
2.1	Installation of IBM DB2 UDB 8.2 Server	14
2.1.1	Base DB2 Installation	14
2.1.2	Check the DB2 installation	26
2.2	Installation of Tivoli Security Compliance Manager Server V 5.1	27
2.2.1	Base ITSCM Server Installation	27
2.2.2	Verify the ITSCM Server installation	33
2.3	Installation of Tivoli Security Compliance Manager Client V 5.1.....	34
2.3.1	Base ITSCM Client Installation.....	34
2.3.2	Verify the ITSCM Client installation.....	38
3	Installation of the IBM Tivoli Security Compliance Manager on SLES 8.....	39
3.1	Installation of IBM DB2 UDB 8.1 Server	39
3.1.1	Base DB2 Installation	39
3.1.2	Installation of DB2 8.2 (ie 8.1 Fixpack 7a).....	47
3.1.3	Check the DB2 installation	50
3.2	Installation of Tivoli Security Compliance Manager Server V 5.1	53
3.2.1	Base ITSCM Server Installation	53
3.2.2	Verify the ITSCM server installation.....	59
3.3	Installation of Tivoli Security Compliance Manager Client V 5.1.....	60
3.3.1	Base ITSCM Client Installation.....	60
4	Installation of the IBM Tivoli Security Compliance Manager on Windows 2000 ...	64
4.1	Installation of IBM DB2 UDB version 8.1	64
4.1.1	Base DB2 Installation	64
4.2	Installation of Tivoli Security Compliance Manager Server V 5.1	73
4.2.1	Base ITSCM Server Installation	73
4.3	Installation of Tivoli Security Compliance Manager Client V 5.1.....	87
4.3.1	Base ITSCM Client Installation.....	87
5	IBM Tivoli Security Compliance Manager Console Installation.....	91
5.1	Installation of a ITSCM Console on Windows 2000 or XP	91
6	Tuning Guidelines	93
6.1	The law of diminishing Returns.....	93
6.2	Tuning just for the sake of tuning.....	93
6.3	Consider the entire system.....	93

6.4	One parameter at a time.....	93
6.5	Tune by levels	93
6.6	Hardware as well as software	93
6.7	Understand the problem.....	94
6.8	Put fall-back procedures in place	94
6.9	The top tuning factors.....	94
7	DB2 Database Installation Considerations and Performance Tuning	95
7.1	DB2 Installation Suggestions.....	95
7.2	DB2 Tuning Suggestions.....	96
7.2.1	Buffer Pools.....	96
7.2.2	Increasing Buffer pool size	97
7.2.3	Placing logs on a separate device.....	97
7.2.4	Increase log file size	97
7.2.5	Clear snapshots	97
7.2.6	Add indexes as necessary	98
7.2.7	Additional Tuning.....	98
8	IBM Tivoli Security Compliance Manager Console Functions	102
8.1	Logging on to ITSCM Server via GUI	102
9	Configuration of IBM Tivoli Security Compliance Manager Clients and Collectors	
	103	
9.1	Managing Clients	103
9.1.1	Before you start	103
9.2	Register the ITSCM Client	103
9.2.1	Automatic Client Registration	103
9.2.2	Manual Client Registration.....	104
9.2.3	Creating Client Groups	107
9.2.4	Creating Nested Client Groups	108
9.3	Configuring Collector Authorization.....	111
9.3.1	Before you Start.....	111
9.3.2	Create Keystore and Authorization Key	112
9.3.3	Set Collector Authorization Level	114
9.4	Managing Collectors	115
9.4.1	Before you Start.....	115
9.4.2	Installing Collectors.....	115
9.4.3	Authorizing Collectors.....	118
9.4.4	Registering Collectors	122
9.4.5	Set Collector Default Schedules	125
9.4.6	Assigning Collectors.....	129
9.4.7	Testing the Collector on a Client	132
9.4.8	Collecting Collector Data	135
10	Configuration of Security Compliance Manager Policies and Compliance Queries	
	137	
10.1	Managing Policies	137
10.1.1	Create the Policy.....	137
10.1.2	The Compliance Query	138
10.1.3	Snapshots.....	146
10.1.4	Suppression	151
10.1.5	Policy Schedules and Collectors	154

10.1.6	Policy Bundles.....	157
10.2	Sample Installation of selected policies: Linux + UNIX policies	165
11	Creating a sample SQL report from the ITSCM administration GUI	169
11.1	SQL Reports.....	169
11.1.1	Configuring a Report	172
11.1.2	Execute a report	176
12	Preparing the W2K client for ITSCM Operational Reporting.....	179
12.1	W2K: Installation DB2 UDB Administration Client V8.2.....	179
12.2	W2K: Installation of IBM HTTP server 1.3.26.2.....	183
12.3	W2K: Install Crystal 9 Enterprise.....	186
12.3.1	Create Windows account for MSDE:.....	186
12.3.2	Install the Server	186
12.4	Installation and Configuration of ITSCM Operational Reports	189
12.4.1	Obtain and prepare the Operational Report Files	189
12.4.2	Configure the CE 9 CGI Web Connector for IBM HTTP Server.....	190
12.4.3	Create IBM HTTP Administrator account	190
12.4.4	Create directory aliases.....	191
12.4.5	Add MIME types.....	192
12.4.6	Associate MIME types with scripts	193
12.4.7	Edit the Crystal Enterprise HTML pages	194
12.4.8	Testing the Configuration	194
12.4.9	Create an Open Database Connectivity (ODBC) data source	196
12.5	Make the Tivoli Security Compliance Manager operational reports available 197	
13	Verify the Operational Reports.....	198
13.1	Reporting Interface.....	198
13.2	Sample Operational Reports	204
13.2.1	Sample-Report: Policy Violations	205
13.2.2	Sample - Report: Client Violations	207
14	Configuration of Security Compliance Manager Users, Groups and Roles	209
14.1	Creating Users	209
14.2	Creating Groups	211
14.3	Creating Templates.....	213
14.4	Creating Roles	215
15	IBM Integrated Security Solution for Cisco Networks (IISCN)	219
15.1	System Overview	219
15.1.1	Network Admission Control - Cisco NAC	220
15.1.2	Compliance – Tivoli Security Compliance Manager 5.1	221
15.1.3	Remediation – Tivoli Provisioning Manager 2.1	221
15.1.4	Tivoli Security Compliance Manager Client for NAC.....	222
15.1.5	Default Remediation Handler	222
15.1.6	ITSCM Collectors for NAC.....	222
15.1.7	Remediation Client	222
15.1.8	Remediation Listener.....	222
15.1.9	Remediation Workflows	222
15.1.10	The Transport Layer (TRAPI)	222
16	Installing the Cisco NAC Components.....	223
16.1	ACS Server.....	223

16.2	IOS NAD.....	223
16.3	Cisco Trust Agent (CTA)	223
17	Installing and configuring the Tivoli Security Compliance Manager components for IISCN	224
17.1	Tivoli Security Compliance Manager Server.....	224
17.2	Tivoli Security Compliance Manager Client	224
18	Installing and configuring the Tivoli Provisioning Manager components	227
18.1	Tivoli Provisioning Manager server	227
18.2	Remediation Workflows.....	228
18.3	Remediation Listener.....	228
19	Installation and configuration of IISCN Components.....	230
19.1.1	Tivoli Security Compliance Manager Posture Plug-in.....	230
19.1.2	Remediation Client	230
19.2	Configuration Setup.....	231
19.2.1	Policy Creation and Assignment.....	231
19.2.2	Remediation Capability	232
19.2.3	Network Configuration.....	232
19.2.4	ACS Server.....	232
19.2.5	IOS NAD	233
20	Cisco NAC Installation/Configuration example for TCR	234
20.1	Install and Configure ACS 3.3.....	234
20.2	Install the ACS Certificate.....	238
20.3	Configure Logging	241
20.4	Configure Downloadable ACLs	242
20.5	Configure Groups	243
20.6	Configure a Clientless User	244
20.7	Configure Global Authentication for EAP.....	245
20.8	Configure External User Database.....	245
21	IOS NAC Configuration for NAC.....	250
21.1.1	Setup.....	250
22	Setup IBM ITSCM NAC Plug-in and Client	253
22.1	Putting it All Together - Creating and deploying a new TCR object	253
22.2	Example Scenarios	255
22.2.1	HotFix	255
22.2.2	Password Length	256
23	Troubleshooting the Deployment	257
24	Hints, Tips, and Tools	261
24.1	General Notes.....	261
24.2	DB2 Installation	261
24.3	SCM Server Installation	261
24.4	Installing the SCM Client	262
24.5	Installing the SCM Administration Utilities	263
24.6	Post Installation	263
24.7	Installing an Email server	264
24.8	Configuration	264
24.9	Implementing a Proxy Agent.....	267
24.10	ACS Server.....	268
24.11	Cisco Trust Agent.....	268

24.12	IBM Tivoli Security Compliance Manager Client	268
24.13	Remediation Client	269
24.14	IBM Tivoli Provisioning Manager Server	269
25	Appendix 1	270
25.1	Reference Information	270

IV Document History

Version	Date	Description	By
1.0	29/09/05	ITSCM Install and function+IISSCN	Phil Billin

V The objective of this document

This cookbook was developed to assist in the planning, installation and configuration of IBM Tivoli's Compliance and remediation solution by Phil Billin of the Product Introduction Centre, (PIC) Hursley. It is designed to be used by IBM Pre-sales, Services, Business Partners and Customers.

The objective of this document is to describe the installation scenarios and configuration option, of Tivoli Security Compliance Manager (ITSCM) 5.1 components as well as the upgrades to Fix Paks. A basic installation and recommended configuration is also provide for Tivoli Provisioning Manager, Cisco ACS server and NAC Router for use in POC's/Pilots or demonstrations of the full function of ITSCM's compliance checking and remediation solution announced in October 2004 and released in December 2004. The configurations described are on Windows and SUSE Linux in VMware sessions and AIX where this platform is supported.

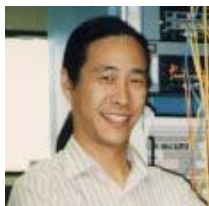
Further step by step instructions on working with best practices / policies, writing compliance queries, SQL reports, Crystal Reports and creating users, groups, roles and role templates are described.

Further updates to this document are planned with additional information. If you have related information to share and would like it included in this document or have requirements for information that is not available here then please send an email to billinp@uk.ibm.com. All material provided must be copyright free. Your comments on the content are welcome as well as any errors or improvements you would like to see.

VI Acknowledgements

It with great thanks to the following people for their contributions of material and time for this cookbook :

David Butler Tivoli Consultant, Dallas USA



Frank Yeh Jr. Tivoli Security Solution Architect, Irvine California USA

Matthias Troeger Tivoli Technical Sales, EMEA Central Region



Paul O'Mahony Tivoli Security Specialist - EMEA Product Introduction Centre



Patricia Saunders Cert SW IT Specialist - World Wide Tivoli Sales Security Enablement

Srdjan Ljubisavljevic Software Sales Consulting IT Specialist – SWIT North Region EMEA

1 Introduction

This document is about IBM Tivoli Security Compliance Manager (ITSCM), a software product that allows the creation of security policies and their regular monitoring for compliance and vulnerabilities. Essentially, ITSCM performs two functions:

1. Collects data from multiple computer systems and stores that data in a central repository.
2. Provides reporting capabilities to show adherence to, or violation of defined security policies.

It can also be integrated with other products to provide compliant access to networks at layer 2 or 3, and manual or automated remediation processes of non-compliance to security policy.

Operating as a data collection service, IBM Tivoli Security Compliance Manager will gather and store a wide variety of information from multiple computer systems. This information can include any data located on the system, such as operating system version information, software patch levels, registry information, file and directory information, application information, and other security-related data. Functioning as a monitoring and reporting service, Tivoli Security Compliance Manager will extract the data collected, analyze the data for conformity, and produce reports that can reveal adherence to internal and industry-standard security policies.¹

As a monitoring and reporting service, IBM Tivoli Security Compliance Manager can extract the data collected, analyze the data for vulnerabilities, and produce reports that can reveal adherence to internal and industry-standard security policies.

Examples of such security and privacy requirements include:

- Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act in the USA
- BASEL II in Europe
- Sarbanes-Oxley Act (SOA)
- Health Insurance Portability and Accountability Act (HIPAA)

1.1 What is IBM Tivoli Security Compliance Manager?

IBM Tivoli Security Compliance Manager is a Java based security policy compliance product that acts as an early warning system by identifying security vulnerabilities and security policy violations for small, medium and large businesses. Tivoli Security Compliance Manager helps organizations define consistent security policies and monitor compliance of these defined security policies. Security policies can be based on both internal security requirements and industry-standard security policies.

1.2 Product Highlights

- Automates scans of servers and desktop systems which can help reduce the cost and time associated with manual security checks
- Provides reports to security officers and compliance auditors with detailed information about the security health of the business so they can take the appropriate steps to make individual systems and departments compliant
- Identifies software security vulnerabilities prior to costly damage being inflicted by security incidents
- Improves business operations and helps to increase efficiencies through automation and centralization
- Assists in addressing compliance issues in regulations and standards by automating compliance tasks, monitoring correspondence, reducing human error, and taming compliance costs
- Integrates with Tivoli's automated security management tools and Security Vulnerability services to help identify and mediate security policy violations and risks

Tivoli Security Compliance Manager is designed for customers who are concerned with compliance and regulations as well as those concerned with identifying and fixing security weaknesses and vulnerabilities in their IT infrastructure. In assisting with compliance issues, the software comes with pre-defined recommended security policies and can be customized to fit specific regulatory, industry or corporate security policies. The software helps provide a more efficient way to gather and manage information about the health of systems, and enterprises can use that data to help them comply with regulations.

Tivoli Security Compliance Manager audits systems and applications for vulnerabilities and identifies violations against security policies. The software uses a red, yellow, green, stoplight-style warning system to alert security administrators and users, whether systems comply with security policy. For example, the software could send reports or an email to administrators showing which systems have passwords set properly, which have anti-viruses signature files are up-to-date, and which have dangerous or unnecessary services running. The software can help identify security vulnerabilities across operating systems and applications on AIX, Solaris, HP-UX, Windows, Novell NetWare, Linux (Intel, & pSeries) and Linux on zSeries.

With additional IBM Global Services it has been possible to add the same compliance checking capabilities to Network devices like Switches and Router as well as a wider range of application than is available out of the box. New out of the box support is made available via the ITSCM download web site:

<http://www.ibm.com/support/docview.wss?uid=swg24007082>

Figure 1, IBM Tivoli Security Compliance Manager (ITSCM) Highlights

Features	Advantages	Benefits
Centralized administration	Centralizes the policy definition and scanning of systems	Consistent security audits across the organization reducing human error

Automation	Automates security scans of servers and desktop systems which can help reduce the cost and time associated with manual security checks	Helps reduce costs by providing a more effective and efficient way to perform routine tasks, which allows administrators to focus on more strategic functions
Security vulnerability scans	Helps to secure business systems	Helps to identify software security vulnerabilities prior to costly damage being inflicted by security incidents
Compliance	Security policy compliance can assist in collecting and managing data about security efforts and systems that companies use as part of their overall regulatory compliance initiatives	Addresses compliance issues in regulations and standards by automating compliance tasks, monitoring correspondence, reducing human error, and taming compliance costs
Auditing and reporting mechanisms	Enables administrators to produce reports with detailed information about the security health of the business so they can take the appropriate steps to make individual systems and departments compliant	Quickly produce reports for audits and ensuring regulatory compliance

1.3 IBM Tivoli Security Compliance Manager Hardware Requirements

Figure 2 shows suggest hardware requirements for enterprise installations of ITSCM based on live deployments internal of IBM and managing various numbers of Servers (ITSCM Clients).

Figure 2, IBM Tivoli Security Compliance Manager (ITSCM) Hardware Requirements

Processor and memory requirements for IBM Tivoli Security Compliance Manager Server			
Type of ITSCM deployment		CPU RQMTS	RAM RQMTS
Small	(1-500 clients)	1	512MB RAM
Medium	(501-2500 clients)	2	512MB RAM
Large	(2501-10000 clients)	2-4	2-4GB RAM
Server package requires 5MB to install			
Disk and memory requirements for client and collectors			
Disk and memory requirements for ITSM Client			
Client platform	Disk Requirements for installation directory	Disk Requirements for temporary directory	RAM RQMTS

AIX	64MB	45MB	75MB RAM
HP-UX	64MB	6MB	75MB RAM
Linux	64MB	46MB	75MB RAM
Solaris	64MB	65MB	75MB RAM
Windows	64MB	44MB	75MB RAM

Note: The HP-UX platform values in the table are much smaller due to the JRE being packaged in the OS

Disk and memory requirements for Administration Utilities

Disk and memory requirements for ITSM Administration Console

Administration Console Platform	Disk Requirements for installation directory	Disk Requirements for temporary directory	RAM RQMTS
Windows	64MB	42MB	128MB RAM Min 256MB RAM Rec

1.4 IBM Tivoli Security Compliance Manager Software Requirements

Figure 3, IBM Tivoli Security Compliance Manager (ITSCM) Software Requirements

Tivoli Security Compliance Manager requires:

IBM DB2 UDB version 7.2 or 8.1

Supported Operating Systems:

The following information are the supported Operating Systems for ITSCM Server, Client, and Administration Console:

IBM Tivoli Security Compliance Manager (ITSCM) Server

Operating System	Level	Patch/Maintenance Level
AIX	5.1, 5.2, 5.3	None required
Windows 2000	Server	Latest Fix Pack
Windows 2003	Server Standard Edition & Enterprise Edition	
Solaris	2.8, 2.9	Latest Fix Pack
SuSe Linux Enterprise Server	8	Latest Fix Pack

IBM Tivoli Security Compliance Manager (ITSCM) Client

Operating System	Level	Patch/Maintenance Level
AIX	5.1, 5.2, 5.3	Latest cumulative patches
HP-UX	11.0, 11i	Latest cumulative patches
Red Hat Linux for Intel (IA32 & xSeries)	6.2, 7.0, 7.1, 7.2, 8.0, 9.0	Latest cumulative patches
Solaris	2.6, 2.7, 2.8, 2.9	Latest cumulative patches
Windows NT	4.0 Server, 4.0 Workstation	Latest service pack and security roll up package
Windows 2000	Server, Advanced Server, Professional	Latest service pack and security roll up package

Windows 2003	Server Standard Edition, Enterprise Edition	Latest cumulative patches
Windows XP	Professional	
Novell Netware	5.1, 6.0, 6.5	ITSCM Fix pack 5.1.0-TIV-SCM-FP0009 required
Red Hat Enterprise Linux (EL) (IA32 & xSeries)	2.1	Latest cumulative patches
Red Hat EL Advanced Server (IA32 & xSeries)	3.0	Latest cumulative patches
Red Hat EL for iSeries/pSeries	3.0	Latest cumulative patches
Red Hat EL for zSeries	7.2	Latest cumulative patches
SuSe Linux	7.0	Latest cumulative patches
SuSe Linux Enterprise Server (ES)	8	Latest cumulative patches
SuSe Linux ES for zSeries	8	Latest cumulative patches
SuSe Linux ES for iSeries/pSeries	8	Latest cumulative patches

IBM Tivoli Security Compliance Manager (ITSCM) Administration Console

Operating System	Level	Patch/Maintenance Level
Windows 2000	Professional	Latest service pack and security roll up package
Windows XP	Professional	
Windows 2003	Server Standard Edition and Enterprise Edition	Latest service pack and security roll up package
RedHat EL Advance Server (IA32 & xSeries)	3.0	
SuSe Linux ES (xSeries)	8	

1.5 VMWARE requirements for use is test and demonstration environments

Because not all components are supported on Unix and Linux this document provides a Windows only solution for them (eg. Crystal Enterprise 9 server for ITSCM Operational Reporting and Cisco ACS Server,

The following base configuration is suggested for a demonstration or Pilot/POC set-up where base systems are not available or ease of transporting is beneficial. This configuration was used in the creation of product installation and functions in this documents :

System 1: SLES 8.0

- DB2 UDB 8.2 server
- ITSCM 5.1 server (incl policies etc.) + Fix Pak 2
- ITSCM 5.1 client + Fix Pak 2
- ITSCM Administration Console Fix Pak 2 required for Linux support (optional)

System 2: Windows 2000 Server

- ITSCM 5.1 GUI (optional)
- DB2 8.2 Client
- IBM HTTP Server 1.2.26.2
- Crystal Enterprise 9 server

System 3: Windows 2000 Server (ACS for IISSCN)

- Cisco ACS server (optionally this could coexist with the Crystal Enterprise 9 Server or ITSCM Server if installed on Windows 2000.)
- ITSCM 5.1 Client + Fix Pak 2

System 4: Windows 2000 Server (for IISCN)

- Tivoli Provisioning Manager v2.1 or 3.1

System 5: Windows 2000 or XP Workstation (for IISCN)

- ITSCM 5.1 client + Fix Pak 2
- Cisco Trust Agent (CTA)
- Cygwin
- Windows .Net 1.1 + MS Security fixes

VM Memory recommendations

System 1: >= 400 MB

System 2: >= 300 MB

System 3: >= 3-500 MB

System 4: >= 500 MB or as much resources as possible

System 5: >= 300 MB

2 Installation of the IBM Tivoli Security Compliance Manager on AIX 5.X

2.1. Installation of IBM DB2 UDB 8.2 Server

2.1.1 Base DB2 Installation

Prepare an X11 environment, (Xwindows environment) and allow access control for x-clients on your X-desktop eg at root (#) prompt. **It is important that you are logged in as root.**

```
# xhost +          <enter>
```

If you are installing DB2 on an AIX machine that does not have a graphics adapter and a graphics screen connected to it, you can perform the installation remotely from a Windows machine (e.g. laptop) by using a freeshare program like X-Deep/32 or Cygwin. One of these programs will give you an X Window Server for Windows that can be used to connect to host systems running LINUX, IBM AIX, HP-UX or Sun Solaris.

Make sure you run:

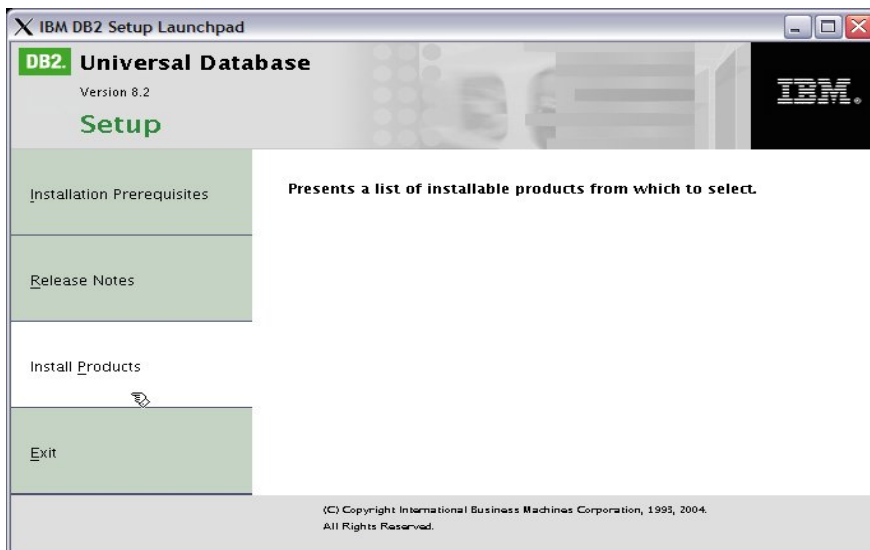
```
# export DISPLAY=your-workstation-ip-address:0
```

on the AIX machine so that you get the DB2 installation screens properly displayed on the workstation by the X Window Server.

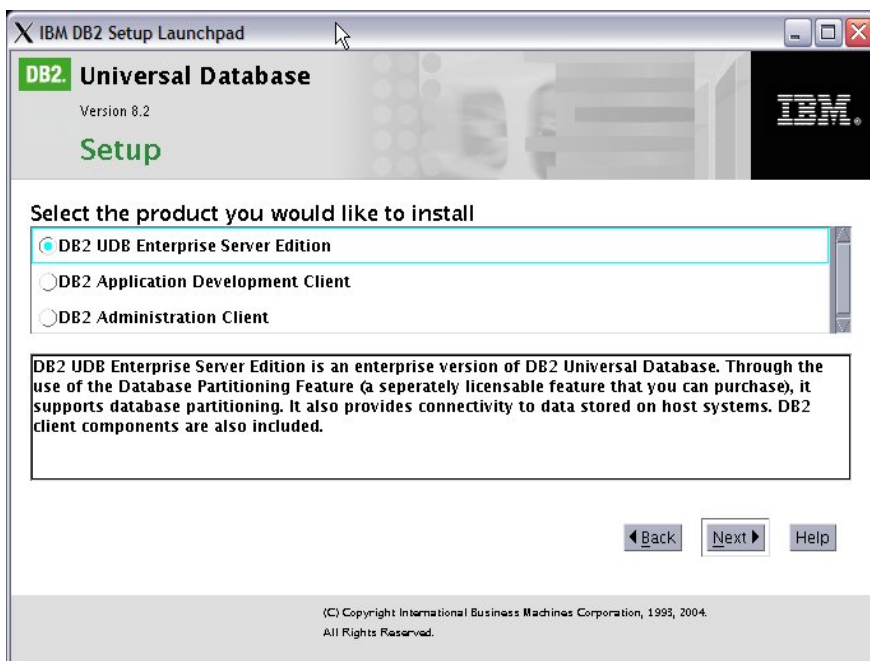
At this point it is probably a good idea to copy the DB2 installation image into a temporary directory (eg /tempfs/SCM) so that the install processes can write temporary files. If downloaded, the DB2 V8.1 installation image will probably come as a compressed *tar* image, so you need to un-tar and uncompress it first.

Now you are ready to commence the DB2 V8.2 installation. Change the directory to where the **db2setup** file is (e.g. cd /tempfs/ese.sbcsaix1)

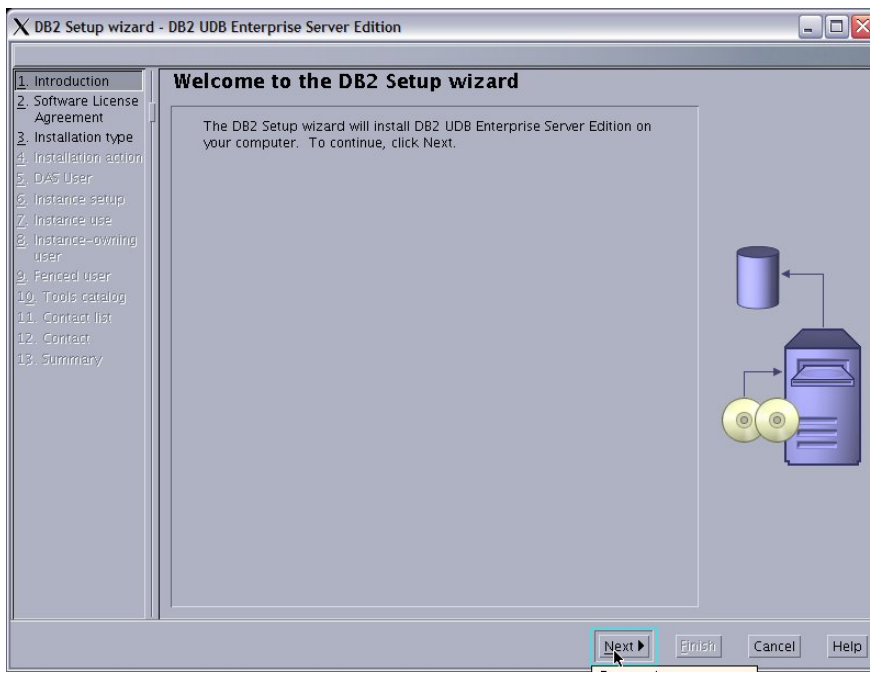
```
# ./db2setup <enter>:
```



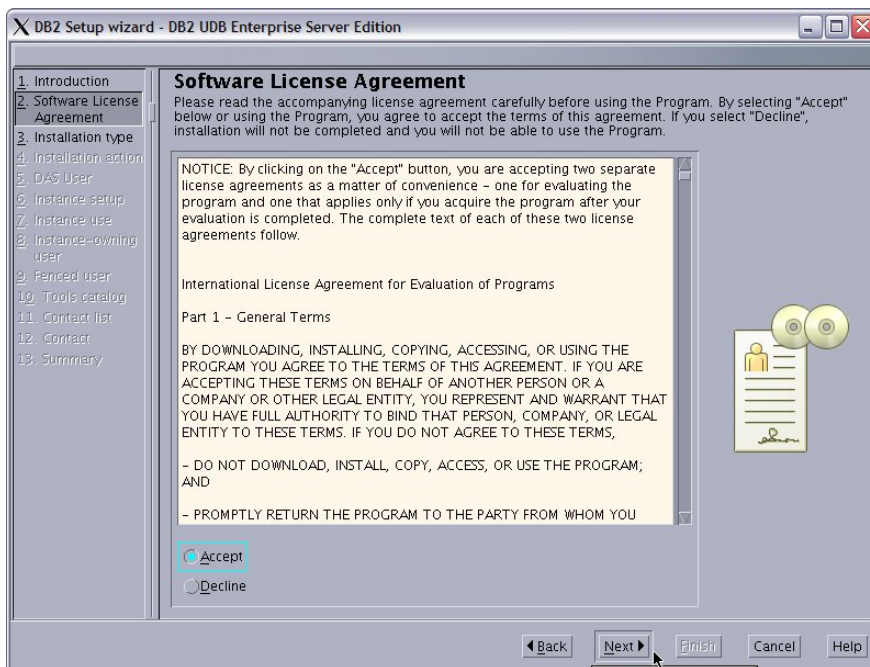
- Select “Install Products” option



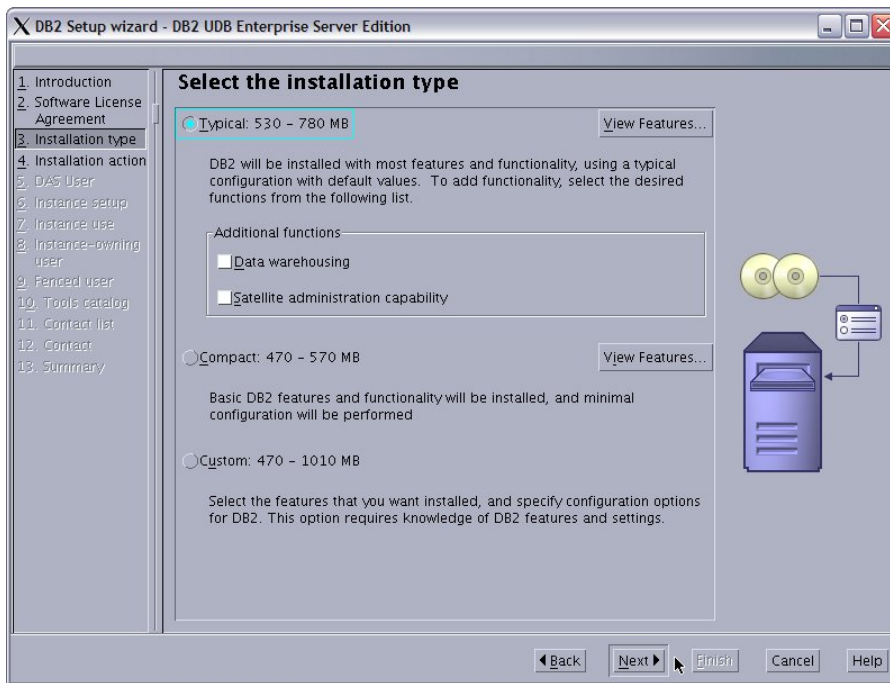
- Select DB2 UDB Enterprise Server Edition



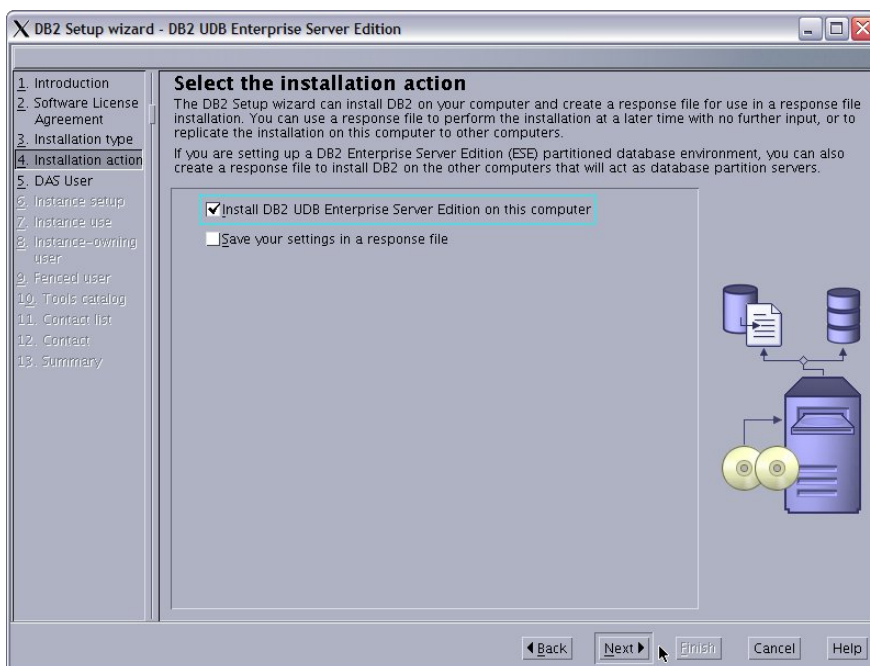
- Click “Next”



- Accept the License Agreement and click “Next”



- Select "Typical" installation type with no additional functions. Click "Next".



- Select “Install DB2 UDB Enterprise Server Edition on this computer” and click “Next”

DB2 Setup wizard - DB2 UDB Enterprise Server Edition

Set user information for the DB2 Administration Server
The DB2 Administration Server (DAS) runs on your computer to provide support required by the DB2 tools. A user account with a minimal set of privileges is required to run the DAS. Specify the required user information for the DAS.

☒ **New user**

User name:

UID:

☒ Use default UID

Group name:

GID:

☒ Use default GID

Password:

Confirm password:

Home directory:

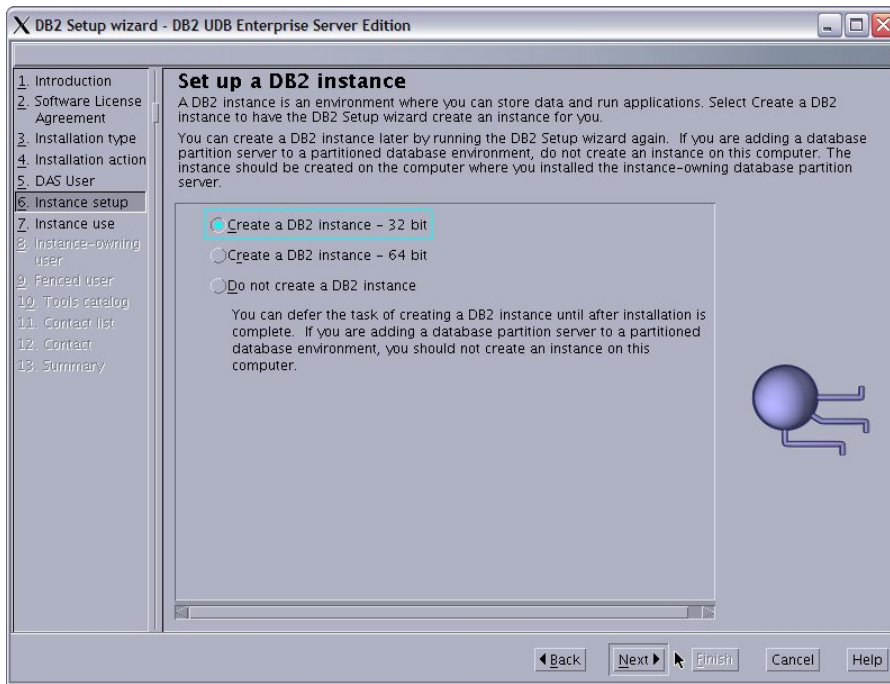
☐ Existing user

User name:

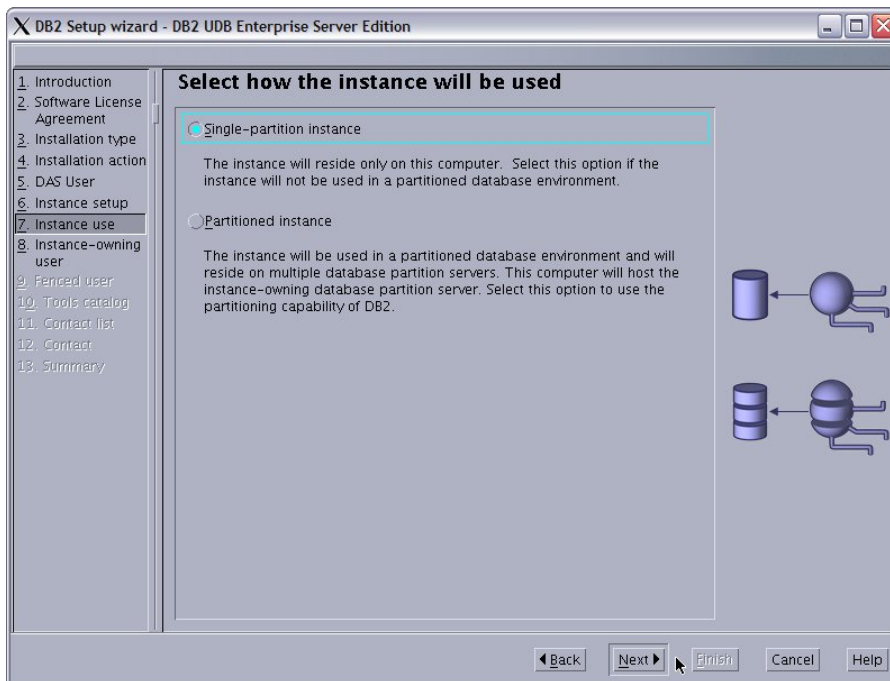
For users of NIS or similar management systems
If the user information in your environment is managed remotely by NIS or a similar system, you must specify an existing user.

◀ Back Next ▶ Finish Cancel Help

- Accept the default values for the User Name and Group Name that will run DB2 Administration Server. These are dasusr1 and dasadm1 respectively. Enter and confirm the password for the user (e.g. passw0rd).



- Select "Create a DB2 instance" by selecting either the 32-bit or 64-bit option depending on the hardware you are using. Click "Next".



- Select “Single-partition instance” and click “Next”.

DB2 Setup wizard - DB2 UDB Enterprise Server Edition

Set user information for the DB2 instance owner
Specify the instance-owning user information for the DB2 instance. DB2 will use this user to perform instance functions, and will store instance information in the user's home directory. The name of the instance will be the same as the user name. You can create a new user or use an existing one.

☒ **New user**

User name:

UID: ☒ Use default UID

Group name:

GID: ☒ Use default GID

Password:

Confirm password:

Home directory:

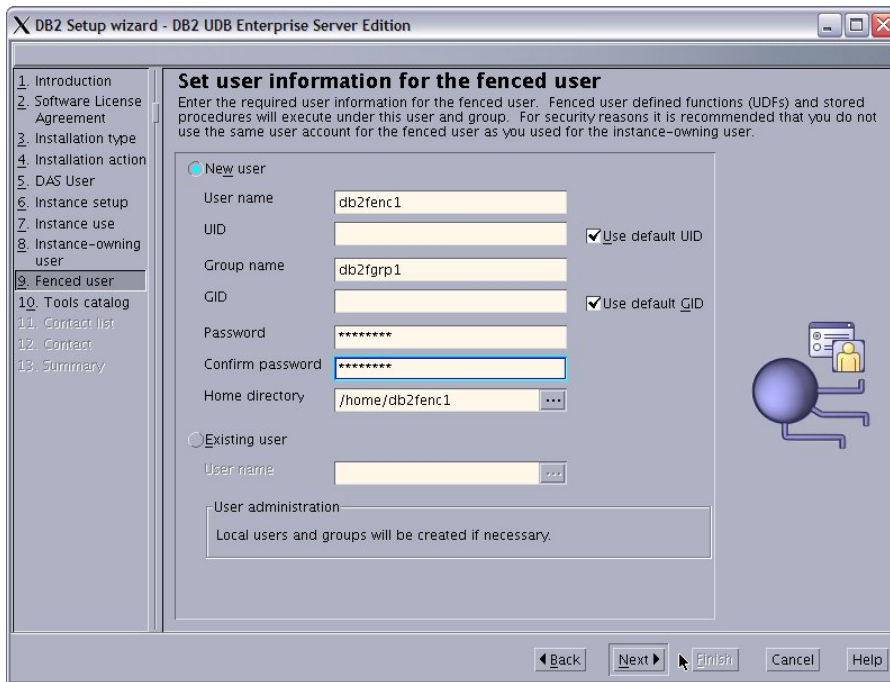
☐ **Existing user**

User name:

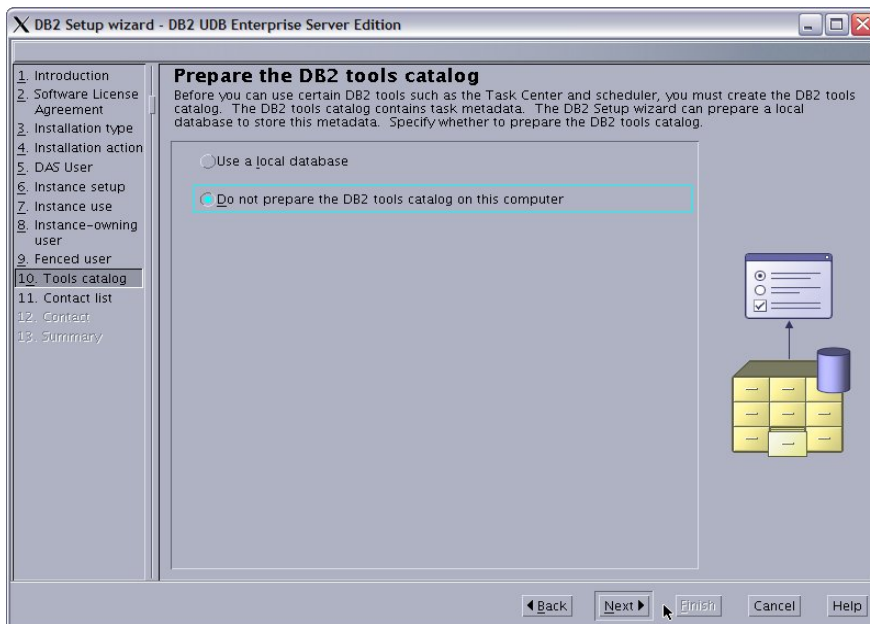
For users of NIS or similar management systems
If the user information in your environment is managed remotely by NIS or a similar system, you must specify an existing user.

Navigation buttons: Back, Next, Finish, Cancel, Help

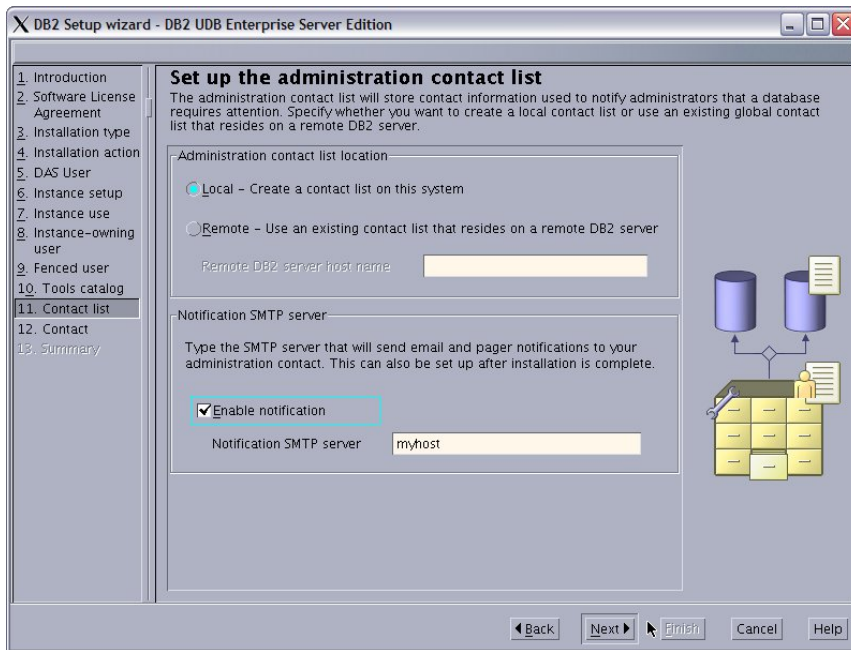
- On the next screen: Provide user information for the DB2 instance owner:
 - o User = db2inst1, Group = db2grp1
 - o Enter password and confirm password (e.g. passw0rd)



- On the next screen: Provide user information for the fenced user
 - User = db2fenc1, group = db2fgrp1
 - Enter password and confirm password (e.g. passw0rd)



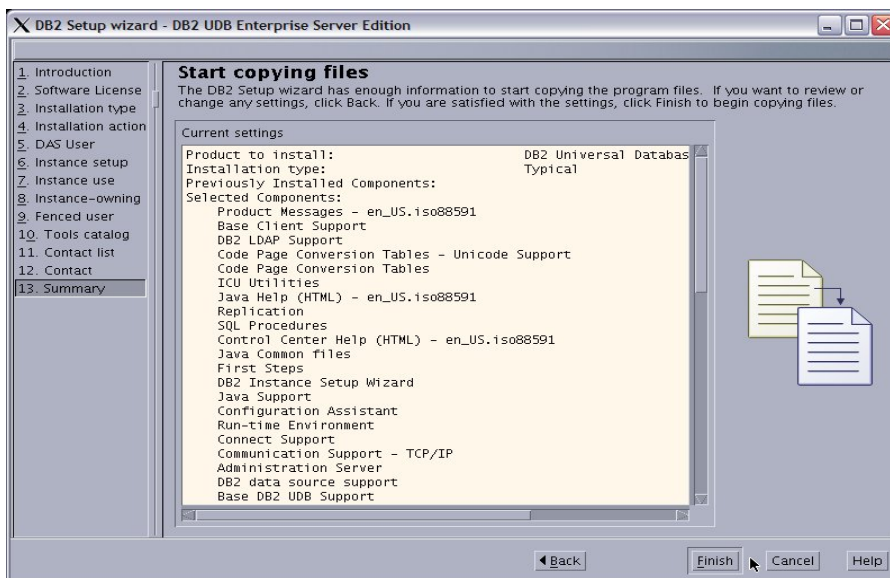
- Select "Do not prepare the DB2 tools catalog on this computer" and click "Next"



- On the next screen:
 - Select: Local - create a contact list on this system
 - Select: Enable notification and enter the server name for notification (e.g. **myhost**)



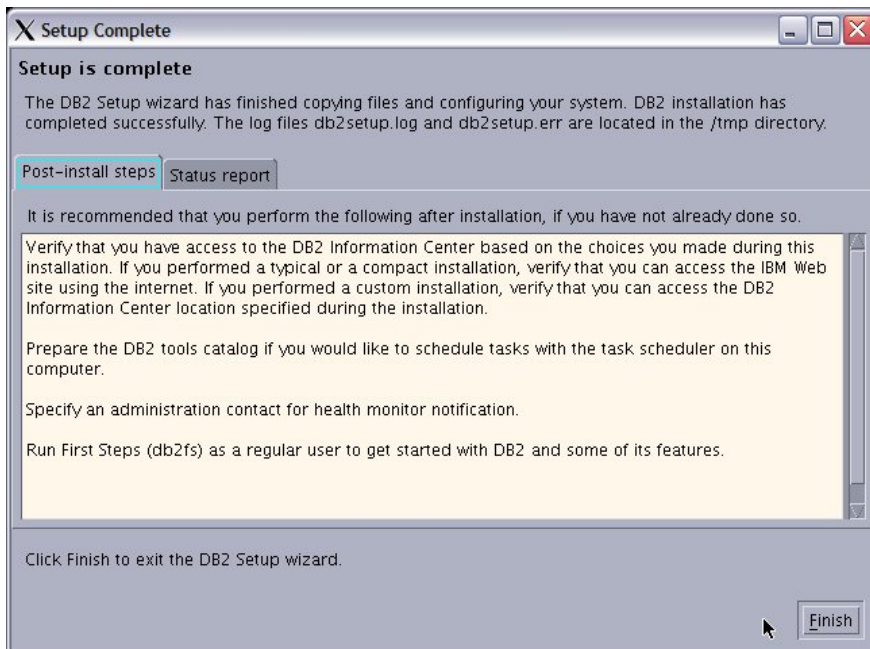
- On the next screen you can select “Defer this task until after installation is complete” and click “Next”. You will be presented with a summary screen where you can review the selected installation options.



- Click “Finish” to commence the installation. You will see a progress screen.



When the installation is completed you will get this screen:



Click on the Status Report tab to review the installation log file. Make sure there are no errors reported before proceeding. Originally, I had missing AIX PTFs which prevented Java 1.4 from being installed. This version of Java is required by DB2 First Steps and DB2 Command Center. One way around this problem is to create a symbolic link /usr/java14 pointing to /usr/java130.

```
# ln -s /usr/java130 /usr/java14
```

Click "Finish".

You can now follow a few steps to verify that DB2 installed successfully.

2.1.2 Check the DB2 installation

1. Check that **db2inst1**, **db2fenc1** and **dasusr1** users and **db2grp1**, **db2fgrp1** and **dasadm1** groups have been created successfully.

```
# pg /etc/passwd  
# pg /etc/group
```

2. Check the DB2 installation directory

```
# cd /usr/opt/db2_08_01
```

There should be loads of files there.

3. Check the installation directory for the db2inst1 instance

```
# su - db2inst1  
$ cd sqllib
```

There should be content there.

4. Run DB2 First Steps to create a sample database

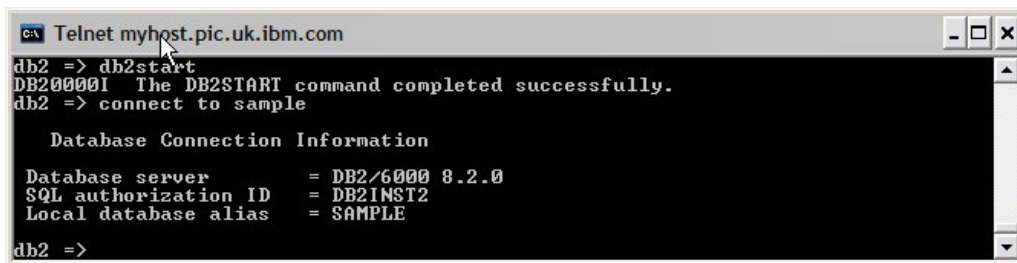
```
$ cd /usr/opt/db2_08_01/bin  
$ ./db2fs
```

Select the "Create Sample Database" option to create a Sample UDB Database.

Now you can test the sample database

```
$ cd /usr/opt/db2_08_01/bin/db2 - this starts a db2 command window
```

```
db2 => db2start  
db2 => connect to sample
```

A screenshot of a Telnet window titled 'Telnet myhost.pic.uk.ibm.com'. The window shows a command prompt 'db2 =>' where the user has entered 'db2start'. The output is 'DB20000I The DB2START command completed successfully.' followed by another 'db2 =>' prompt where the user has entered 'connect to sample'. Below this, the 'Database Connection Information' is displayed: 'Database server = DB2/60000 8.2.0', 'SQL authorization ID = DB2INST2', and 'Local database alias = SAMPLE'. The prompt 'db2 =>' is visible at the bottom of the window.

```
C:\ Telnet myhost.pic.uk.ibm.com  
db2 => db2start  
DB20000I The DB2START command completed successfully.  
db2 => connect to sample  
  
Database Connection Information  
Database server      = DB2/60000 8.2.0  
SQL authorization ID = DB2INST2  
Local database alias = SAMPLE  
db2 =>
```

```
db2 => list db directory  
db2 => list tables  
db2 => disconnect sample
```

2.2 Installation of Tivoli Security Compliance Manager Server V 5.1

2.2.1 Base ITSCM Server Installation

For Details see:

Tivoli® Security Compliance Manager Installation Guide: All Component Version 5.1

http://publib.boulder.ibm.com/tividd/td/ITSCM/GC32-1592-00/en_US/PDF/scm51_install.pdf

Make sure DB2 is up and running.

```
# su - db2inst1
```

```
$ db2start
```

The Installation Guide recommends that the non-graphical mode is used if the installation is performed from a remote host. This is because the installation program does not run correctly with some window managers when run remotely.

Hence, we will invoke the installation program with the `-console` option.

Go to the directory which contains the ITSCM installation code and execute:

```
# ./scm_aix -console
```

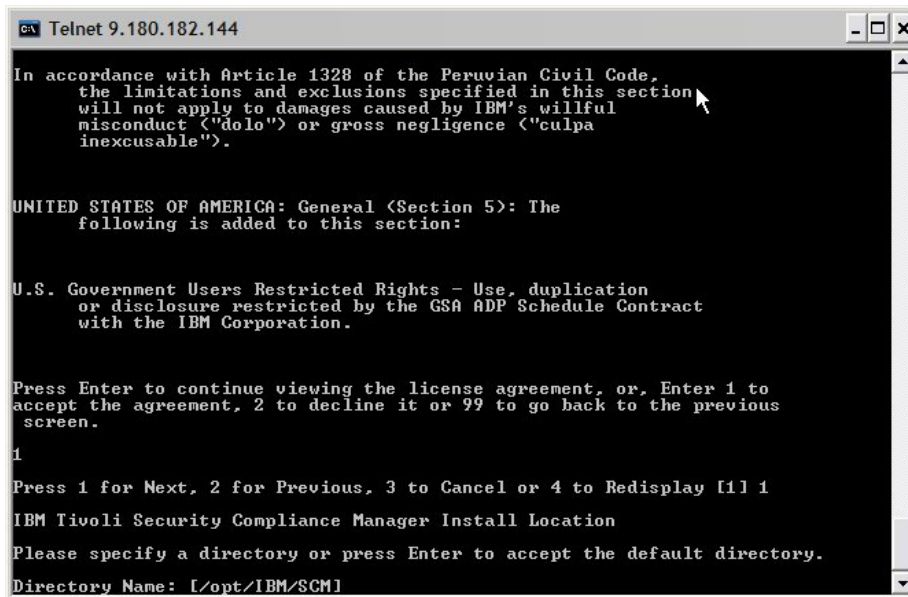
```
C:\ Telnet 9.180.182.144
Initializing InstallShield Wizard...
Preparing Java(tm) Virtual Machine...
.....
Select a language to be used for this wizard.

[ ] 1 - German
[X] 2 - English
[ ] 3 - French
[ ] 4 - Italian
[ ] 5 - Japanese
[ ] 6 - Korean
[ ] 7 - Portuguese <Brazil>
[ ] 8 - Simplified Chinese
[ ] 9 - Spanish
[ ] 10 - Traditional Chinese

To select an item enter its number, or 0 when you are finished: [0]
```

Select the language you wish to use during the installation, e.g. English and press <Enter>.

After you accept the license agreement you will be presented with the following screen.



```
Telnet 9.180.182.144

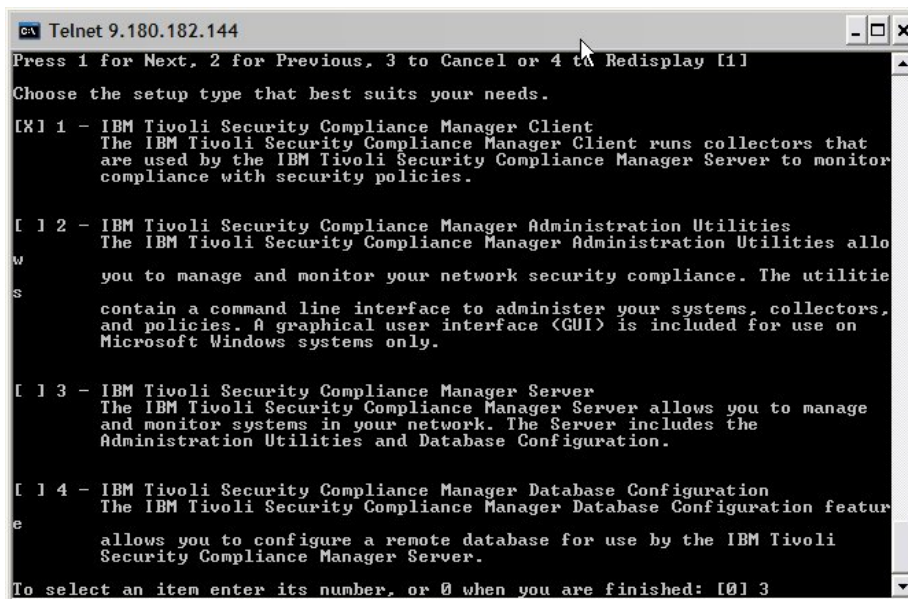
In accordance with Article 1328 of the Peruvian Civil Code,
the limitations and exclusions specified in this section
will not apply to damages caused by IBM's willful
misconduct ("dolo") or gross negligence ("culpa
inexcusable").

UNITED STATES OF AMERICA: General (Section 5): The
following is added to this section:

U.S. Government Users Restricted Rights - Use, duplication
or disclosure restricted by the GSA ADP Schedule Contract
with the IBM Corporation.

Press Enter to continue viewing the license agreement, or, Enter 1 to
accept the agreement, 2 to decline it or 99 to go back to the previous
screen.
1
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1] 1
IBM Tivoli Security Compliance Manager Install Location
Please specify a directory or press Enter to accept the default directory.
Directory Name: [/opt/IBM/SCM]
```

Accept the default installation directory by pressing <Enter>. Then enter "1" to go to the next screen.



```
Telnet 9.180.182.144

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
Choose the setup type that best suits your needs.

[ X ] 1 - IBM Tivoli Security Compliance Manager Client
The IBM Tivoli Security Compliance Manager Client runs collectors that
are used by the IBM Tivoli Security Compliance Manager Server to monitor
compliance with security policies.

[ ] 2 - IBM Tivoli Security Compliance Manager Administration Utilities
The IBM Tivoli Security Compliance Manager Administration Utilities allow
you to manage and monitor your network security compliance. The utilities
contain a command line interface to administer your systems, collectors,
and policies. A graphical user interface (GUI) is included for use on
Microsoft Windows systems only.

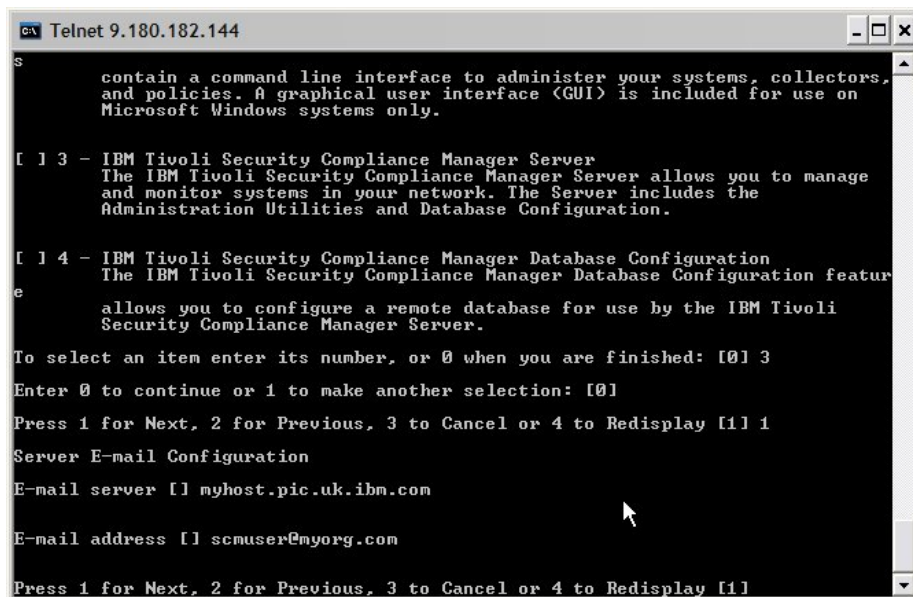
[ ] 3 - IBM Tivoli Security Compliance Manager Server
The IBM Tivoli Security Compliance Manager Server allows you to manage
and monitor systems in your network. The Server includes the
Administration Utilities and Database Configuration.

[ ] 4 - IBM Tivoli Security Compliance Manager Database Configuration
The IBM Tivoli Security Compliance Manager Database Configuration feature
allows you to configure a remote database for use by the IBM Tivoli
Security Compliance Manager Server.

To select an item enter its number, or 0 when you are finished: [0] 3
```

Now select the correct package to install. The default option is “1” IBM Tivoli Security Compliance Manager Client. Make sure you change this to IBM Tivoli Security Compliance Manager Server by typing “3” and hitting <Enter>. Then enter “0” to continue, and “1” to go to the next screen.

Now you have the option to enter the E-mail server and E-mail address. An example is given below:



```

c:\ Telnet 9.180.182.144
s
    contain a command line interface to administer your systems, collectors,
    and policies. A graphical user interface <GUI> is included for use on
    Microsoft Windows systems only.

[ 1 3 - IBM Tivoli Security Compliance Manager Server
    The IBM Tivoli Security Compliance Manager Server allows you to manage
    and monitor systems in your network. The Server includes the
    Administration Utilities and Database Configuration.

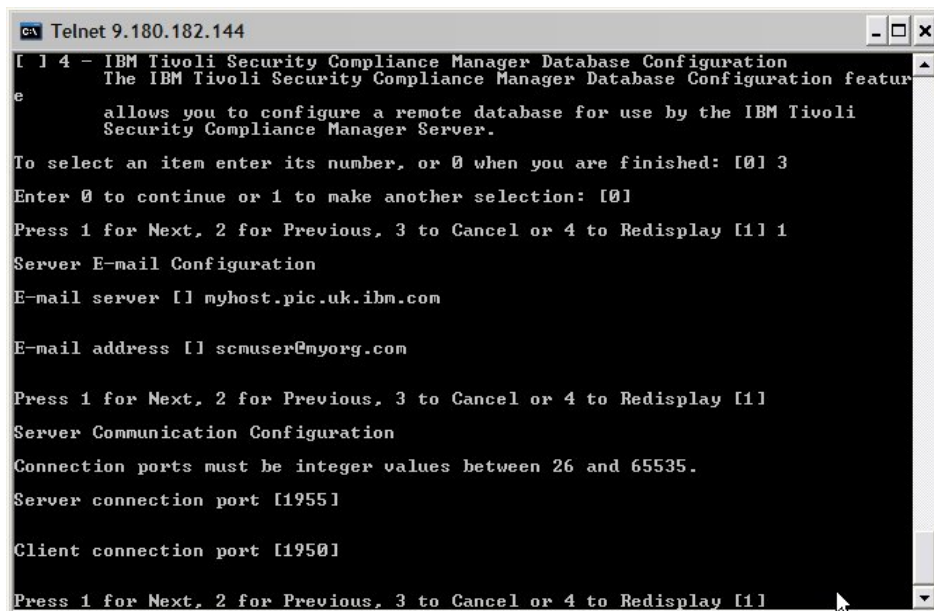
[ 1 4 - IBM Tivoli Security Compliance Manager Database Configuration
    The IBM Tivoli Security Compliance Manager Database Configuration featur
    e
    allows you to configure a remote database for use by the IBM Tivoli
    Security Compliance Manager Server.

To select an item enter its number, or 0 when you are finished: [0] 3
Enter 0 to continue or 1 to make another selection: [0]
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1] 1
Server E-mail Configuration
E-mail server [1] myhost.pic.uk.ibm.com
E-mail address [1] scmuser@myorg.com
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]

```

Enter “1” to go to the next screen.

Accept the defaults for the Server connection port (i.e. 1955) and Client connection port (i.e. 1950).



```

c:\ Telnet 9.180.182.144
[ 1 4 - IBM Tivoli Security Compliance Manager Database Configuration
    The IBM Tivoli Security Compliance Manager Database Configuration featur
    e
    allows you to configure a remote database for use by the IBM Tivoli
    Security Compliance Manager Server.

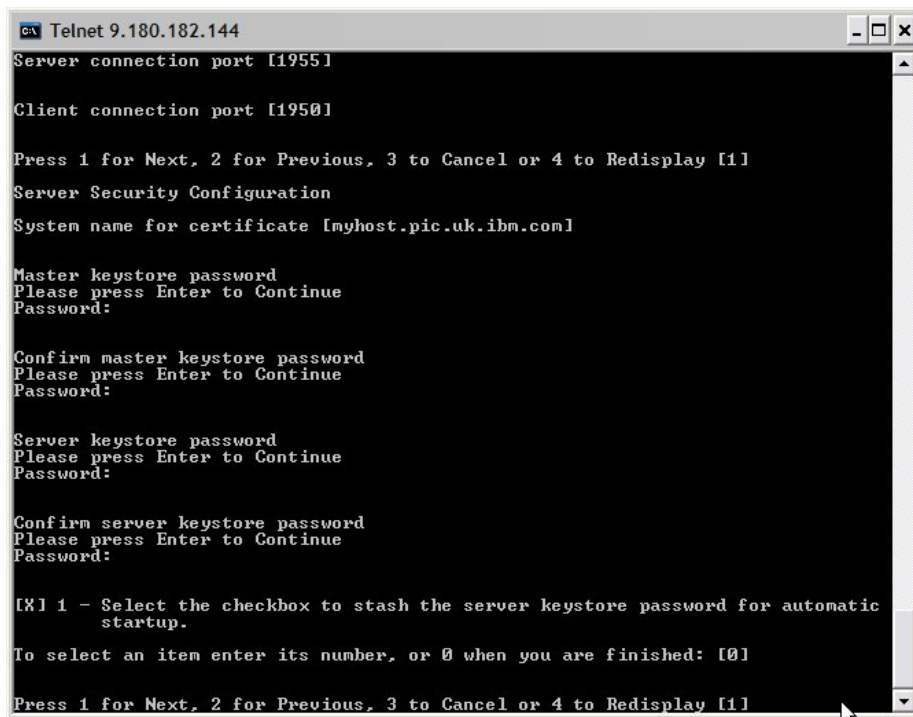
To select an item enter its number, or 0 when you are finished: [0] 3
Enter 0 to continue or 1 to make another selection: [0]
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1] 1
Server E-mail Configuration
E-mail server [1] myhost.pic.uk.ibm.com
E-mail address [1] scmuser@myorg.com

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
Server Communication Configuration
Connection ports must be integer values between 26 and 65535.
Server connection port [1955]
Client connection port [1950]
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]

```

Enter “1” to go to the next screen.

Now you must enter your choices for Server Security Configuration. An example is given below. All passwords are *passw0rd*.



```
ca Telnet 9.180.182.144
Server connection port [1955]
Client connection port [1950]
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
Server Security Configuration
System name for certificate [myhost.pic.uk.ibm.com]
Master keystore password
Please press Enter to Continue
Password:
Confirm master keystore password
Please press Enter to Continue
Password:
Server keystore password
Please press Enter to Continue
Password:
Confirm server keystore password
Please press Enter to Continue
Password:
[X] 1 - Select the checkbox to stash the server keystore password for automatic
      startup.
To select an item enter its number, or 0 when you are finished: [0]
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
```

Enter “1” to go to the next screen. Now you will enter:

- the database location – this should be set to local
- database user id – this should be **db2inst1**. Note the “deliberate” mistake in the screenshot, where this value was entered as **db2inst2**. As I installed and uninstalled DB2 several times for the purposes of writing this cookbook, at one point in time I had to create a new instance and user id called **db2inst2**. You should specify the correct instance owner which in your case will probably be **db2inst1**.
- Database user id password – in our case this is **passw0rd**.
- Leave the database location as blank. The default location (**/home/db2inst1**) will be assumed.
- Select the option to create the database now.

A screen capture with these choices is given below:

```
CA Telnet 9.180.182.144

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
Database Location
Specify where your database is located:
[X] 1 - The database is on the local system.
[ ] 2 - The database is on a remote system.
To select an item enter its number, or 0 when you are finished: [0]

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1] 1
Database Configuration
Database user ID [db2inst1] db2inst2

Database user ID password
Please press Enter to Continue
Password:

Confirm password
Please press Enter to Continue
Password:

Database Location [ ]

[X] 1 - Select the checkbox to create your database now.
To select an item enter its number, or 0 when you are finished: [0]

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
```

Enter “1” to go to the next screen. Now you will enter data for the primary ITSCM administrator. For example,

- System Administrator User ID – **admin**
- System Administrator User ID password – **passw0rd**

```
Telnet 9.180.182.144
Database user ID password
Please press Enter to Continue
Password:

Confirm password
Please press Enter to Continue
Password:

Database Location []

[X] 1 - Select the checkbox to create your database now.
To select an item enter its number, or 0 when you are finished: [0]

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1] 1

Administrator User ID Configuration
<HTML>The user information below is for the primary administrator of the IBM
Tivoli Security Compliance Manager deployment.</HTML>

System administrator user ID [admin]

System administrator user password
Please press Enter to Continue
Password:

Confirm password
Please press Enter to Continue
Password:

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
```

Enter "1" to go to the next screen. This will display the summary of what will be installed and upon confirmation the installation will commence. A progress screen will be displayed during the installation.

```
Telnet 9.180.182.144

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
IBM Tivoli Security Compliance Manager will be installed in the following
location:
/opt/IBM/SCM
with the following features:
IBM Tivoli Security Compliance Manager Administration Utilities
IBM Tivoli Security Compliance Manager Server
IBM Tivoli Security Compliance Manager Database Configuration
for a total size:
62 MB
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
Installing IBM Tivoli Security Compliance Manager. Please wait...
0 % complete
10 % complete
20 % complete
30 % complete
40 % complete
50 % complete
60 % complete
70 % complete
80 % complete
90 % complete
100 % complete

Creating uninstaller...
Configuring IBM Tivoli Security Compliance Manager Server...
0 % complete
20 % complete
100 % complete

Configuring IBM Tivoli Security Compliance Manager Database...
0 % complete
10 % complete
20 % complete
30 % complete
80 % complete
100 % complete

The InstallShield Wizard has successfully installed IBM Tivoli Security
Compliance Manager. Choose Finish to exit the wizard.
Press 3 to Finish or 4 to Redisplay [3]
```

Enter "3" to Finish.

This completes the installation of ITSCM Server.

2.2.2 Verify the ITSCM Server installation

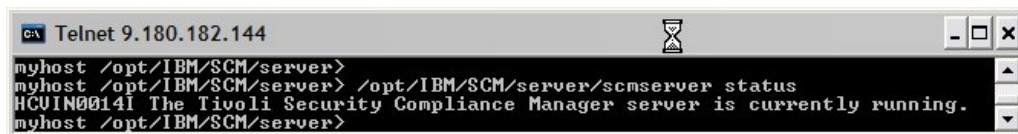
Verify that the ITSCM database has been created. The database is called **JAC**.

```
# su - db2inst1
$ db2 list db directory
```

Also, check the ITSCM server status:

```
# /opt/IBM/SCM/server/scmserver status
```

If you get a message similar to this, all is well:

A screenshot of a Telnet window titled 'Telnet 9.180.182.144'. The window shows a command prompt where the user enters the command '/opt/IBM/SCM/server/scmserver status'. The output of the command is 'HCUIN00141 The Tivoli Security Compliance Manager server is currently running.'.

```
myhost /opt/IBM/SCM/server>  
myhost /opt/IBM/SCM/server> /opt/IBM/SCM/server/scmserver status  
HCUIN00141 The Tivoli Security Compliance Manager server is currently running.  
myhost /opt/IBM/SCM/server>
```

Apart from **status**, other useful options of the **ITSCMserver** command to remember are: **start**, **stop** and **version**.

2.3 Installation of Tivoli Security Compliance Manager Client V 5.1

2.3.1 Base ITSCM Client Installation

For Details see:

Tivoli® Security Compliance Manager Installation Guide: All Component Version 5.1

http://publib.boulder.ibm.com/tividd/td/ITSCM/GC32-1592-00/en_US/PDF/scm51_install.pdf

To install ITSCM Client on AIX we will use the *-console* mode for the same reasons as before. The first few installation steps are similar to installing the ITSCM Server.

Go to the directory which contains the ITSCM installation code and execute:

```
# ./scm_aix -console
```



```
Telnet 9.180.182.144
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1] 1
Choose the setup type that best suits your needs.

[X] 1 - IBM Tivoli Security Compliance Manager Client
The IBM Tivoli Security Compliance Manager Client runs collectors that
are used by the IBM Tivoli Security Compliance Manager Server to monitor
compliance with security policies.

[ ] 2 - IBM Tivoli Security Compliance Manager Administration Utilities
The IBM Tivoli Security Compliance Manager Administration Utilities allow
you to manage and monitor your network security compliance. The utilities
contain a command line interface to administer your systems, collectors,
and policies. A graphical user interface <GUI> is included for use on
Microsoft Windows systems only.

[ ] 3 - IBM Tivoli Security Compliance Manager Server
The IBM Tivoli Security Compliance Manager Server allows you to manage
and monitor systems in your network. The Server includes the
Administration Utilities and Database Configuration.

[ ] 4 - IBM Tivoli Security Compliance Manager Database Configuration
The IBM Tivoli Security Compliance Manager Database Configuration feature
allows you to configure a remote database for use by the IBM Tivoli
Security Compliance Manager Server.

To select an item enter its number, or 0 when you are finished: [0]
```

Accept the default option to install: "1" IBM Tivoli Security Compliance Manager Client.
Then enter "0" to continue, and "1" to go to the next screen.

```
Telnet 9.180.182.144
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1] 1
Client Communication Mode Configuration
Connection ports must be integer values between 26 and 65535.
Client connection port [1950]

Client communication mode:
[X] 1 - Push <Communication can be initiated by either the client or the server>
[ ] 2 - Pull <Communication is initiated only by the server>

To select an item enter its number, or 0 when you are finished: [0]
```

Accept the default value (1950) for the Client connection port.
For the Client communication mode, select **Push**, end then enter 0.

Now you can enter Server Communication Information.

Enter the Server host name, for example **myhost.pic.uk.ibm.com** .
For the Server connection port just accept the default value, **1951** .

Depending on whether the client uses DHCP select the appropriate box.

Then enter "1" to commence the installation.

```
Telnet 9.180.182.144

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1] 1
Server Communication Configuration
Server host name [1] myhost.pic.uk.ibm.com
Server connection port [19511]

[ ] 1 - Select the checkbox if this client uses DHCP.
To select an item enter its number, or 0 when you are finished: [0]

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1] 1
IBM Tivoli Security Compliance Manager will be installed in the following
location:
/opt/IBM/SCM
with the following features:
IBM Tivoli Security Compliance Manager Client
for a total size:
10.6 MB
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
```

The progress of the installation process will be reported as follows:

```
Telnet 9.180.182.144

IBM Tivoli Security Compliance Manager will be installed in the following
location:
/opt/IBM/SCM
with the following features:
IBM Tivoli Security Compliance Manager Client
for a total size:
10.6 MB
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
Installing IBM Tivoli Security Compliance Manager. Please wait...
0 % complete
10 % complete
20 % complete
30 % complete
40 % complete
50 % complete
60 % complete
70 % complete
80 % complete

The InstallShield Wizard has successfully installed IBM Tivoli Security
Compliance Manager. Choose Finish to exit the wizard.
Press 3 to Finish or 4 to Redisplay [3]
```

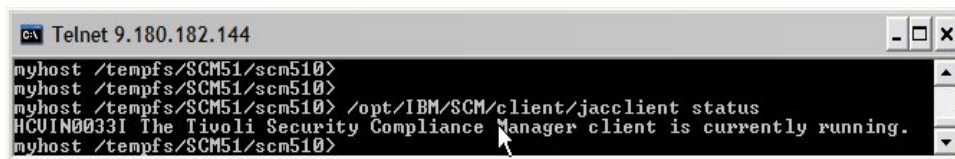
Enter "3" to finish the installation.

2.3.2 Verify the ITSCM Client installation

Check the ITSCM client status:

```
# /opt/IBM/SCM/client/jacclient status
```

If you get a message similar to this, all is well:

A screenshot of a Telnet window titled 'Telnet 9.180.182.144'. The window shows a command prompt with the following text:

```
myhost /tempfs/SCM51/scm510>  
myhost /tempfs/SCM51/scm510>  
myhost /tempfs/SCM51/scm510> /opt/IBM/SCM/client/jacclient status  
HCUIN0033I The Tivoli Security Compliance Manager client is currently running.  
myhost /tempfs/SCM51/scm510>
```

Apart from **status**, other useful options for the **jacclient** command to remember are: **start**, **stop**, **version**, and **restart**.

3 Installation of the IBM Tivoli Security Compliance Manager on SLES 8

3.1 Installation of IBM DB2 UDB 8.1 Server

3.1.1 Base DB2 Installation

Prepare an X11 environment, (Xwindows environment) and allow access control for x-clients on your X-desktop eg at root (#) prompt. **It is important that you are logged in as root.**

```
# xhost +          <enter>
```

At this point it is probably a good idea to copy the DB2 installation image into a temporary directory somewhere (eg /tmp/db2) so that the install processes can write temporary files

If you need to mount your CD, the easiest way is either to use yast2 (admin tool), or (once CD is in the CDROM drive) type:

```
# mount /cdrom (it assumes a default CDROM device file system setup in /etc/fstab)
```

Go to the directory that contains the db2setup command. (alternatively – from the /tmp/db2 directory, launch the db2setup command from the full path to the CD. viz.)

```
# /cdrom/009_ESE_LNX_32_NLV_1/db2setup <enter>
```

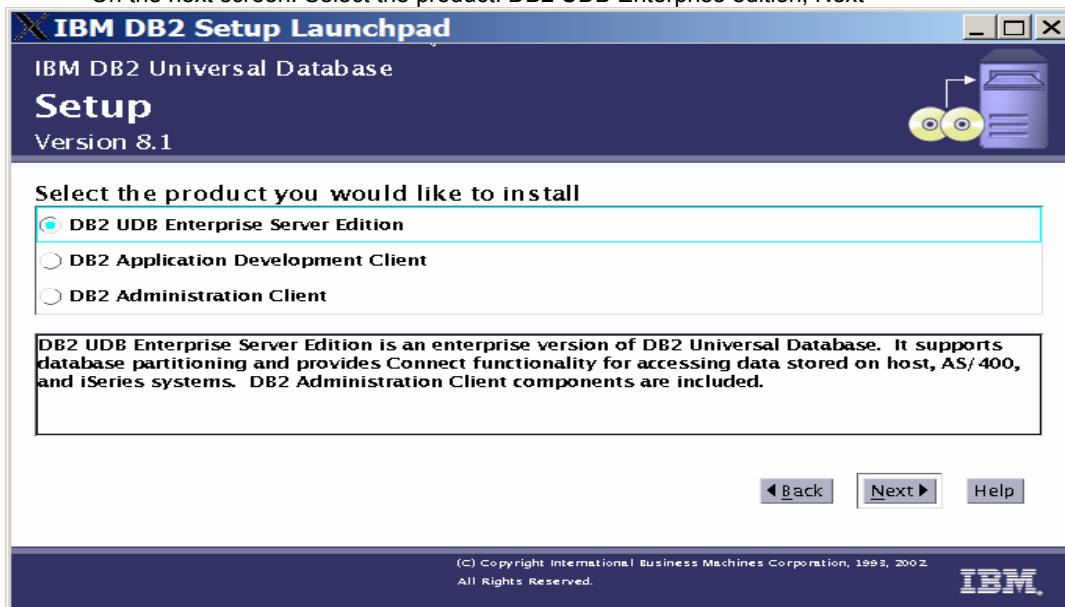
```
# ./db2setup <enter>:
```

```

xterm
suse8linux:/tmp/009_ESE_LNX_32_NLV # 1
total 101
drwxr-xr-x  5 root  root    432 Oct 29 2002 ./
drwxrwxrwt 13 root  root    528 Nov  2 23:50 ../
drwxr-xr-x  5 root  root    192 Oct 29 2002 db2/
-rwxr-xr-x  1 root  root   4529 Oct 29 2002 db2_deinstall*
-rwxr-xr-x  1 root  root   4557 Oct 29 2002 db2_install*
-r-xr-xr-x  1 root  root   4672 Oct 29 2002 db2setup*
drwxr-xr-x 14 daemon bin     336 Oct 29 2002 doc/
drwxr-xr-x  3 daemon bin     72 Oct 29 2002 doc.cmn/
-rw-r--r--  1 daemon bin   7572 Oct 29 2002 readme.cn
-rw-r--r--  1 daemon bin   9260 Oct 29 2002 readme.jp
-rw-r--r--  1 daemon bin   8851 Oct 29 2002 readme.kr
-rw-r--r--  1 daemon bin  11450 Oct 29 2002 readme.pl
-rw-r--r--  1 daemon bin  10870 Oct 29 2002 readme.ru
-rw-r--r--  1 daemon bin   7646 Oct 29 2002 readme.tw
-rw-r--r--  1 daemon bin  10845 Oct 29 2002 readme.txt
suse8linux:/tmp/009_ESE_LNX_32_NLV # ./db2setup
DBI1190I db2setup is preparing the DB2 Setup Wizard which will
        guide you through the program setup process. Please
        wait.

```

- Accept the Welcome screen, Next
- On the next screen: Select the product: DB2 UDB Enterprise edition, Next



- On the next screen: Select Next on the "Welcome to the DB2 setup wizard" screen
- On the next screen: Accept the licence agreement, Next
- On the next screen: Select the installation type: typical, Next



- On the next screen: Select Install DB2 UDB Enterprise Server Edition on this computer, Next
- On the next screen: Provide user information for the DB2 Administration server:
User = dasusr1, Group = dasadm1

DB2 Setup wizard - DB2 UDB Enterprise Server Edition

1. Introduction
 2. Software Licen...
 3. Installation type
 4. Installation acti...
5. DAS User
 6. Instance setup
 7. Instance use
 8. Instance-owni...
 9. Fenced user
 10. Tools catalog
 11. Contact list
 12. Contact
 13. Summary

Set user information for the DB2 Administration Server

The DB2 Administration Server (DAS) runs on your computer to provide support required by the DB2 tools. A user account with a minimal set of privileges is required to run the DAS. Specify the required user information for the DAS.

☒ **New user**

User name:

UID: ☒ Use default UID

Group name:

GID: ☒ Use default GID

Password:

Confirm password:

Home directory: ...

☐ **Existing user**

User name: ...

For users of NIS or similar management systems
 If the user information in your environment is managed remotely by NIS or a similar system, you must specify an existing user.

Back Next Finish Cancel Help

- On the next screen: Select Create DB2 Instance, Next
- On the next screen: Select Single-partition instance, Next

- On the next screen: Provide user information for the DB2 instance owner:
 - User = db2inst1, Group = db2grp1
 - Enter password and confirm password (e.g. passw0rd)

DB2 Setup wizard - DB2 UDB Enterprise Server Edition

Set user information for the DB2 instance owner

Specify the instance-owning user information for the DB2 instance. DB2 will use this user to perform instance functions, and will store instance information in the user's home directory. The name of the instance will be the same as the user name. You can create a new user or use an existing one.

☒ **New user**

User name:

UID: ☒ Use default UID

Group name:

GID: ☒ Use default GID

Password:

Confirm password:

Home directory:

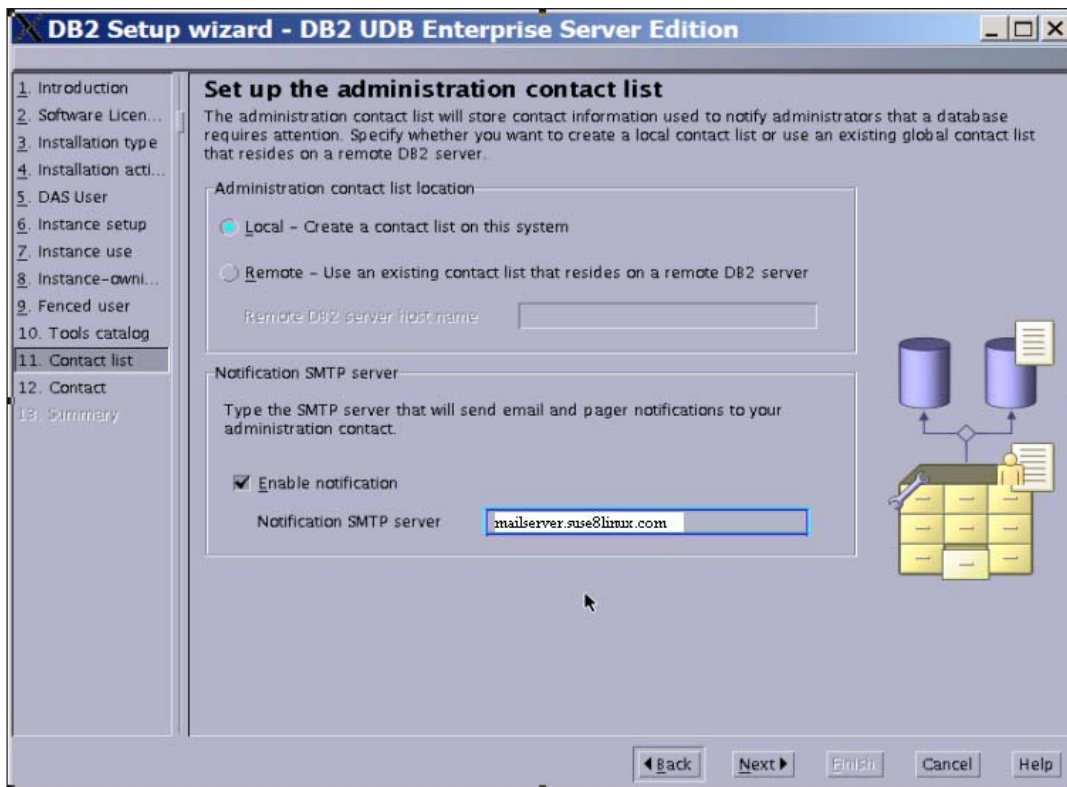
☐ **Existing user**

User name:

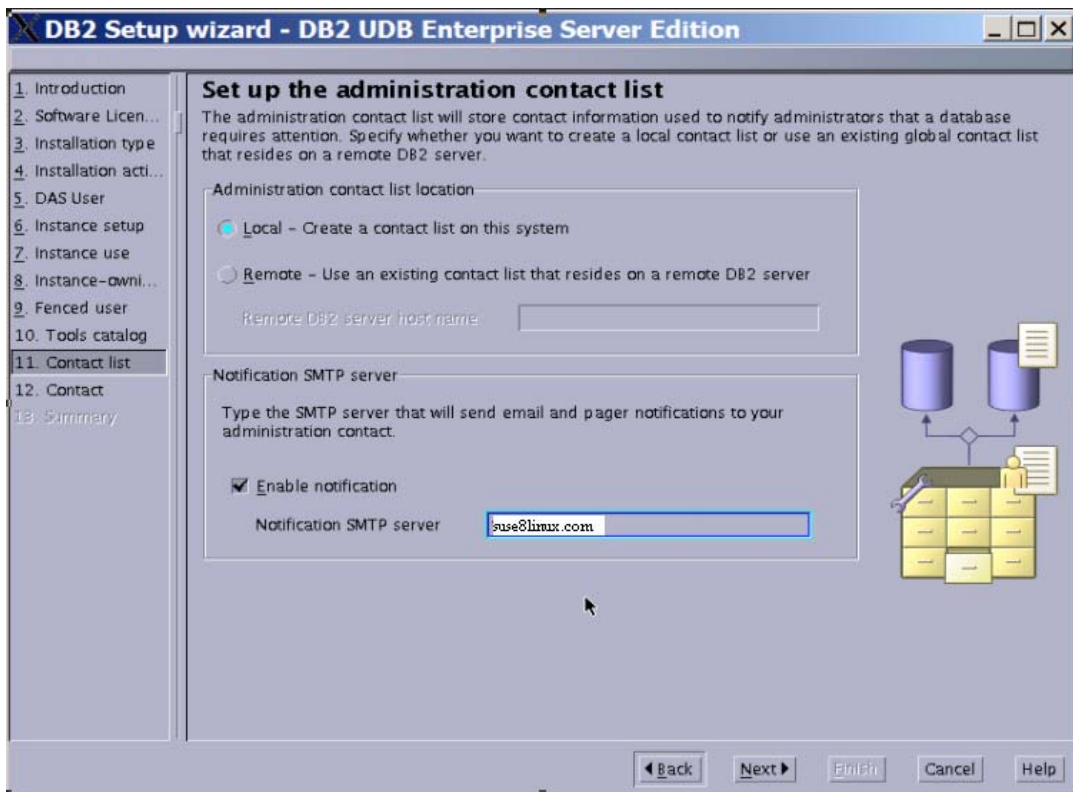
For users of NIS or similar management systems—
If the user information in your environment is managed remotely by NIS or a similar system, you must specify an existing user.

Navigation buttons: Back, Next, Finish, Cancel, Help

- On the next screen: Provide user information for the fenced user
 - User = db2fenc1, group = db2fgrp1
 - Enter password and confirm password (e.g. passw0rd)

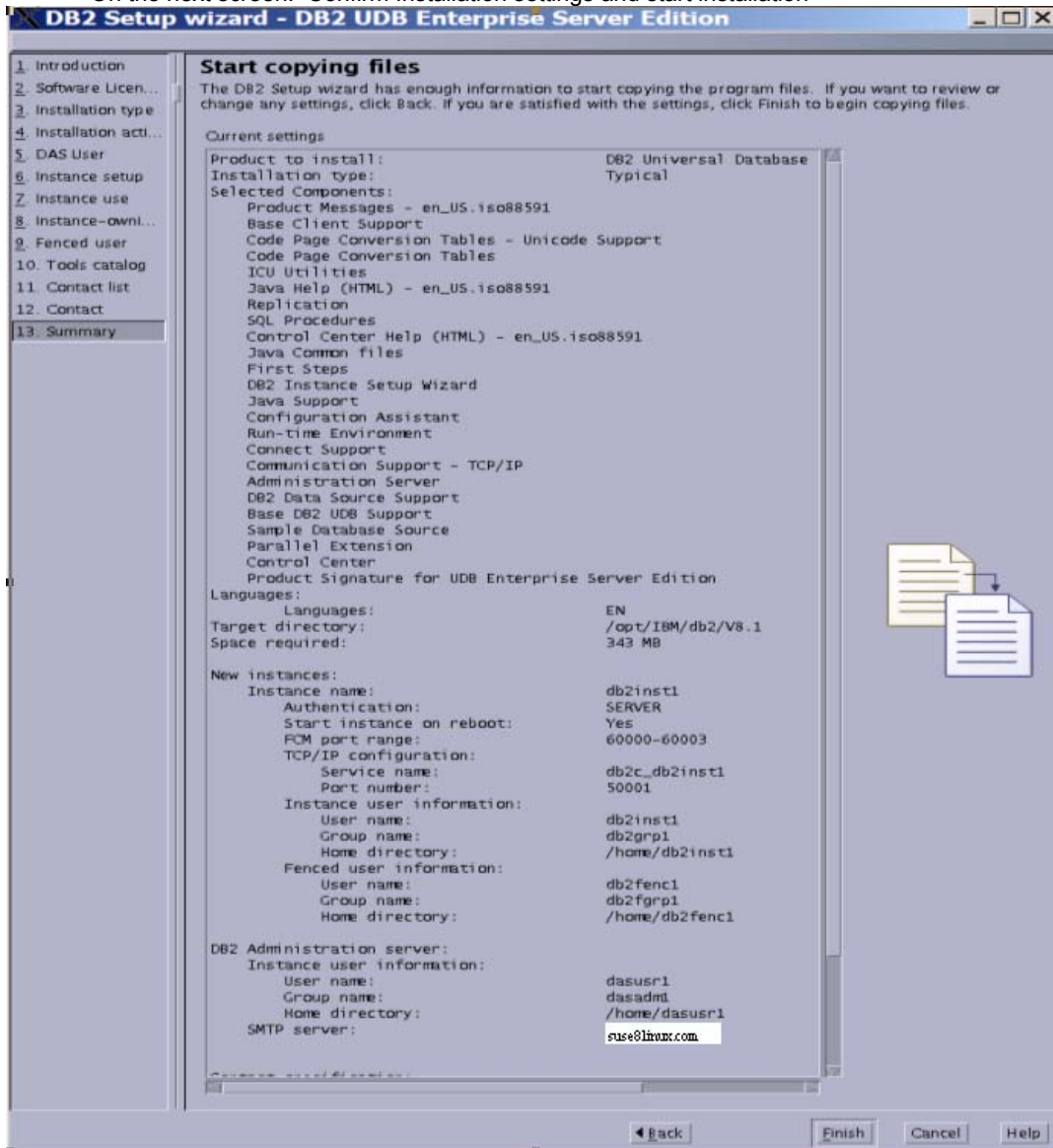


- On the next screen: select Do not Prepare the DB2 tools catalogue, Next
- On the next screen: e.g. mailserver.suse8linux.com
 - select Local , create a contact list on this system
 - select enable notification, set server name for notification



- On the next screen: Specify a contact for health monitor notification

- On the next screen: Confirm Installation settings and start installation



3.1.2 Installation of DB2 8.2 (ie 8.1 Fixpack 7a)

It is strongly recommended to have the Fixpack 7a Readme available .
For detailed instructions see Fixpack Readme.

Installation of IBM DB2 Universal Database Version 8.2 (= Version 8.1 FP7a)

Prepare Installation

Verify, that DB2 Version 8.1 is already installed

```
# rpm -qa | grep db2 | grep db2cliv81
IBM_db2cliv81-8.1.0-0
```

Stop all DB2-processes

```
# su - db2inst1
$ . $HOME/sqllib/db2profile
$ db2 force applications all
    DB20000I The FORCE APPLICATION command completed successfully.
    DB21024I This command is asynchronous .....effective immediately.
$ db2 terminate
    DB20000I The TERMINATE command completed successfully.
$ db2stop
    10-14-2004 17:53:29 0 0 SQL1064N DB2STOP .....was successful.
    SQL1064N DB2STOP processing was successful.
$ db2licd -end
```

Call the following commands:

```
# su - dasusr1
$. $HOME/das/dasprofile
$ db2admin stop
    SQL4407W The DB2 Admi...Server was stopped successfully.
$ exit
$ logout
```

Stop all Instances, stop the Fault Monitor, you must switch back out to root (above)
Stop the Fault Monitor Coordinator and the Fault Monitor:

```
# db2fmcu -d
# db2fm -d
```

Execute the following:

```
# su - db2inst1
$ $HOME/sqllib/bin/ipclean
/home/db2inst1/sqllib/bin/ipclean: Removing DB2 engine and
client's
                                IPC resources for db2inst1.
```

Installation of FP 7a (Version 8.2)

Switch to root

Change to the fixpack directory and call:

```
suse8linux:/code #
```

```
suse8linux:/code # ./installFixPak -y
```

```

Updating ...
Updating to IBM_db2msen81-8.1.0-72.i386.rpm ...
IBM_db2msen81 #####
Updating to IBM_db2cliv81-8.1.0-72.i386.rpm ...
IBM_db2cliv81 #####
Updating to IBM_db2cucs81-8.1.0-72.i386.rpm ...
.....
.....
.....
.....

IBM_db2engn81 #####
Updating to IBM_db2smp181-8.1.0-72.i386.rpm ...
IBM_db2smp181 #####
Updating to IBM_db2pext81-8.1.0-72.i386.rpm ...
IBM_db2pext81 #####
Updating to IBM_db2cc81-8.1.0-72.i386.rpm ...
IBM_db2cc81 #####
Updating to IBM_db2essg81-8.1.0-72.i386.rpm ...
IBM_db2essg81 #####

```

suse8linux:/code #

Finishing the Installation

Update Instances

As root

```
# /opt/IBM/db2/V8.1/instance/db2iupdt db2inst1
DBI1070I Program db2iupdt completed successfully.
```

Update DVS Instances

```
# /opt/IBM/db2/V8.1/instance/dasupdt dasusr1
SQL4410W The DB2 Administration Server is not active.
SQL4406W The DB2 Administration Server was started successfully.
DBI1070I Program dasupdt completed successfully.
1.3.3 Neustarten der Exemplare und Verwaltungsserver (this is German)
```

Restart Instances:

```
# su - db2inst1
```

```
$ d2start
```

```
10/14/2004 21:10:19 0 0 SQL1026N The database manager is already active.
SQL1026N The database manager is already active.
```

```
$ db2stop
```

```
10/14/2004 21:10:31 0 0 SQL1064N DB2STOP processing was successful.
SQL1064N DB2STOP processing was successful.
```

```
$ db2start
```

```
10/14/2004 21:10:41 0 0 SQL1063N DB2START processing was successful.
SQL1063N DB2START processing was successful.
```

Start the Administration server:

```
# su - dasusr1
```

```
$ db2admin start
```

```
SQL4409W The DB2 Administration Server is already active.
```

```
$ db2admin stop
```

```
SQL4407W The DB2 Administration Server was stopped successfully.
```

```
$ db2admin start
```

```
SQL4406W The DB2 Administration Server was started successfully.
```

Note

Other additional Actions (described in the ReadMe) like rebinding Files, rebinding specific packets or databases are not necessary, because there is no database created at this moment.

3.1.3 Check the DB2 installation

I prefer the following simple database test, this is optional.

Create the sample database:

```
# su - db2inst1
$ /opt/IBM/db2/V8.1/bin/db2sampl
```

Test of the sample database:

Verify, that you can access the sample database:

```
db2inst1@suse8linux:/opt/IBM/db2/V8.1/bin> db2
```

```
(c) Copyright IBM Corporation 1993,2002
Command Line Processor for DB2 SDK 8.2.0
You can issue database manager commands and SQL statements from the command
prompt. For example:
db2 => connect to sample
db2 => bind sample.bnd
.....
```

```
db2 => connect to sample
```

```
Database Connection Information
Database server      = DB2/LINUX 8.2.0
SQL authorization ID = DB2INST1
Local database alias = SAMPLE
```

```
db2 => list db directory
```

```
System Database Directory
Number of entries in the directory = 1
Database 1 entry:
Database alias           = SAMPLE
Database name            = SAMPLE
Local database directory = /home/db2inst1
Database release level   = a.00
Comment                  =
Directory entry type     = Indirect
Catalog database partition number = 0
Alternate server hostname =
Alternate server port number =
```

```
db2 => list tables
```

Table/View	Schema	Type	Creation time
CL_SCHED		DB2INST1	T 2004-10-14-21.34.56.927747
DEPARTMENT		DB2INST1	T 2004-10-14-21.34.54.938139
EMP_ACT		DB2INST1	T 2004-10-14-21.34.55.150914
EMP_PHOTO		DB2INST1	T 2004-10-14-21.34.55.465497
EMP_RESUME		DB2INST1	T 2004-10-14-21.34.56.497451
EMPLOYEE		DB2INST1	T 2004-10-14-21.34.54.992568
IN_TRAY		DB2INST1	T 2004-10-14-21.34.57.004186
ORG		DB2INST1	T 2004-10-14-21.34.54.330485
PROJECT		DB2INST1	T 2004-10-14-21.34.55.376569
SALES		DB2INST1	T 2004-10-14-21.34.56.757315
STAFF		DB2INST1	T 2004-10-14-21.34.54.800129

11 record(s) selected.

```
db2 => select * from ORG
```

DEPTNUMB	DEPTNAME	MANAGER	DIVISION	LOCATION
10	Head Office	160	Corporate	New York
15	New England	50	Eastern	Boston
20	Mid Atlantic	10	Eastern	Washington
38	South Atlantic	30	Eastern	Atlanta
42	Great Lakes	100	Midwest	Chicago

51 Plains	140 Midwest	Dallas
66 Pacific	270 Western	San Francisco
84 Mountain	290 Western	Denver

8 record(s) selected.

db2 => disconnect sample

DB20000I The SQL DISCONNECT command completed successfully.

Note:

I observed a performance problem: The cpu of the Linux system occupies 100% cpu power with a cycle of about 10 sec,

sar 2 3

```
Linux 2.4.21-138-default (tnt2)          10/16/04
09:23:31      CPU      %user   %nice   %system   %idle
09:23:33      all      97.50    0.00    2.50    0.00
09:23:35      all     100.00    0.00    0.00    0.00
09:23:37      all     100.00    0.00    0.00    0.00
Average:      all      99.17    0.00    0.83    0.00
```

The reason is not clear at the moment, but the causer of the problem is the DB2 Fault Monitor Process.

My workaround:

disable the start of the DB2 Fault Monitor Process:

remove the following entry from **/etc/inittab**:

```
fmc:2345:respawn:/opt/IBM/db2/V8.1/bin/db2fmcd      #DB2 Fault Monitor
Coordinator
```

3.2 Installation of Tivoli Security Compliance Manager Server V 5.1

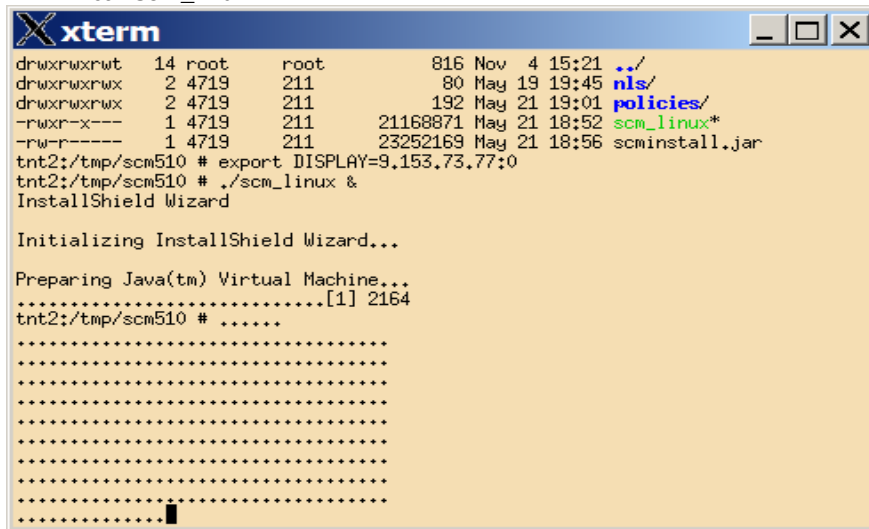
3.2.1 Base ITSCM Server Installation

For Details see:

Tivoli® Security Compliance Manager Installation Guide: All Component Version 5.1

http://publib.boulder.ibm.com/tividd/td/ITSCM/GC32-1592-00/en_US/PDF/scm51_install.pdf

- Prepare an X11 environment,
- go to the directory that contains the ITSCM installation code
- call **scm_linux**



```
xterm
drwxrwxrwt  14 root    root      816 Nov  4 15:21 ../
drwxrwxrwx   2 4719    211        80 May 19 19:45 nls/
drwxrwxrwx   2 4719    211       192 May 21 19:01 policies/
-rwxr-x---   1 4719    211    21168871 May 21 18:52 scm_linux*
-rw-r-----   1 4719    211    23252169 May 21 18:56 scminstall.jar
tnt2:/tmp/scm510 # export DISPLAY=9.153.73.77:0
tnt2:/tmp/scm510 # ./scm_linux &
InstallShield Wizard

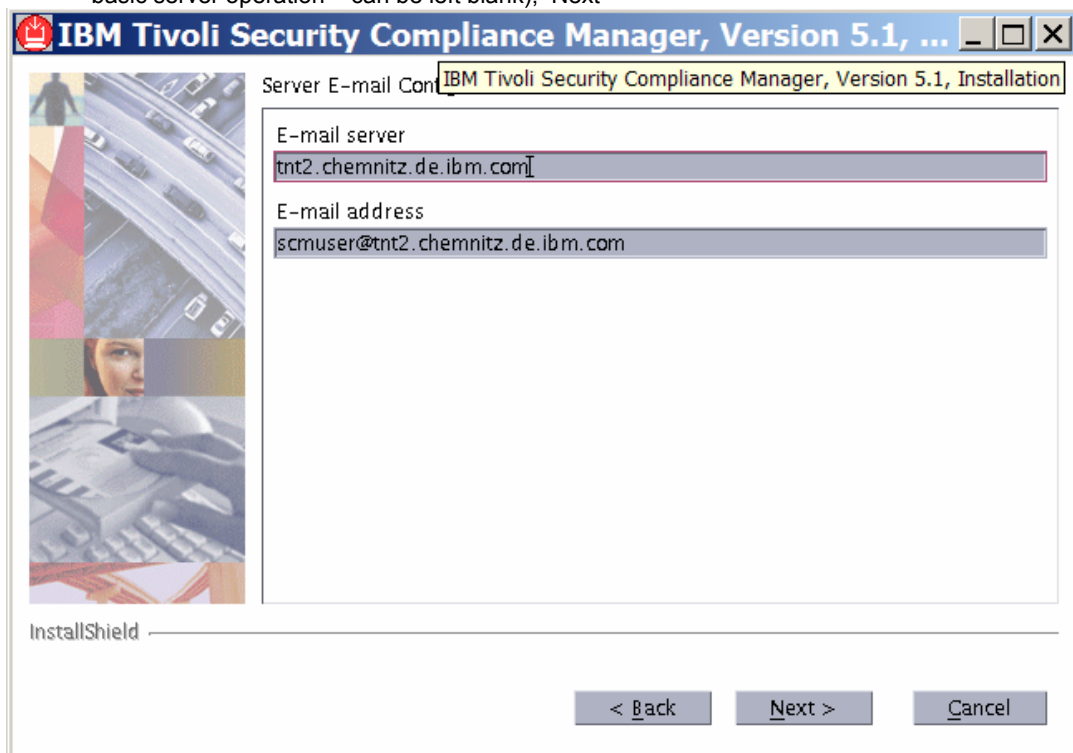
Initializing InstallShield Wizard...

Preparing Java(tm) Virtual Machine...
.....[1] 2164
tnt2:/tmp/scm510 # .....
```

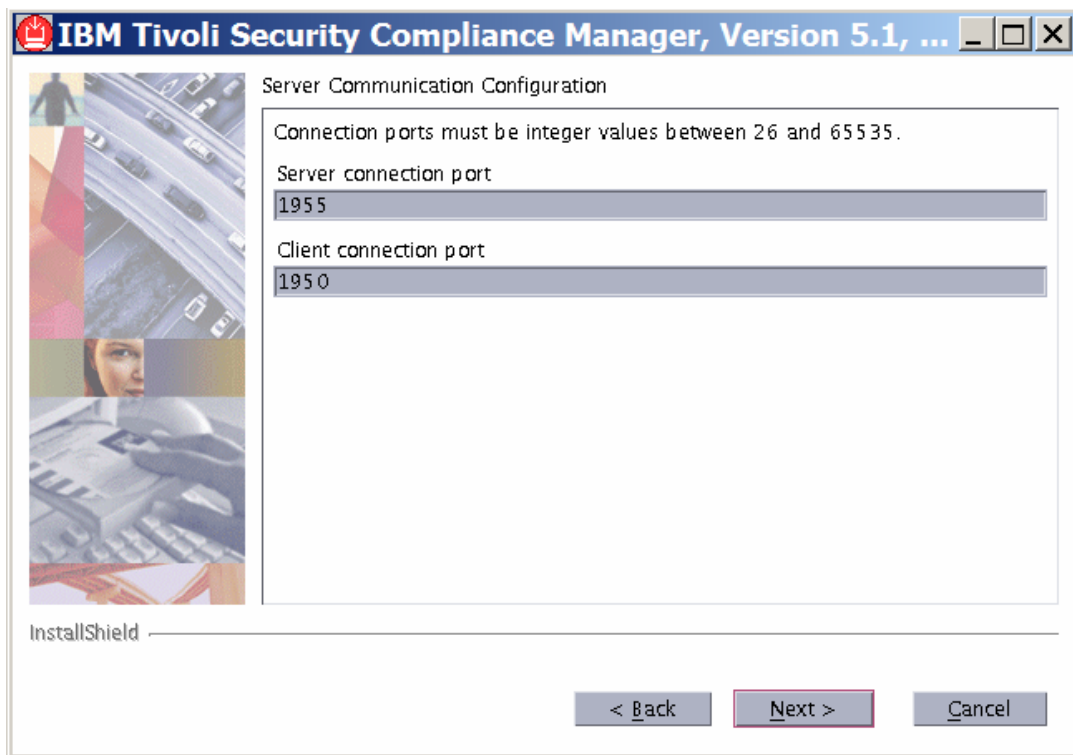
- On the first screen: Select language used for the installation wizard, ok
- On the next screen: Accept the Welcome screen, Next
- On the next screen: Accept the licence agreement, Next
- On the next screen: Specify the installation directory, the Default is: /opt/IBM/SCM , Next
- On the next screen: Select: IBM Tivoli Security Compliance Manager Server



- On the next screen: You may provide a mail server and a mail address, (not required for basic server operation – can be left blank), Next



- On the next screen: Provide Server and Client connection port, use defaults, Next



- On the next screen:
Provide System Name, Master keystore password and Server keystore password, (e.g. Passw0rd) press Next
(The passwords are required but after installation are not externally used with the current version of code. They will be used in the future with functions like certificate revalidation.)

IBM Tivoli Security Compliance Manager, Version 5.1, ...

Server Security

System name for certificate
tnt2.local

Master keystore password

Confirm master keystore password

Server keystore password

Confirm server keystore password

☒ Select the checkbox to stash the server keystore password for automatic star

InstallShield

< Back Next > Cancel

- On the next screen: select The database is local ..., Next
- On the next screen: provide database user information, I used: db2inst1, Next

IBM Tivoli Security Compliance Manager, Version 5.1, ...

Database Configuration

Database user ID
db2inst1

Database user ID password

Confirm password

Database Location

☒ Select the checkbox to create your database now.

InstallShield

< Back Next > Cancel

Note:

For **UNIX-based and Linux** platforms enter the following information:

- The DB2 user ID and password. e.g. ID=db2inst1 PW=passw0rd
- The location to create the DB2 database. If this field is left blank, the installation will use the default location of the database instance ID home. If a location is specified in this field, that location will be used as the location of the database.

- On the next screen: provide user and password for ITSCM administration (default: ID=admin and PW=passw0rd), Next

Administrator User ID

The user information below is for the primary administrator of the IBM Tivoli Security Compliance Manager deployment.

System administrator user ID

admin

System administrator user password

Confirm password

InstallShield

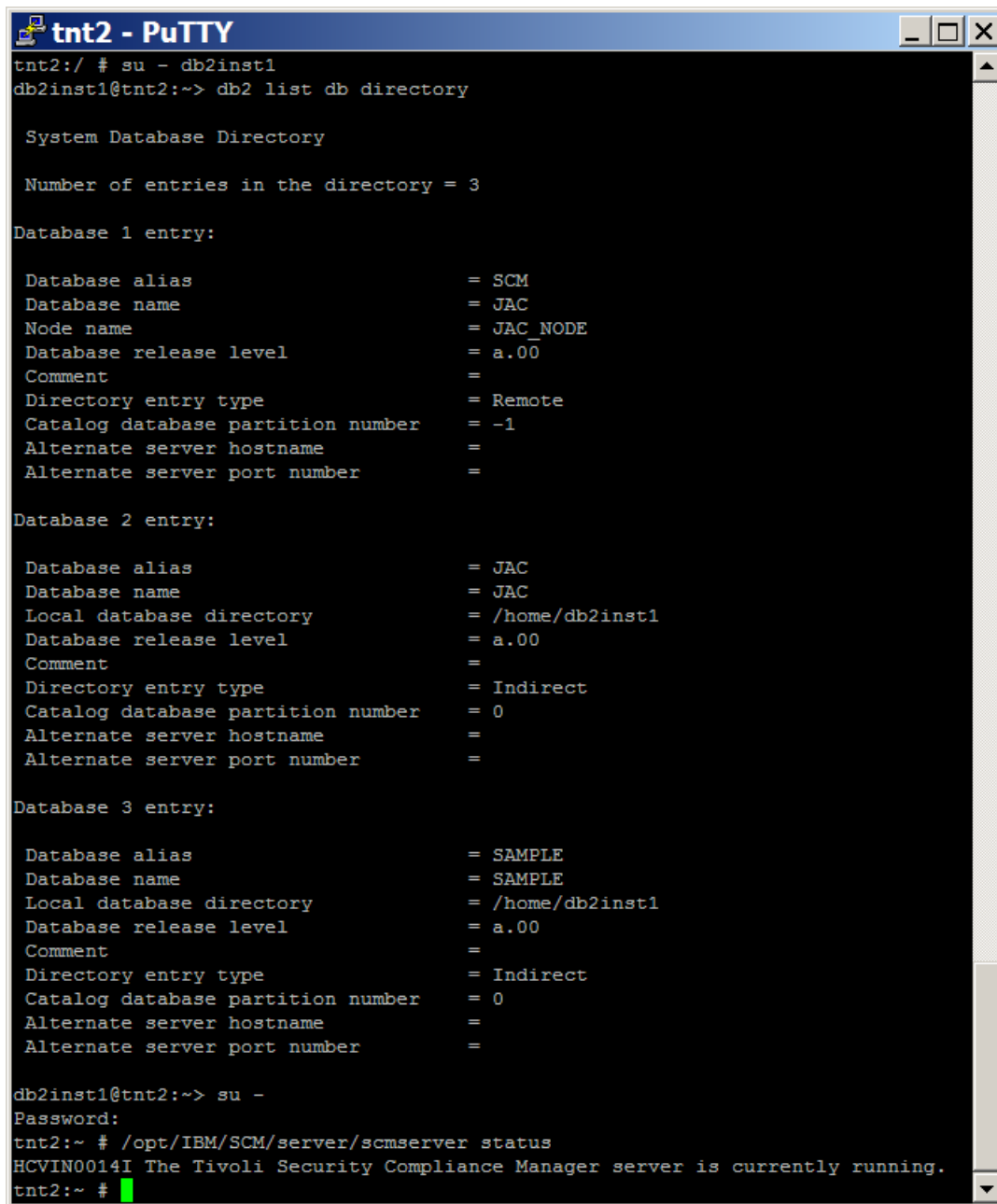
< Back Next > Cancel

- On the next screen: Confirm the installation settings, Next, Finished!



3.2.2 Verify the ITSCM server installation

Verify, that the ITSCM database has been created



```
tnt2:/ # su - db2inst1
db2inst1@tnt2:~> db2 list db directory

System Database Directory

Number of entries in the directory = 3

Database 1 entry:

Database alias           = SCM
Database name            = JAC
Node name                = JAC_NODE
Database release level   = a.00
Comment                  =
Directory entry type     = Remote
Catalog database partition number = -1
Alternate server hostname =
Alternate server port number =

Database 2 entry:

Database alias           = JAC
Database name            = JAC
Local database directory = /home/db2inst1
Database release level   = a.00
Comment                  =
Directory entry type     = Indirect
Catalog database partition number = 0
Alternate server hostname =
Alternate server port number =

Database 3 entry:

Database alias           = SAMPLE
Database name            = SAMPLE
Local database directory = /home/db2inst1
Database release level   = a.00
Comment                  =
Directory entry type     = Indirect
Catalog database partition number = 0
Alternate server hostname =
Alternate server port number =

db2inst1@tnt2:~> su -
Password:
tnt2:~ # /opt/IBM/SCM/server/scmserver status
HCVIN0014I The Tivoli Security Compliance Manager server is currently running.
tnt2:~ #
```

and check the ITSCM server status:

scmserver status

3.3 Installation of Tivoli Security Compliance Manager Client V 5.1

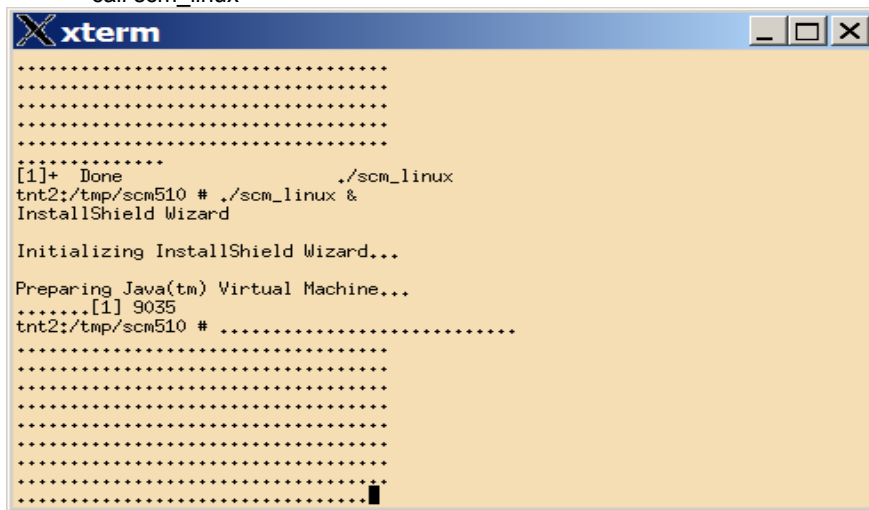
3.3.1 Base ITSCM Client Installation

For Details see:

Tivoli® Security Compliance Manager Installation Guide: Client Component Version 5.1

http://publib.boulder.ibm.com/tividd/td/ITSCM/GC32-1593-00/en_US/PDF/scm51_install_client.pdf

- Prepare an X11 environment,
- go to the directory that contains the ITSCM installation code
- call scm_linux



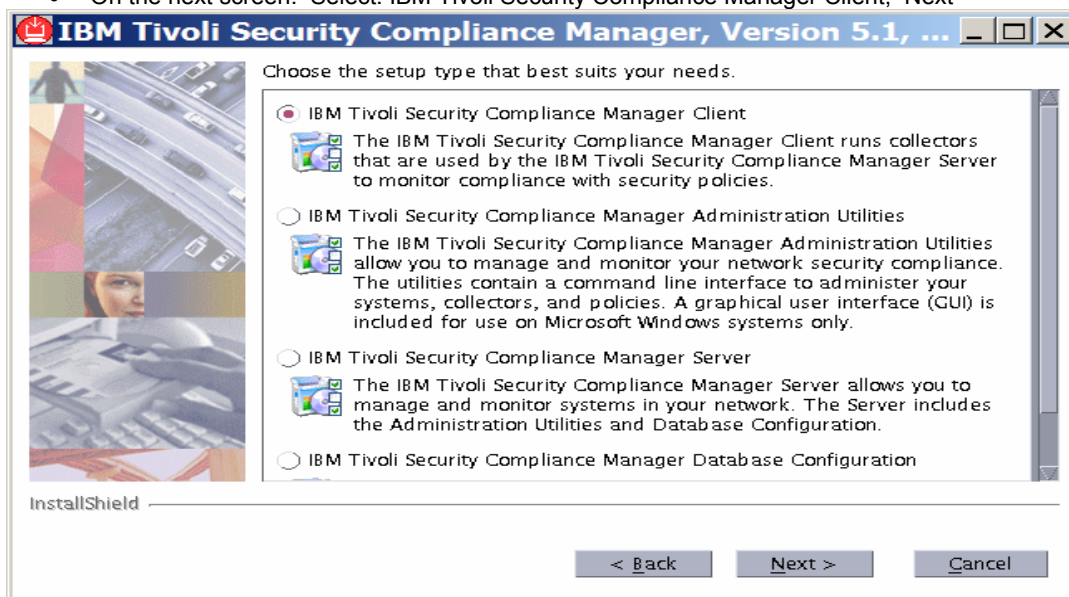
```
xterm
.....
.....
.....
.....
.....
[1]+  Done                  ./scm_linux
tnt2:/tmp/scm510 # ./scm_linux &
InstallShield Wizard

Initializing InstallShield Wizard...

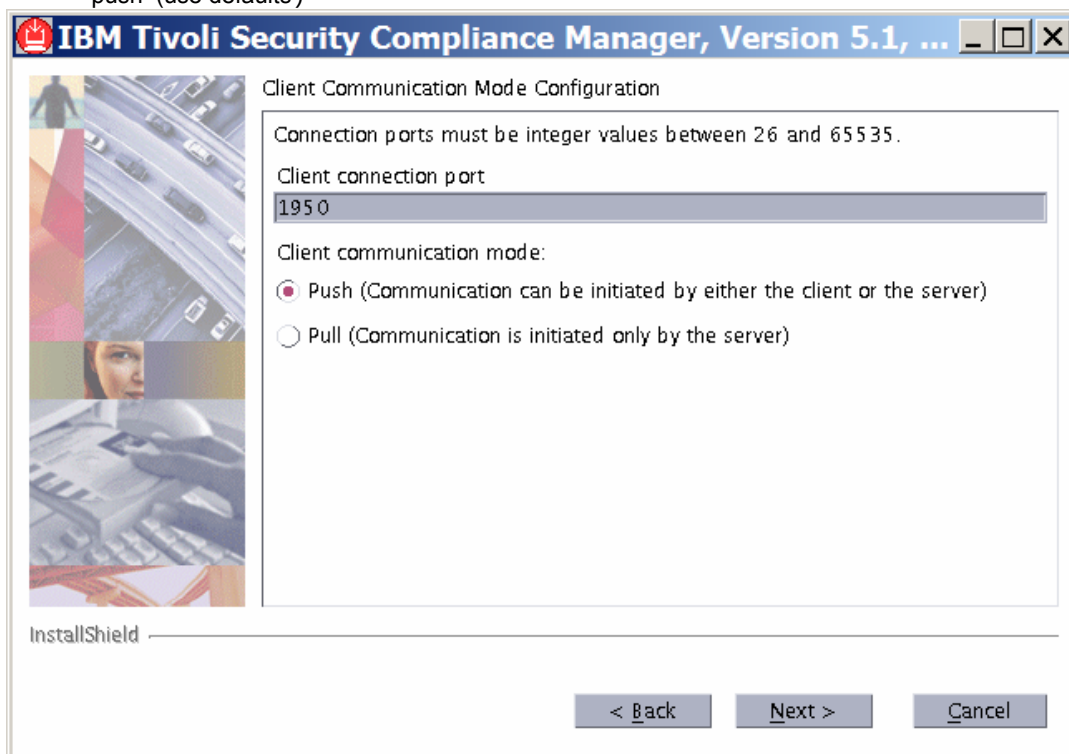
Preparing Java(tm) Virtual Machine...
.....[1] 9035
tnt2:/tmp/scm510 # .....
```

- On the first screen : Select language used for the installation wizard, ok
- On the next screen: Accept the Welcome screen, Next
- On the next screen: Accept the licence agreement, Next
- On the next screen: Specify the installation directory, Next

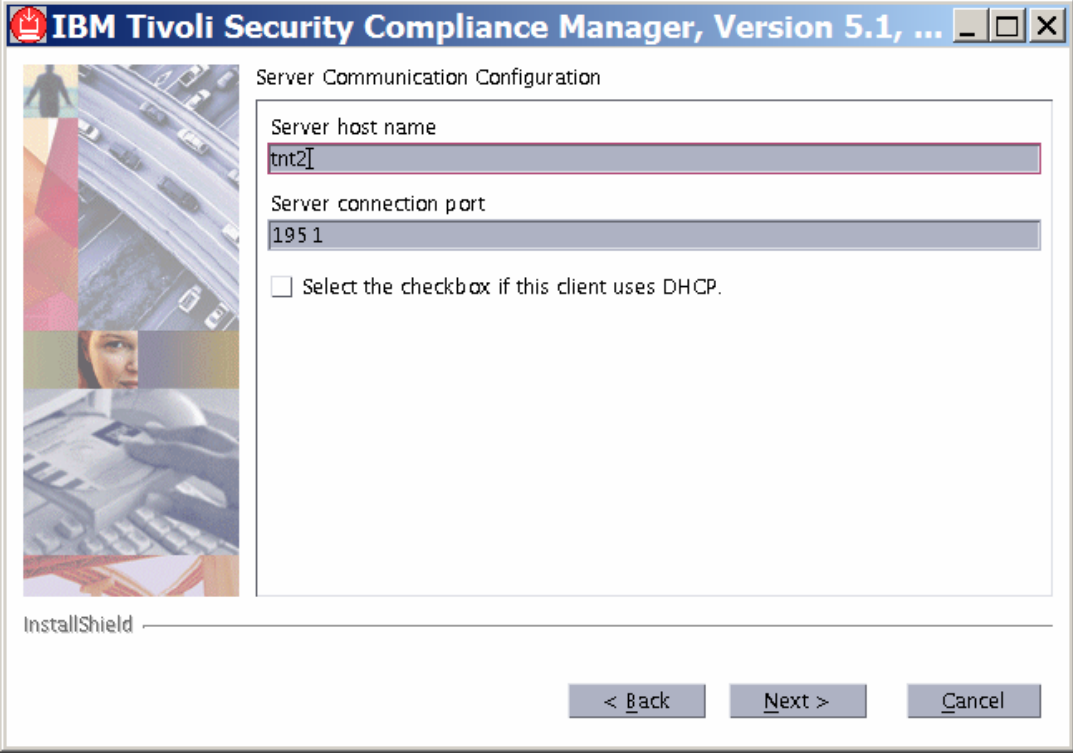
- On the next screen: Select: IBM Tivoli Security Compliance Manager Client, Next



- On the next screen: Confirm client connection port 1950 and client connection mode: push (use defaults)



- On the next screen: Specify server hostname and confirm server connection port 1951 (default)



The screenshot shows a Windows-style window titled "IBM Tivoli Security Compliance Manager, Version 5.1, ...". The window has a vertical sidebar on the left with a collage of images including a person, a highway, a woman's face, and a computer keyboard. The main area is titled "Server Communication Configuration" and contains two text input fields. The first field, labeled "Server host name", contains the text "tnt2". The second field, labeled "Server connection port", contains the text "1951". Below these fields is a checkbox labeled "Select the checkbox if this client uses DHCP.", which is currently unchecked. At the bottom of the window, there is a progress bar labeled "InstallShield" and three buttons: "< Back", "Next >", and "Cancel".

IBM Tivoli Security Compliance Manager, Version 5.1, ...

Server Communication Configuration

Server host name
tnt2

Server connection port
1951

☐ Select the checkbox if this client uses DHCP.

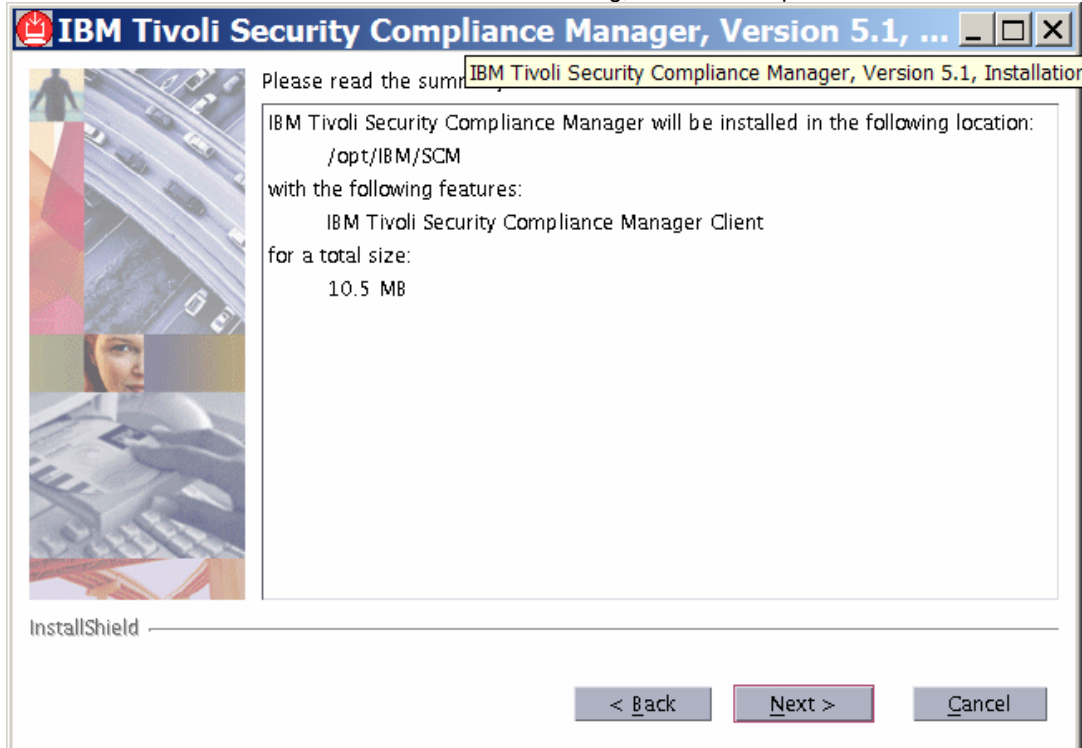
InstallShield

< Back Next > Cancel

Info:

One may want to also select DHCP for both fixed IP addresses and dynamic IP addresses. The difference is that not selecting this means the IP address is used to register the SCM client machine to the server. When selection DHCP a fingerprint is generated based on the digital certificate and that is used to register to the SCM server. The fingerprint makes it easier should the fixed IP address client ever need's to have its IP address changed for any reason. The only reason this cannot be selected is if the client is a pull client although this is likely to change in a future release of the product. Using DHCP will also allow for specifying an alias which can be used at registration or changed at that time and also the ability to set the server to auto register the client if this is required. (see install doc and edit the server.ini file.)

- On the next screen: Confirm the installation setting, Next and complete installation!



4 Installation of the IBM Tivoli Security Compliance Manager on Windows 2000

4.1 Installation of IBM DB2 UDB version 8.1

You are going to install DB2 on Server1.

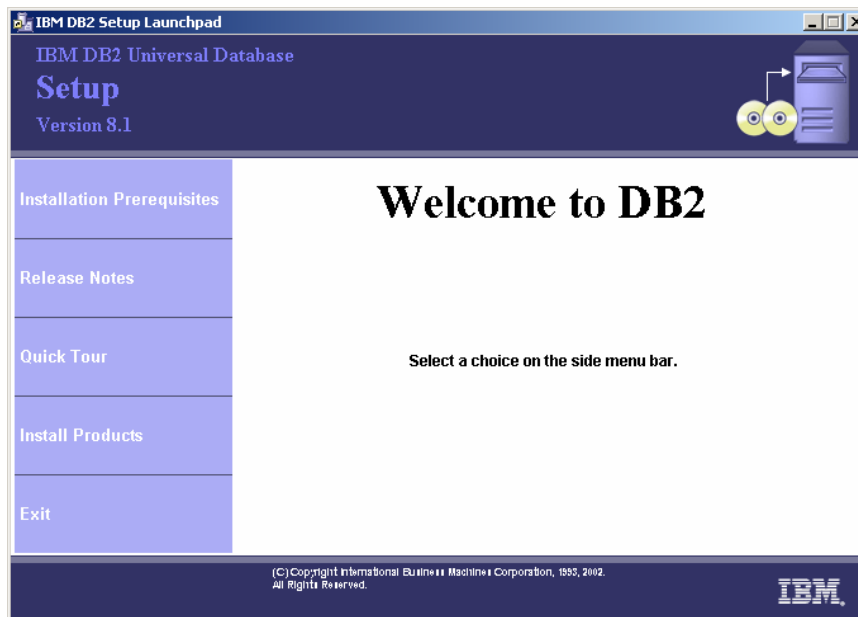
When installing DB2, you will need to know:

Name of the user DB2 will use to logon to your system: **db2admin**
Password for this user will be: **passw0rd**

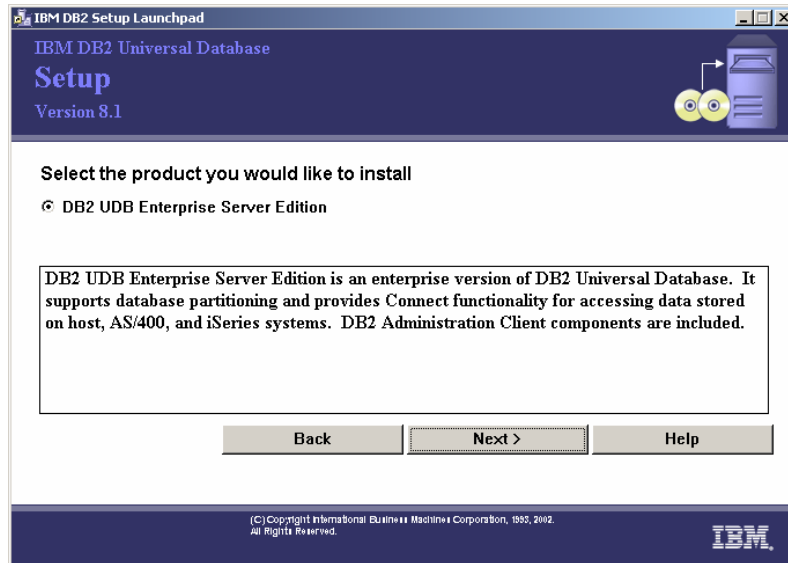
There is nothing unique that Security Compliance Manager requires for DB2, so the DB2 installation can be completed using most of the defaults provided.

4.1.1 Base DB2 Installation

Using the DB2 install image, use Windows Explorer to launch the setup.exe file. On the first screen (shown below) select the **Install Products** option on the left hand side of the screen.

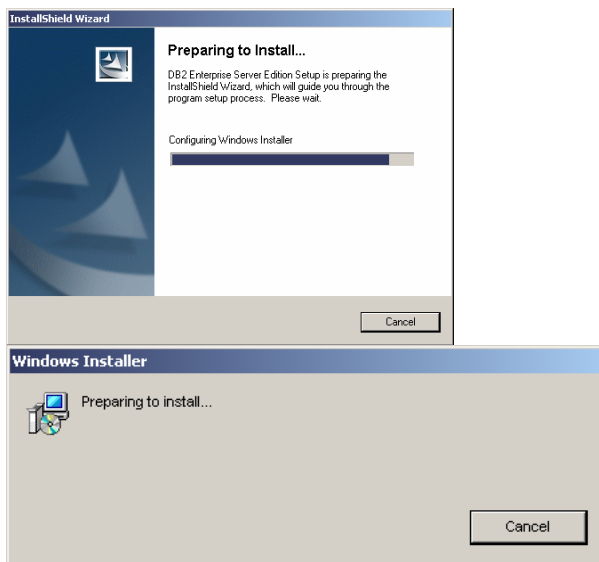


At the next screen, ensure that the radio button associated with **DB2 UDB Enterprise Server Edition** is selected.

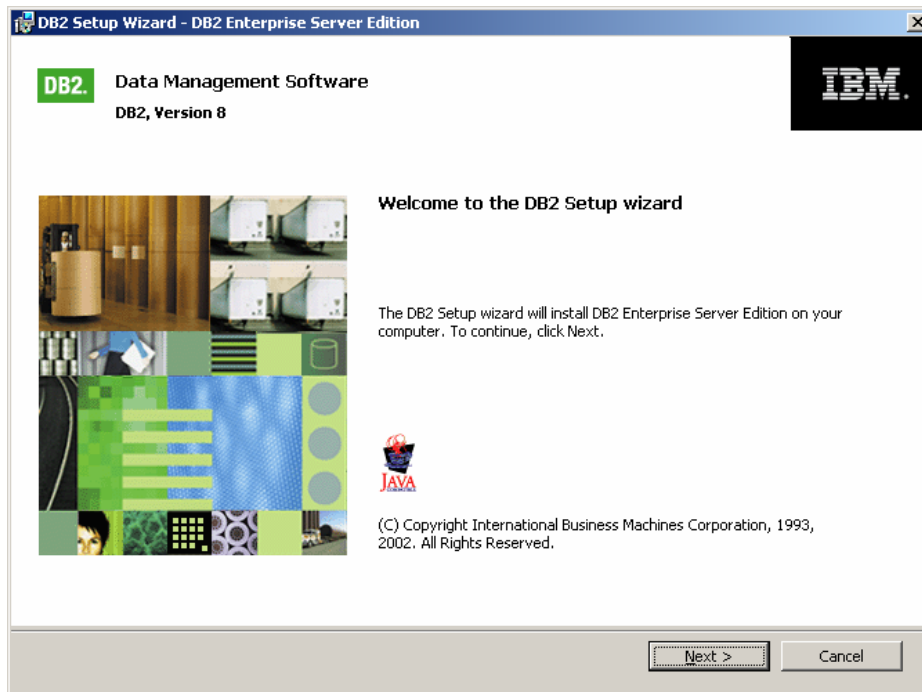


Press Next to continue.

The process then continues with two more screens as shown below ...



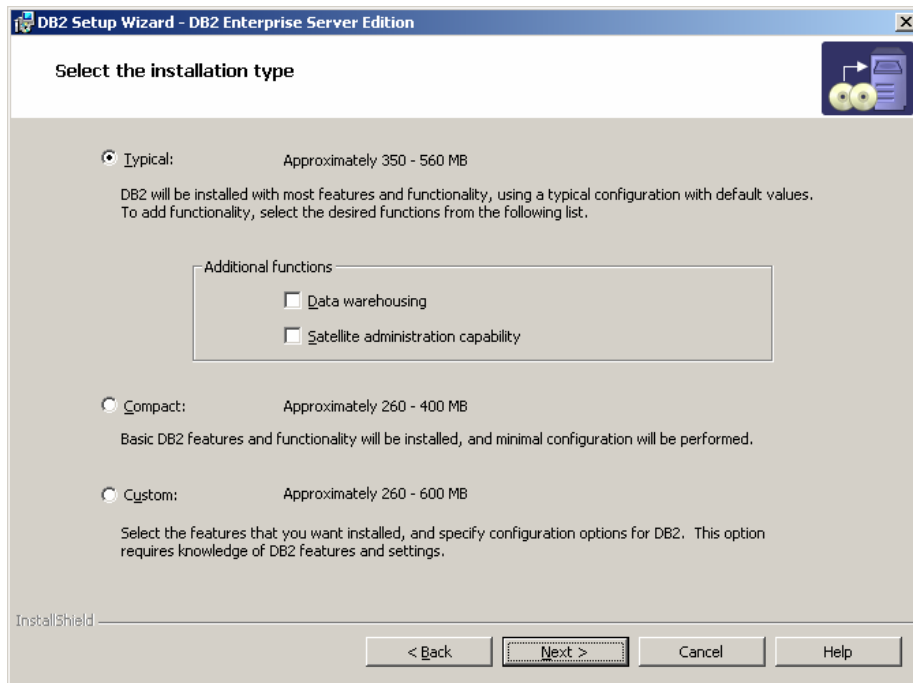
... before stopping at the **Setup Wizard** shown here.



Press *Next* to continue.

At the next screen (not shown), accept the licence agreement by checking the radio button and then press Next.

The screen shown below will then appear. Ensure that **Typical** install option is selected with all other check boxes and radio buttons are deselected.



Press **N**ext to continue.

After several seconds a warning dialogue box will appear containing the message “**If you are using APPC to connect to remote servers.....**” At this point press **OK**; do not press cancel.

The next dialogue gives you the option to **Install DB2 Enterprise Server Edition on this Server**. Check the box associated with this and leave the **Save your settings in a response file** unchecked.

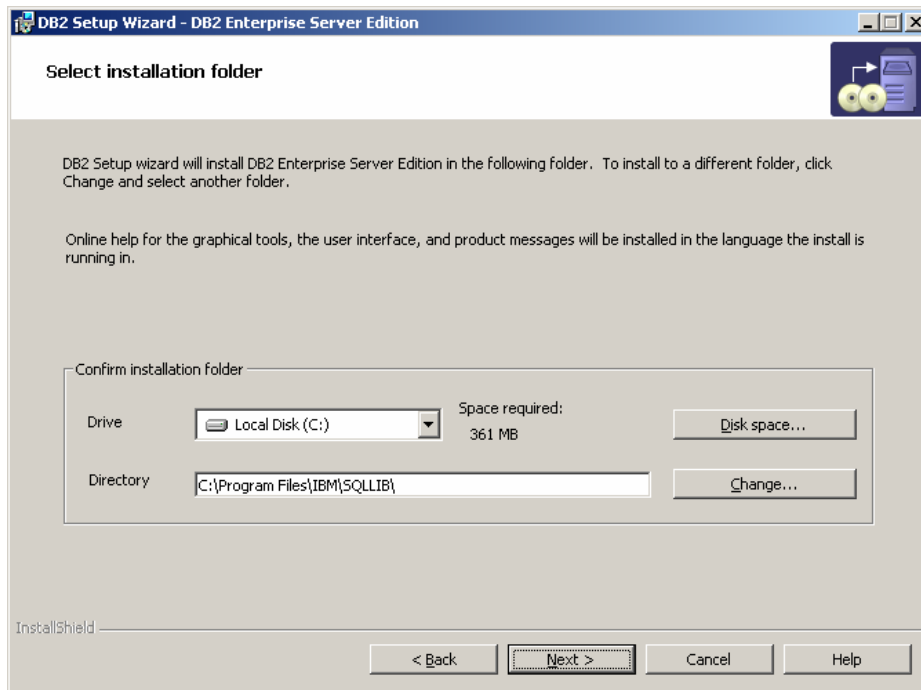
Check that the defaults on the next screen are:

Drive = **Local Disk (C:)**

and

Directory = **c:\Program Files\IBM\SQLLIB**

Press **N**ext to continue.



Then press **Next** to continue.

At the next screen, leave the domain name blank and check that the user name is **db2admin** and then enter **passw0rd** in the password field and confirm password field. Check the **Use the same user name.....** box.

DB2 Setup Wizard - DB2 Enterprise Server Edition

Set user information for the DB2 Administration Server

Enter the user name and password that the DB2 Administration Server (DAS) will use to log on to your system. You can use a local user or a domain user.

User information

Domain: [dropdown menu]

User name: db2admin

Password: *****

Confirm password: *****

☒ Use the same user name and password for the remaining DB2 services

InstallShield

< Back Next > Cancel Help

Press **Next** to continue.

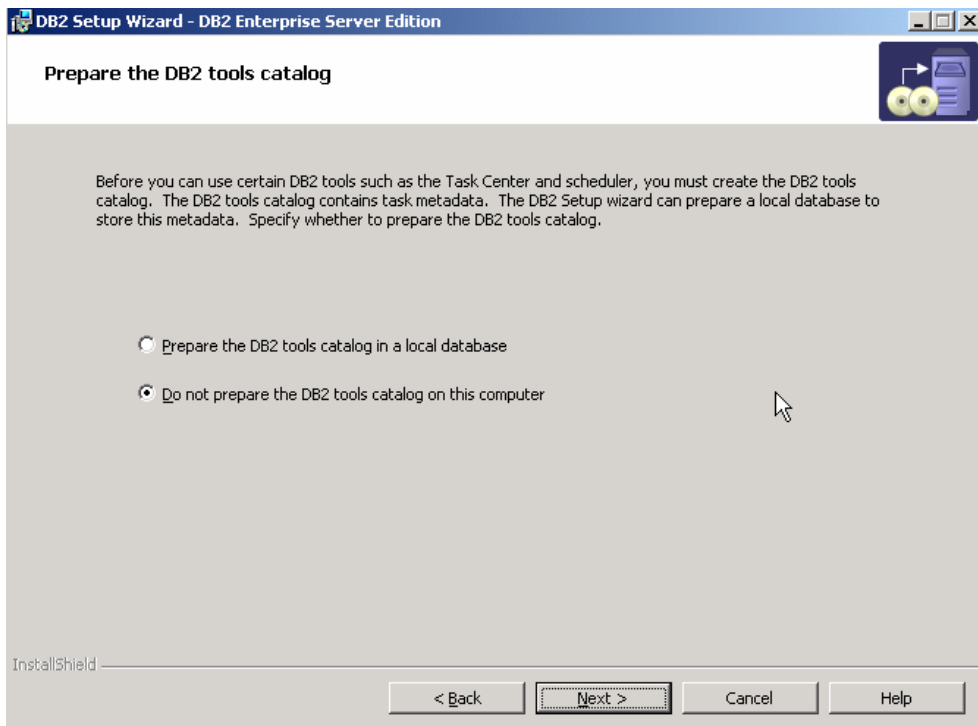
The next screen should have the radio button **local** selected. If it has, click **Next** to continue.

■ (This screen is not reproduced here)

A warning will then appear concerning the “**Notification SMTP server.....**”. To continue, simply press **OK**.

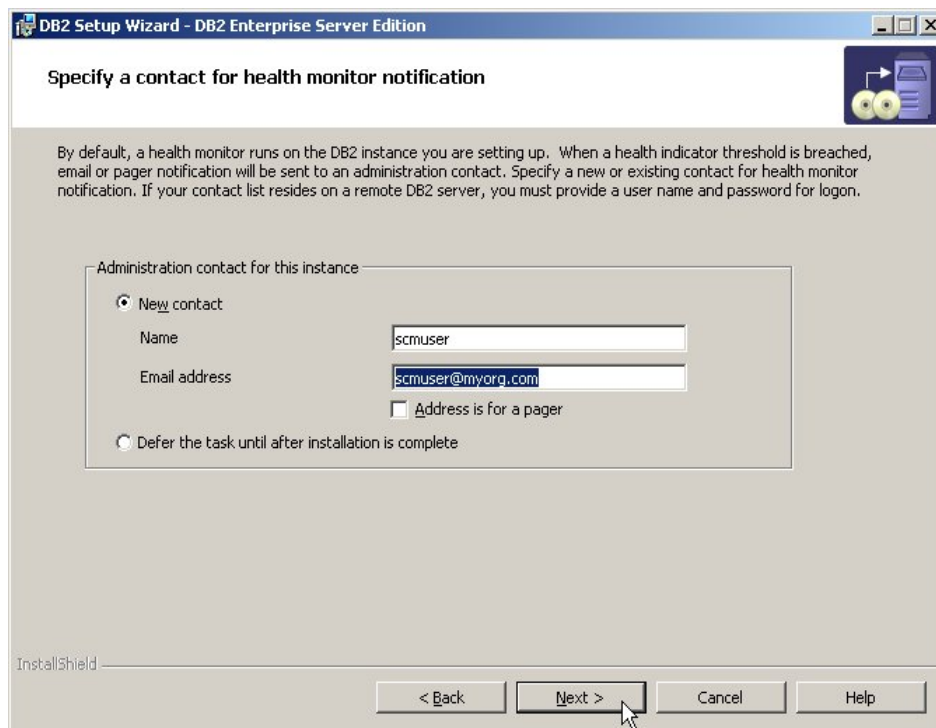
■ (This screen is not reproduced here)

On the next screen select “**Do not prepare the DB2 tools catalogue on this computer.**”

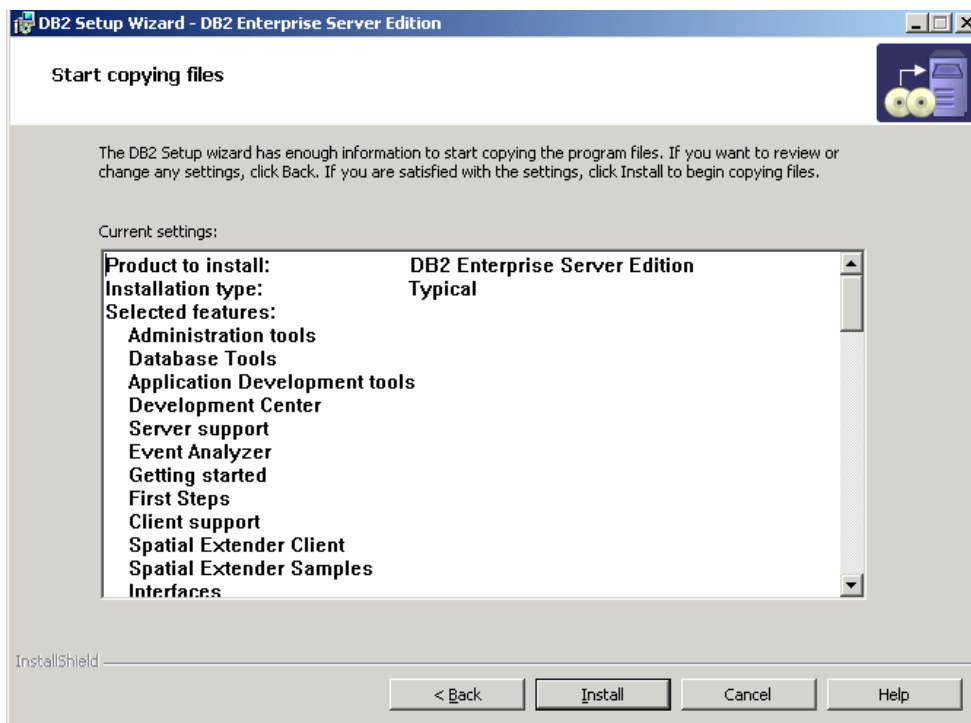


Press **Next** to continue.

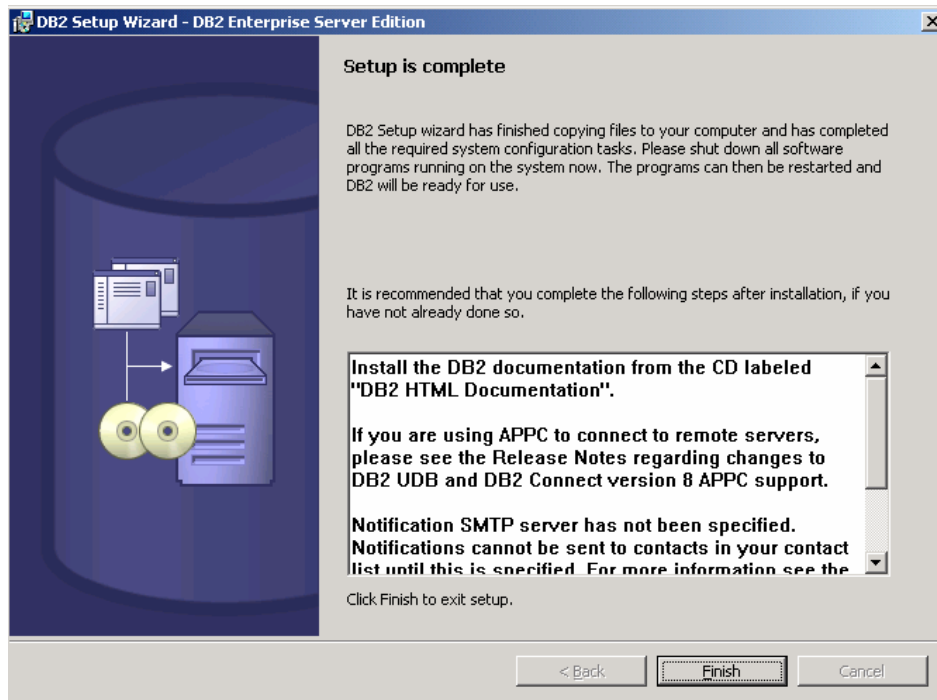
This screen is not essential for Security Compliance Manager, but it may be useful to send indications of DB2 performance events to a Security Compliance Manager administrator. In this case we have set up the user name of **SCMuser** with an **e-Mail address** of scmuser@myorg.com.



Once you have entered these details click Next to continue.



This screen lists all the information settings to start the install of DB2. Simply press **Install** to continue. After this screen, a status screen is shown and subsequently the **Setup is complete** screen is shown.



Click **Finish** to continue.

On the final screen titled **First Steps**, select **Exit First Steps** from the left hand side to finish the DB2 installation. You can check to see if the DB2 Services running through the Microsoft Services tool. If correctly installed, they should look like those below:

DB2 - DB2-0	Allows applica...	Started	Automatic	.\db2admin
DB2 Governor	Collects statis...		Manual	LocalSystem
DB2 JDBC Applet Server	Provides JDBC...	Started	Automatic	LocalSystem
DB2 License Server	Monitors DB2 I...	Started	Automatic	LocalSystem
DB2 Remote Command Server	Supports rem...	Started	Automatic	.\db2admin
DB2 Security Server	Authenticates...	Started	Automatic	LocalSystem
DB2DAS - DB2DAS00	Supports local...	Started	Automatic	.\db2admin
DefWatch		Started	Automatic	LocalSystem

In order to ensure that the DB2 instance is correctly started and that environment variables have been registered in windows, **reboot the server now**.

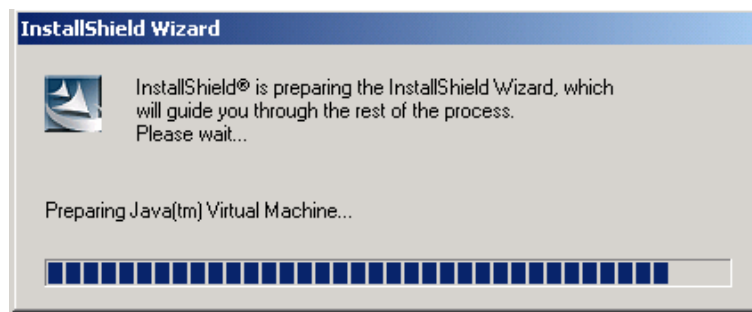
4.2 Installation of Tivoli Security Compliance Manager Server V 5.1

After installing the prerequisite DB2 database, you can install the IBM Tivoli Security Compliance Manager V5.1 on the same **Server1** system. You will need to know:

Name of user DB2 will use to logon to your system:	<i>db2admin</i>
Password for this user will be:	<i>passw0rd</i>

4.2.1 Base ITSCM Server Installation

Go to the directory or CD drive where the IBM Tivoli Security Compliance Manager Installation files reside. Use Windows Explorer to launch the **scm_win32.exe** install file. The **InstallShield Wizard** will then prepare the Java virtual system and continues to the next screen.



This next screen allows you to select the language you wish to use.



Select **English** and click **OK** to continue.



This above screen contains information about the IBM Tivoli Security Compliance Manager product. The complete text is reproduced in the table below so that you can refer to it if you wish to.

Press Next to continue.

Welcome to the IBM Tivoli Security Compliance Manager, Version 5.1, Installation Utility

You are about to install a component of IBM Tivoli Security Compliance Manager, Version 5.1. You can choose to install the client, the administration utilities, the server, or the database utilities component.

Required Information

Descriptions of the components and the information you will need to supply during their installation are listed below. For more information, please see the IBM Tivoli Security Compliance Manager Installation Guide.

IBM Tivoli Security Compliance Manager Client

Select this component to install the client function on the target system. To successfully install the client, you must provide the following information:

- The port number over which the client/server communication will be performed.
- The communication method: push or pull.

Push Mode - The connection originates from the client.

Pull Mode - The connection originates from the server.

If you select push mode, you will be required to supply the hostname and server port for communication.

- Indicate if the client uses DHCP, and enter a DHCP client alias if desired
- For HP-UX installations, provide the location of the Java runtime environment.

IBM Tivoli Security Compliance Manager Administration Utilities

Select this component to install the system administration GUI, as well as the command line interface on the target system. For HP-UX installations, provide the location of the Java runtime environment. No additional configuration information is needed.

IBM Tivoli Security Compliance Manager Server

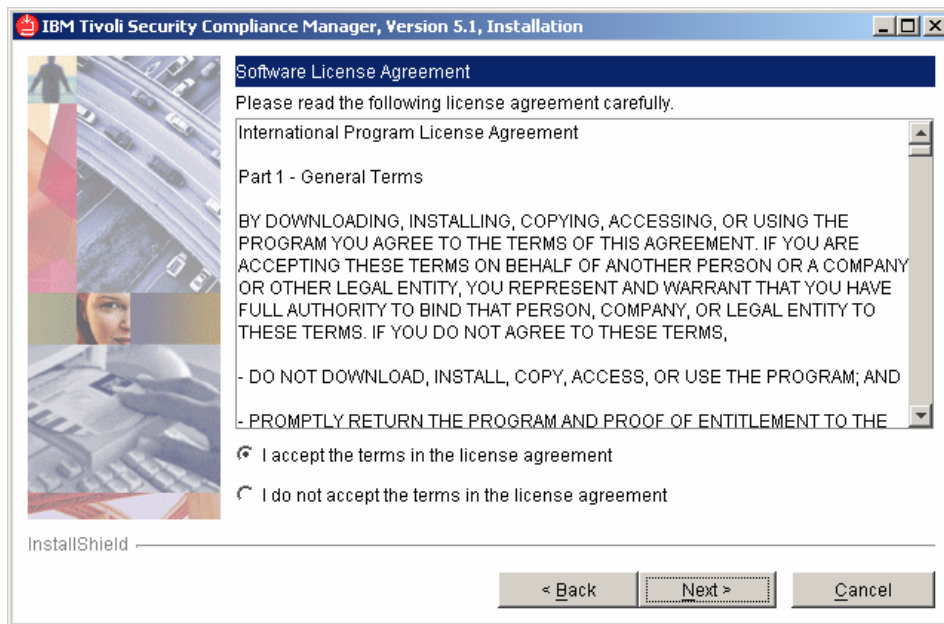
Installing the server provides you with the server function, and local database configuration, on the target system. To successfully install the server, you must provide the following information:

- For HP-UX installations, provide the location of the Java runtime environment.
- E-mail - provide the e-mail server name and the address to send server notification e-mail to
- Server and client connection ports
- Passwords to be used for the master and server keystores
- The user ID and password to be used for the system administration GUI
- The user ID and password for the database
- For remote databases or Microsoft Windows installations, the location of the jar or zip file that contains the JDBC driver and the URL to use for database connectivity

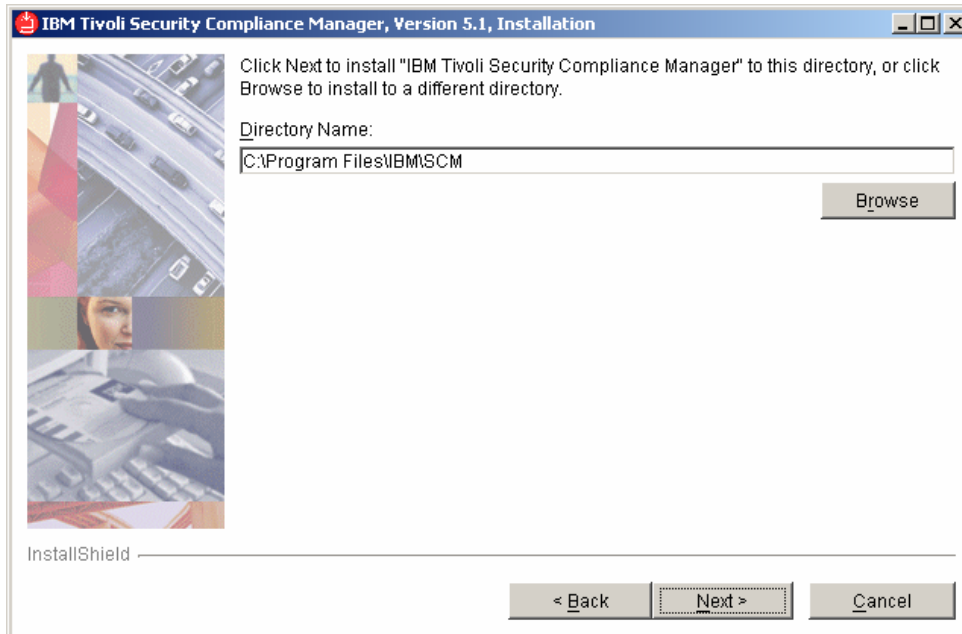
IBM Tivoli Security Compliance Manager Database Utilities

Installing the database utilities will perform the necessary database configuration on a remote database. To successfully use the database utilities, you must provide the following information:

- For HP-UX installations, provide the location of the Java runtime environment.
- The user ID and password to be used for the system administration GUI
- The user ID and password for the database
- The location of the jar or zip file that contains the JDBC driver and the URL to use for database connectivity

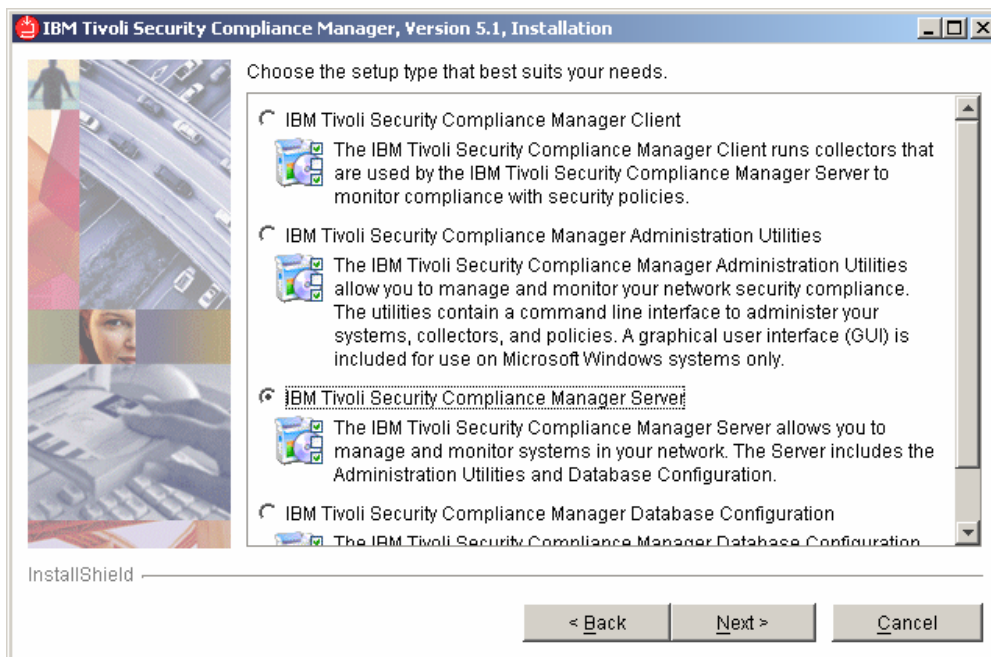


Check the **I accept the terms in the licence agreement** radio button and press **Next** to continue.



The above screen shows the default location for the installation of the IBM Tivoli Security Compliance Manager components.

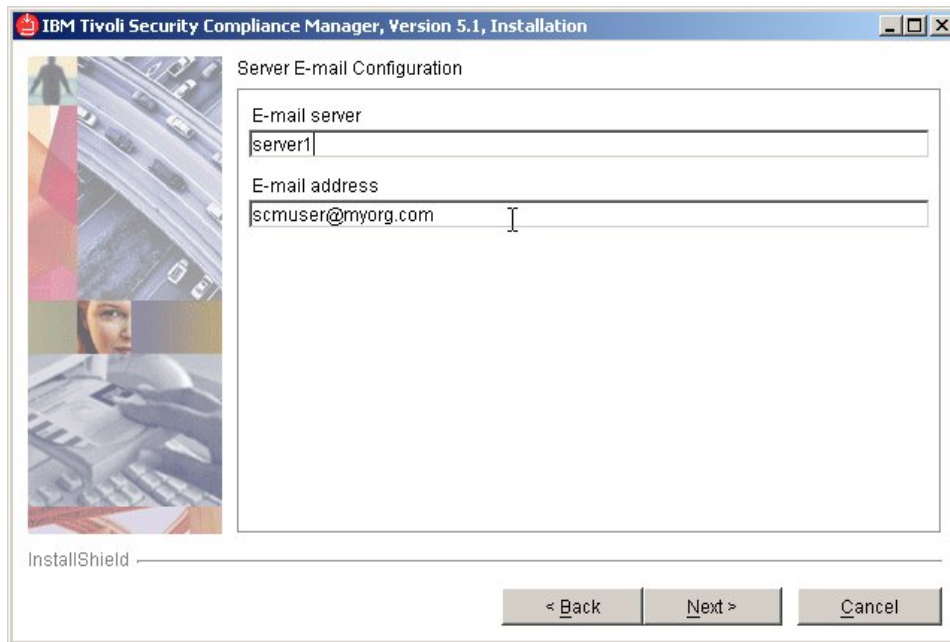
This should read **C:\Program Files\IBM\SCM**. If it does, press Next to continue.



This part of the installer shows the list of install options. Be sure to select the third radio button on the list for the **IBM Tivoli Security Compliance Manager Server**.

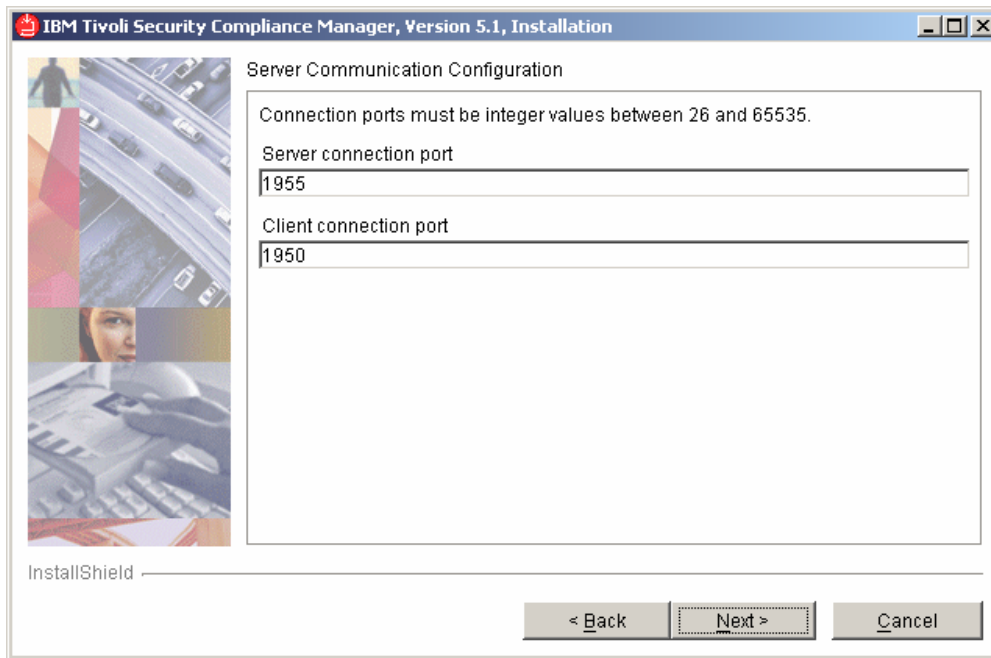
■ Note that the default is for the Client install.

Once you have selected the correct option, press Next to continue.



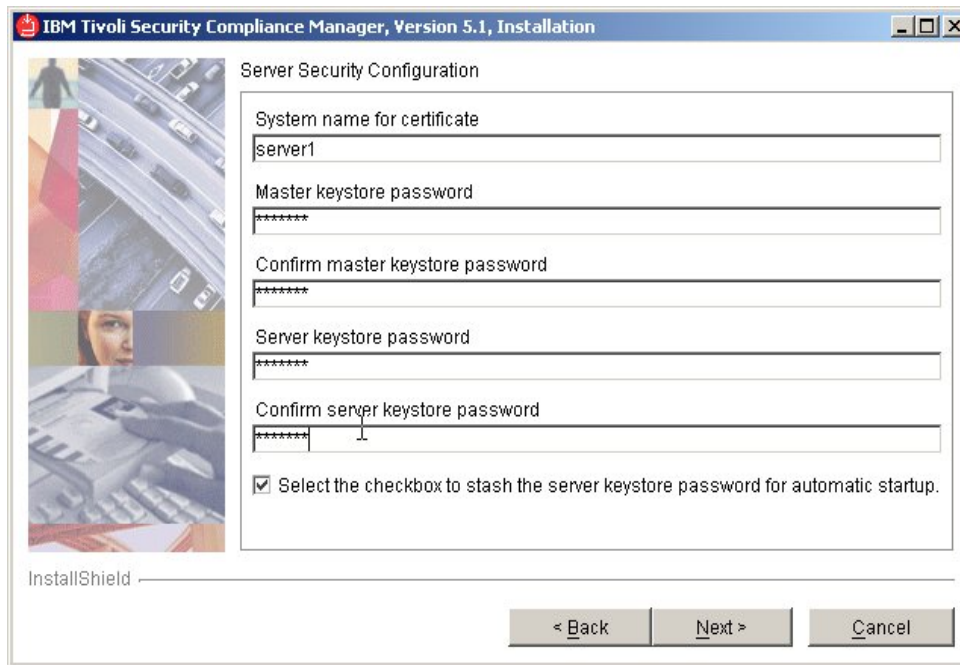
This screen accepts the parameters that will be placed in the **server.ini** file to allow IBM Tivoli Security Compliance Manager to send eMail messages.

For this workshop, there is a mail server configured on the ACS-SCM VMWare system. You should enter the hostname (**Win2k-ACS-SCM**) as the **E-mail server** setting and scmuser@myorg.com as the **E-mail address**. For your own installation environment after this workshop, you should enter the appropriate settings in place of the E-mail server and E-mail address variables in the screen above.



This screen allows you to configure the communication ports available to IBM Tivoli Security Compliance Manager Server. Once again, these variables are stored in the **server.ini** file and can be changed directly at a later time. Accept the defaults of 1955 for Server connection port and 1950 for Client connection port.

Press **Next** to continue.

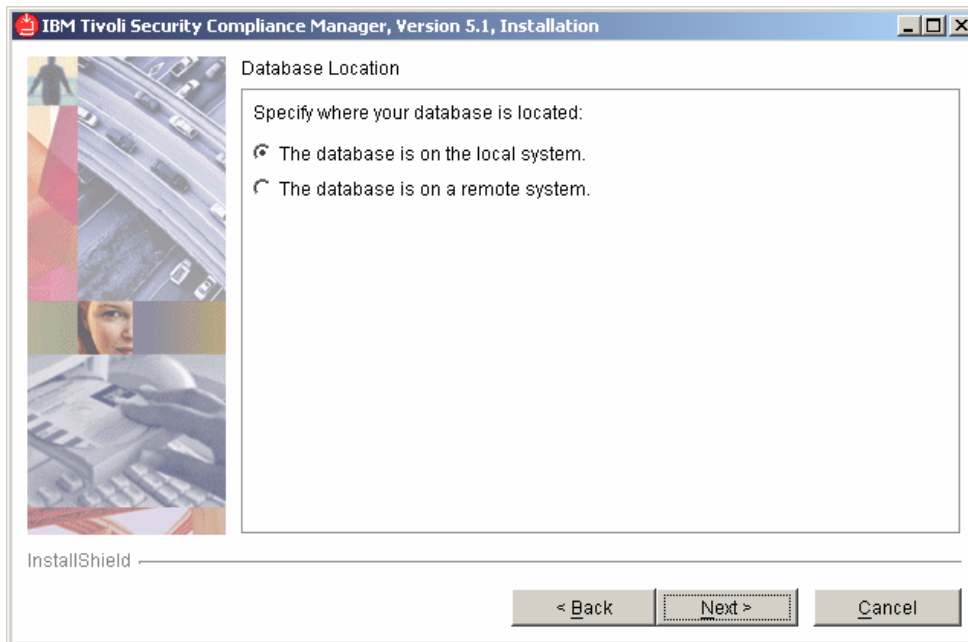


This screen allows you provide the system name used in the creation of certificates. Typical practice is to use the fully qualified hostname of the server machine. This screen also allows you to enter the passwords to be used for both the master and server keystores.

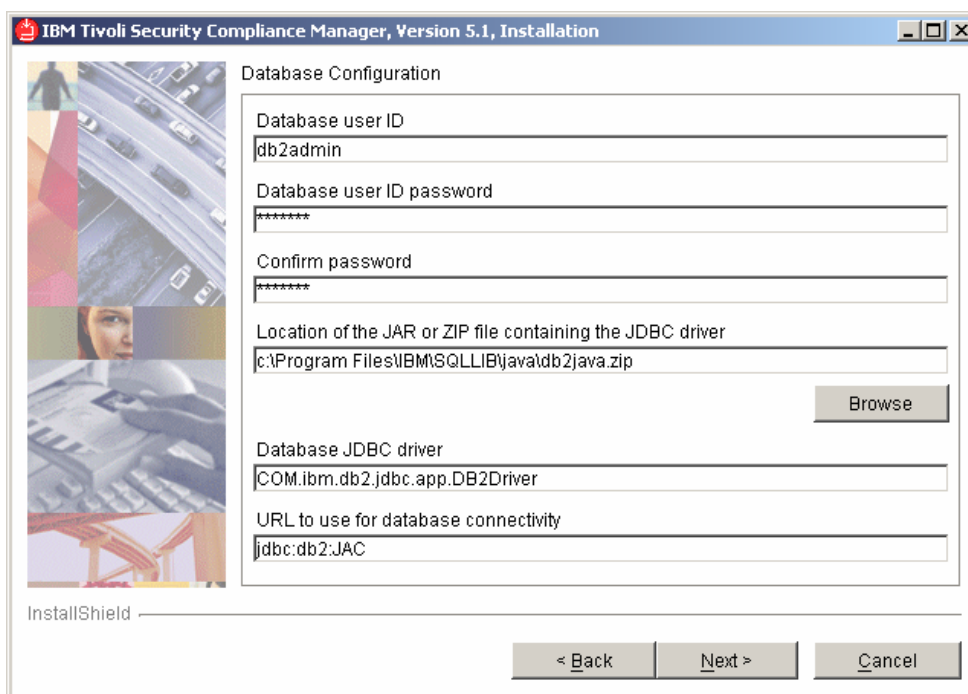
The tick box at the bottom of the dialogue box should be checked. This allows the installation process to create the Security Compliance Manager Server as a Windows service. If you do not tick this box, you will have to manually launch the server using the **jacserver** command.

Set all the password fields to be **passw0rd** and press **Next** to continue.

On this next screen you will specify the location of the database, either local or remote.



For this installation, the database is local and is located on the same server as the IBM Tivoli Security Compliance Manager Server. Therefore you should ensure that the **local system** option is checked. Press Next to continue.



This screen is concerned with the configuration of and connectivity to the DB2 database instance.

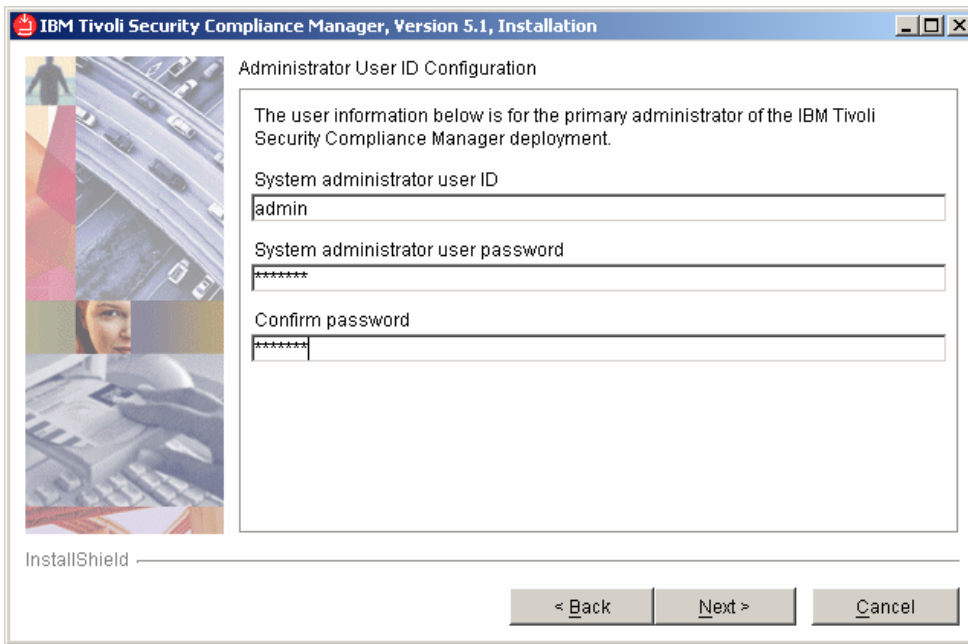
The user ID and password for DB2 are ***db2admin*** and ***passw0rd*** respectively.

You can type the location of the DB2 JDBC driver file into the location field, but it is a good idea to use the browse button to ensure that the correct file is located in the location specified. For Windows, the JDBC driver, db2java.zip, is usually found in the DB2 default install directory, C:\Program Files\IBM\SQLLIB\java.

The remaining two fields should show the defaults for the driver and URL displayed in the screen shot.

If you cannot see the final field on this screen you can either resize the window (as above) or use the scroll bar which will be found on the right hand side when the screen is first displayed.

Press **Next** to continue.

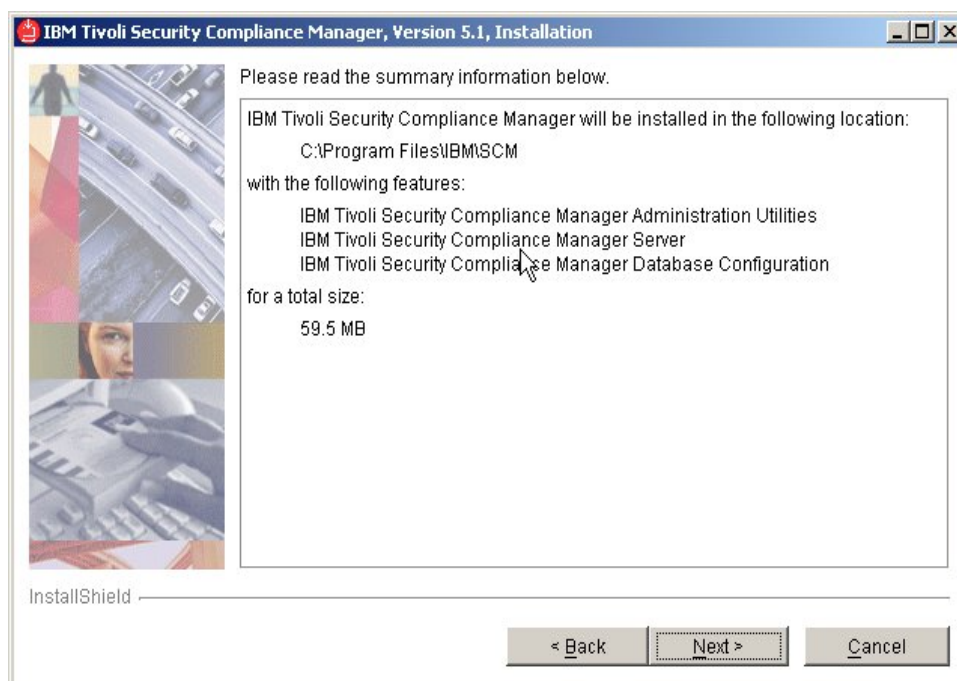


On this screen you set the IBM Tivoli Security Compliance Manager Administrator ID and password. This ID and password will be used to logon to the Administration Console. Use the following for these lab exercises:

User ID:	<i>admin</i>
Password:	<i>passw0rd</i>

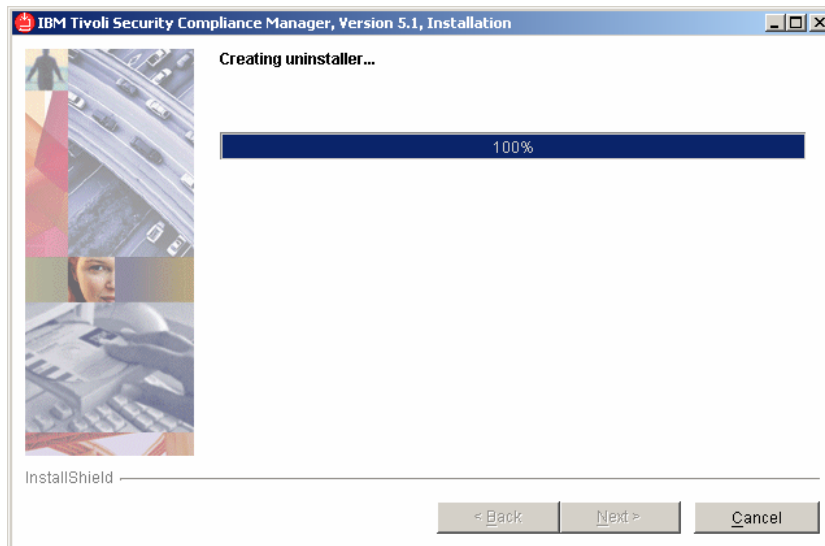
Press **N****ext** to continue.

The screen below shows what configuration options you have selected for the installation. You should note that since you have identified that the database is local on this server, the Security Compliance Manager database configuration software will be installed at the same time as the IBM Tivoli Security Compliance Manager server itself. Also note that the Administration Utilities will be installed. On Windows, this means the Administration Console and the Administrative Command Line Interface will be installed.



This is the last screen that allows you to make changes using the **Back** button. Pressing the **Next** button at this point begins the installation

Press **Next** to continue.



The installation process now begins.

The installation process has now begun and the flash screen will eventually reach the **Creating Uninstaller** phase.

```

C:\DB2 CLP - db2setcp.bat C:\DOCUME~1\ADMINI~1\STA\LOCALS~1\Temp\scminst32756.bat
DB20000I The SQL DISCONNECT command completed successfully.
CONNECT TO JAC

Database Connection Information
Database server      = DB2/NT 8.1.0
SQL authorization ID = ADMINIST...
Local database alias = JAC

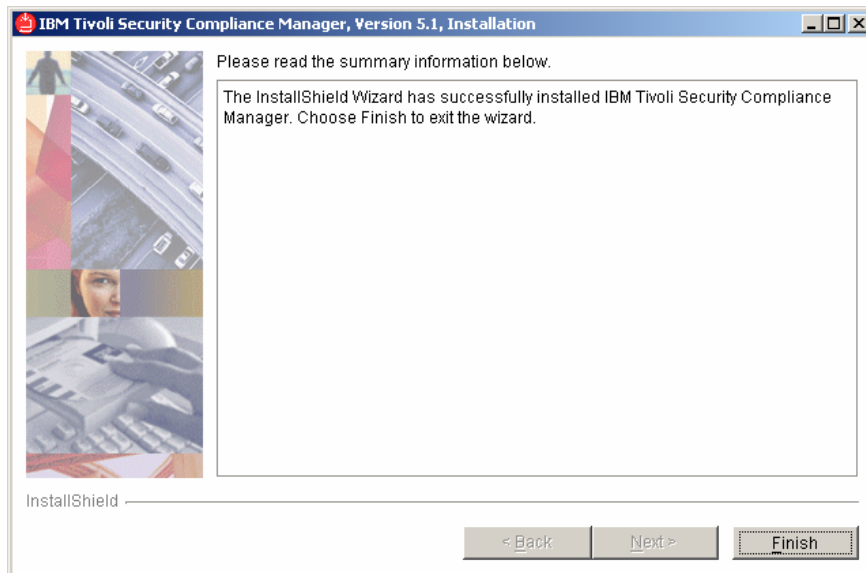
CREATE REGULAR TABLESPACE JAC_DTS IN NODEGROUP IBMDEFAULTGROUP PAGESIZE 32K MANA
GED BY SYSTEM USING ('JAC_DTS') EXTENTSIZ 32 PREFETCHSIZE 32 BUFFERPOOL JAC_BP
DB20000I The SQL command completed successfully.

CREATE TEMPORARY TABLESPACE JAC_TTS IN NODEGROUP IBMTMPGROUP PAGESIZE 32K MANA
ED BY SYSTEM USING ('JAC_TTS') EXTENTSIZ 32 PREFETCHSIZE 32 BUFFERPOOL JAC_BP
DB20000I The SQL command completed successfully.

CREATE TABLE "JAC SYS"."CLIENTS" ( "CLI_ID" INTEGER NOT NULL, "PRIMARY_IP" VAR
CHAR(15), "ROU_ID" INTEGER, "PORT" INTEGER, "CAN_MASQUERADE" CHAR(1), "ALIAS" VA
RCHAR(100), "TYPE" VARCHAR(4), "OFFLINE" CHAR(1), "DESCRIPTION" VARCHAR(250), "F
INGERPRINT" CHAR(47), "DHCP" INTEGER, "OS_NAME" VARCHAR(20), "OS_VERSION" VARCHA
R(20), "OS_ARCH" VARCHAR(20)) IN "JAC_DTS"

```

At the same time, the installation of the database configuration components begins in parallel, but in a command prompt window.



Allow all command windows to finish and close themselves before you press **Finish** to complete the server installation.

4.3 Installation of Tivoli Security Compliance Manager Client V 5.1

4.3.1 Base ITSCM Client Installation

For Details see:

Tivoli® Security Compliance Manager Installation Guide: Client Component Version 5.1

http://publib.boulder.ibm.com/tividd/td/ITSCM/GC32-1593-00/en_US/PDF/scm51_install_client.pdf

For installation of a ITSCM Client call **scm_win32.exe** from the ITSCM code directory

- go to the directory that contains the ITSCM installation code
- call **scm_win32.exe**
- On the first screen : Select language used for the installation wizard, ok
- On the next screen: Accept the Welcome screen, Next
- On the next screen: Accept the licence agreement, Next
- On the next screen: Specify the installation directory, Next
- On the next screen: Select: IBM Tivoli Security Compliance Manager Client, Next



- On the next screen: Confirm client connection port 1950 and client connection mode: push (use defaults)



- On the next screen: Specify server hostname and confirm server connection port 1951 (default)

 **IBM Tivoli Security Compliance Manager, Version 5.1, ...** [Minimize] [Maximize] [Close]



Server Communication Configuration

Server host name
tnt2

Server connection port
195 1

☐ Select the checkbox if this client uses DHCP.

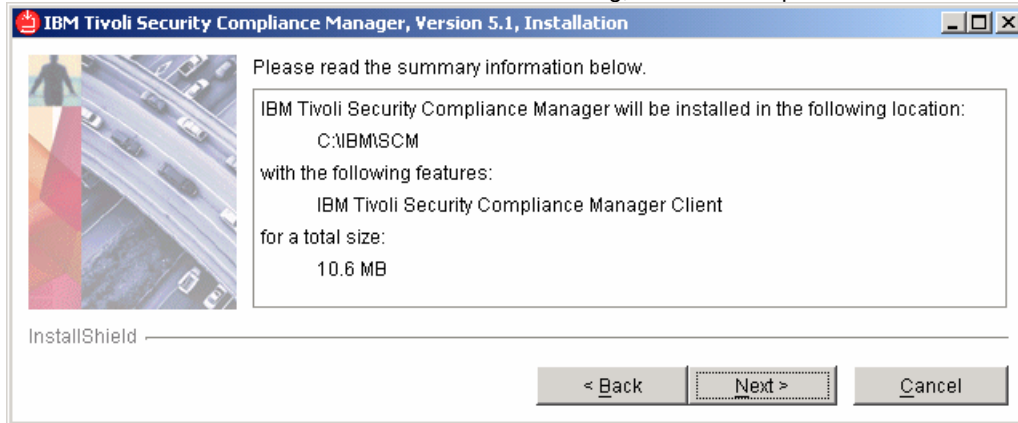
InstallShield

< Back Next > Cancel

Info:

One may want to also select DHCP for both fixed IP addresses and dynamic IP addresses. The difference is that not selecting this means the IP address is used to register the SCM client machine to the server. When selection DHCP a fingerprint is generated based on the digital certificate and that is used to register to the SCM server. The fingerprint makes it easier should the fixed IP address client ever need's to have its IP address changed for any reason. The only reason this cannot be selected is if the client is a pull client although this is likely to change in a future release of the product. Using DHCP will also allow for specifying an alias which can be used at registration or changed at that time and also the ability to set the server to auto register the client if this is required. (see install doc and edit the server.ini file.)

- On the next screen: Confirm the installation setting, Next and complete installation!



5 IBM Tivoli Security Compliance Manager Console Installation

5.1 Installation of a ITSCM Console on Windows 2000 or XP

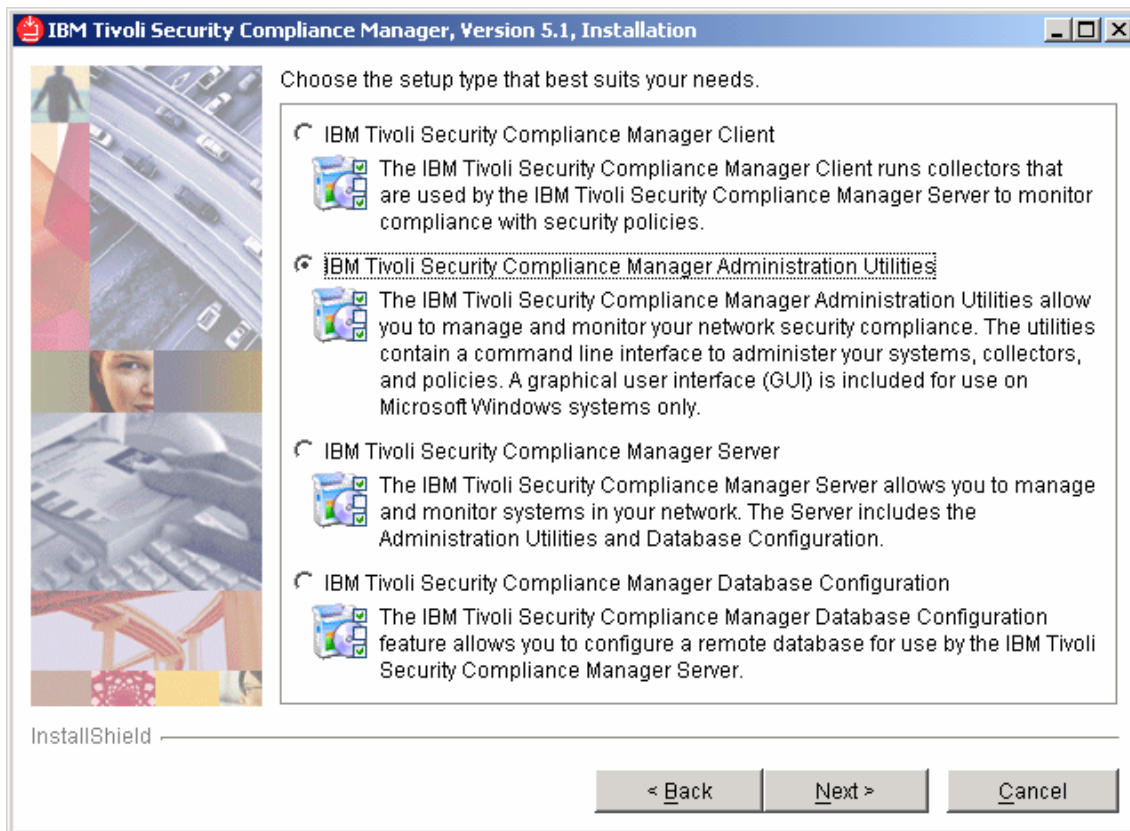
For Details see:

Tivoli® Security Compliance Manager Installation Guide: Client Component Version 5.1

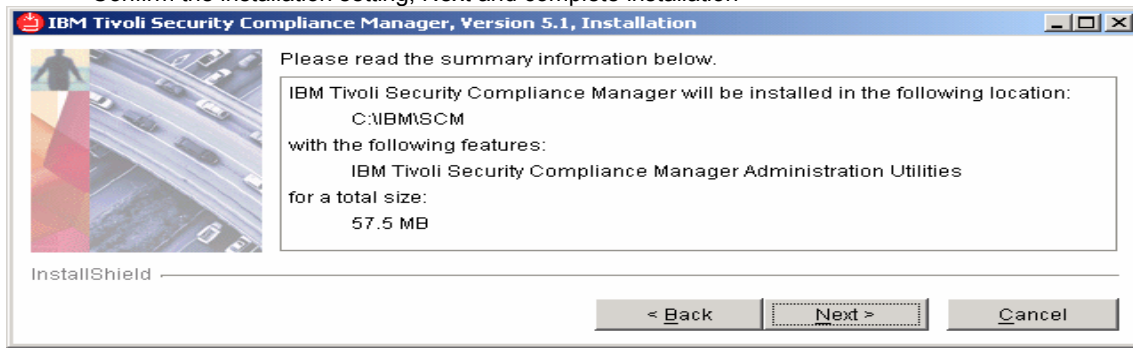
http://publib.boulder.ibm.com/tividd/td/ITSCM/GC32-1593-00/en_US/PDF/scm51_install_client.pdf

For installation of the ITSCM console call scm_win32.exe from the ITSCM code directory

- Select language used for the installation wizard, ok
- On the next screen: Accept the Welcome screen, Next
- On the next screen: Accept the licence agreement, Next
- On the next screen: Specify the installation directory, Next
- On the next screen: Select: IBM Tivoli Security Compliance Manager Administration Utilities, this includes the java GUI for Win32 OS.



- Confirm the installation setting, Next and complete installation



6 Tuning Guidelines

6.1 *The law of diminishing Returns*

The greatest performance improvements usually result from the initial efforts at tuning.

6.2 *Tuning just for the sake of tuning*

Only adjust identified limitations. If non-associated resources are tuned, these will have little or no effect on response time until the major constraints are relieved. Major resource barriers are the ones that significantly impact performance the most.

6.3 *Consider the entire system*

Never tune in isolation. This means that tuning should not be done without considering the entire system.

6.4 *One parameter at a time*

Don't change more than one parameter at a time. Even if you're sure that all the changes will be beneficial, you will have no way of evaluating how much each change contributed. Also, the trade-offs cannot be judged effectively. Every time a parameter is adjusted to improve one area, it almost always affects at least one other area that may not be considered. By changing only one at a time, this allows you to have a benchmark to evaluate whether the change does what you want.

6.5 *Tune by levels*

For the same reasons that you should only change one parameter at a time, tune one level of your system at a time. You can use the following list of levels within a system as a guide:

- Hardware
- Operating System
- Application Server
- Database Manager
- SQL Statements
- Application Programs

6.6 *Hardware as well as software*

Some performance problems may be corrected by applying service either to your hardware, or to your software, or to both. Do not spend excessive time monitoring and tuning your system when simply applying service may make it unnecessary.

6.7 Understand the problem

Even if it seems that additional storage or processor power could immediately improve performance, take the time to understand where your bottlenecks are. You may spend money on additional disk storage only to find that you do not have the processing power or the channels to exploit it.

6.8 Put fall-back procedures in place

As noted earlier, some tuning can cause unexpected performance results. If this leads to poorer performance, it should be reversed and alternative tuning tried. If the former setup is saved in such a manner that it can be simply recalled, the backing out of the incorrect information becomes much simpler.

6.9 The top tuning factors

1. Make sure there is enough disk space
2. Buffer pools should use 50-75% of available memory for high-end production servers
3. Runstats should be performed on all tables
4. Use the Configuration Advisor to configure the database for the application environment
5. Logging should be to separate high-speed disks. This is done via the NEWLOGPATH configuration parameter.
6. Commit often to increase concurrency.
7. To avoid sort overflows, increase SORTHEAP.
8. Table space should be SMS for the system catalog temporary or DMS for the rest.
9. Use parameter markers for repeated SQL statements.

7 DB2 Database Installation Considerations and Performance Tuning

The purpose of this section is to address the tuning requirements of DB2 UDB in the context of IBM Tivoli Security Compliance Manager (ITSCM) and the proper handling of additional components.

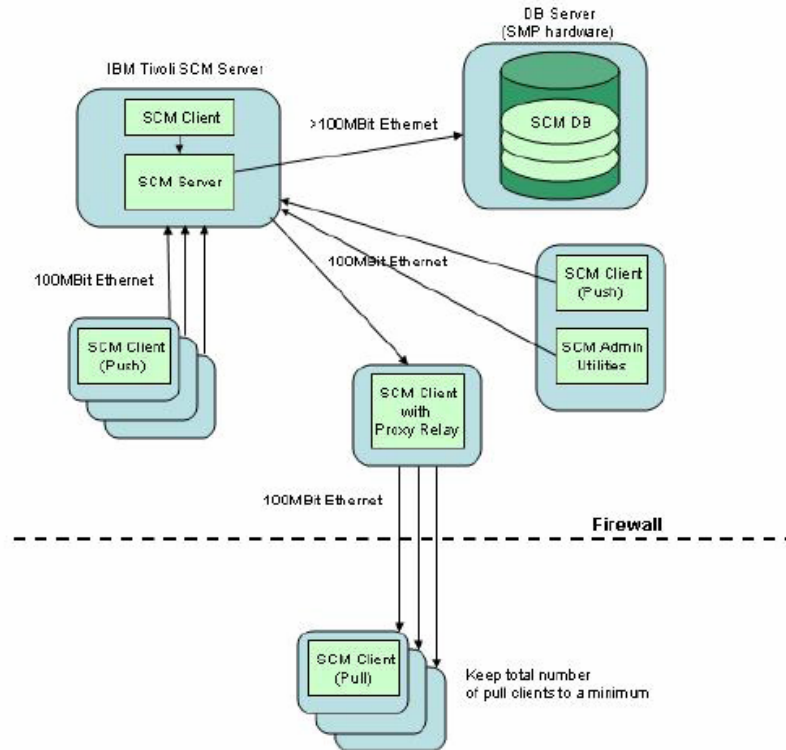
The ITSCM data collection function, into a DB2 UDB Relational Database Management System (RDBMS), often results in a condition where system resources are exhausted, or unavailable, creating a situation that requires immediate intervention.

To this end, a correct implementation, and/or successful tuning, of the DB2 UDB RDBMS used for data collection of ITSCM information promises a more stable deployment, greater uptime, and a clearer path to an evident Return-On-Investment (ROI).

7.1 DB2 Installation Suggestions

The DB2 UDB database server functions as the storage area for ITSCM data. This database may be installed on the same system as the ITSCM Server, although performance would improve if it was installed on a separate, dedicated system with multiple CPUs. The following diagram illustrates a suggested configuration for a high volume setup.

Suggested Configuration



7.2 DB2 Tuning Suggestions

1. Increase Buffer Pool size
2. Place logs on a separate device
3. Increase log file size
4. Clear snapshots regularly
5. Add indexes as necessary

7.2.1 Buffer Pools

Properly defining buffer pools is one of the major keys to having a well-performing system. With 32-bit operating systems, it is important to be aware of the limit on shared memory, which restricts a database's buffers pools (that is, database global memory) from exceeding the following limits (64-bit systems do not have this limit):

- AIX - 1.75 GB

- Linux - 1.75 GB
- Sun - 3.35 GB
- HP-UX - approximately 800 MB
- Windows - 2-3 GB (use '3GB' switch in boot.ini on NT/2000)

A buffer pool is memory storage that temporarily stores information read and changed prior to being written back to disk. The primary purpose of buffer pools is to improve database performance. Essentially, the fewer hard read/write operations made to disk, the better.

7.2.2 Increasing Buffer pool size

Depending on available memory, increase the JAC_BP significantly as follows (system memory >= 2GB):

```
db2 connect to jac
db2 alter bufferpool jac_bp 16384
db2 select jac_bp from syscat.bufferpools
```

7.2.3 Placing logs on a separate device

If placing log files on a separate device, verify the device exists prior to proceeding. Set the location for log file output:

Win32:

```
db2 update db cfg for jac using newlogpath=\\D:
```

Unix/Linux:

```
db2 update db cfg for jac using newlogpath=/newlogdevice
```

7.2.4 Increase log file size

A database that has a large number of update, delete, or insert transactions running against it which will cause the log file to become full very quickly, typically by the error "transaction log full". These parameters are:

```
LOGPRIMARY
LOGSECOND
LOGFILSIZ
```

Note: SCM 5.1 has these properties set appropriately by default.

7.2.5 Clear snapshots

To delete (clear) one or more snapshots that are no longer needed:

- A. Open the Storage Management View

- a. From the Control Center window, expand the object tree until you find the database, database partition group, or table space you want to examine in the Storage Management view.
 - i. Right-click the desired database and select Manage Storage from the pop-up menu. The Storage Management view opens.
 - b. From the Storage Management view, expand the object tree until you find the database, table space, or database partition group object associated with the snapshot you want to remove.
 - c. Right-click the object and select Remove Historical Snapshots from the pop-up menu. The Snapshot Deletion window opens.
- B. Select one or more snapshots from the list of historical snapshots.
- C. Click OK. The Snapshot Deletion window closes and the specified snapshots are deleted.

7.2.6 Add indexes as necessary

As an example, create the index on the *cli_id* and *instance_id* columns for the JAC_IDATA.CUSTOM_COLLECTOR_V5 table using the *create index* command:

```
# db2 create index CUSTOM_COLLECTOR_INDEX on
JAC_IDATA.CUSTOM_COLLECTOR_V5 (cli_id,instance_id)
```

Note: Testing has indicated that additional indexes do not improve DB2 performance appreciably.

7.2.7 Additional Tuning

The IBM Tivoli Security Compliance Manager is foundationally based on the database and thus efficiency of SQL statements is key not only to the operation of the IBM Tivoli Security Compliance Manager components but also to user defined queries such as those used in reports and policies and accessing tables for in-house collectors. The following describes a method that can be utilized to pinpoint sub optimal SQL execution and optimize the efficiency of the execution. As of the time of this publication the IBM Tivoli Security Compliance Manager provides support for the IBM DB2 database; the following section focuses on this database software. It is recommended that a DBA or the database manager be chosen to perform these recommended procedures.

The IBM DB2 UDB program includes provisions that allow the database administrator to enable monitors within the database program that keep track of the amount of time and work that is required for SQL statements to execute. You can view the current settings with the *get monitor switches* command.

```
# db2 get monitor switches
```

Monitor Recording Switches

```
Switch list for db partition number 0
Buffer Pool Activity Information (BUFFERPOOL) = OFF
```

Lock Information	(LOCK) = OFF
Sorting Information	(SORT) = OFF
SQL Statement Information	(STATEMENT) = OFF
Table Activity Information	(TABLE) = OFF
Take Timestamp Information	(TIMESTAMP) = ON
Unit of Work Information	(UOW) = OFF

By default the monitor switches, save the timestamp monitor, are disabled. To enable the monitor switches use the *update monitor switches* command. Normally, it's safe to just enable all the switches; this is what you do in this example here although you are only interested in the *statements* monitor.

```
# db2 update monitor switches using bufferpool on
# db2 update monitor switches using lock on
# db2 update monitor switches using sort on
# db2 update monitor switches using statement on
# db2 update monitor switches using table on
```

Followed by:

```
# db2 get monitor switches
```

Monitor Recording Switches

Switch list for db partition number	0
Buffer Pool Activity Information	(BUFFERPOOL) = ON
Lock Information	(LOCK) = ON
Sorting Information	(SORT) = ON
SQL Statement Information	(STATEMENT) = ON
Table Activity Information	(TABLE) = ON
Take Timestamp Information	(TIMESTAMP) = ON
Unit of Work Information	(UOW) = OFF

After the monitor switches have been enabled, operations throughout the IBM Tivoli Security Compliance Manager that cause database activity can be performed. After these operations have been completed, take a snapshot of the monitors using the *get snapshot* command.

```
# db2 get snapshot for all on JAC > snapshot.txt
# cat snapshot.txt
```

```
...
Number of executions          = 1
Number of compilations        = 1
Worst preparation time (ms)    = 4
Best preparation time (ms)     = 4
Internal rows deleted         = 0
Internal rows inserted        = 0
```

```

Rows read                                = 2095777
Internal rows updated                    = 0
Rows written                             = 0
Statement sorts                          = 0
Total execution time (sec.ms)            = 64.718209
Total user cpu time (sec.ms)              = 7.520000
Total system cpu time (sec.ms)           = 0.350000
Statement text                           = delete from
JAC_IDATA.CUSTOM_COLLECTOR_V5 where CLI_ID=1636 and
INSTANCE_ID=37

```

The snapshot will display information about each query executed such as *rows read* and *total execution time*. You can see in this example that this particular delete query takes over a minute to execute. Using the IBM DB2 *explain* tool you can discover how DB2 is executing the query.

The explain tool output tells you that the database is using a *table scan* to locate prospective entries. Table scans are notoriously slow on larger tables (i.e. over a million rows) and are usually replaced automatically with indexes. In some instances the IBM DB2 optimizer will automatically generate indexes for large tables, in some instances it will not, and thus you may choose to manually create the indexes if the query is to be executed frequently.

In this particular instance you can create the index on the *cli_id* and *instance_id* columns for the JAC_IDATA.CUSTOM_COLLECTOR_V5 table using the *create index* command:

```

# db2 create index CUSTOM_COLLECTOR_INDEX on
JAC_IDATA.CUSTOM_COLLECTOR_V5 (cli_id,instance_id)

```

To reset the database monitors use the reset monitor command. Next you should repeat the operations you performed through the IBM Tivoli Security Compliance Manager. Finally, you can take another snapshot and/or use the *explain* tool to verify the predicted optimization.

```

# db2 reset monitor for database jac

# db2 get snapshot for all on JAC > snapshot.txt
# cat snapshot.txt

...
Number of executions                    = 1
Number of compilations                  = 1
Worst preparation time (ms)             = 4
Best preparation time (ms)              = 4
Internal rows deleted                   = 0
Internal rows inserted                  = 0
Rows read                              = 0
Internal rows updated                   = 0
Rows written                           = 0
Statement sorts                         = 0
Total execution time (sec.ms)           = 0.005257
Total user cpu time (sec.ms)            = 0.010000
Total system cpu time (sec.ms)          = 0.000000

```

```
Statement text          = delete from  
JAC_IDATA.CUSTOM_COLLECTOR_V5 where CLI_ID=1636 and  
INSTANCE_ID=37
```

You can see in this example that the rows read decreased from millions to 0 due to the use of the index. The corresponding decrease in time of execution was from 64 seconds to a few milliseconds. You can view the SQL execution path with the *explain* tool.

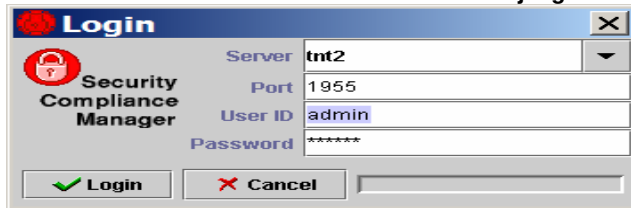
The explain tool output shows that no table scans were used, instead only indexes were referred to when executing the query. Again this method can be utilized to optimize SQL statement execution for tables created for custom collectors and for SQL statements created for reports and policies.

8 IBM Tivoli Security Compliance Manager Console Functions

8.1 Logging on to ITSCM Server via GUI

On the Windows System, start the ITSCM GUI (this GUI is available on Linux with Fix Pak 2):

Use the red icon  or call C:\IBM\SCM\admin\jacgui.bat



- Enter the Administrator ID and Password defined in the installation (ID = admin
PW = passw0rd)

9 Configuration of IBM Tivoli Security Compliance Manager Clients and Collectors

9.1 Managing Clients

9.1.1 Before you start

So far you have the IBM Tivoli Security Compliance Manager Server (and DB2), the Security Compliance Manager Administration Console and the Security Compliance Manager Client installed and running on Windows Linux or AIX. On the

Registering Clients

Security Compliance Manager Clients have to be registered with the Server. Clients configured as 'push' or 'pull' type clients are registered manually by using the Administration Console. The fix IP address of these machines is used to uniquely identify each register system. IF the IP address ever needs to be changed then the system would need to be de-registered, the client certificate removed and the client with the new IP address registered and put back in to the associate groups.

If there are DHCP machines in your environment, then the Security Compliance Manager Client should be installed as DHCP clients (option during the installation process – if the client has not been registered with the server this option can be changed by editing the client.pref file). These DHCP clients can be registered manually using the Administration Console like the 'push' and 'pull'. In addition, the Security Compliance Manager server provides a mechanism to allow for the automatic registration of Security Compliance Manager DHCP Clients. This is done by setting the parameter *jac.dhcp_auto_register* to **true** in the *server.ini* file. After restarting the Security Compliance Manager Server for the change to take effect, Security Compliance Manager DHCP Clients that contact the server will automatically be registered.

ITSCM Clients configured as DHCP, have the advantage of auto registration, pre-defined aliases and that when they are registered in the ITSCM server a fingerprint generated from the client's digital certificate is used to create a unique identity instead of the IP address and therefore a fixed IP address could be changed with out and lose of connection or compliance data tracking in the ITSCM Server database.

Most machines in a network are recommended to be installed as DHCP clients regardless on having a fix IP or a dynamic IP address. The only clients that have to be non DHCP ITSCM Clients are those in push mode. These are generally behind firewalls in DMZ or other low security zones that should not have the ability to initiate a connection to the ITSCM Server zone. Configuring clients with the ITSCM DHCP option is the recommended configuration although it is probably not the best term to describe this function.

9.2 Register the ITSCM Client

Clients can be manually registered using the GUI as described below or automatically.

9.2.1 Automatic Client Registration

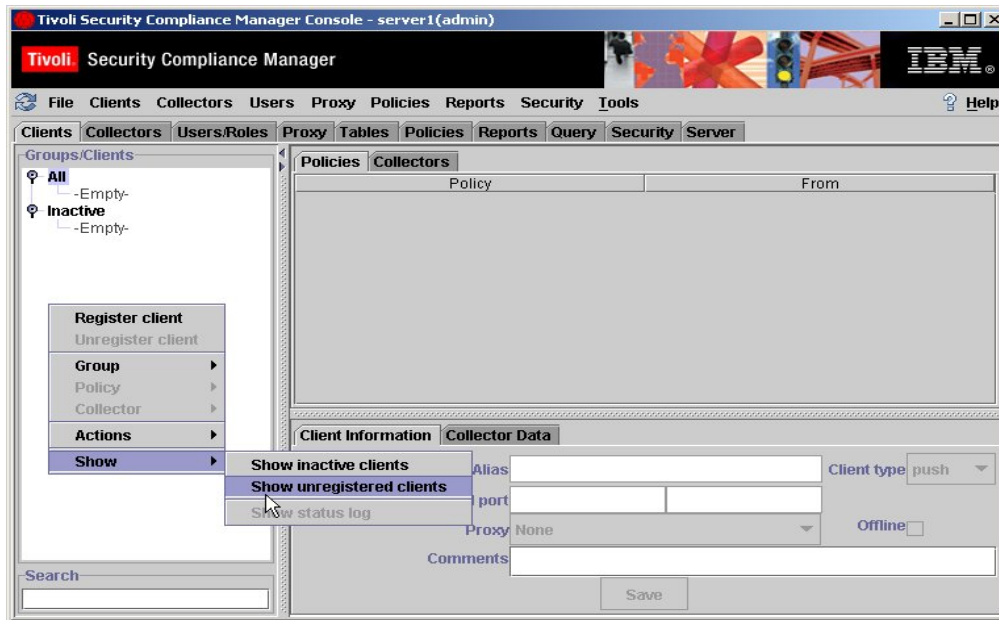
To have client automatically register it is necessary to edit the *server.ini* file

- On an AIX system it will be found :

- On a Linux system it will be found :
- On a Windows system it will be found : c:\Programs File\IBM\scm\server\

9.2.2 Manual Client Registration

- To register the clients that have been installed, launch the Administration Console, then go to the **Clients** tab.
- The “Groups” can be opened by clicking with the left mouse button on the toggle icon
- Right click in the Groups/Clients area and select **Show** and then **Show Unregistered Clients** from the popup menu.



The resulting dialogue box shows any unregistered clients that have contacted the Security Compliance Manager Server.



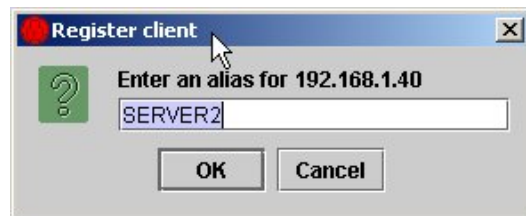
- Select the system you wish to register and click **Register** to continue. The next screen asks for the IP address or hostname to be entered, but will usually bring up the default value associated with your selection.



- The IP address, or host name you selected in the previous step now appears. Click **OK** to continue.

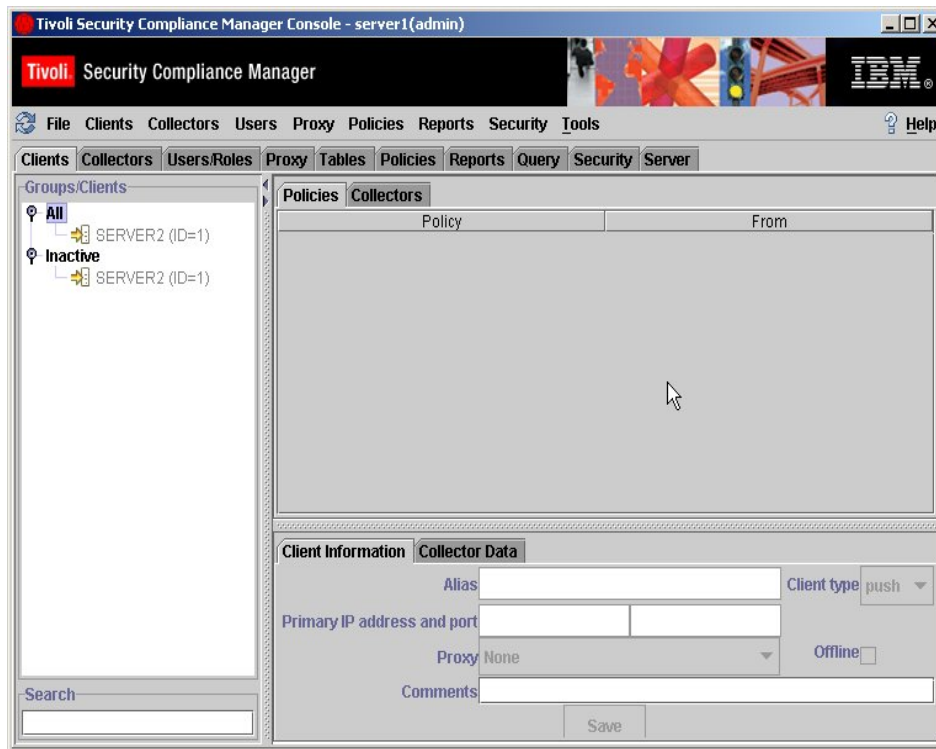
The next screen asks for an alias to be entered. This will default to the fully qualified hostname of the client system, but can be any value you choose. This alias is the name that will appear on the Administration Console, and has no relevance to the hostname of the machine. In this lab we'll make it the same as the hostname. If this was a DHCP client and an Alias name was specified in the installation of the client then that Alias name is displayed in this box. It can be changed at this time if required. The Alias name was configured in the **client.pref** at install time.

- Click **OK** to continue.



The final dialogue in the registration process asks if you want to include the registered client in any client groups. If no groups have been created, this dialogue should be empty, and simply click **OK** to continue. It would be recommended to create client groups before registering too many clients manually to ease the administration of adding client to groups at a later stage. Refer to [creating client groups](#) for further details.

By default, any registered client is included in the **All** group even if you do not select other groups for the client to be a member of. Until the Client heartbeat expires, the client will appear inactive on the Administration Console.



After registration, the new client will appear in the **All** container located under the Client tab. It will also appear initially in the **Inactive** container until there is actual communication between the client and server for the first time. The client entry appears greyed out, but once communication has been established the client entry will appear in a bold font. When this happens, it will also disappear from the Inactive container. The time taken for this change will depend upon the timing settings contained within the client.pref file (default 10 min). Use the refresh button on the Administration Console to check to see if the client has become active. Once it has become active, this can be verified by selecting the client name, right clicking and selecting **Actions** and **Check client connection**.

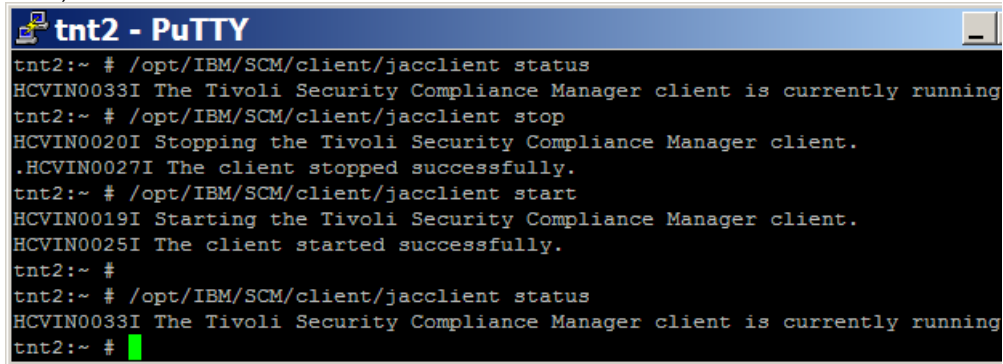
To make the client active without waiting for the default heartbeat timer it is necessary to restart the ITSCM client.

9.2.2.1 Restarting ITSCM Client on Linux

Note:

If “Check client connection” fails you have two choices

- a) Wait until next Heartbeat (10 min per default)
- b) Restart the SCM client:



```
tnt2:~ # /opt/IBM/SCM/client/jacclient status
HCVIN0033I The Tivoli Security Compliance Manager client is currently running
tnt2:~ # /opt/IBM/SCM/client/jacclient stop
HCVIN0020I Stopping the Tivoli Security Compliance Manager client.
.HCVIN0027I The client stopped successfully.
tnt2:~ # /opt/IBM/SCM/client/jacclient start
HCVIN0019I Starting the Tivoli Security Compliance Manager client.
HCVIN0025I The client started successfully.
tnt2:~ #
tnt2:~ # /opt/IBM/SCM/client/jacclient status
HCVIN0033I The Tivoli Security Compliance Manager client is currently running
tnt2:~ #
```

The next “Check the client connection” should be successful.

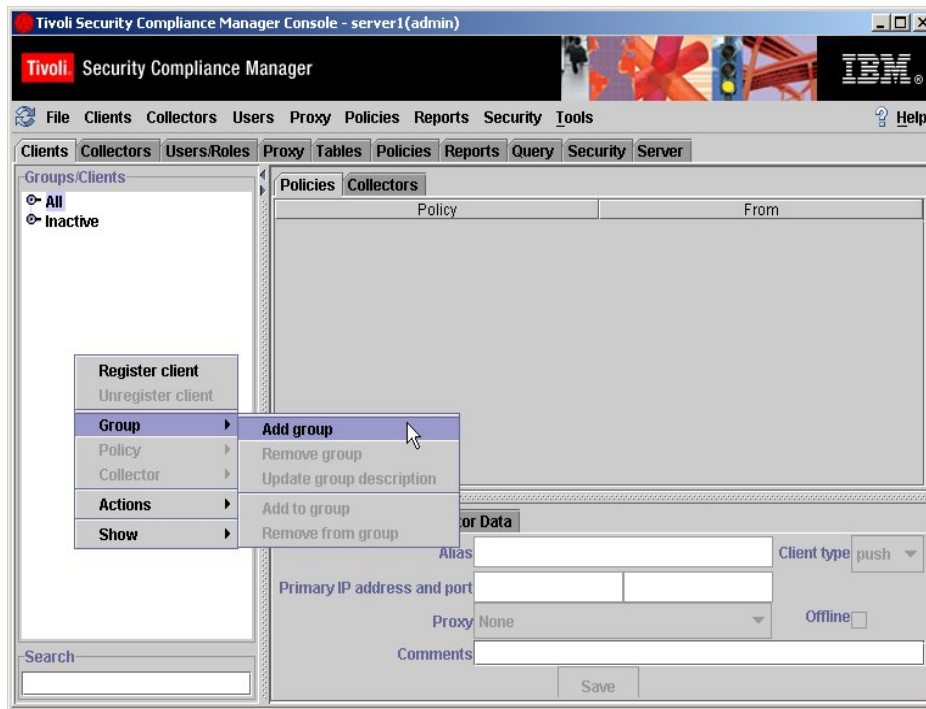
9.2.2.2 Restarting ITSCM Client on Windows

The ITSCM client can be stopped and started from the Services window which can be found in the Control Panel/Administrative Tools/Services

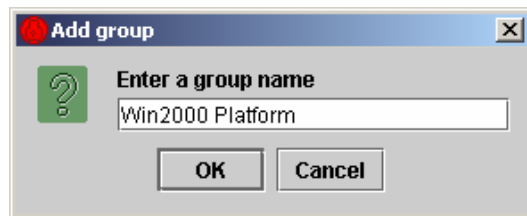
9.2.3 Creating Client Groups

Using client groups allows one to more efficiently manage collectors, policies and reports when running on large numbers of client systems. For example, you can create group names that categorize client systems by operating system, location, application or security policy. In addition, groups can be nested into sub-groups.

To create a client group, go to the **Clients** tab and select **Group** and then **Add Group** from the **Clients** menu. (You can also use the keyboard short cut *Ctrl*+*G* from the **Clients** tab).



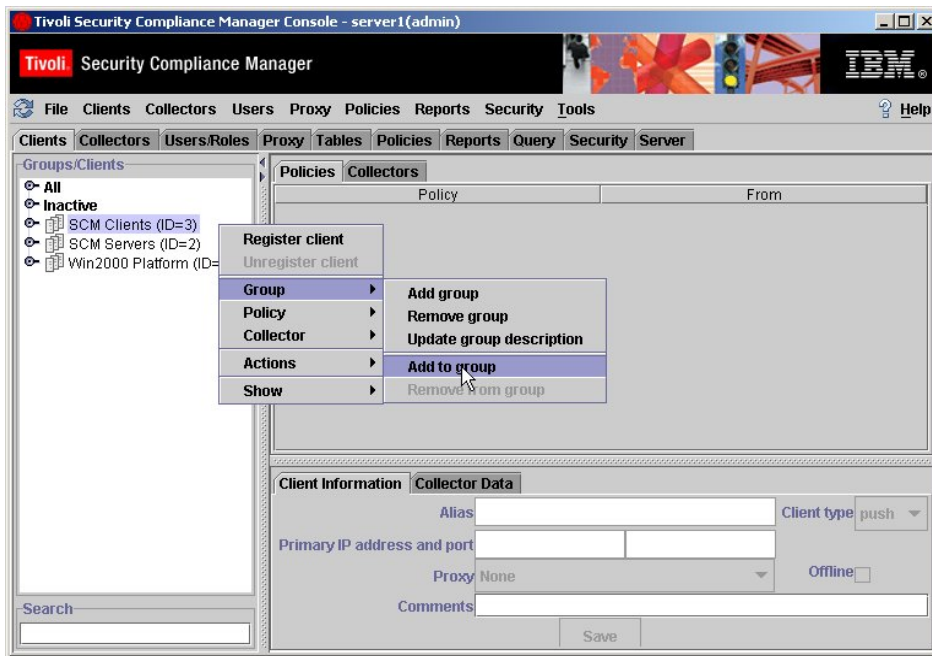
Enter the new group name **Win2000 Platform** in the **Add Group** dialog box and press **OK**.



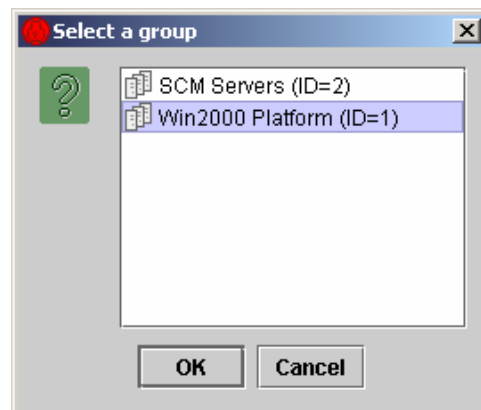
You should now have three groups – **All**, **Inactive**, **Win2000 Platform**.

9.2.4 Creating Nested Client Groups

Create two new groups, example called **ITSCM Servers** and **ITSCM Clients**. Right click on the **ITSCM Clients** group once it appears and select the **Group** and **Add To Group** sub menus from the pop ups.

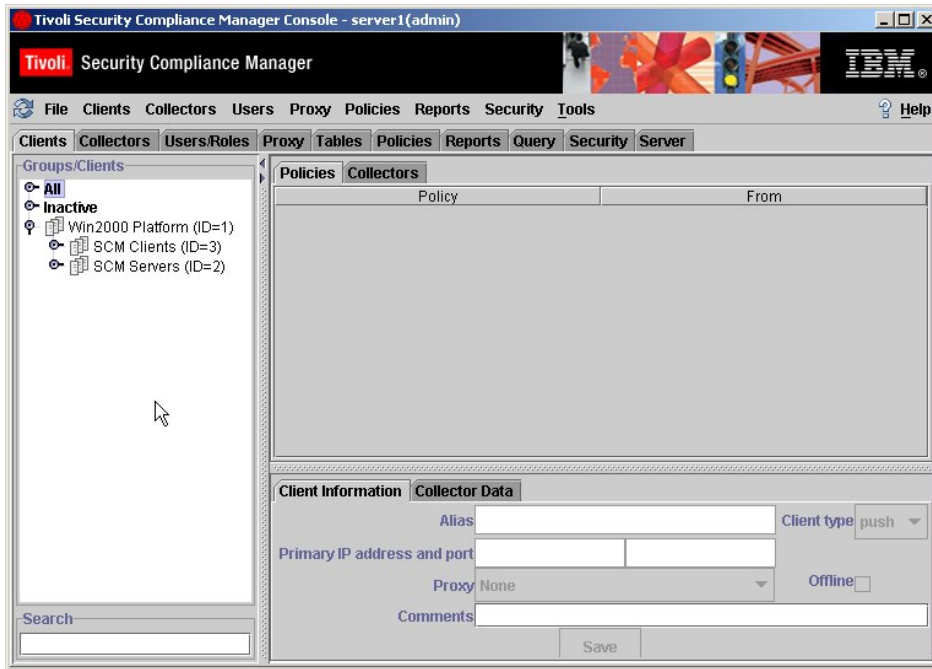


The new dialogue box will show all the groups you have created excluding the group you selected. This prevents you adding a group to itself.



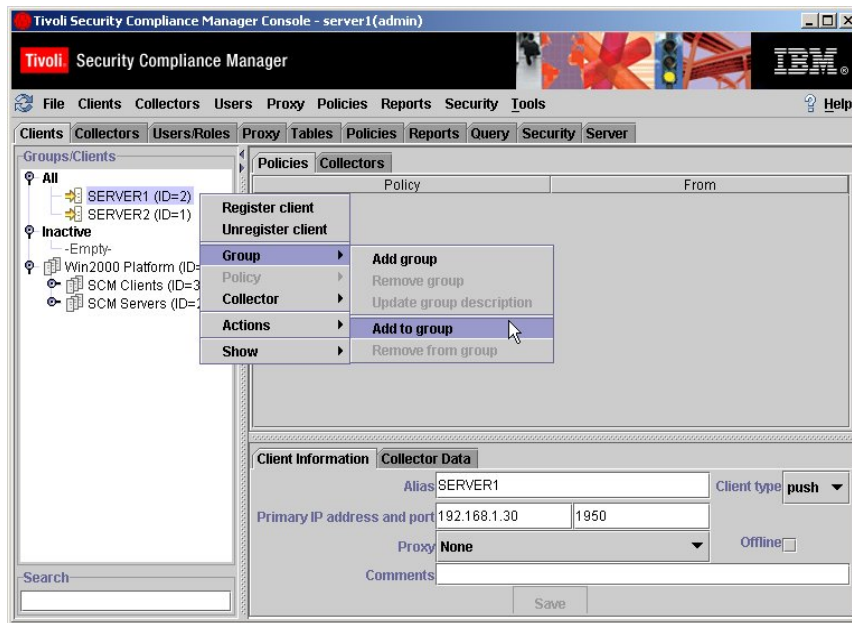
Select the **Win2000 Platform** group and press **OK** to continue. This will move the new **ITSCM Clients** group into the Win2000 Platform group.

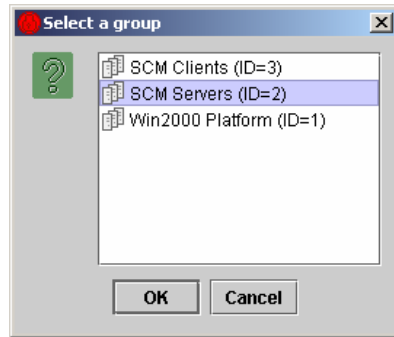
Repeat these steps for the **ITSCM Servers** group.



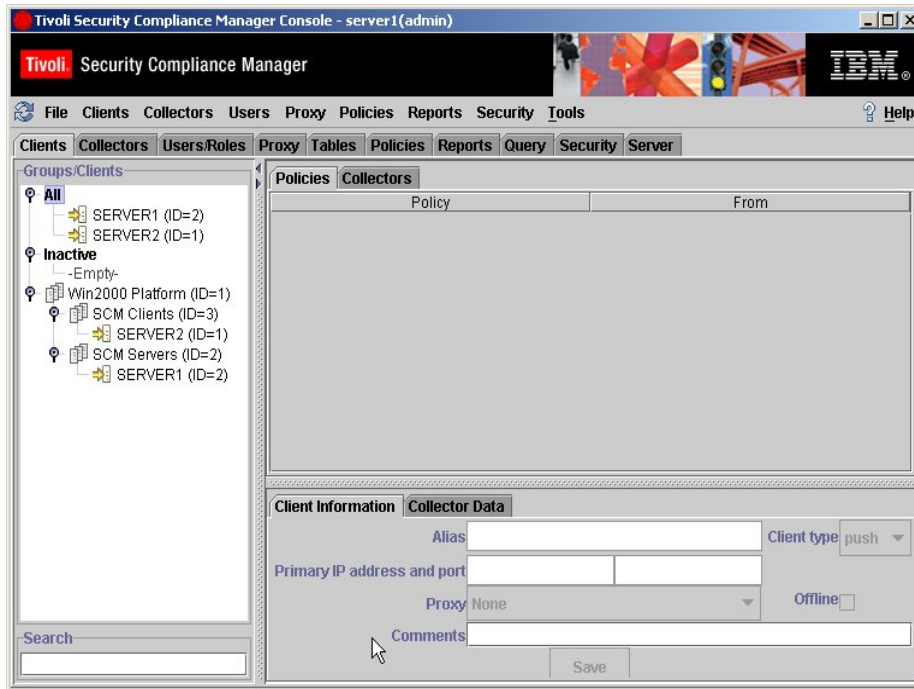
After completing the steps, both groups should appear as subgroups under the parent group, **Win2000 platform**.

Client systems are added to groups in exactly the same way. Select a registered **ITSCM client**; right click and select **Group**, then **Add to group**, then **ITSCM Servers** and finally click **OK**





Now to add another client (Example **Server2** client) to the group called **ITSCM Clients**.



You have now created a nested hierarchy of groups and clients which will allow you to add policies and collectors to systems, and set access rights for users with the appropriate roles.

9.3 Configuring Collector Authorization

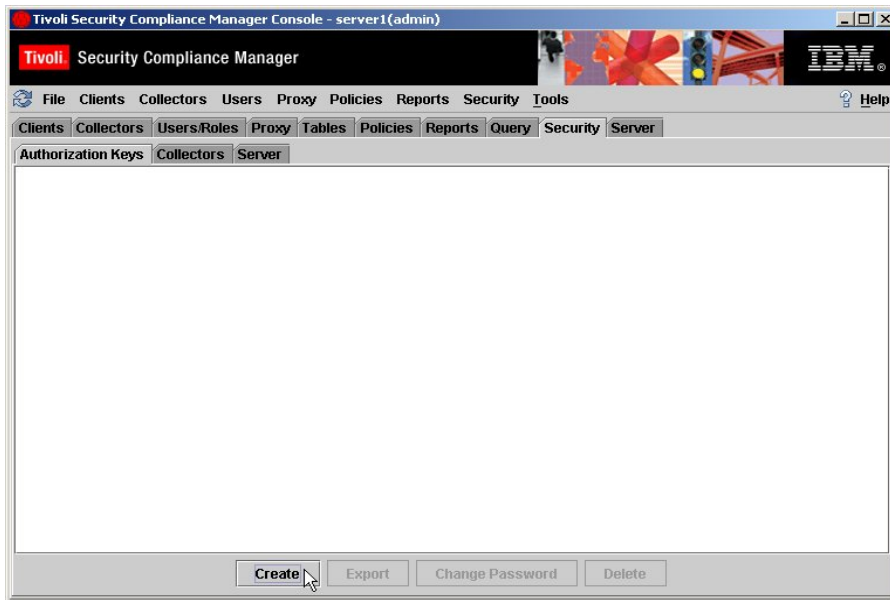
9.3.1 Before you Start

By default, when the Security Compliance Manager Server is installed, the collector authorization level is set to zero. This means that collectors only require the IBM Collector certificate (base certificate for all collectors) to be registered and used in the Security Compliance Manager environment. In an environment set up in this manner, an installed collector is automatically moved to the 'authorized' state and is ready to be registered and then deployed to clients.

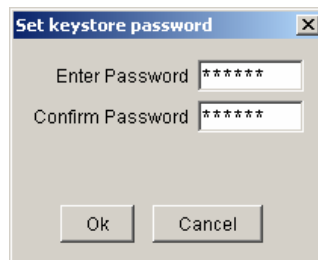
Administrators may want to establish an additional level of security and require collectors to be signed with additional certificates specific to their environment. This can be accomplished by setting the collector authorization level on the Security Compliance Manager server. The collector authorization level should be set prior to installing collectors.

9.3.2 Create Keystore and Authorization Key

First, create a keystore for the authorization keys. Go to the **Security** tab then select the **Authorization Keys** tab. Select **Create**.



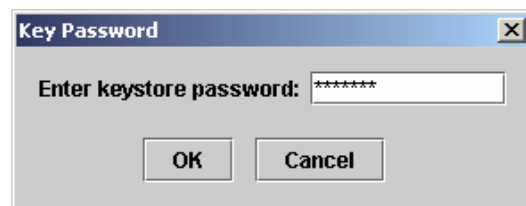
Specify the password for the keystore being created (Example: **passw0rd**).



Once the keystore is created, authorization keys can be created. Right click in the **Authorization Keys** display area to display the menu; select **Request New**.



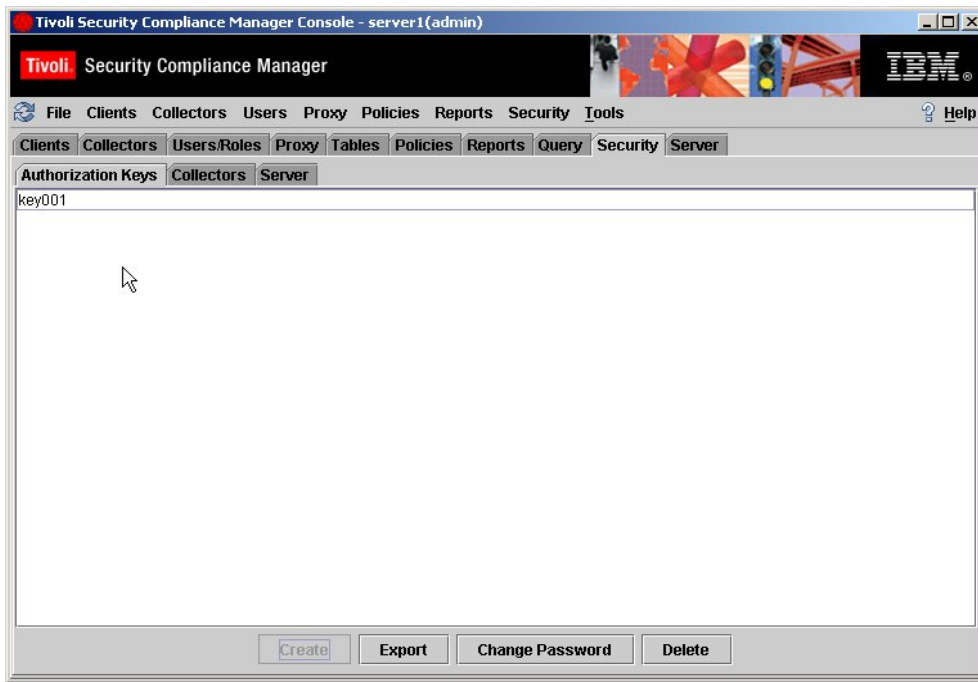
Provide the keystore password (passw0rd).



Next provide a name for the authorization key being created then select 'OK'.



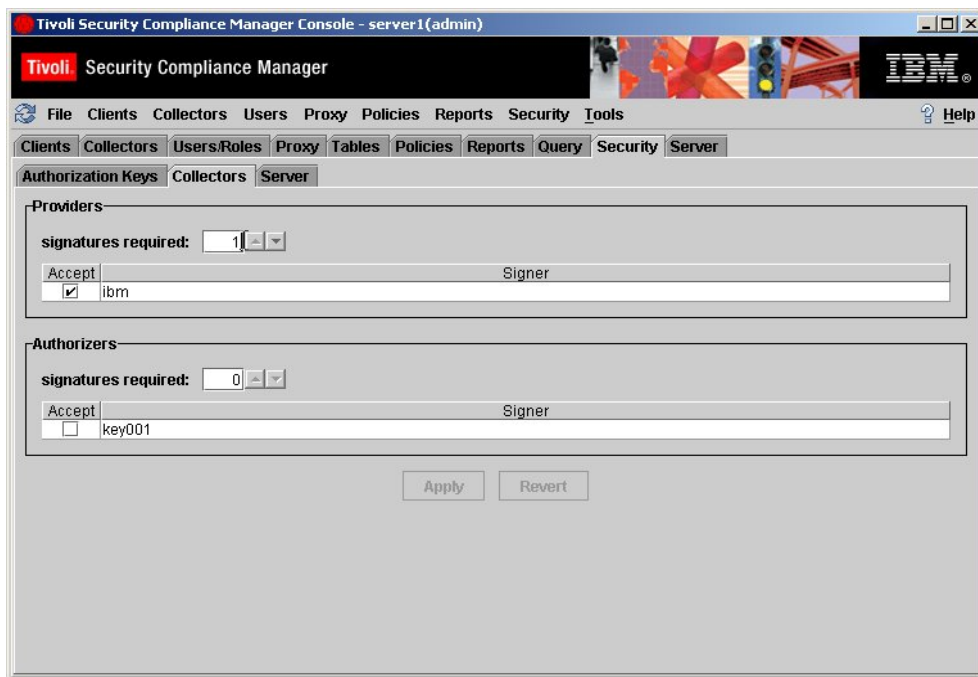
The authorization key is created and displayed in the **Authorization Keys** view.



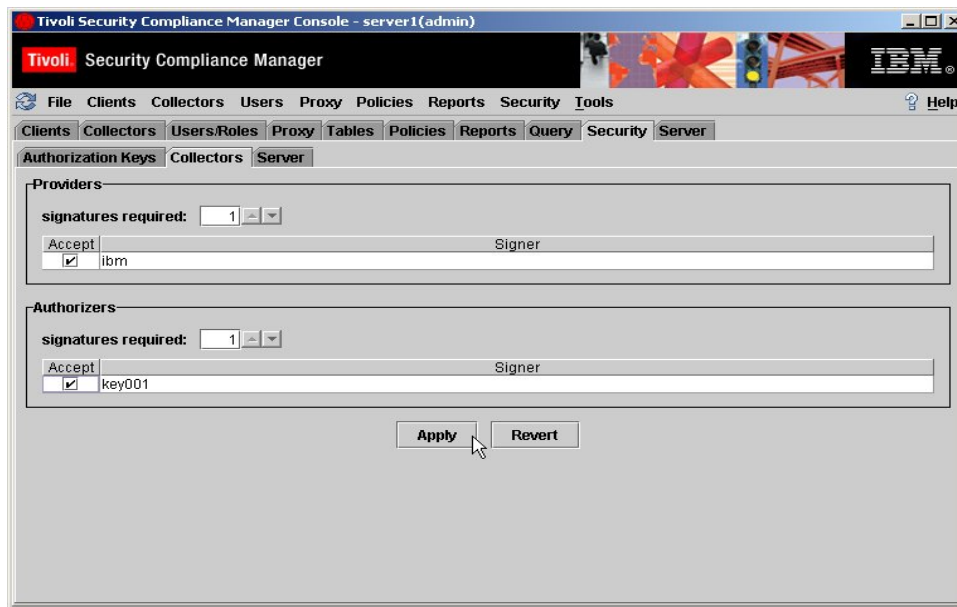
9.3.3 Set Collector Authorization Level

Once an authorization key is created, the authorizations required for collectors in this Security Compliance Manager environment can be set to a value greater than zero.

Under the **Security** tab, select the **Collectors** tab.



Select the newly created key. Use the arrow buttons next to the **signature required** field to increment the value to one; select **Apply**.



Collectors in this Security Compliance Manager environment are now required to be signed with the newly created authorization key before these collectors can be registered with the server and deployed to clients in the environment.

9.4 Managing Collectors

9.4.1 Before you Start

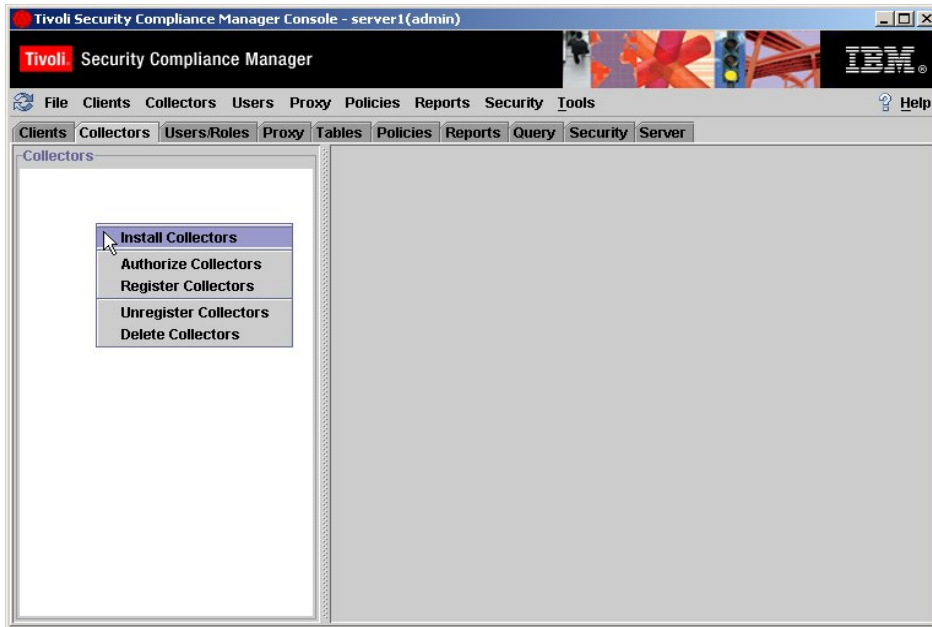
It is possible to install and run collectors individually, although the normal mode of operation will be to create or import Policies and run the required collectors as part of a Policy. If individual collectors are required for a new policy or a collector has been developed or a new function this process will also be needed so that the collector can be added to the policy.

This section is designed to help you understand the mechanics of collectors in isolation from Policies. This will be done by installing and running collectors. The collectors should be available on the local disk of the system with the administrator console.

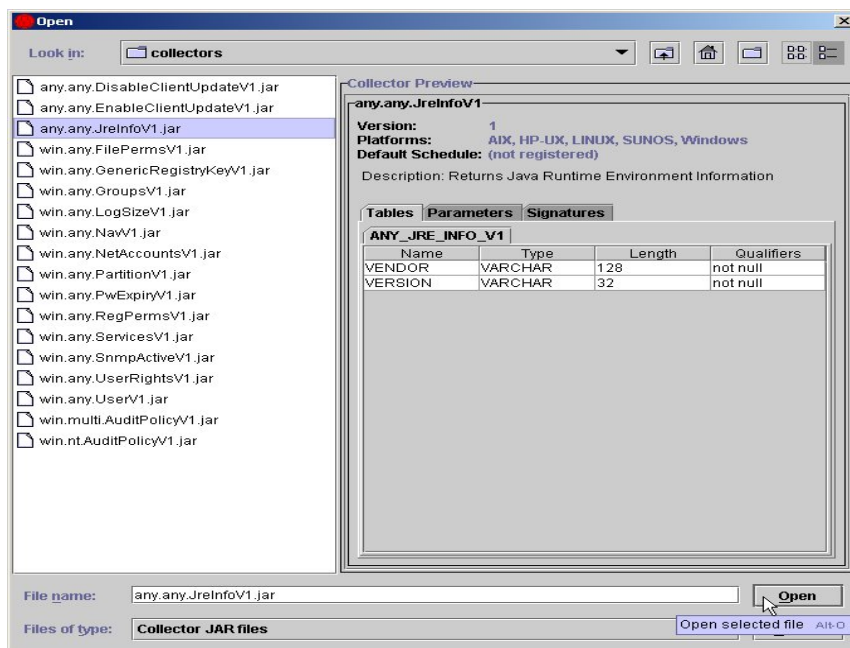
9.4.2 Installing Collectors

Launch the IBM Tivoli Security Compliance Manager Administration Console and click on the **Collectors** tab. The view should be empty; no collectors installed unless you have previously installed a compliance policy.

Right click on the white space to display the Collectors menu and select **Install Collectors**.

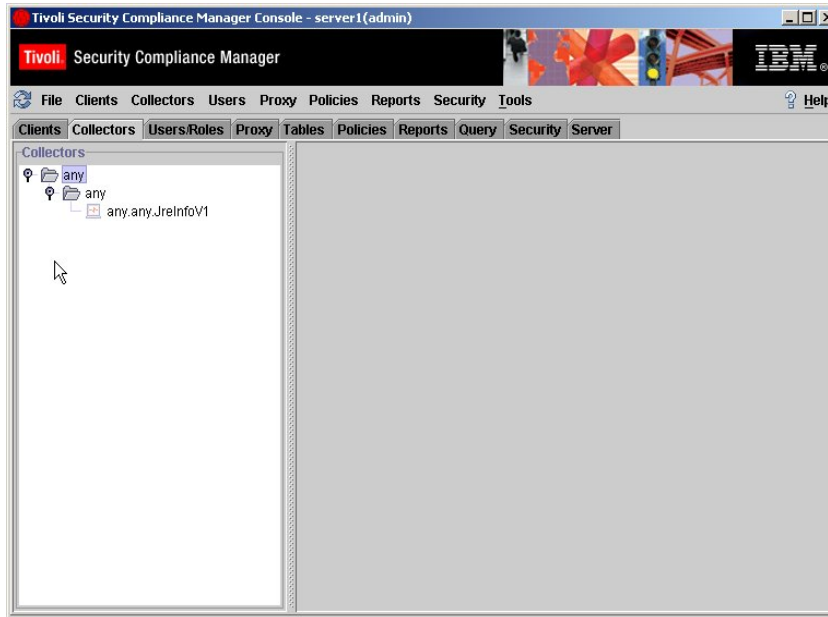
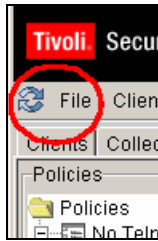


Use the **Look In** field to browse to the find the collectors in the local or linked directory.

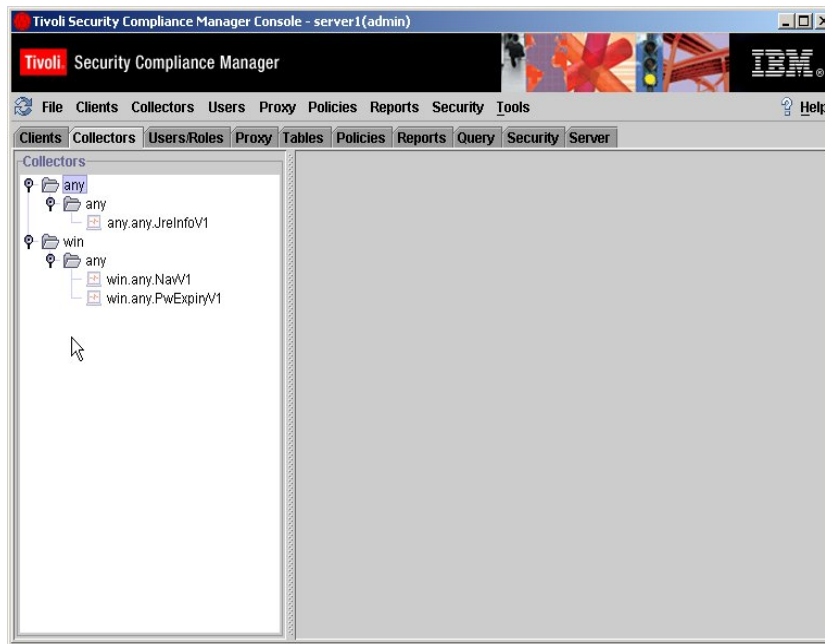


Select the collector(s) required, Example **any.any.JreInfoV1.jar** file, then select 'Open'.

Click the refresh button at the top left of the Administration Console and the installed collectors will appear. Notice the collector is grouped under folders associated with the collector name.



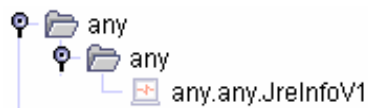
Install some additional collectors. Again, right click on the white space under the **Installed** tab and select **Install Collectors** from the menu that appears
 Select the 2 Jar files – **win.anyNavV1.jar** and **win.any.PwExpiryV1.jar** .



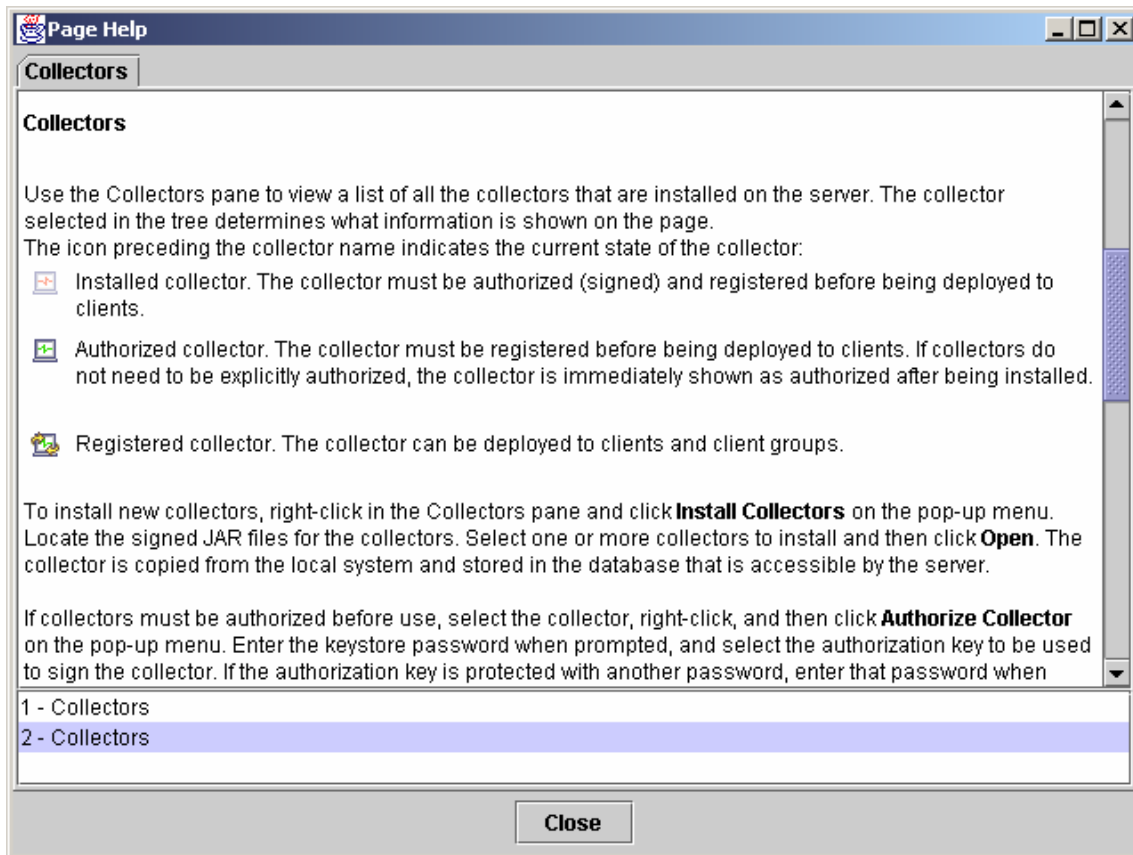
Notice the collectors are grouped into folders and sub-folders based upon the collector names.

9.4.3 Authorizing Collectors

Once installed, the collectors must be authorized (signed) and registered before being deployed to clients. The default behaviour for the Tivoli Security Compliance Manager software, however, is that installing collectors automatically authorizes them. This can be seen from the icon next to each collector in the **Collectors** tab. If the small screen has a green line across it then a collector is authorized. A red line across the screen icon indicates that a collector is not yet authorized.

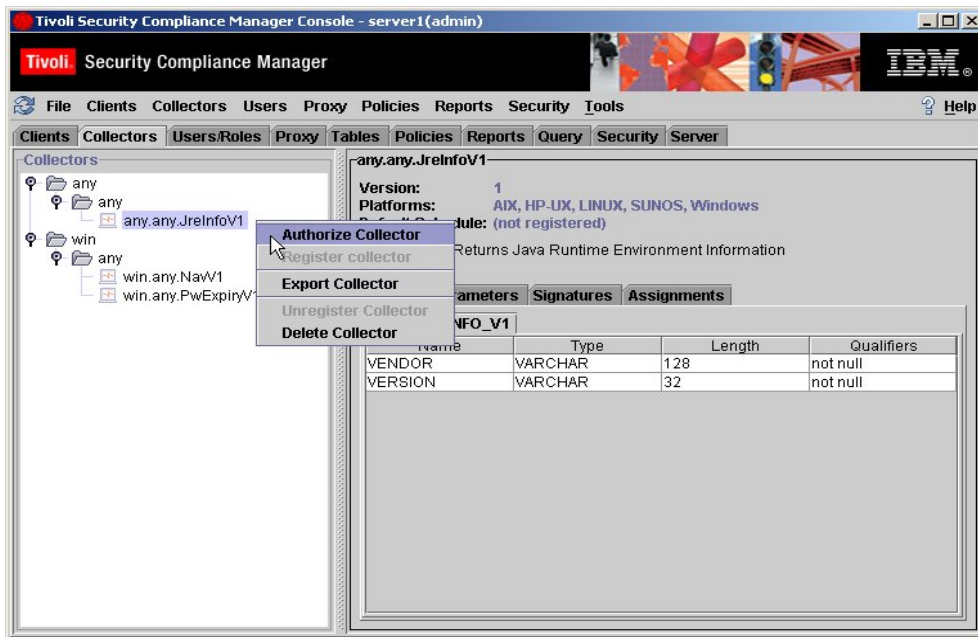


The on-line help provides details describing the icons used to represent collector states:



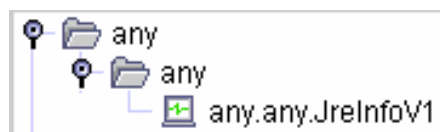
To authorize a collector, select it and then right click and choose the **Authorize Collector** option from the menu.

The [collector authorization level](#) has been set on the Security Compliance Manager Server, therefore you will be prompted to select a signing key when authorizing a collector. Choose the key from the **Select Key** window then select **OK**.



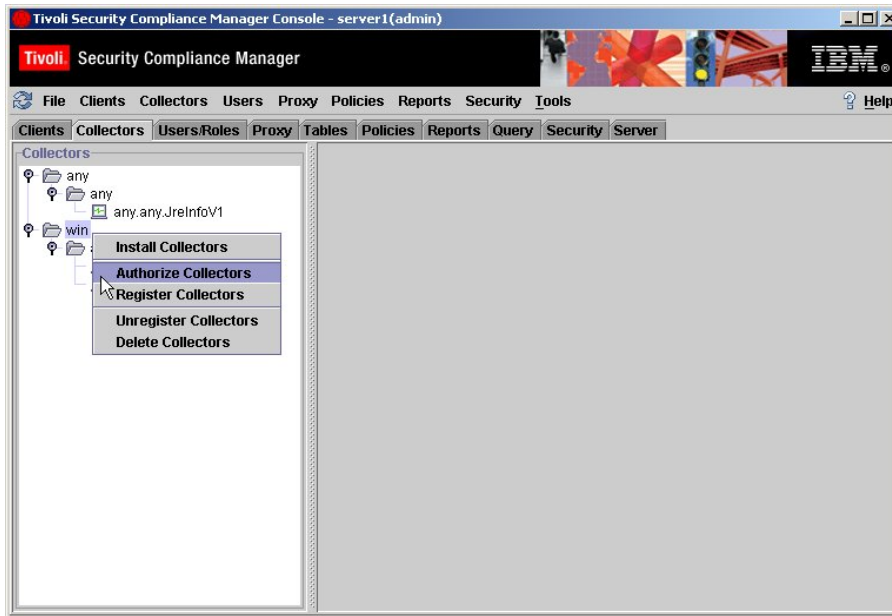
Once the collector has been signed with the required authorization keys, the collector icon will change to show that a collector has been authorized.

Notice how the icon has changed in the image below.

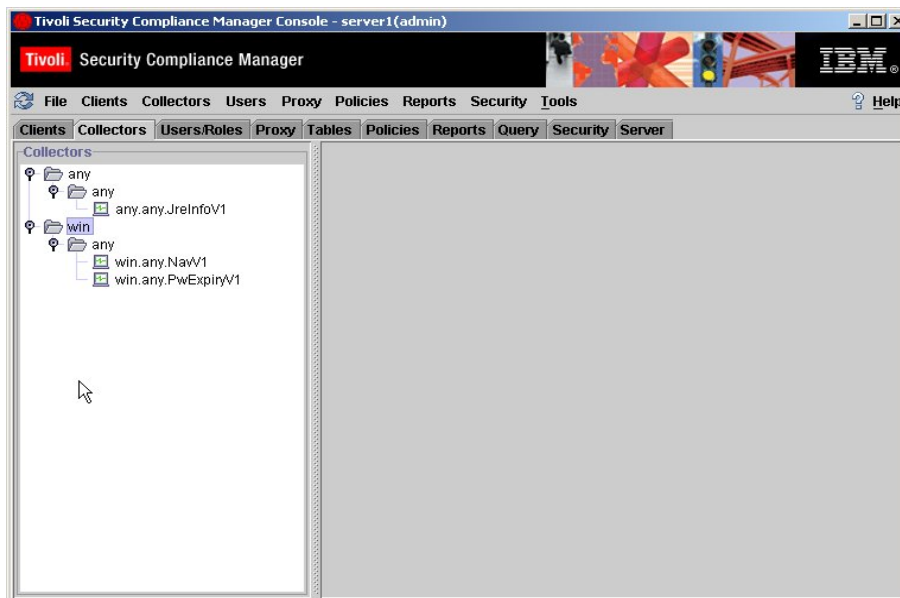


Multiple collectors can be acted upon by selecting multiple collectors then selecting the action to perform on those collectors. Selecting a folder will, in effect, select all collectors in the folder. For

example, select the **win** folder in this view. The right click to display the collectors menu then select **Authorize Collectors**.



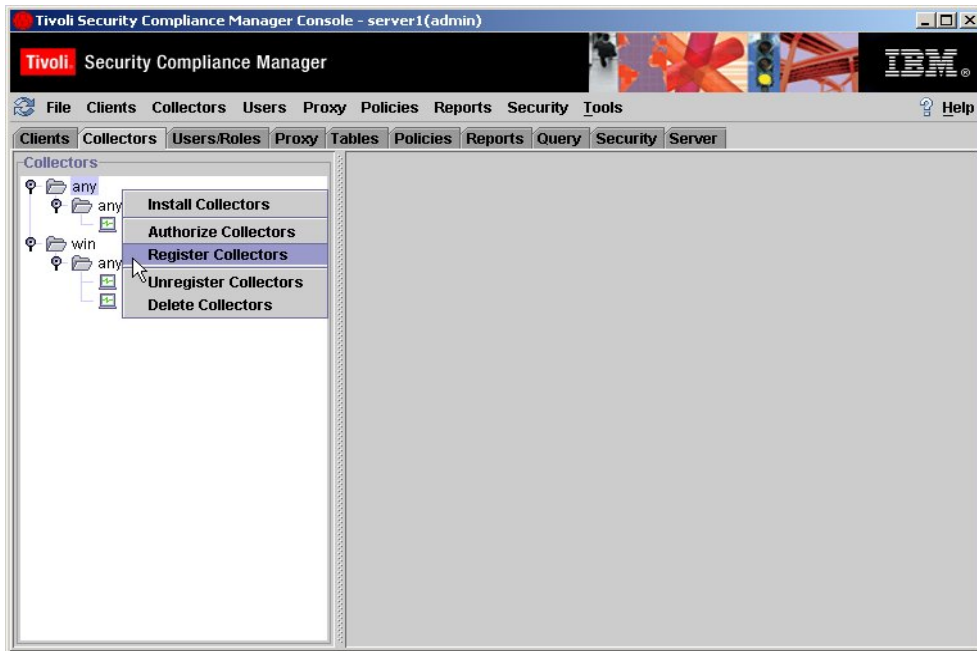
All collectors in the **win** folder will be signed by the key selected.



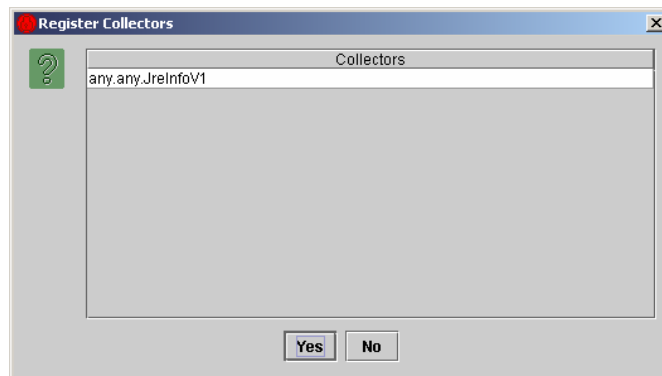
All three collectors are now authorized.

9.4.4 Registering Collectors

Registration of the collectors must be done before deploying to clients. Once again, registration is done by right clicking on a collector or group of collectors and selecting **Register Collector** from the popup menu. Select the **any** folder, then select **Register Collector** from the collector menu.

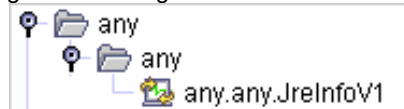


The **Register Collectors** window will appear listing the collectors to be registered. Select Yes to continue.

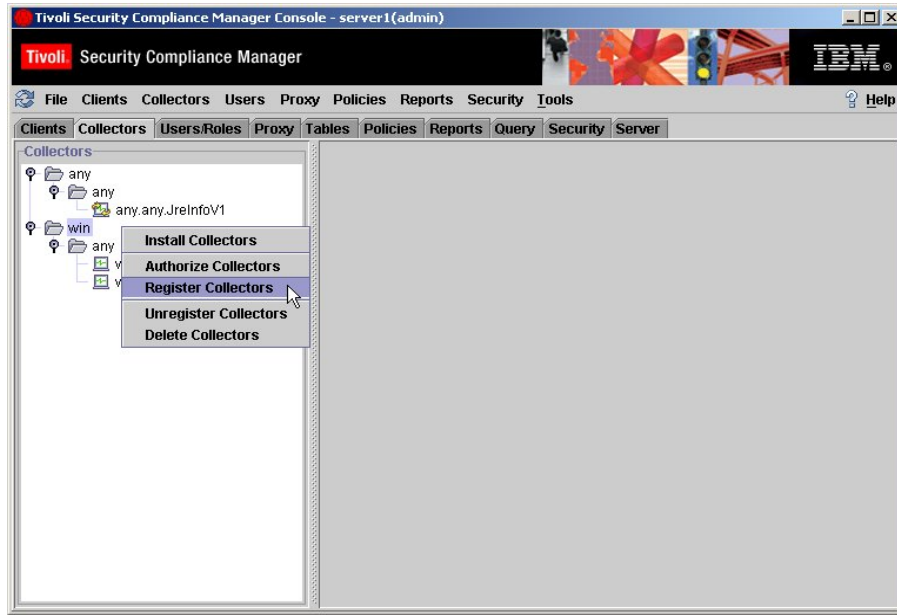


Once registered, the collector icon will change to show that a collector has been registered.

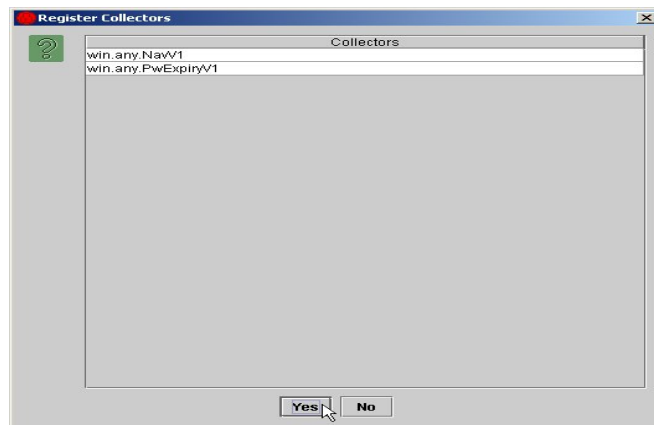
Notice how the icon has changed in the image below.



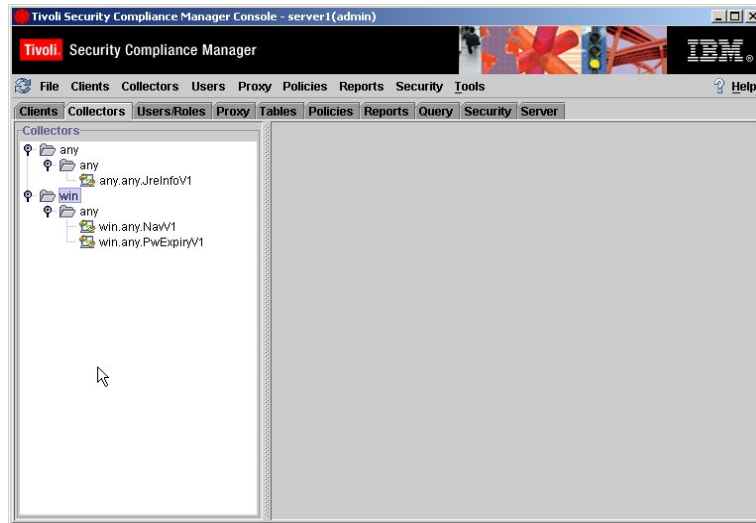
To register the remaining collectors, select the **win** folder. Register the collectors by right clicking to display the collector menu and select **Register Collector**.



The **Register Collectors** window will appear listing the collectors to be registered. Select **Yes** to continue.

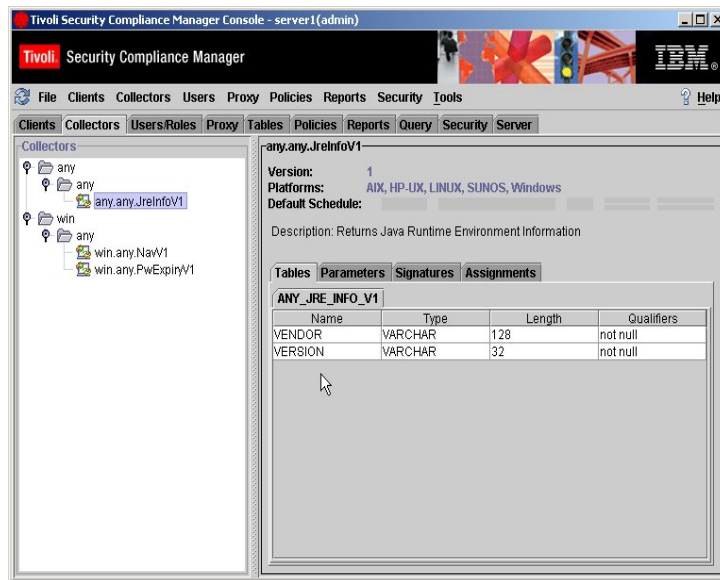


All collectors are now registered.

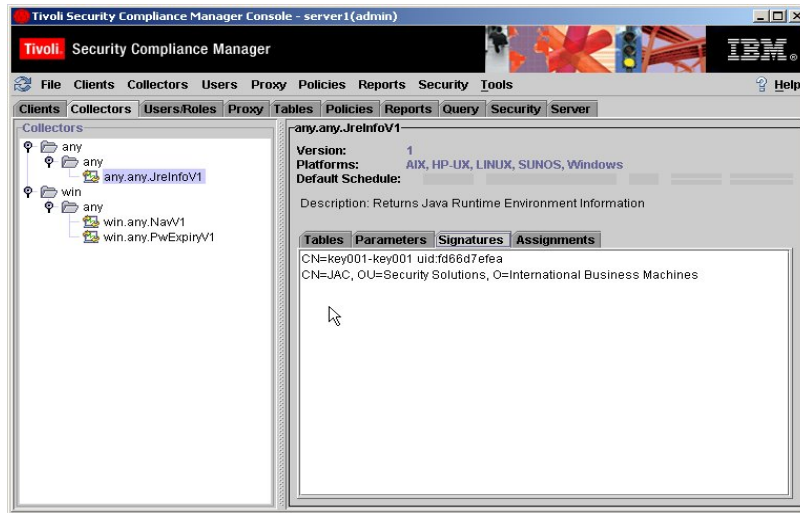


Click on the lever icon to the left of each folder to drill down to the individual collectors that you have registered and examine the properties displayed in the right frame. Select a collector then select a tab (**Tables**, **Parameters**, **Signatures**, **Assignments**) to display the associated details.

View collector tables:



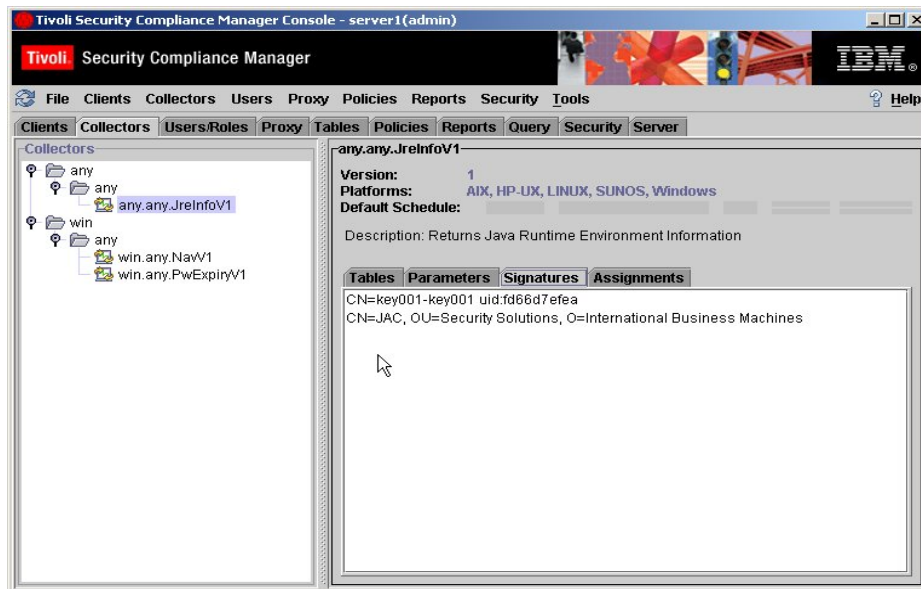
View Collector Signatures:



9.4.5 Set Collector Default Schedules

Once a collector is registered, a default schedule can be defined for the collector. Defining a default schedule prevents having to assign a schedule each time the collector is assigned to a client or group of clients. Note, this default schedule does not apply to collectors included in imported policies.

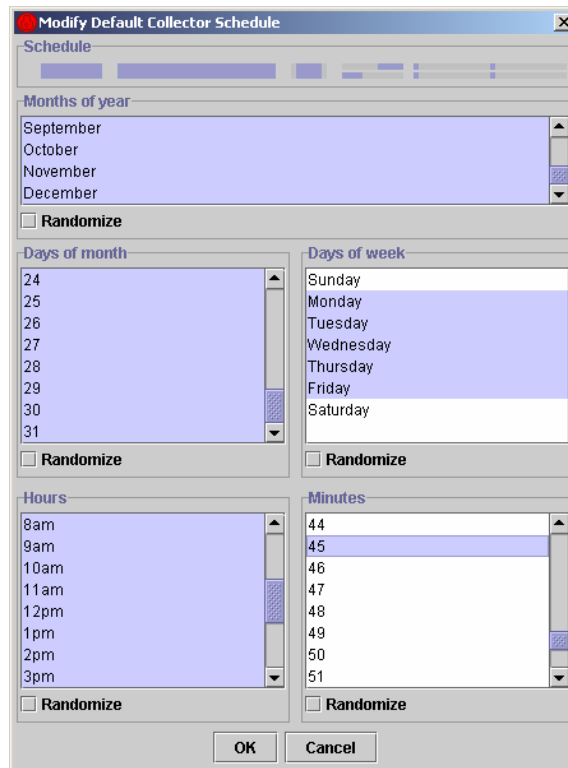
From the Collectors view, select a collector. Notice that the right-hand frame shows the **Version**, **Platforms**, **Default Schedule** along with tabs to display more details about the collector.



The grey bars to the right of **Default Schedule** is a graphical representation of the collector schedule. To set the default schedule for a collector, select the collector, then double-click on any of the grey bars. This will display the **Modify Default Collector Schedule** window.

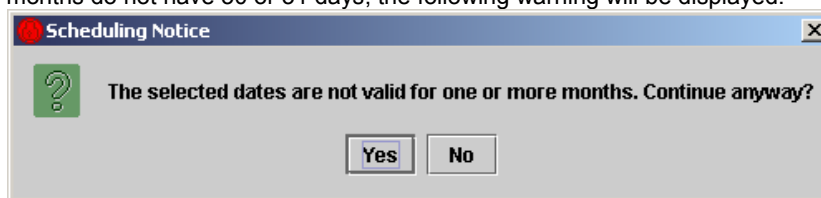
For this example select:

- all **Months of year**
- all **Days of month**
- Monday-Friday for **Days of week**
- 7am – 3pm for **Hours**
- 0, 15, 30, 45 for **Minutes**



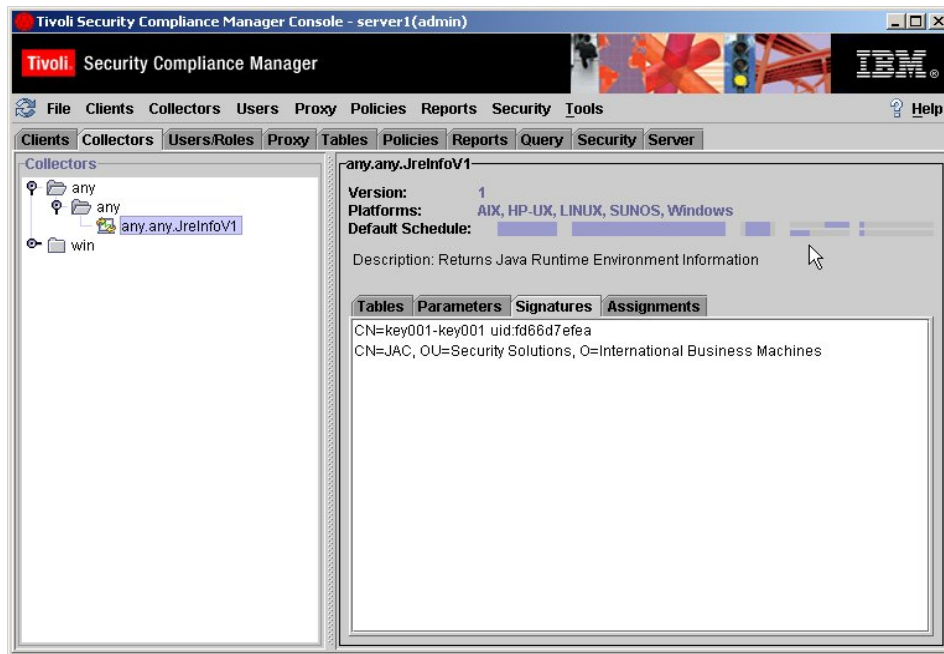
Note the graphical Schedule at the top of the window will reflect the choices. Select **OK** to save. This collector's default schedule is set to run every Monday through Friday, between 7am and 3pm, on the hour and at 15, 30 and 45 minutes past the hour. Note, in a production environment, collectors would not be run this frequently.

Since all months do not have 30 or 31 days, the following warning will be displayed:



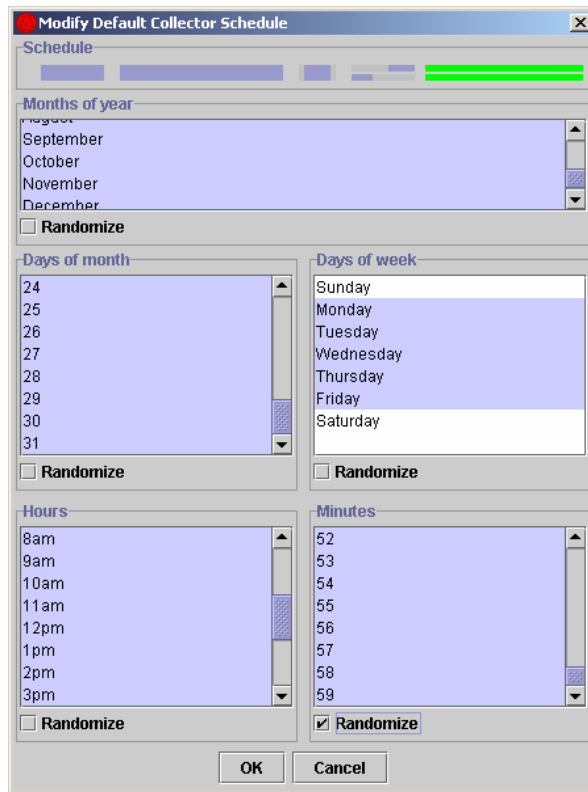
Select **Yes** to continue.

Refresh the Administration Console; select the collector again to review the default schedule.

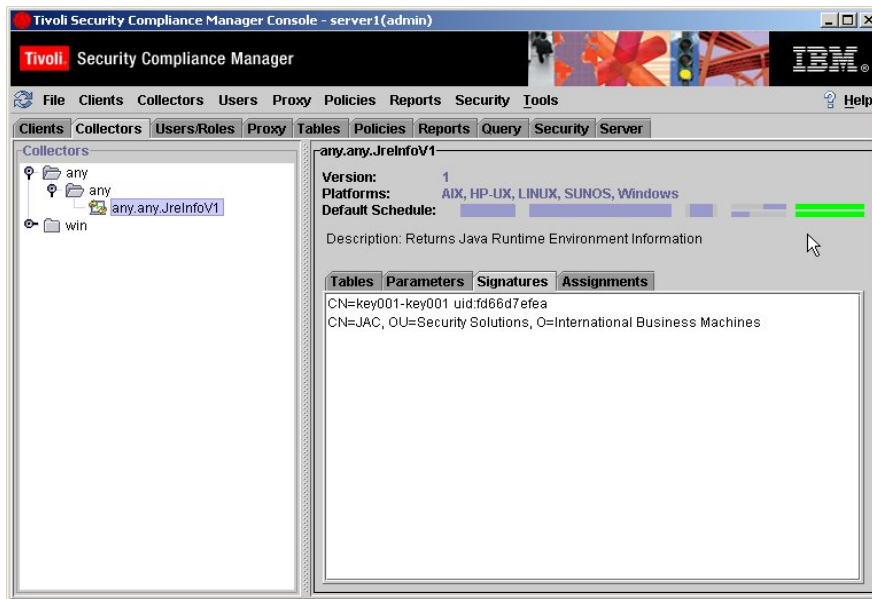


You can repeat this procedure to set the default schedules for the other collectors.

When setting schedules, you can select to 'randomize' one or more of the time criteria. In the example below, the collector will run every Monday-Friday, between 7am-3pm, at a randomized minute past the hour. Once the collector is assigned to a client, the client will set the randomized value and that value will remain set until the client is restarted.

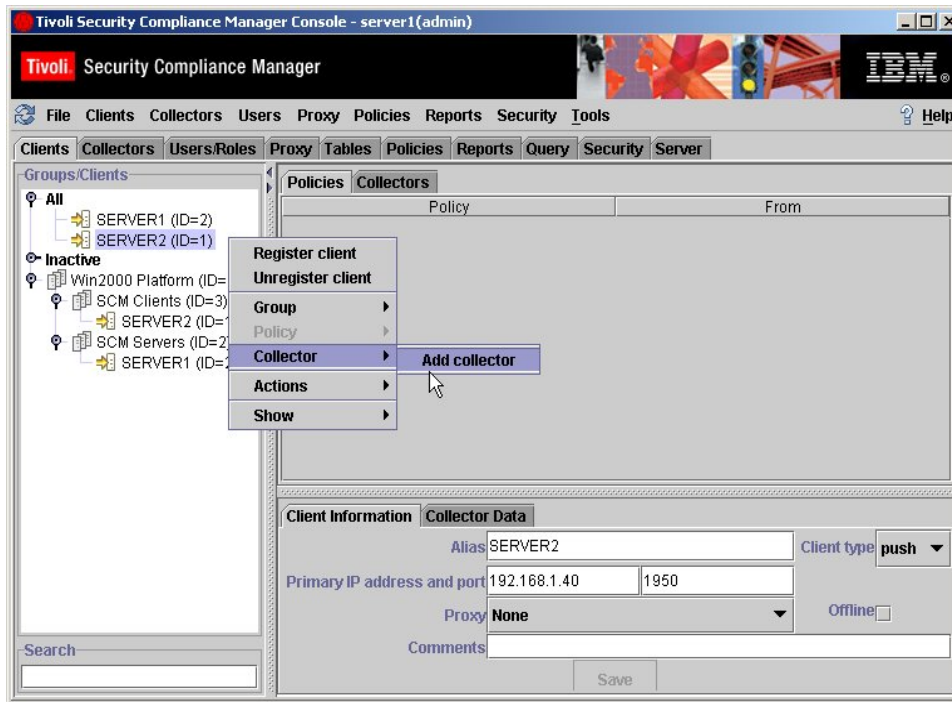


Note that randomized values appear in green on the graphical representation of the schedule.



9.4.6 Assigning Collectors

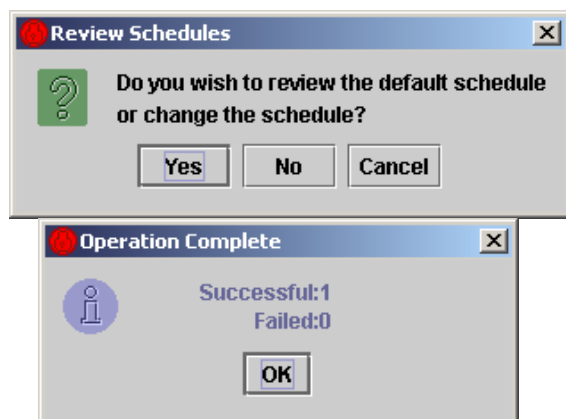
Collectors can be assigned to individual clients, multiple clients, groups of clients or groups of groups. Collectors assigned to groups will be inherited by clients and sub-groups that are part of that group. To assign collectors, go to the **Clients** tab. Select the (**Server2**) client. Right click to display the client menu; select **Collector** then select **Add collector**.



The **Select a collector** window will appear. Select the **win.any.PwExpiryV1** collector; select **OK**.

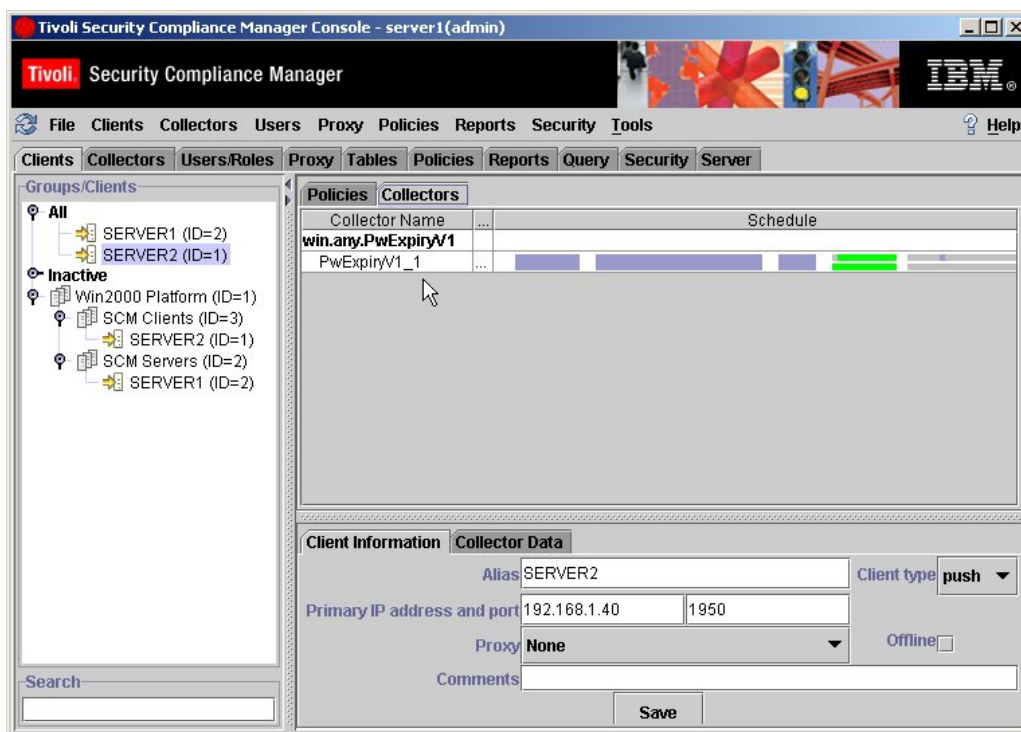


The **Review schedules** window appears. To keep the collector's default schedule, select **No**.



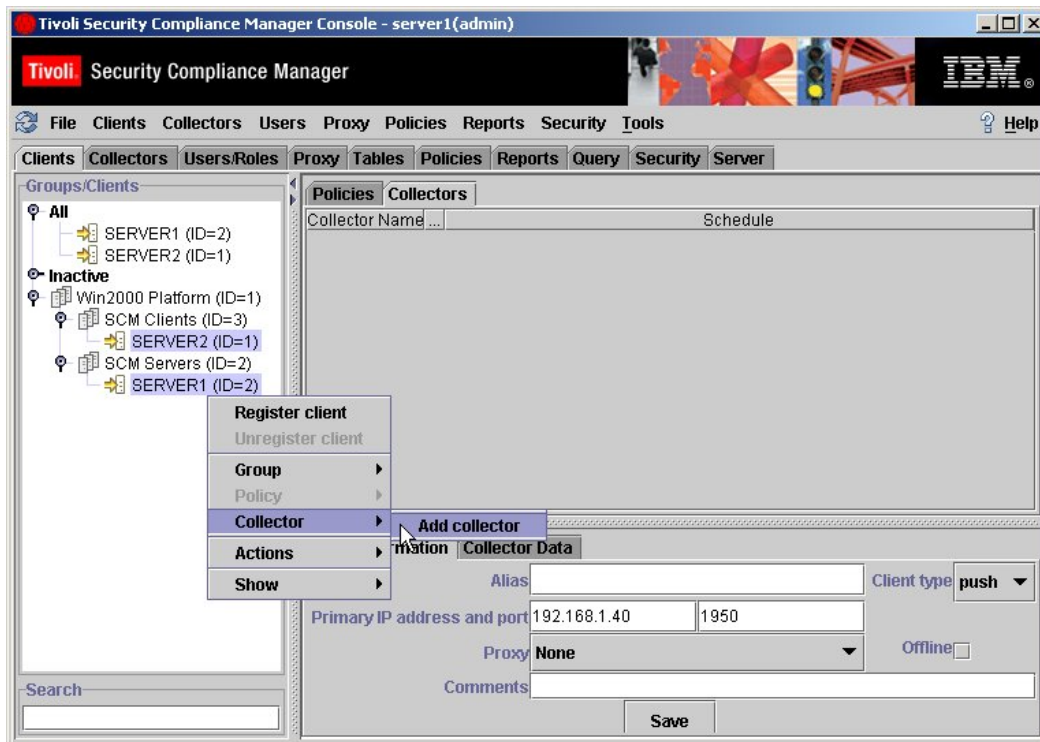
An **Operation Complete** window will be displayed to indicate whether the collector assignment was successful. Select **OK** to continue.

Refresh the Administration Console, then select the **(Server2)** client to review the collectors assigned to the client.



Repeat assigning the **win.any.PwExpiryV1** collector to the **Server1** client.

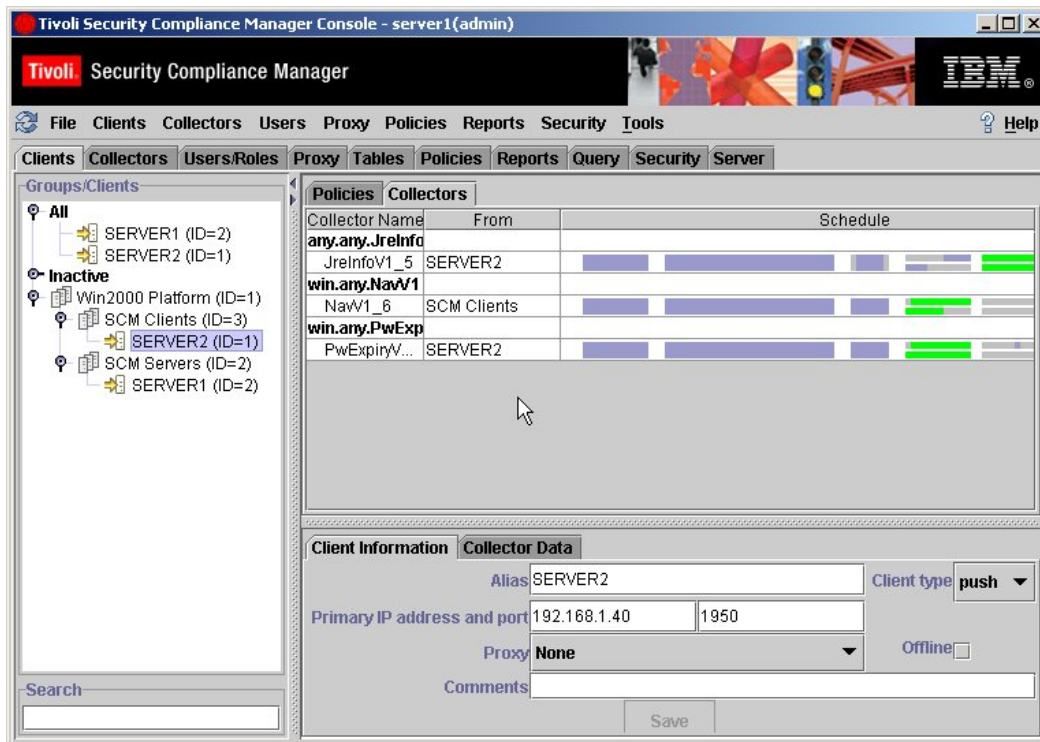
To assign a collector to multiple clients, select multiple clients (using CTRL-click). Right click to display the client menu; select **Collector** then select **Add collector**.



The **Select a collector** window will appear. Select the **any.any.JreInfoV1** collector, then select **OK**. The **Review schedules** window appears. To keep the collector's default schedule, select **No**. An **Operation Complete** window will be displayed to indicate whether the collector assignment was successful. Select **OK** to continue. Refresh the Administration Console, then select one of the clients to review the collectors assigned to the client.

Next assign the **win.any.NavV1** collector to the **ITSCM Clients** group and the **ITSCM Servers** group. This operation can be performed on individual groups or multiple groups.

After completing, select one of clients. The collector assignment should look something like this:

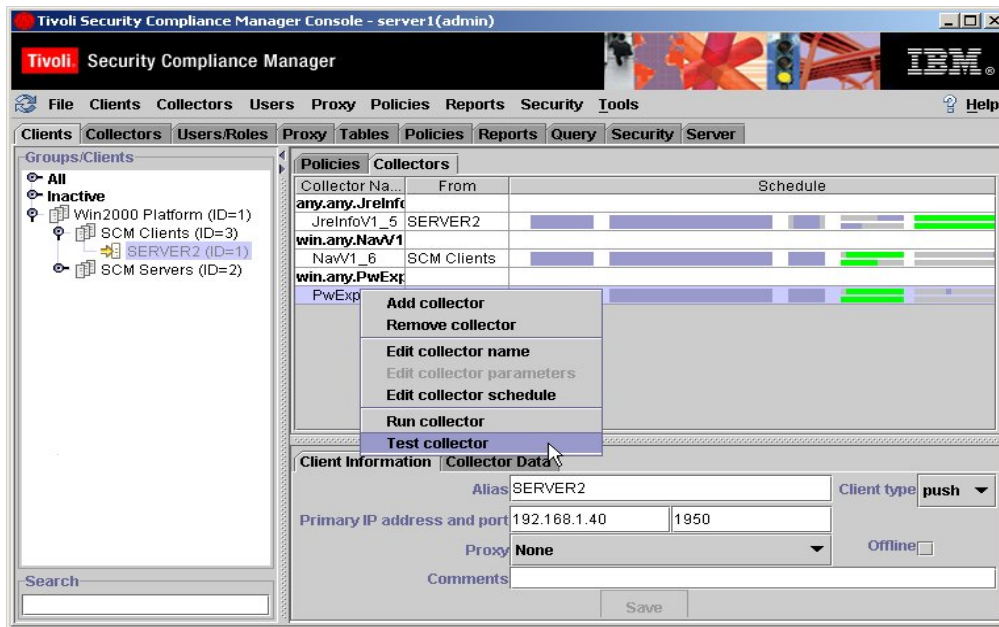


Note the **From** column in the **Collectors** view shows the origin of the collector assignment. In the case of the **win.any.NavV1** collector, it was assigned at the group level (ITSCM Clients).

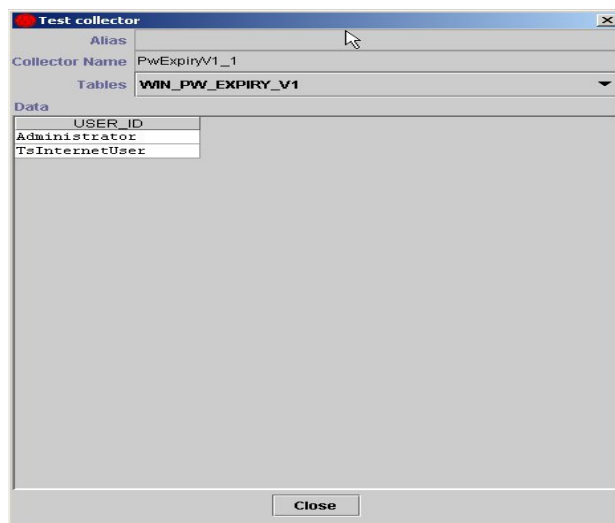
9.4.7 Testing the Collector on a Client

You may want to run a collector on a client to verify that collector is suitable for a client and to get a sample of the data being returned. To do this, you can test to see an immediate collection of collector data from the client.

To make sure that the collectors are running on a client, click on the **Clients** tab, and highlight one of the clients. In the right frame, all the collectors assigned to the client should be listed. Highlight each collector in turn and right click to get the menu displayed.

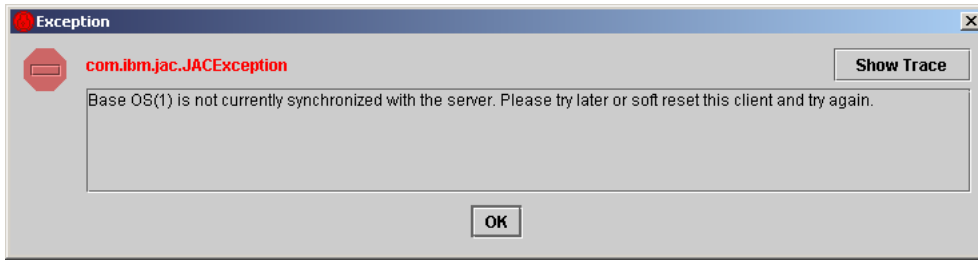


Select the **Test collector** menu item. A window appears showing the data that the collector has retrieved.

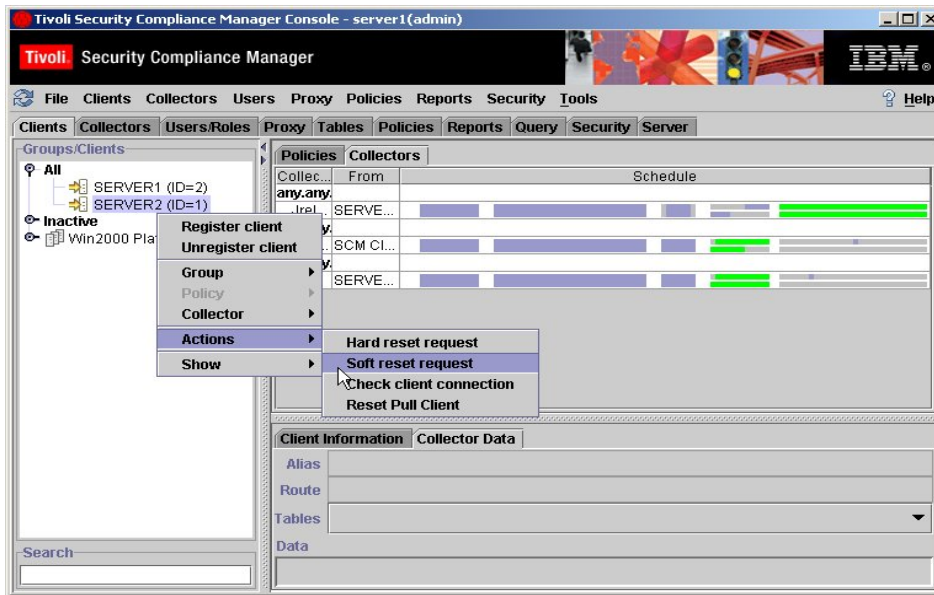


Test collector is useful for examining collector results. This does not place data in the database but only returns the results to the Administration Console.

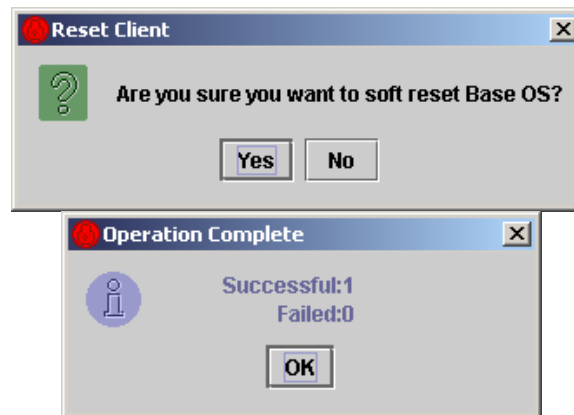
Note: If you have just assigned a collector to a client and try to retrieve data either via the **Run collector** or **Test collector** options, the collector on the client may not have yet synchronized with the server and the following error message is displayed:



To correct this, you can execute a soft reset on the client to force synchronization. To do this, right click on the client and select the **Actions -> Soft Reset** option.



Confirm your wish to reset your client, then you will see the **Operation Complete** window indicate if the operation is successful.

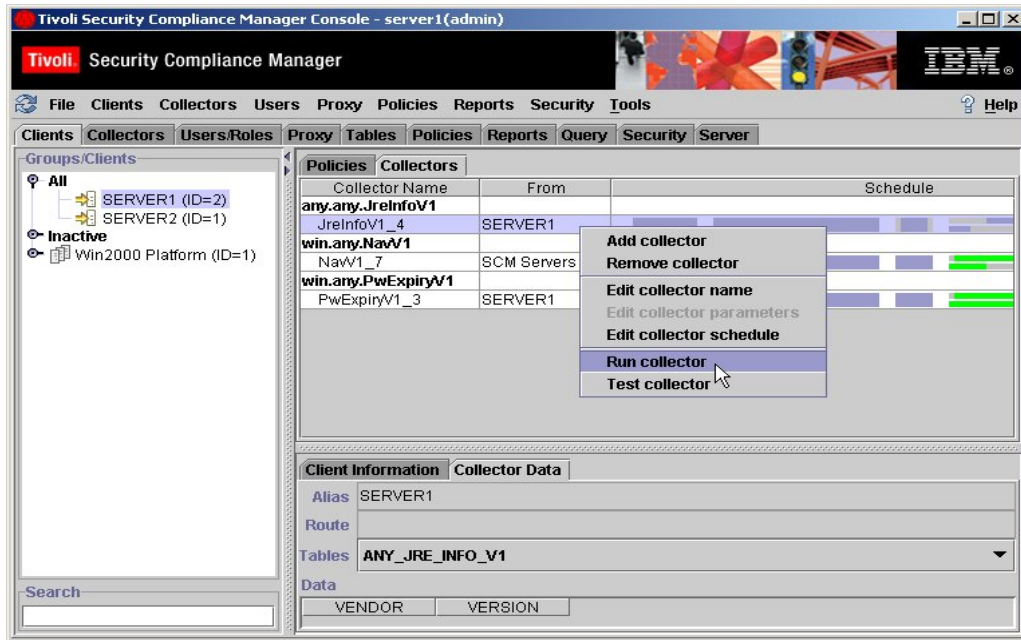


Now you should be able to run your data collection.

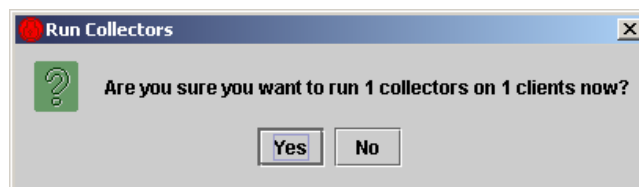
9.4.8 Collecting Collector Data

The schedule (either default or custom) set when a collector is assigned to a client is the 'active' schedule used by the client to run the collector. If you do not want to wait until the collector schedules are run to get data into the Security Compliance Manager database, the **Run collector** option can be used. This option runs the collector on the client and places data into the relevant collector data table in the database.

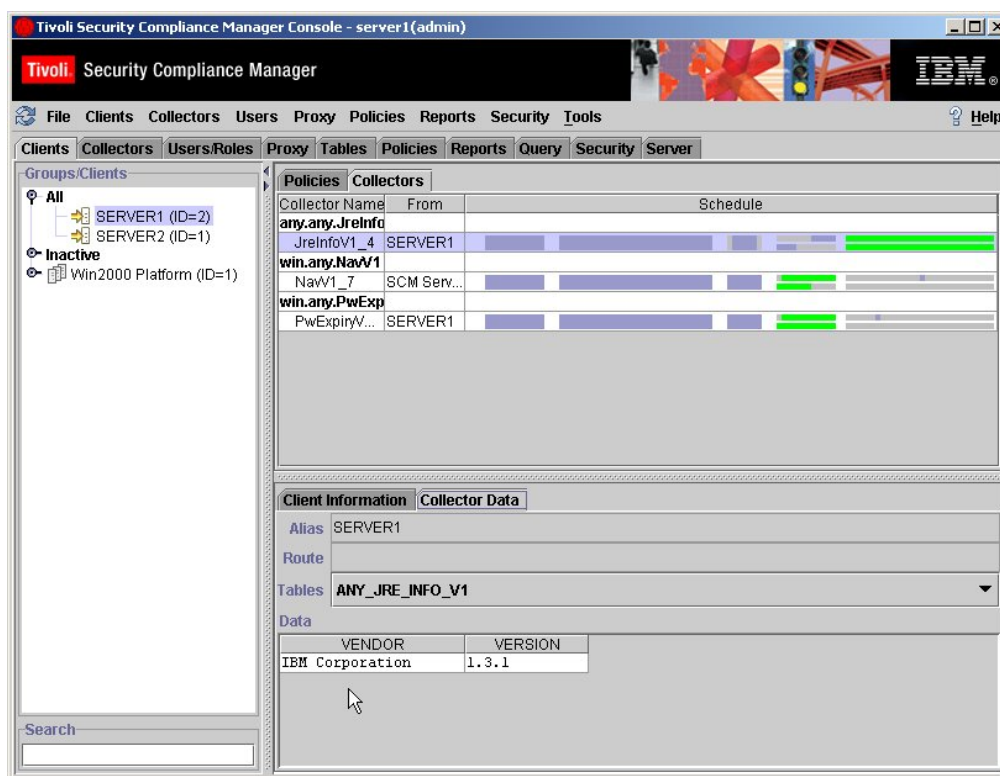
In the **Clients** tab, select a client and in the Collector column of the right pane, select one of the collectors. Right click in the collector pane and choose the **Run collector** option. Note, if the collector schedule has not yet executed, there will be no data for this collector in the **Collector Data** view.



You will be asked if you want to run the collector on 1 client. Once you select **Yes**, a message will be displayed showing successful execution.



Refresh the Administration Console; then select the client and collector to view the collector data. Notice that the **Collector Data** view now shows the collected data.



When the collectors have executed, either because of their assigned schedule or by using the **Run collector** option, you can view the collector data by:

- 1) selecting your client under the **Clients** tab
- 2) highlighting your collector in the top right pane, and
- 3) selecting the **Collector Data** pane in the lower right hand pane.

If the collector has executed, the Administration Console has been refreshed and there is still no data for a collector in the **Collector Data** view, it could be that the client does not have any data to be collected for that particular collector (i.e. no data for the **win.any.NavV1** collector means that Norton Antivirus is not installed).

You have now completed the Collector lab session. You will use some of the basics learned here in the Policy lab session.

10 Configuration of Security Compliance Manager Policies and Compliance Queries

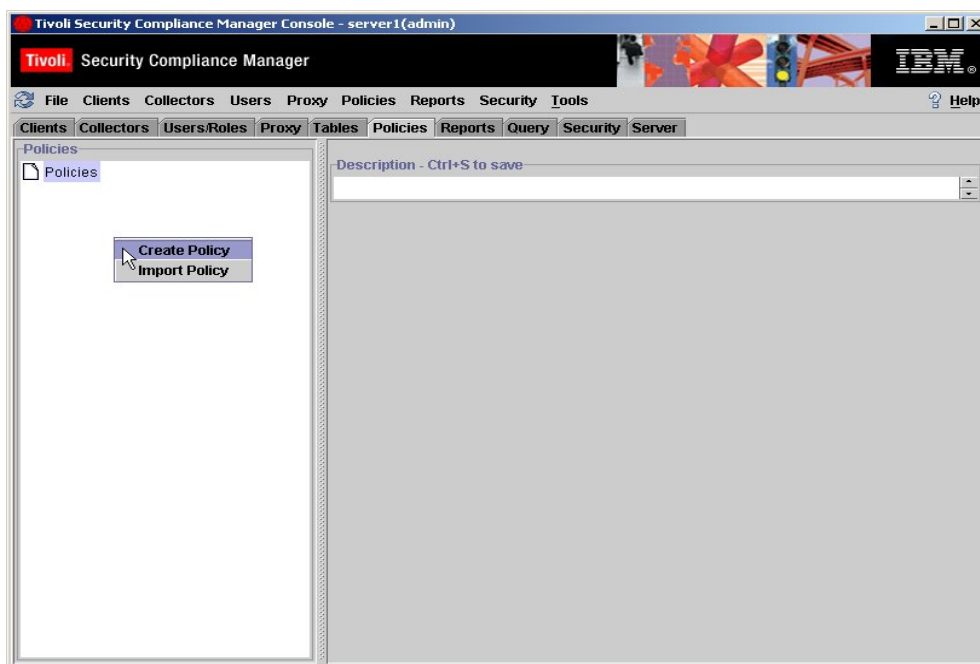
10.1 Managing Policies

A policy is an object containing one or more SQL queries against collector data tables populated with data from collectors running on clients. These queries are specifically written to reveal the compliance or violation of security requirements.

This section will step you through the process to create a policy manually and later on import a pre-defined policy. The policy will be created to ensure that the Windows Administrator ID and the db2admin ID (if present) have passwords with a set length for expiry.

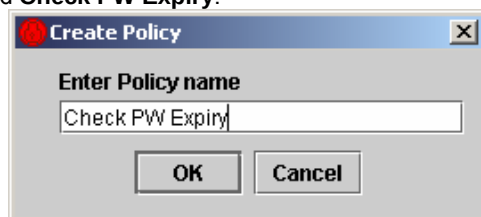
10.1.1 Create the Policy

Navigate to the Policies Tab in the Admin Console. Right click in the left pane to get the menu to **Create Policy**.



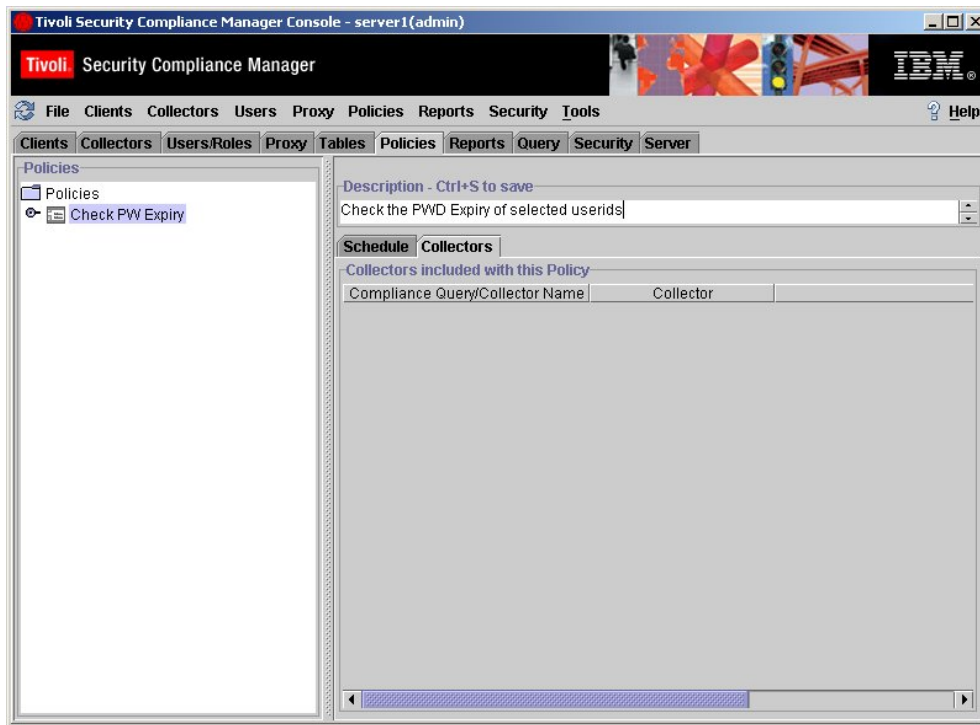
Alternatively you can select the **Policies** menu item and select **Create Policy**.

Create a new policy called **Check PW Expiry**.



The new Policy container object should appear in the list of Policy objects.

Enter a description for the policy in the **Description** field; remember to save the description by typing a **<Ctrl> +S**.



The policy object has two additional components, the Schedule and Collectors. You will return to define these objects after you have fully defined the policy.

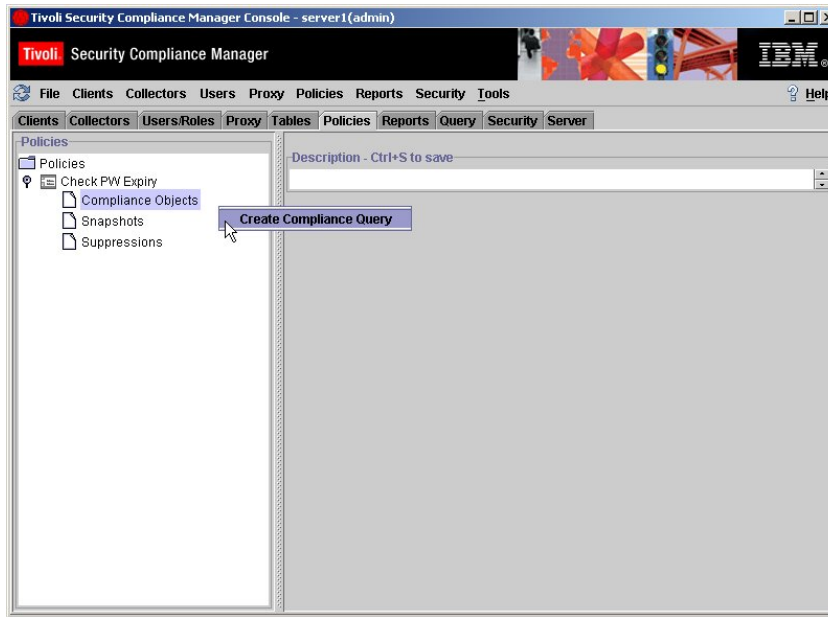
Next, expand the Policy object to see the subcomponents. The 3 sub components of the policy are Compliance Objects, Snapshots and Suppressions.

10.1.2 The Compliance Query

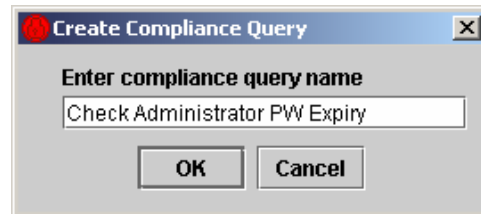
The next step is to create one or more compliance queries for the policy. Create a query to check if the password of Windows Administrator ID is set to never expire. A list of userids whose passwords never expire is returned by the **win.any.PwExpiryV1** collector.

Since this collector will be used, ensure that the collector has been installed, authorized and registered. Also to assist with the creation and testing of the SQL queries, ensure the collector has been assigned to the clients and that data has been collected (i.e. use **Run collector**).

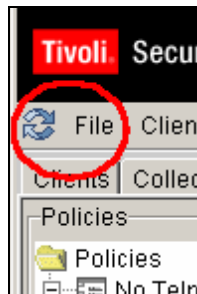
Right click on the Compliance Object sub component to create a new compliance query.



Name your query **Check for Administrator PW Expiry**. Click **OK** to continue.



You may need to use the **Refresh** button in order for your new query to appear in the container list.

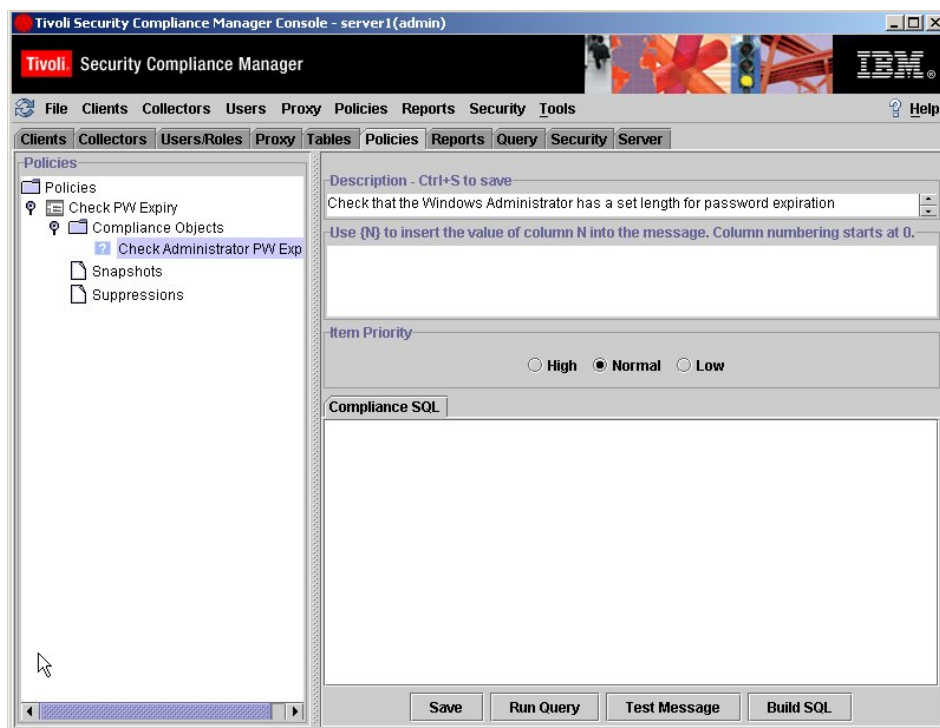


Expand the Policy Object and then the Compliance Objects container by clicking on the lever icon and select your new compliance query. You will now create a query to check for the non-compliance.

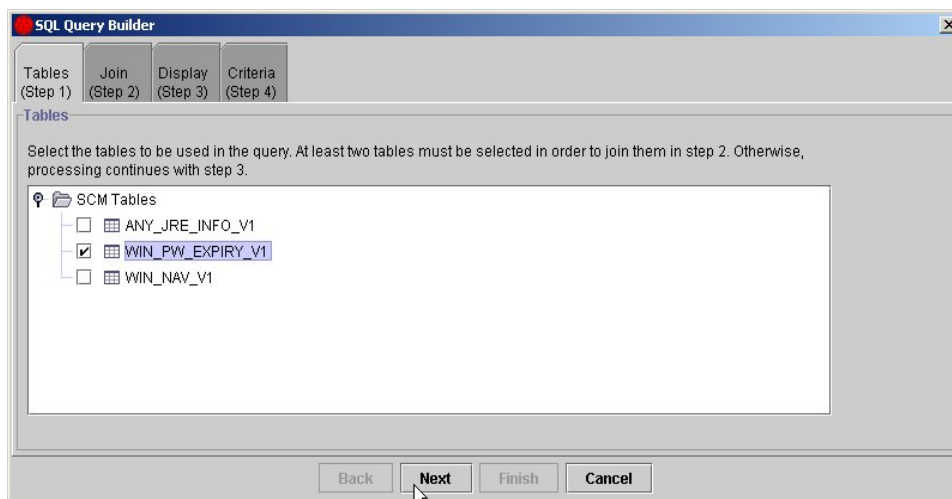
In the right hand pane, make sure the **Compliance Query** tab is the current selection.

In the query work space, you can enter a SQL query definition or you can use the **Build SQL** utility to build your query. Here you will use the **Build SQL** utility to create the compliance query. Expand or maximize the view of the Administration Console to see all the options available.

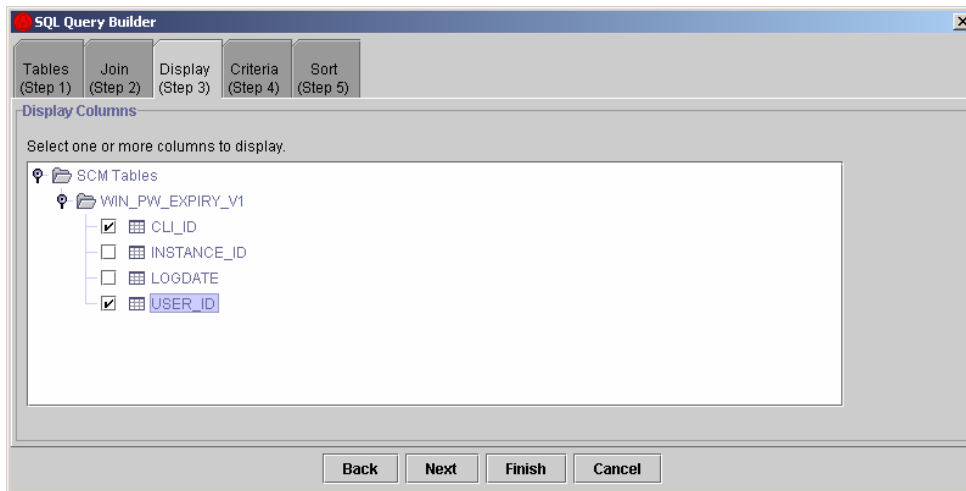
Click on the **Build SQL** button to start the utility.



The SQL Query Builder window is now displayed and you begin with the **Tables** tab.



Check the tables you wish to work with. Check the **WIN_PW_EXPIRY_V1** table. Click **Next** to continue. If you had selected more than one table, then you would go to the Join tab (Step2). Since only one table was selected, the SQL Builder takes you to step 3, Display.

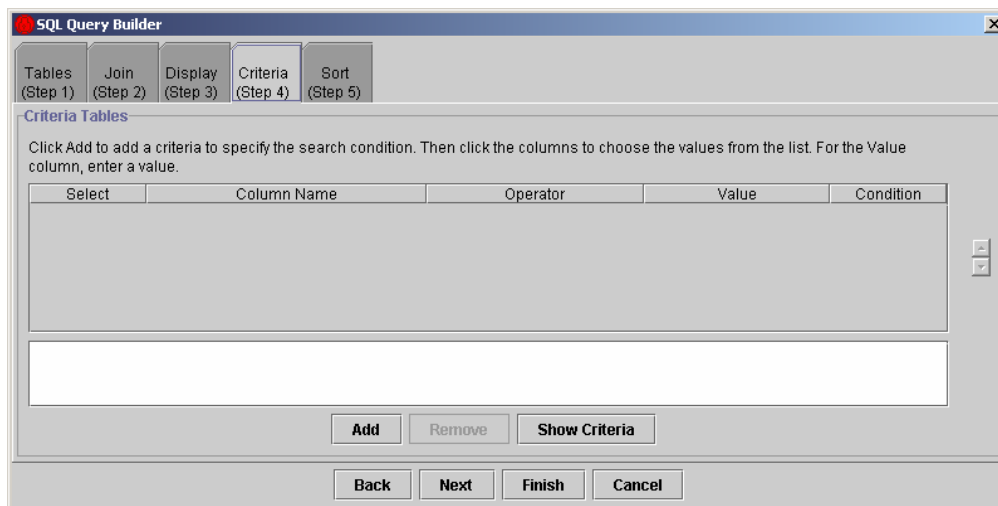


Expand the table **WIN_PW_EXPIRY_V1** by clicking on the lever icon to see the fields. Select the **CLI_ID** and **USER_ID** fields. This will display the CLI_ID and USER_ID in the query results.

Note: the compliance query must return the value of the CLI_ID column in order to reveal the client system identity. The CLI_ID is a value assigned by the Security Compliance Manager Server that uniquely identifies the client system in the Security Compliance Manager environment.

If other tables were selected, they would be displayed here and you could choose to display additional fields from these tables.

Select **Next** to continue with the next step or select the **Criteria (Step 4)** tab.



Here you will specify the selection criteria. Click on the **Add** button to get a new line to build your selection criteria as shown in the example above. Complete the row so it appears as below.

SQL Query Builder

Tables (Step 1) | Join (Step 2) | Display (Step 3) | **Criteria (Step 4)** | Sort (Step 5)

Criteria Tables

Click Add to add a criteria to specify the search condition. Then click the columns to choose the values from the list. For the Value column, enter a value.

Select	Column Name	Operator	Value	Condition
☒	WIN_PW_EXPIRY_V1.USER_ID	IN	Administrator	AND

Add Remove Show Criteria

Back Next Finish Cancel

Column Name : **WIN_PW_EXPIRY_V1.USER_ID**
 Operator: **IN or Equal (=)**
 Value: **Administrator.** (this is a text string. The collector stores userid string in it's data base table if the password is set to never expire.)

When the row has been completed, select the **Finish** button. You do not need Sort Criteria for this compliance query.

SQL Query Builder

Tables (Step 1) | Join (Step 2) | Display (Step 3) | Criteria (Step 4) | **Sort (Step 5)**

Sort Tables

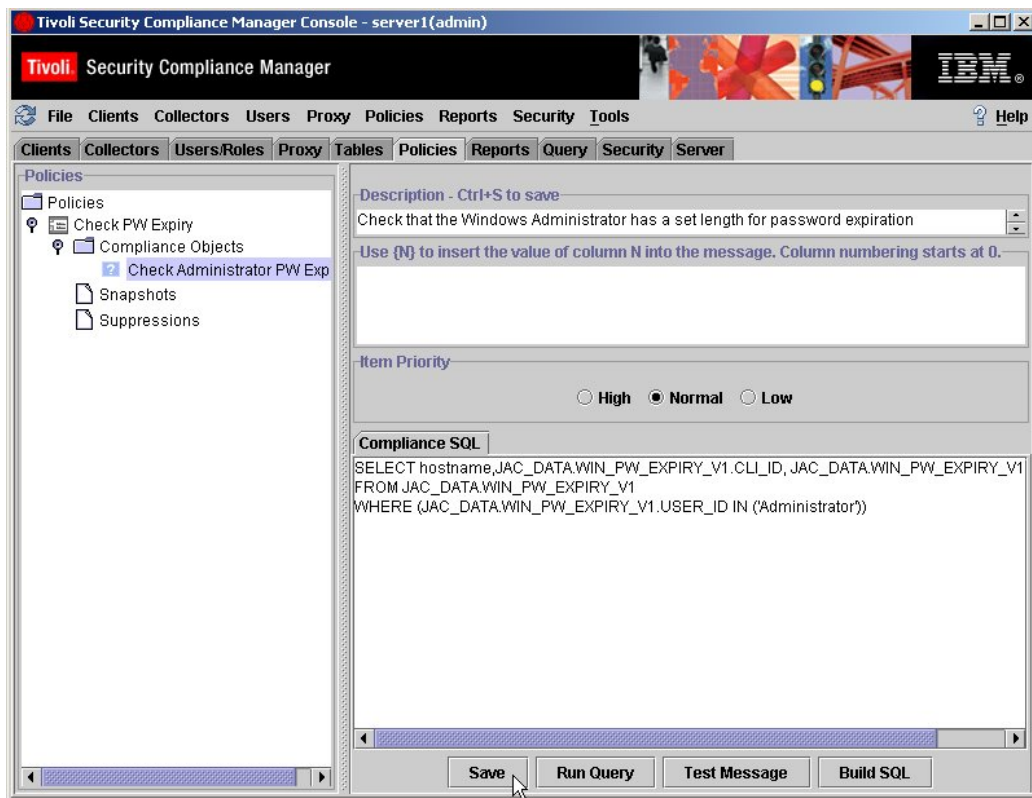
Click Add to add a sort order. Then click the column to choose a value from the list.

Select	Column Name	Order
--------	-------------	-------

Add Remove

Back Next Finish Cancel

Your next screen should have the information as the one below (see Note).



Note: in the Compliance SQL pane above, line breaks were inserted to show the query detail in a more readable view. In your example, the query will be one long line. We added **hostname** as part of the query. You can reformat as above. Select **Save**.

To test the compliance query, select **Run query**. The results are displayed in the **Compliance Query results** window.

The screenshot shows the 'Compliance Query results' window. It contains a table with the following data:

HOSTNAME	CLI_ID	USER_ID
SERVER2	1	Administrator
SERVER1	2	Administrator

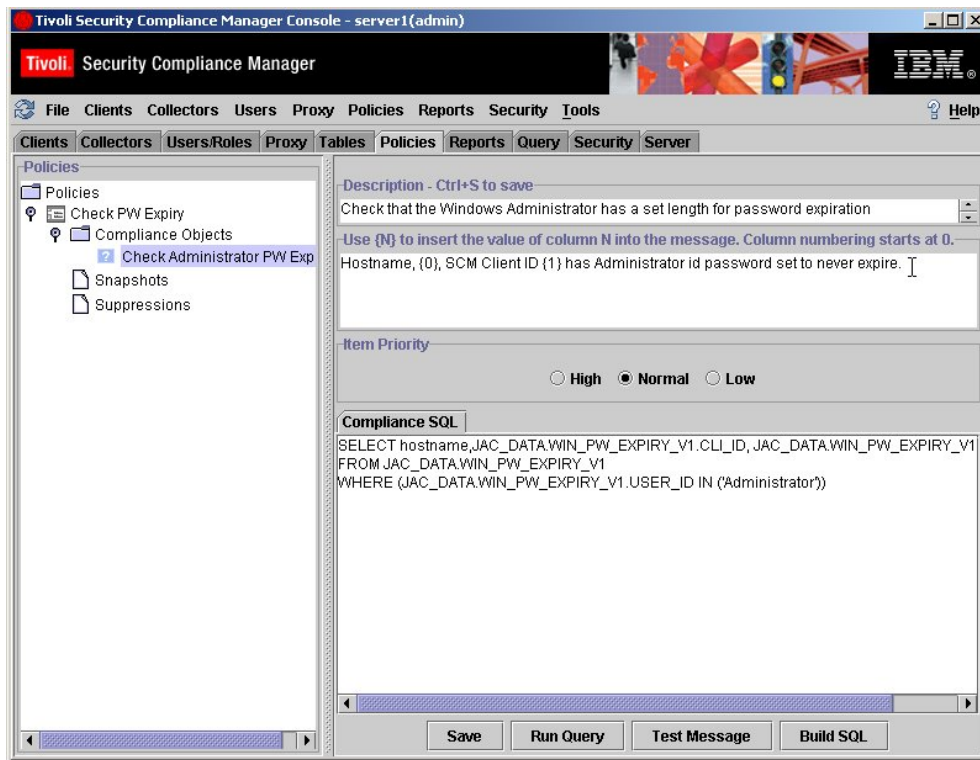
Below the table, it indicates '2 rows received'. At the bottom right are buttons for 'Copy', 'Save', and 'Close'.

The violation message for each compliance query can be customized. The middle box in the right hand frame allows you to create the message. Use of bracketed numbers allows the display of the column values from the query results. For example, we can set the violation message to be:

Hostname, {hostname}, ITSCM Client ID {ID number} has Administrator id password set to never expire.

Using the column numbers (starting with column zero) type the following in the message box:

Hostname, {0}, SCM Client ID {1} has Administrator id password set to never expire.



Select **Save** to save the Compliance object. Select **Test Message** to see the violation messages displayed. Following are the results:

Compliance Query results	
Client ID	Violation Message
1	Hostname, SERVER2, SCM Client ID 1 has Administrator id password set to never expire.
2	Hostname, SERVER1, SCM Client ID 2 has Administrator id password set to never expire.

2 rows received

Copy Save Close

Create another compliance query for this policy that checks whether the db2admin has its password set to never expire.

Create Compliance Query

Enter compliance query name

Check DB2 administrator PW Expiry

OK Cancel

The following shows how the description, violation message and compliance SQL should appear.

Tivoli Security Compliance Manager Console - server1(admin)

Tivoli Security Compliance Manager

File Clients Collectors Users Proxy Policies Reports Security Tools Help

Clients Collectors Users/Roles Proxy Tables Policies Reports Query Security Server

Policies

- Policies
 - Check PW Expiry
 - Compliance Objects
 - Check Administrator PW Exp
 - Check DB2 administrator PW
 - Snapshots
 - Suppressions

Description - Ctrl+S to save

Check that the DB2 administrator id has a set length for password expiration

Use (N) to insert the value of column N into the message. Column numbering starts at 0.

Hostname {0}, SCM Client ID {1} DB2ADMIN ID never expires.

Item Priority

☐ High ☒ Normal ☐ Low

Compliance SQL

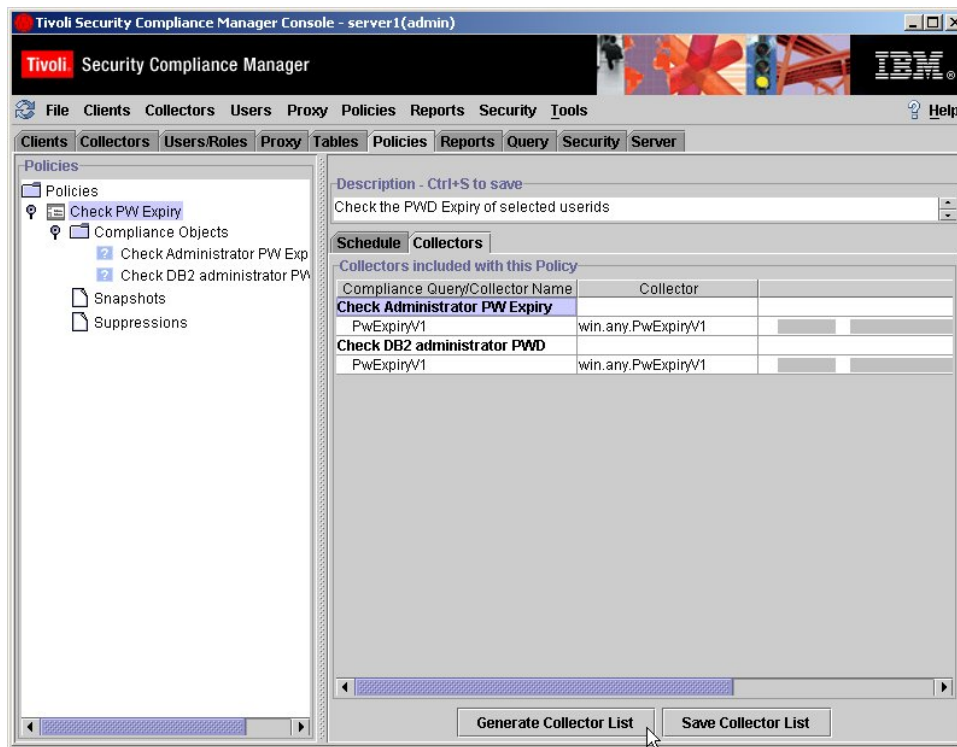
```
SELECT hostname, JAC_DATA.WIN_PW_EXPIRY_V1.CLI_ID, JAC_DATA.WIN_PW_EXPIRY_V1
FROM JAC_DATA.WIN_PW_EXPIRY_V1
WHERE (JAC_DATA.WIN_PW_EXPIRY_V1.USER_ID IN ('db2admin'))
```

Save Run Query Test Message Build SQL

Note: Again in the Compliance SQL area above, line breaks were inserted to show the query detail in a more readable view.

Remember to save the query using the **Save** button. You may have to expand the Administration Console to view the option buttons displayed at the bottom of the console.

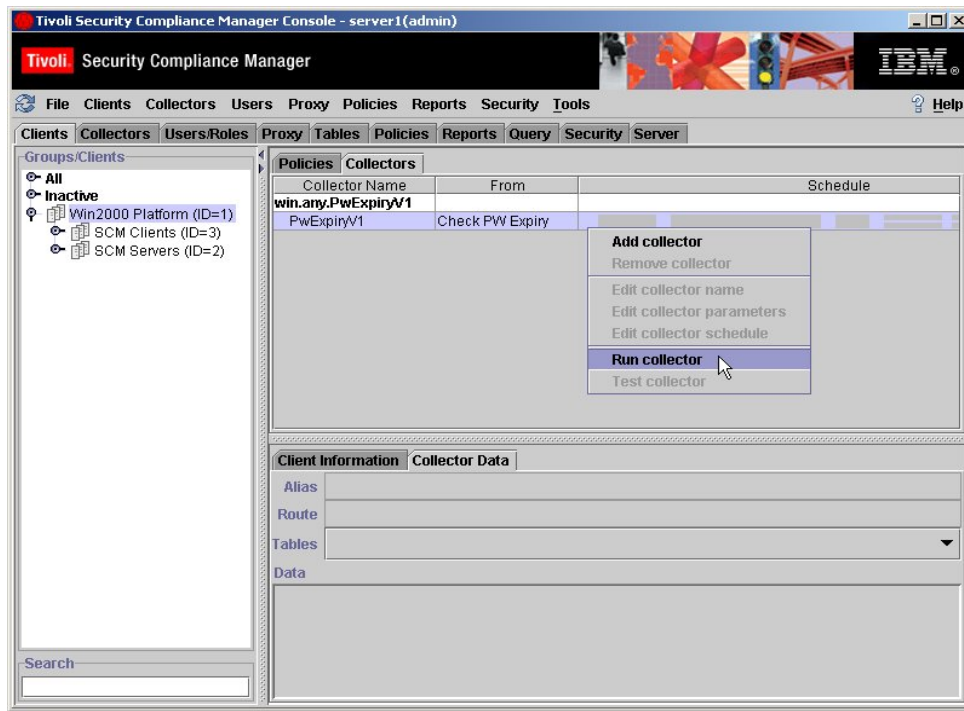
The next step is to generate a collector list for this policy. Select the policy name and then in the right hand window click on the **Generate Collector List** button. This will add the **win.any.PwExpiryV1** collector to the policy. Now, click on the **Save Collector List** button.



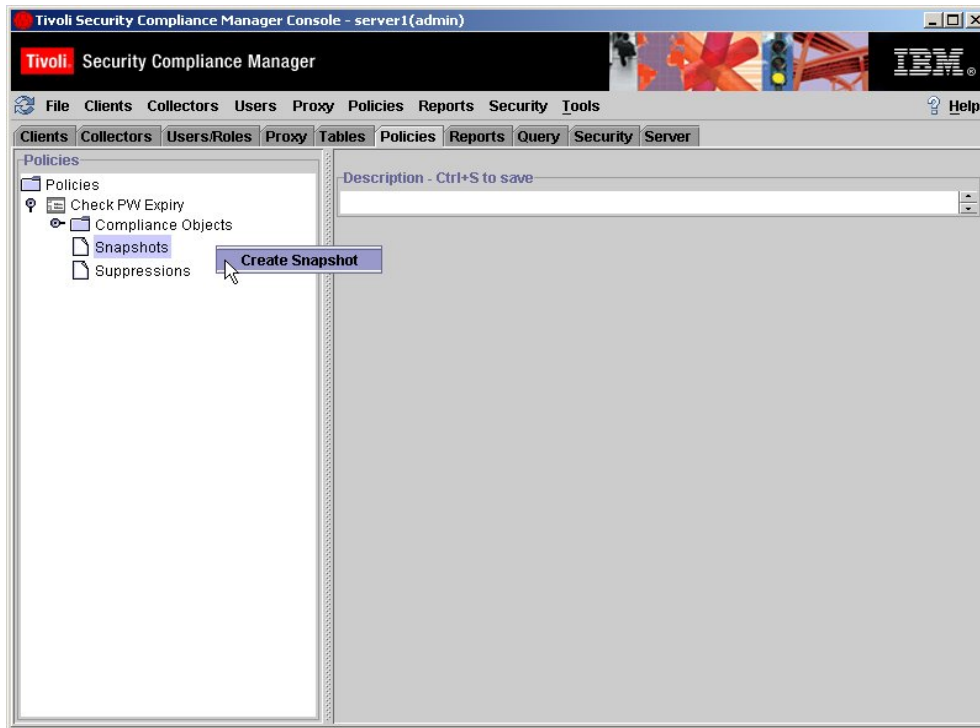
10.1.3 Snapshots

The next step is to create a snapshot. A snapshot will generate a test of the Policy. You will create a snapshot to run against Win2000 Platform group.

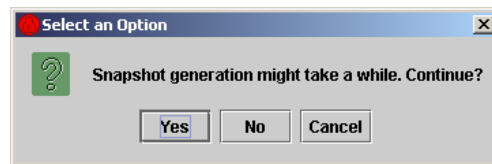
Before running snapshots, ensure the necessary collectors are installed, authorized and registered. Assign the policy to the Win2000 Platform group. Go to the **Clients** tab, from the **Collectors** view, run the policy's collector instance (FROM column identifies the policy; CHECK_PW_EXPIRY), as shown below.



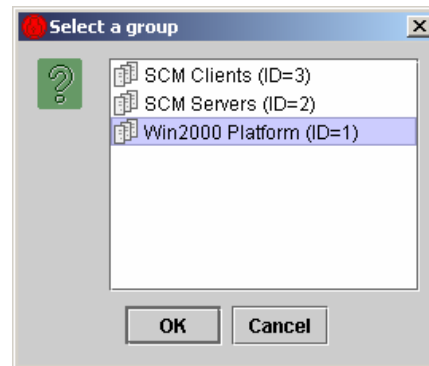
Return to the **Policies** tab, right click the Snapshot object and select **Create Snapshot**.



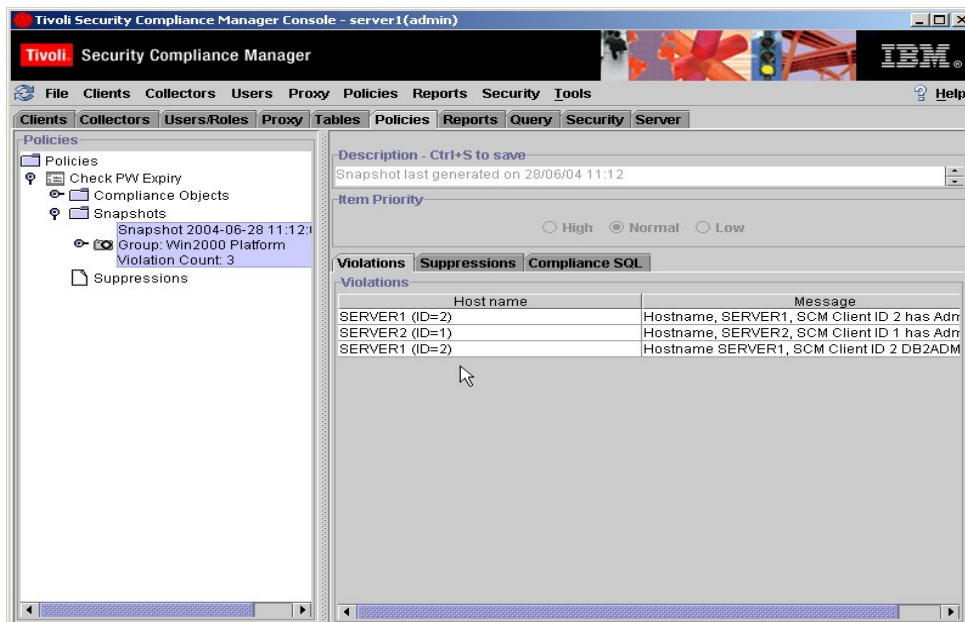
Answer **Yes** to the following dialogue box.



Answer **Yes** to restrict this snapshot to a group; select the **Win2000 Platform** group.



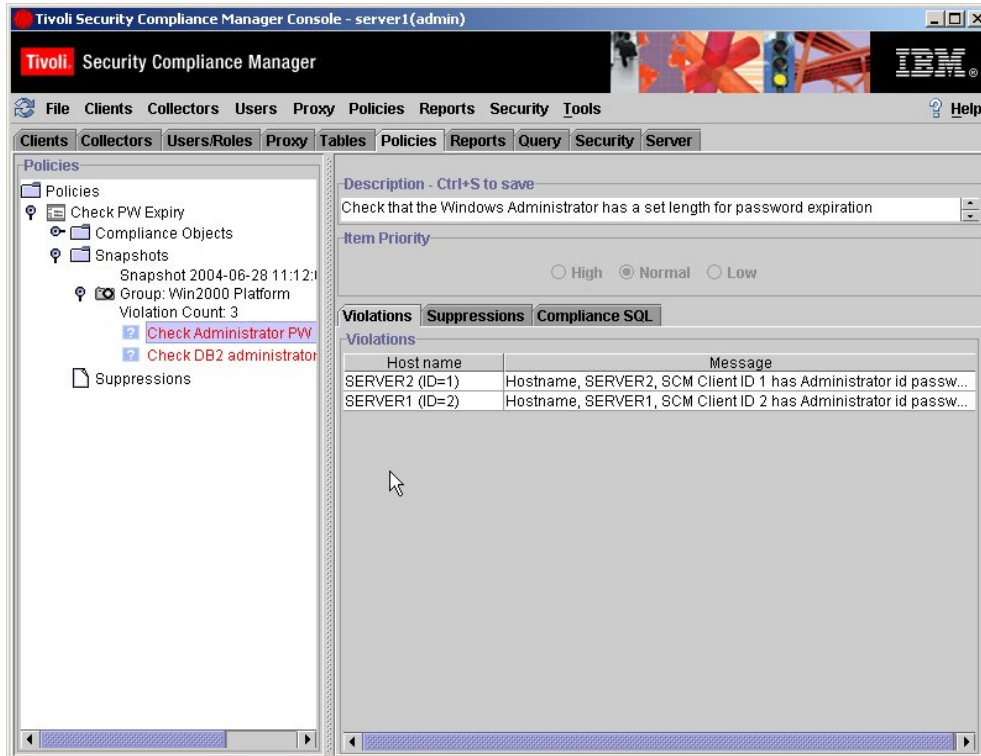
Expand the snapshot by clicking the lever icon next to the snapshot. You should see a snapshot for Group: Win2000 Platform with several violations. Details of the violations are displayed in the right hand frame under the **Violations** tab. Notice the custom message that we created earlier.



Click the level icon next to the individual snapshot to view the detailed results for each compliance query. You can see that the Compliance object is coloured red, indicating a non-compliance has been found. The colour is determined by the **Item Priority** setting in the Compliance query object pane.

Bold Red = High
 Red = Normal
 Yellow = Low

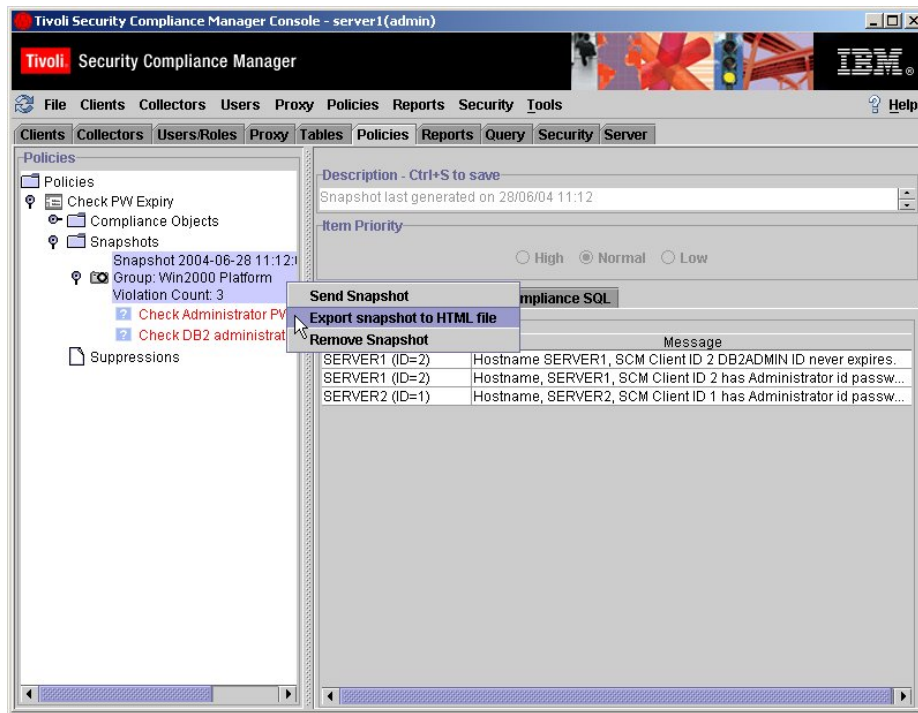
Click on the compliance object in red to see the violation details for each compliance query.



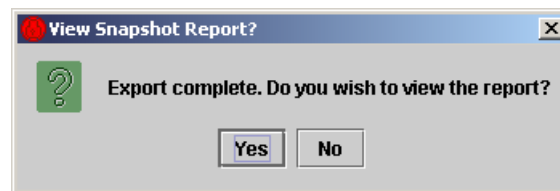
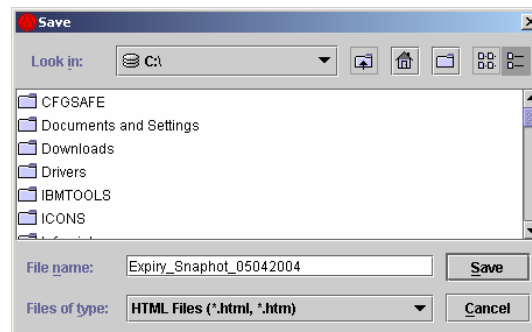
Now that a snapshot has been generated, you can save the snapshot to html or you can email the snapshot to the e-mail address defined in the Policy object.

This will take you through generating html output for the snapshot.

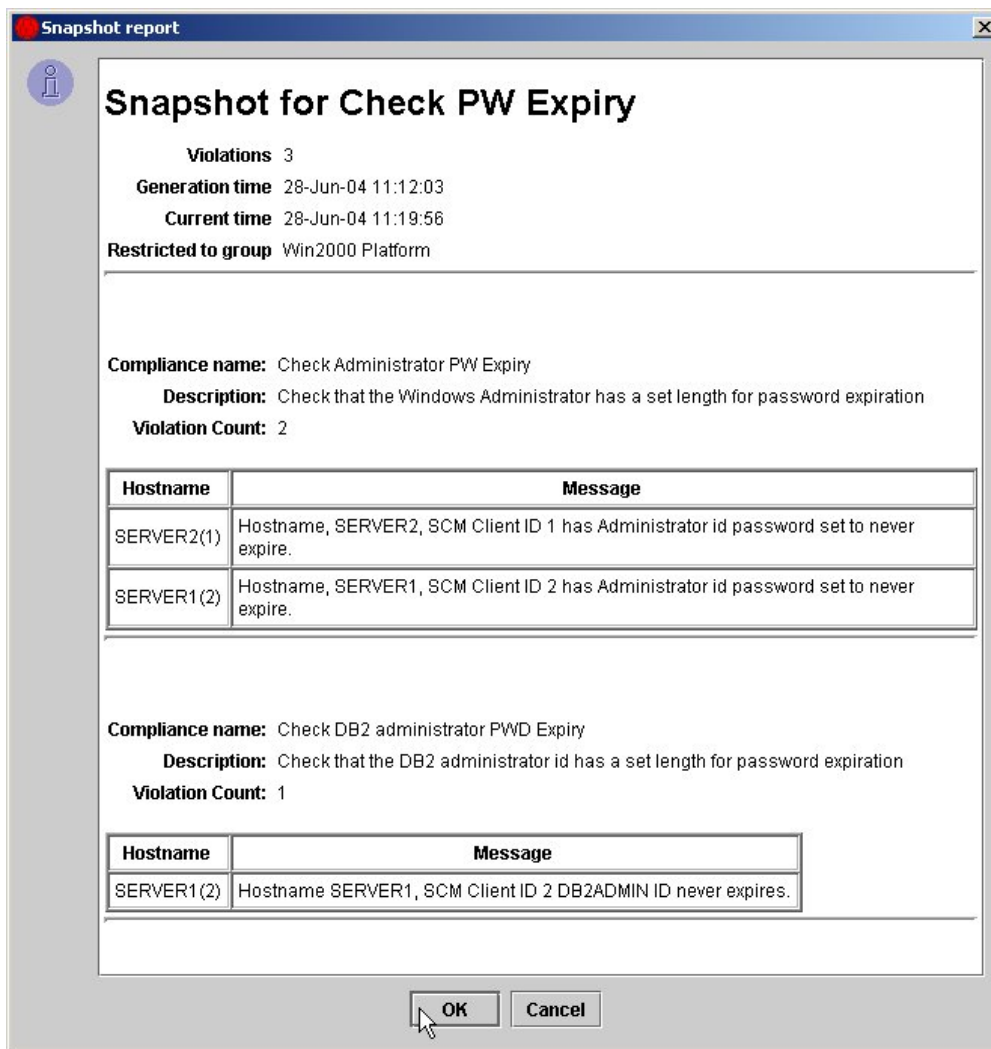
Right click on the Snapshot object to get the Snapshot options menu. Select **Export Snapshot to HTML**.



You will be prompted with the Windows file manager save dialog box. Choose a location on your system to save the html file. Once you save the file, you will have the opportunity to view it.



Select **Yes** to see the report. A popup now appears containing a view of your report.

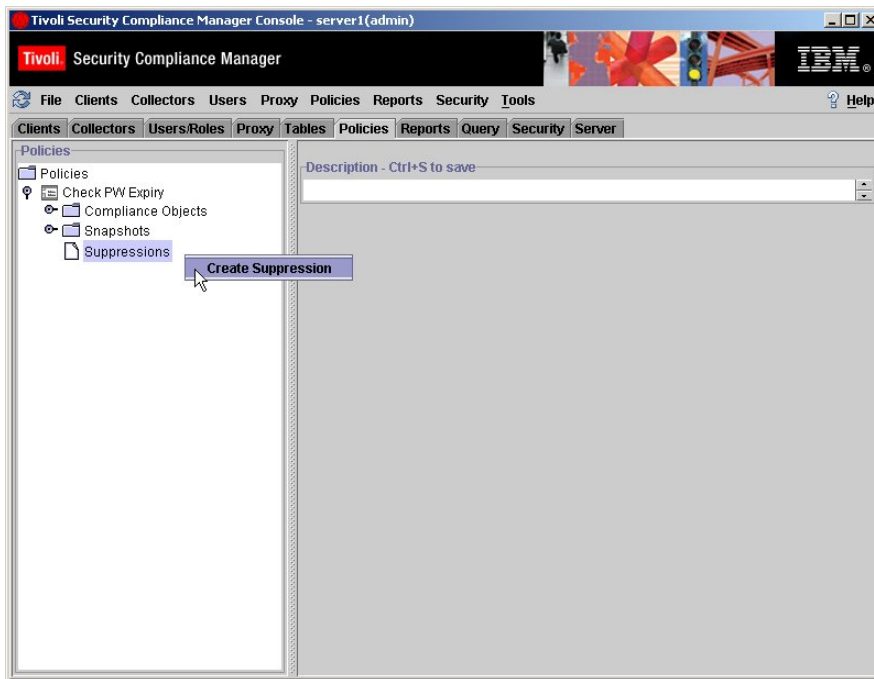


10.1.4 Suppression

In some cases, there may be valid reasons for policy violations. In these cases, policy violations can be suppressed. Suppression can be established based on clients, client groups and/or compliance queries. The suppression can be set with an expiration date. An example where suppression could be used is in the case of new machines being rolled out. A suppression can be created to allow a grace period during which new machines can be brought to the proper level of compliance.

Next, a suppression will be created for the **Server2** machine until July 10, 2006 because it is part of a roll-out of new machines.

To define a suppression, right click **Suppression** in the Policies view and select **Create suppression**.



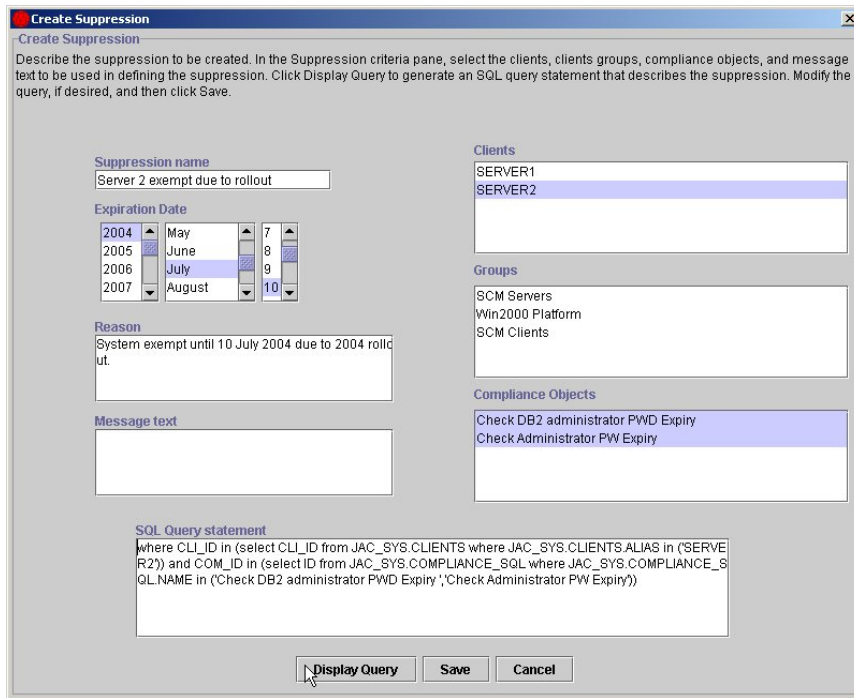
Provide Suppression name; set the expiration date to a future date 2006, July 10; select **Server2** under **Clients**; select both **Compliance Objects**.

The 'Create Suppression' dialog box contains the following fields and lists:

- Suppression name:** A text box containing 'Server 2 exempt due to rollout'.
- Expiration Date:** A date picker showing the year 2006, month July, and day 10.
- Reason:** A text box containing 'System exempt until 10 July 2004 due to 2004 rollout'.
- Message text:** An empty text box.
- SQL Query statement:** An empty text box.
- Clients:** A list box containing 'SERVER1' and 'SERVER2', with 'SERVER2' selected.
- Groups:** A list box containing 'SCM Servers', 'Win2000 Platform', and 'SCM Clients'.
- Compliance Objects:** A list box containing 'Check DB2 administrator PWD Expiry' and 'Check Administrator PW Expiry', with 'Check DB2 administrator PWD Expiry' selected.

At the bottom of the dialog are three buttons: 'Display Query', 'Save', and 'Cancel'.

Select **Display Query** to generate the SQL statement then select **Save**.

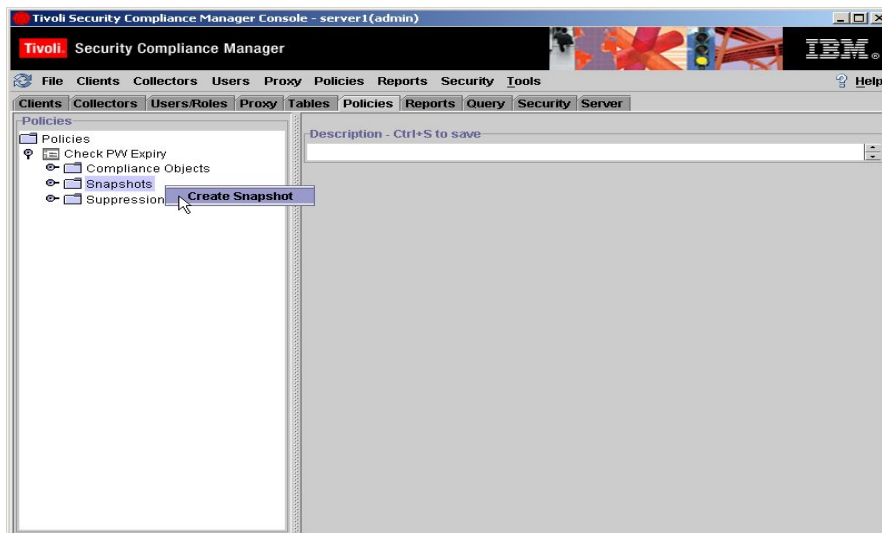


The 'Create Suppression' dialog box contains the following fields and lists:

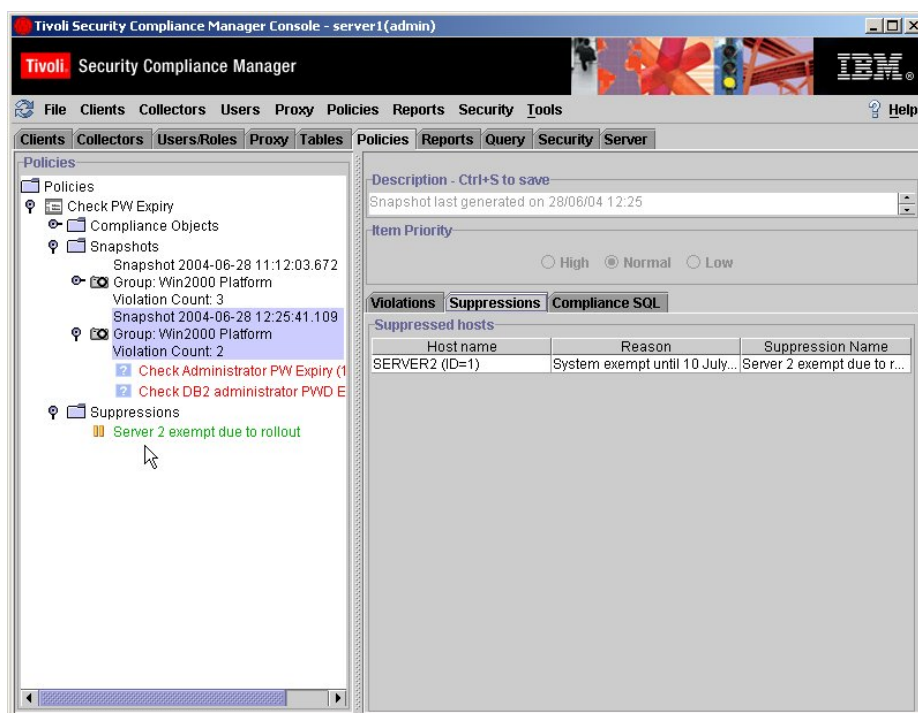
- Suppression name:** Server 2 exempt due to rollout
- Expiration Date:** 2004 May 7
- Reason:** System exempt until 10 July 2004 due to 2004 rollout.
- Message text:** (Empty text box)
- Clients:** SERVER1, SERVER2 (SERVER2 is selected)
- Groups:** SCM Servers, Win2000 Platform, SCM Clients
- Compliance Objects:** Check DB2 administrator PWD Expiry, Check Administrator PW Expiry (Both are selected)
- SQL Query statement:**

```
where CLI_ID in (select CLI_ID from JAC_SYS.CLIENTS where JAC_SYS.CLIENTS.ALIAS in ('SERVER2')) and COM_ID in (select ID from JAC_SYS.COMPLIANCE_SQL where JAC_SYS.COMPLIANCE_SQL.NAME in ('Check DB2 administrator PWD Expiry','Check Administrator PW Expiry'))
```
- Buttons:** Display Query, Save, Cancel

Select **Create Snapshot** to generate a new snapshot and see how the suppression works.



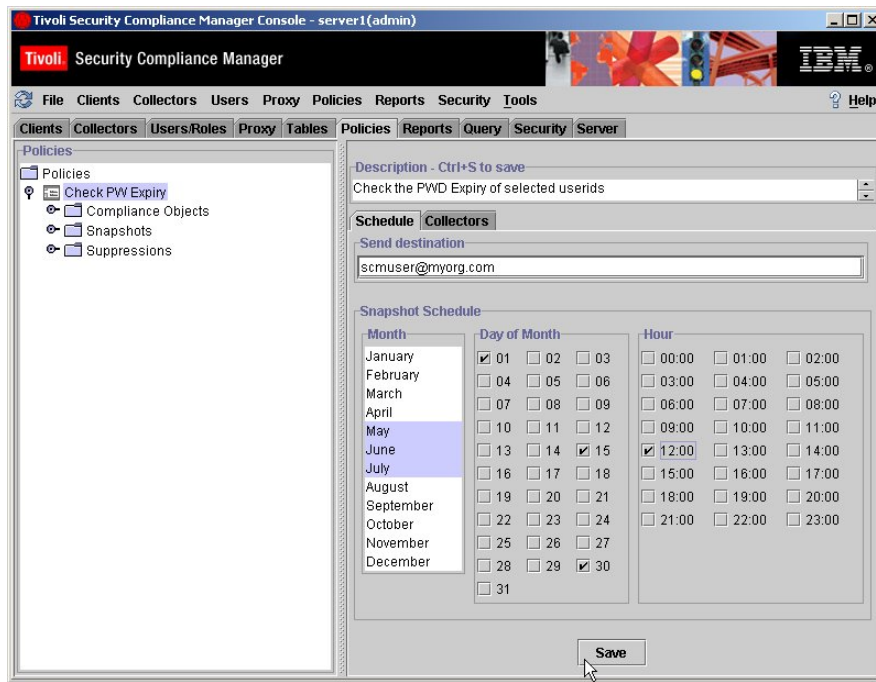
Instead of three violations, the snapshot only has two violations. In the left frame, under **Suppressions**, you see the suppression created for the Server2 client.



10.1.5 Policy Schedules and Collectors

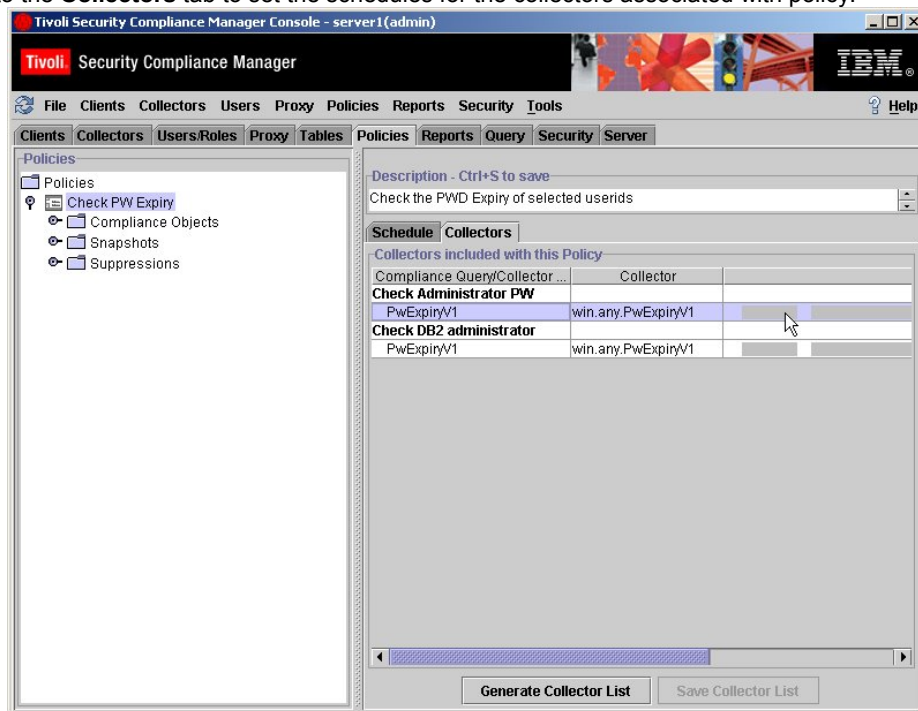
A schedule can be set to run the Policy at regular dates and times. In addition, the snapshots can be emailed to the proper administrators.

Select the **Check PW Expiry** policy, and then select the **Schedule** tab. set the **Send destination** to **scmuser@myorg.com**. Select the months, days of the month and times you want the snapshots to be run. The email address in the **Send destination** field is also used with the **Send now** option for policy snapshots. If a mail server is not available refer to [Installing an Email server](#) in this cookbook.

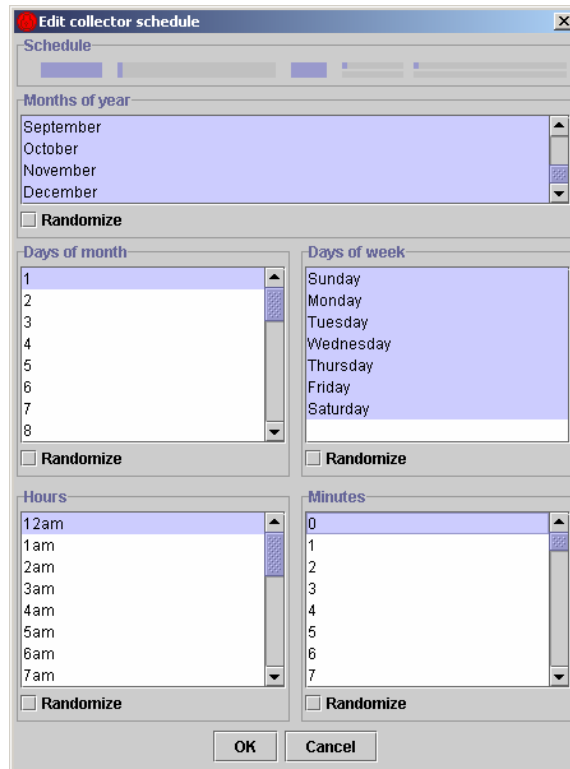


Select **Save**. When the snapshot is executed, the resulting snapshot can be displayed on the Administration Console. In addition, the snapshot will be sent to the email address specified in the **Send destination** field.

Go to the **Collectors** tab to set the schedules for the collectors associated with policy.



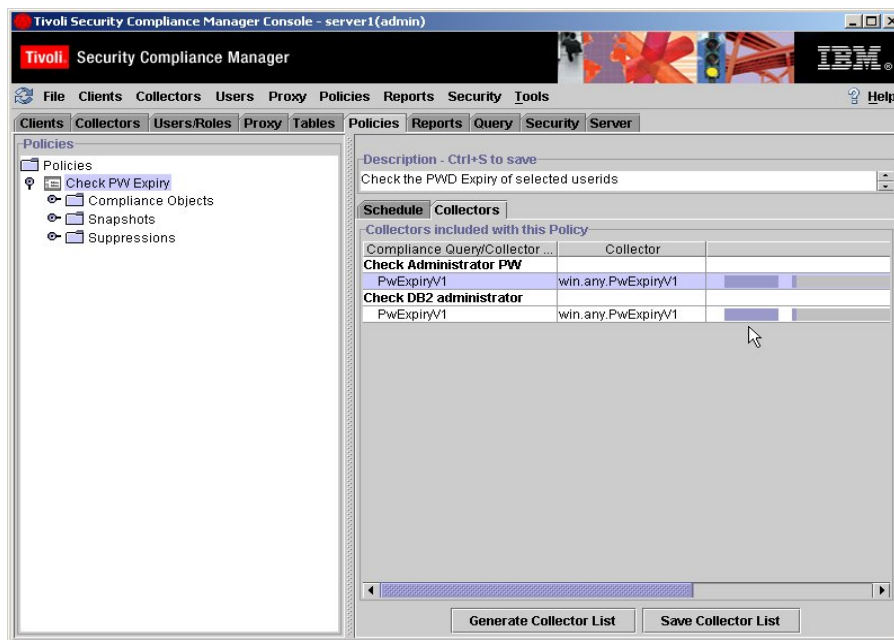
Double click the schedule icon (grey bars) for the collector. The **Edit collector schedule** window will appear.



The 'Edit collector schedule' window is a dialog box with a title bar. It contains several sections for configuring a schedule:

- Schedule**: A horizontal bar at the top.
- Months of year**: A list box showing September, October, November, and December. A 'Randomize' checkbox is below it.
- Days of month**: A list box showing days 1 through 8. A 'Randomize' checkbox is below it.
- Days of week**: A list box showing Sunday through Saturday. A 'Randomize' checkbox is below it.
- Hours**: A list box showing times from 12am to 7am. A 'Randomize' checkbox is below it.
- Minutes**: A list box showing minutes from 0 to 7. A 'Randomize' checkbox is below it.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom.

Set the collector schedule; then select **OK**.



The 'Tivoli Security Compliance Manager Console' window shows the 'Policies' tab. The left pane shows a tree view with 'Policies' expanded, containing 'Check PW Expiry', 'Compliance Objects', 'Snapshots', and 'Suppressions'. The right pane shows the details for the 'Check PW Expiry' policy, including a description and a table of collectors.

Collector
win.any.PwExpiryV1
PwExpiryV1

At the bottom of the right pane are 'Generate Collector List' and 'Save Collector List' buttons.

Note that both compliance queries use the same collector so the schedule change is reflected for both compliance queries.

Use **Generate Collector List** and **Save Collector List** to include the necessary policies, collectors and schedules into this policy (creating the policy bundle).

If you use **Send Snapshot** with a snapshot, the snapshot is sent to the email address specified in the **Send destination** field under the **Schedule** tab for the Policy. To view the snapshot email, be sure the ArGoSoft mail server is running on the VMWare session. Execute **Send Snapshot** for the policy snapshot. On the VMWare session, open Outlook Express. It has been configured to receive email for scmuser@myorg.com.

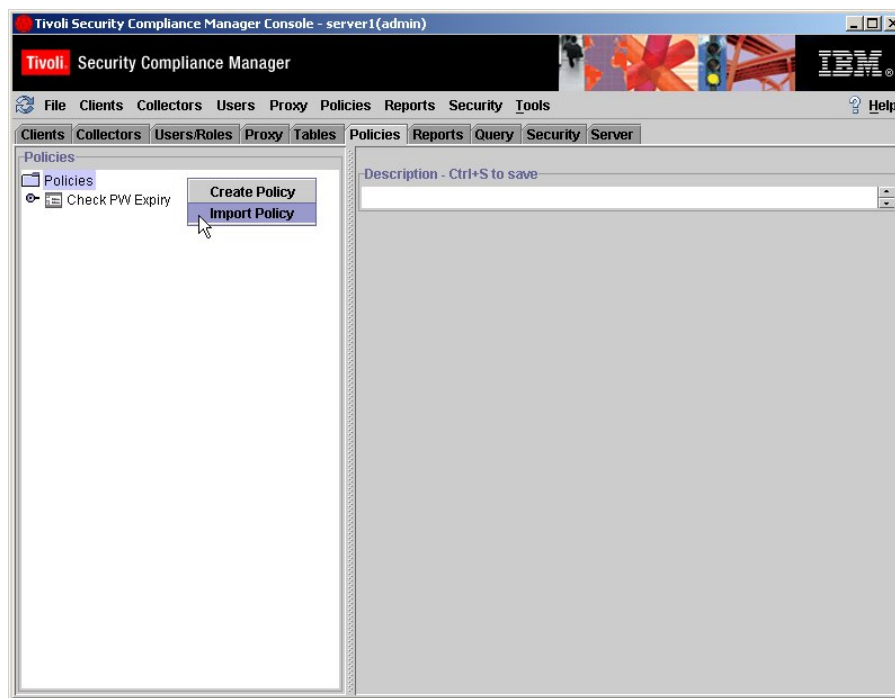
10.1.6 Policy Bundles

Policy Bundles are special files that contain all the resources and information required to produce a snapshot report of the given policy. With policies, all collectors, collector schedule and parameters, and compliance queries required to produce an accurate and meaningful snapshot can be added to the appropriate client systems and client groups.

In this section you will import a Policy that comes packaged with IBM Tivoli Security Compliance Manager.

Latest versions of the policies are available from the ITSCM download web site

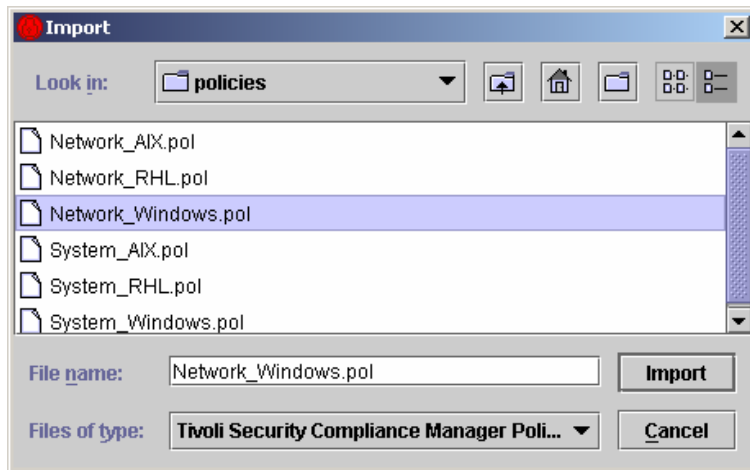
Select the Policy Container object in the **Policy** tab. Right click on the Policy object and select **Import Policy**.



You will be prompted with the Windows standard file manger selection box. Navigate to the following directory:

C:\SCM Demo\SCM Code\scm510\policies

Select **Network_Windows.pol** and then select the **Import** button.

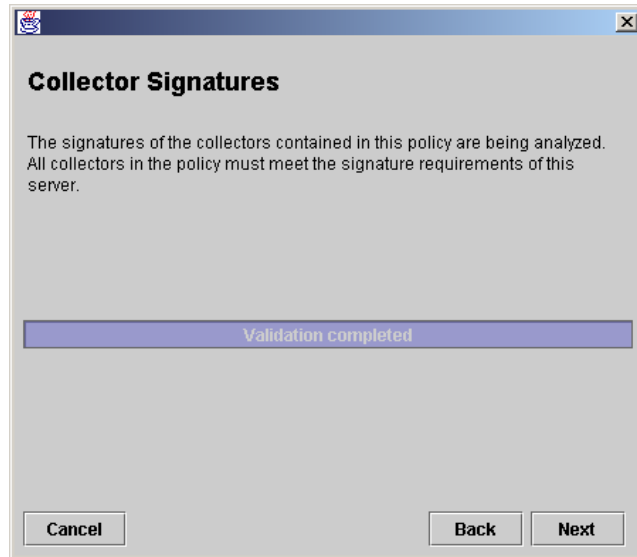


You are prompted to give the policy a name that will appear in the Policy container object.

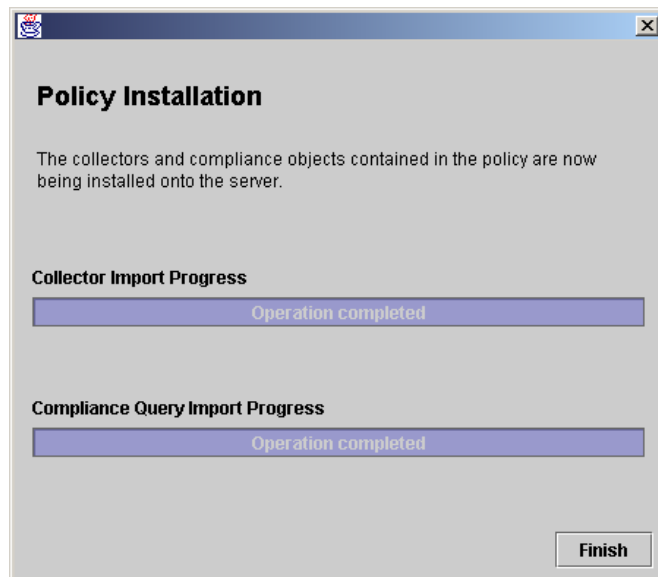


Here, the name was specified as **Network_Windows Policy**. Select **Next**.

The import process now begins with the import of Collector Signatures.



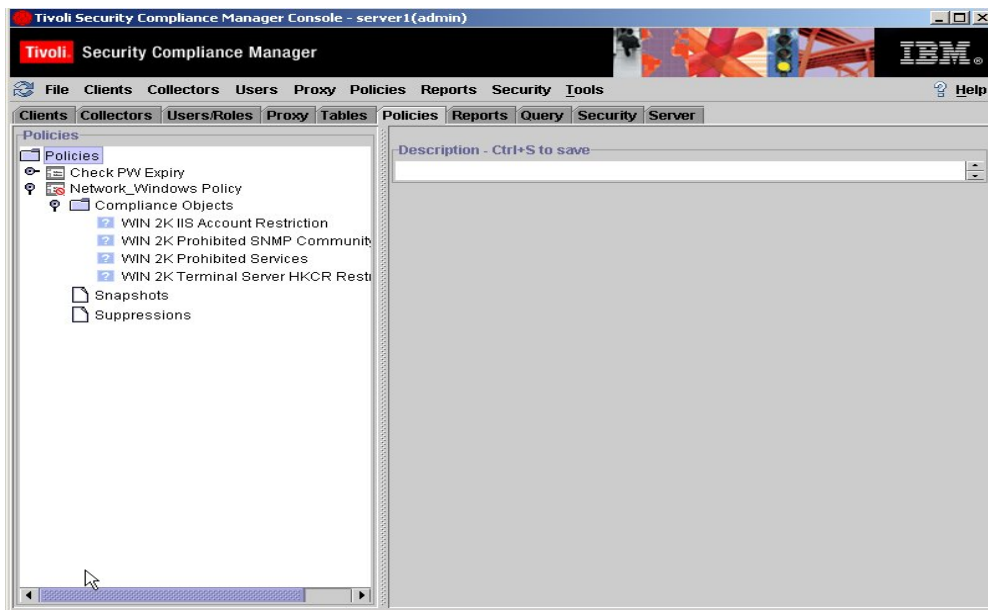
Click **Next** to continue the import process.



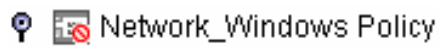
After the Policy Installation completes, select **Finish** to complete the import process.

Return to the Policy object list and expand your imported policy by clicking on the lever icon.

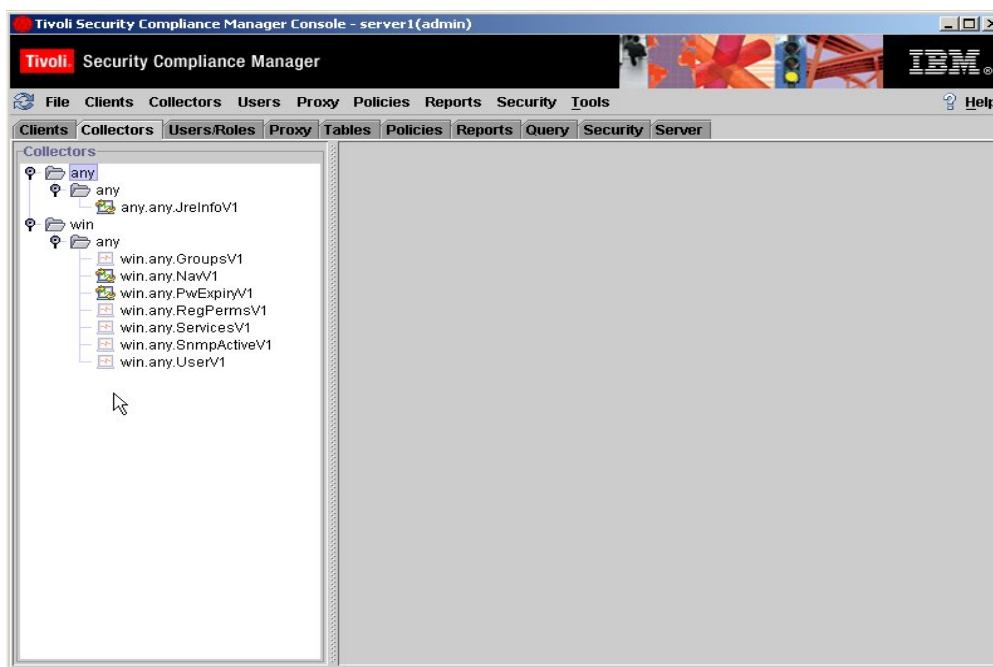
If you expand the Policy object for the newly imported policy, you will see a list of the compliance query objects that have been imported.



The next step is to register the collectors to make them available for clients. You can tell that there are unregistered collectors that are part of the policy bundle by red circle icon in the Policy object.

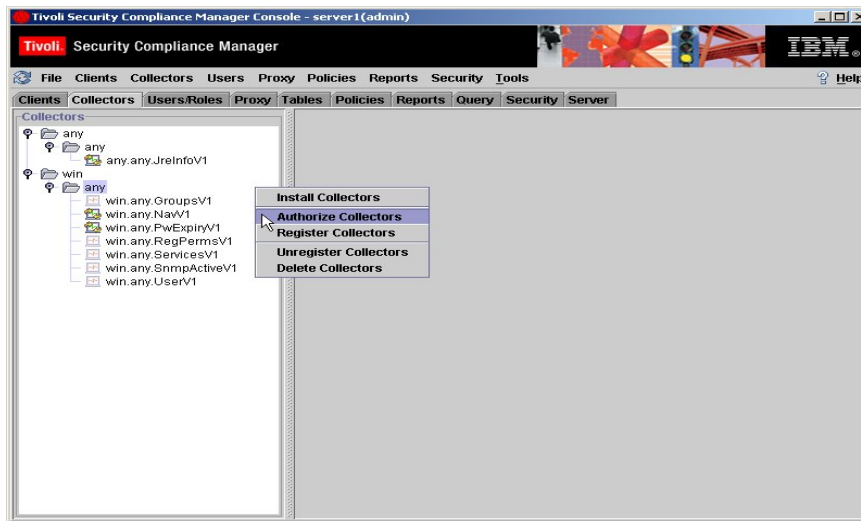


Return to the **Collectors** tab, expand the groups of collectors.

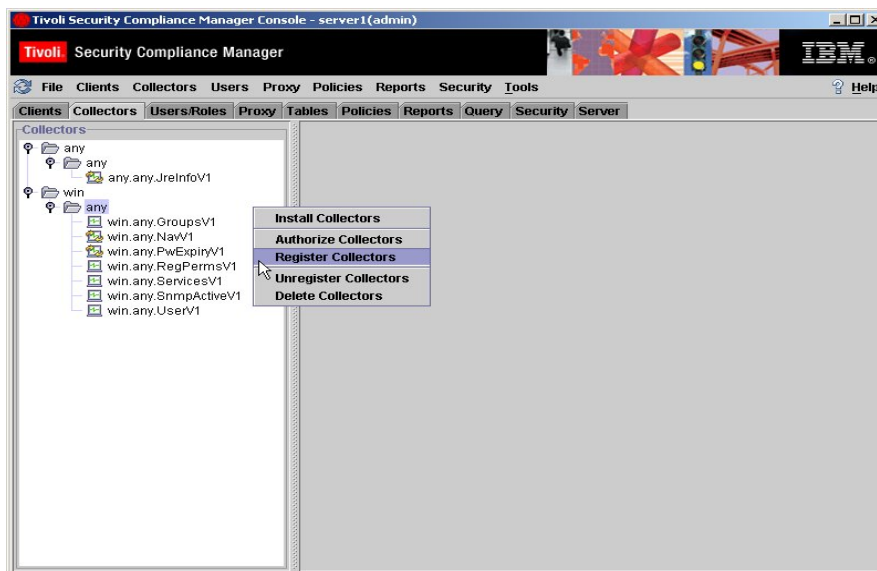


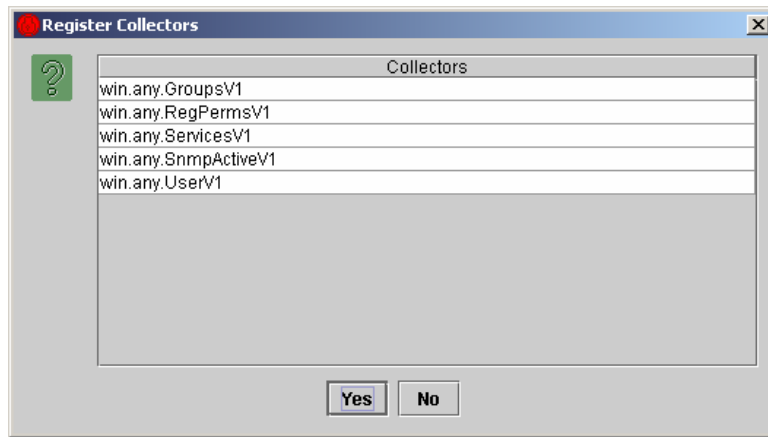
You can see that the new collectors that have been imported as part of the policy bundle are not authorized or registered (notice their icon).

Right click on the **win** or **win -> any** folder and select **Authorize Collectors**.



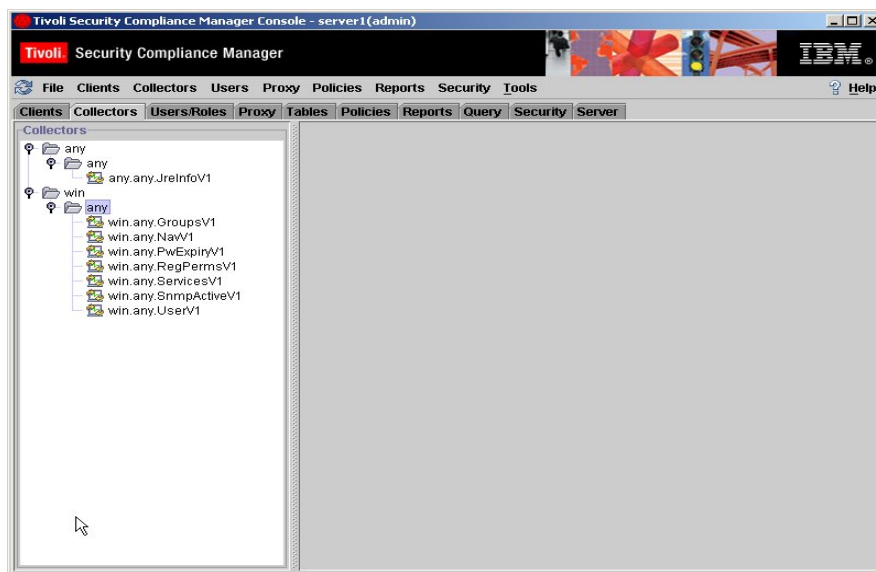
Select the authorization key (**key001**) and provide the keystore password (**passw0rd**). After the collectors have been authorized, again select the **win** or **win -> any** folder, right click and select **Register Collectors**.



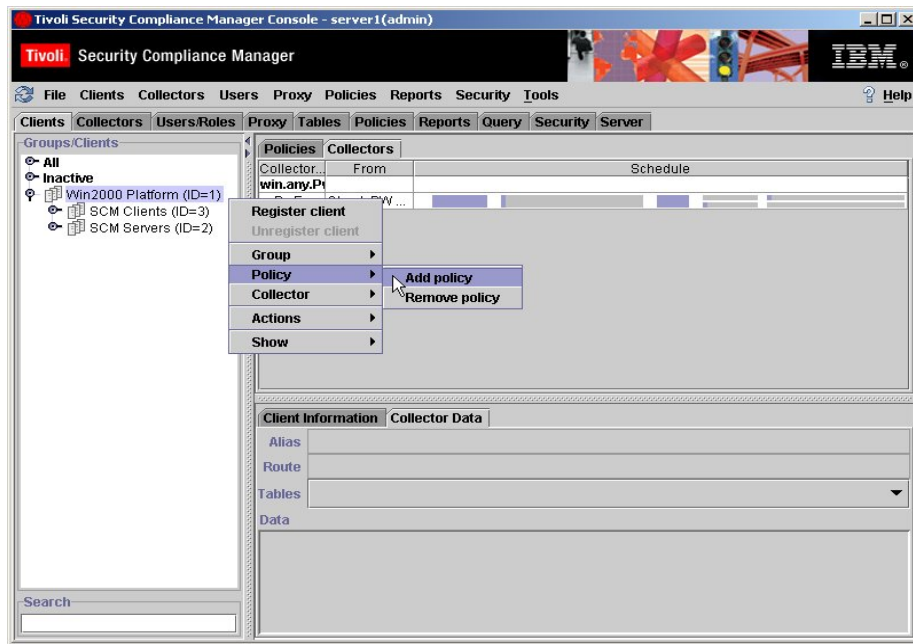


Select **Yes** to register all the collectors.

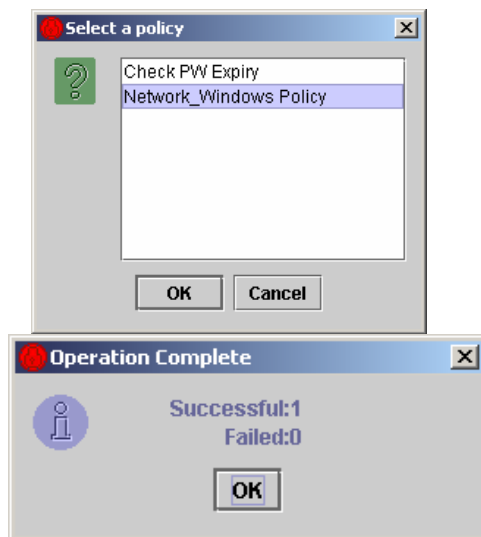
The icons will change for the individual collectors to Registered status.



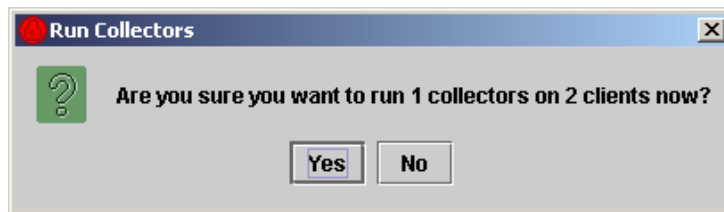
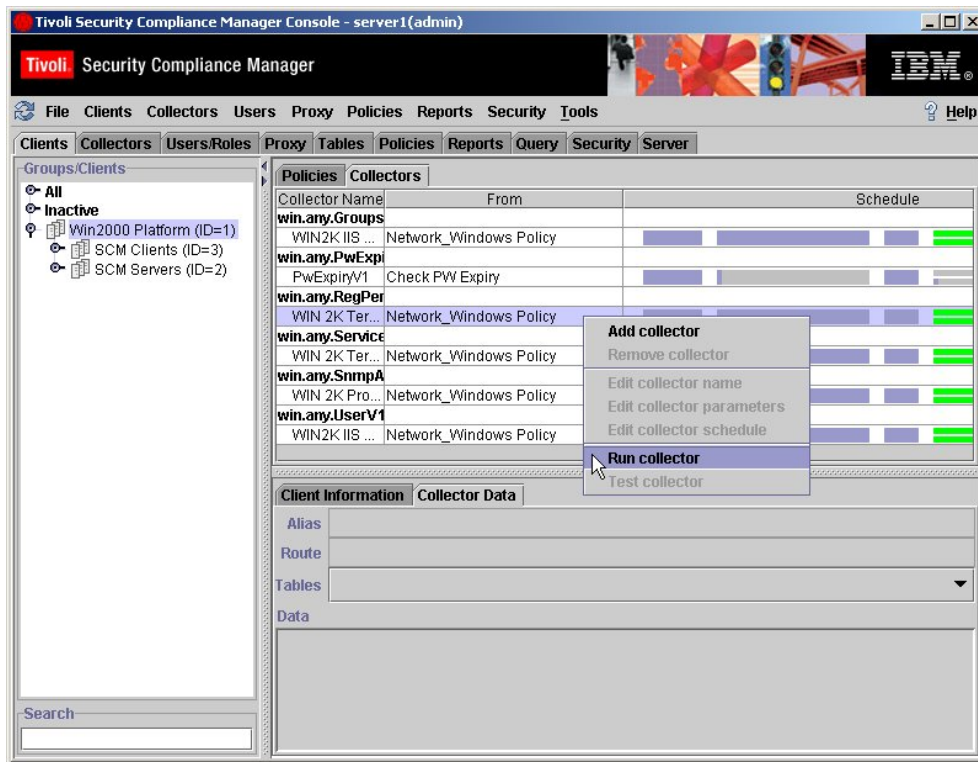
Go to the **Clients** tab. Add the policy to the **Win2000 Platform** group.



Select the **Network_Windows Policy**; select **OK**.

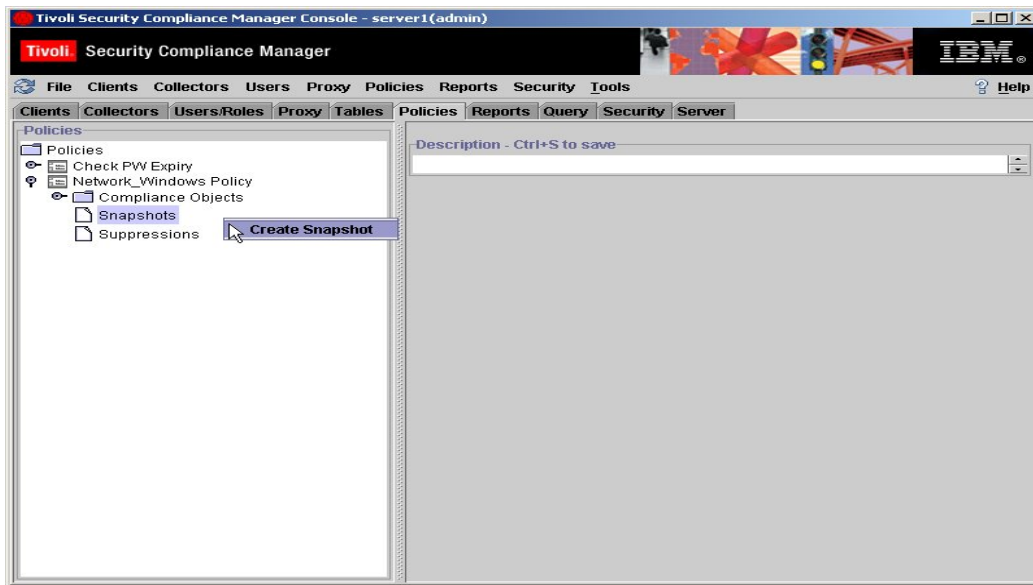


To ensure data has been collected, use **Run collector** to run each of the policy's collectors. Use the **From** column in the **Collectors** view to determine which collectors belong to the policy. In a production environment, the policy's collectors would be assigned a schedule so that collector data is retrieved based on schedule.



Return to the **Policies** tab and refresh the display. You will see that the Policy object icon no longer indicates that the policy's collectors are unregistered.

Now create a snapshot for the policy and assign to your **Win2000 Platform** group. Review the results and investigate what data the individual Compliance Queries are looking for.



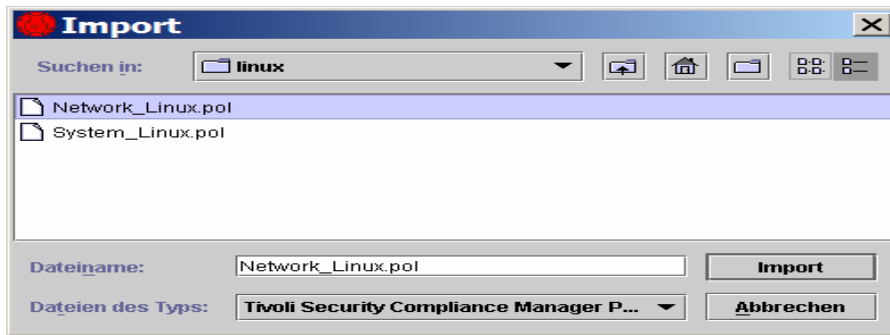
You will most likely see one or more violations. Verify ITSCM, test some ITSCM Base Functions

10.2 *Sample Installation of selected policies: Linux + UNIX policies*

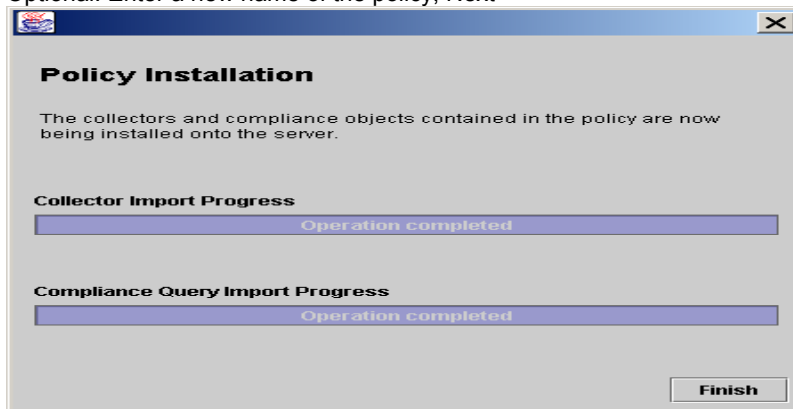
Go to the Policy Tab and select: Import Policies



Point to the correct directory



Optional: Enter a new name of the policy, Next



Repeat this step for the System_Linux_Policy

Verify the Network Linux Policy in the Policy Tab, in the screenshot below the right panel shows the included collectors

File Clients Collectors Users Proxy Policies Reports Security Tools

Clients Collectors Users/Roles Proxy Tables Policies Reports Query Security Server

Policies

- Network_Linux Policy
 - Compliance Objects
 - .NETRC Restrictions
 - .RHOSTS Restrictions
 - /ETC/EXPORTS Restriction
 - /ETC/HOSTS.EQUIV Prohibit
 - /ETC/PAM.D/OTHER Restrict
 - /ETC/PAM.D/RLOGIN Restrict
 - /ETC/PAM.D/RSRSH Restriction
 - /ETC/SYSCTL.CONF Restrict
 - Anon FTP Access Permissio
 - Anon FTP Directory Configur
 - Anon FTP Directory Permissi
 - FTP World-Writable Files Re
 - NIS Maps Prohibited
 - Prohibit NIS YPPASSWD
 - Prohibit REXD
 - Prohibited Community Name
 - TFTP Required Startup Optio
 - Snapshots
 - Suppressions
- System_Linux Policy
 - Compliance Objects
 - / Restrictions
 - /TMP Restrictions
 - /USR Restrictions
 - /VAR Restrictions
 - /VAR/TMP Restrictions
 - Home Directory Restrictions
 - Log Files Required
 - Login Success or Failure for
 - Login Success or Failure for
 - Maximum Password Age
 - Minimum Password Length
 - Prohibited Services
 - Snapshots
 - Suppressions

Description - Ctrl+S to save

Policy for checking the network-related security characteristics of a Linux server.

Schedule Collectors

Collectors included with this Policy

Compliance Query/Collector Name	Collector		
.NETRC Restrictions			
.RHOSTS Restrictions_30	unix.any.HomeFsV1		
.RHOSTS Restrictions			
.RHOSTS Restrictions_30	unix.any.HomeFsV1		
/ETC/EXPORTS Restriction			
/ETC/EXPORTS Restriction_25	unix.any.FilePermsV1		
FTP World-Writable Files Restr...	unix.any.ProcessesV1		
/ETC/HOSTS.EQUIV Prohibited			
/ETC/HOSTS.EQUIV Prohibited_...	unix.any.HostsEquiV1		
/ETC/PAM.D/OTHER Restrictions			
/ETC/PAM.D/RSRSH Restrictions_39	unix.any.PamV1		
/ETC/PAM.D/RLOGIN Restrictions			
/ETC/PAM.D/RSRSH Restrictions_39	unix.any.PamV1		
/ETC/PAM.D/RSRSH Restrictions			
/ETC/PAM.D/RSRSH Restrictions_39	unix.any.PamV1		
/ETC/SYSCTL.CONF Restrictions			
/ETC/SYSCTL.CONF Restriction...	linux.any.SysctlV1		
Anon FTP Access Permissions			
FTP World-Writable Files Restr...	unix.any.AnonFtpFilePer...		
Anon FTP Directory Configuration			
FTP World-Writable Files Restr...	unix.any.AnonFtpFilePer...		
Anon FTP Directory Permissions			
FTP World-Writable Files Restr...	unix.any.AnonFtpFilePer...		
FTP World-Writable Files			
FTP World-Writable Files Restr...	unix.any.AnonFtpFilePer...		
FTP World-Writable Files Restr...	unix.any.ProcessesV1		
NIS Maps Prohibited			
NIS Maps Prohibited_38	unix.any.NisMapsV1		
Prohibit NIS YPPASSWD			
FTP World-Writable Files Restr...	unix.any.ProcessesV1		
NIS Maps Prohibited_38	unix.any.NisMapsV1		
Prohibit REXD			
FTP World-Writable Files Restr...	unix.any.ProcessesV1		
Prohibited Community Names			
FTP World-Writable Files Restr...	unix.any.ProcessesV1		
Prohibited Community Names_...	unix.any.SnmpdV1		
TFTP Required Startup Options			
FTP World-Writable Files Restr...	unix.any.ProcessesV1		

Generate Collector List Save Collector List

Verify the System Linux Policy in the Policy Tab, in the screenshot below the right panel shows the included collectors

The screenshot displays the Tivoli Security Compliance Manager Console interface. The left pane shows a tree view of policies, with 'System_Linux Policy' selected. The right pane shows the configuration for this policy, including a description and a list of collectors.

Description - Ctrl+S to save
Policy for checking the system-related security characteristics of a Linux server.

Schedule **Collectors**

Collectors included with this Policy

Compliance Query/Collector Name	Collector	
/Restrictions		
Log Files Required_25	unix.any.FilePermsV1	
/TMP Restrictions		
Log Files Required_25	unix.any.FilePermsV1	
/USR Restrictions		
Log Files Required_25	unix.any.FilePermsV1	
/VAR Restrictions		
Log Files Required_25	unix.any.FilePermsV1	
/VAR/TMP Restrictions		
Log Files Required_25	unix.any.FilePermsV1	
Home Directory Restrictions		
Home Directory Restrictions_30	unix.any.HomeFsV1	
Log Files Required		
Log Files Required_25	unix.any.FilePermsV1	
Login Success or Failure for		
Login Success or Failure for *_46	unix.any.SyslogConfV1	
Login Success or Failure for *		
Login Success or Failure for *_46	unix.any.SyslogConfV1	
Maximum Password Age		
Maximum Password Age_15	linux.any.LoginDefsV1	
Minimum Password Length		
Maximum Password Age_15	linux.any.LoginDefsV1	
Prohibited Services		
ProcessesV1	unix.any.ProcessesV1	
Prohibited Services_34	unix.any.InetdV1	
XinetdV1	unix.multi.XinetdV1	

Buttons: **Generate Collector List** **Save Collector List**

Follow a similar process to the windows policy install and testing as previous described for the linux Policies or for Unix policies.

11 Creating a sample SQL report from the ITSCM administration GUI

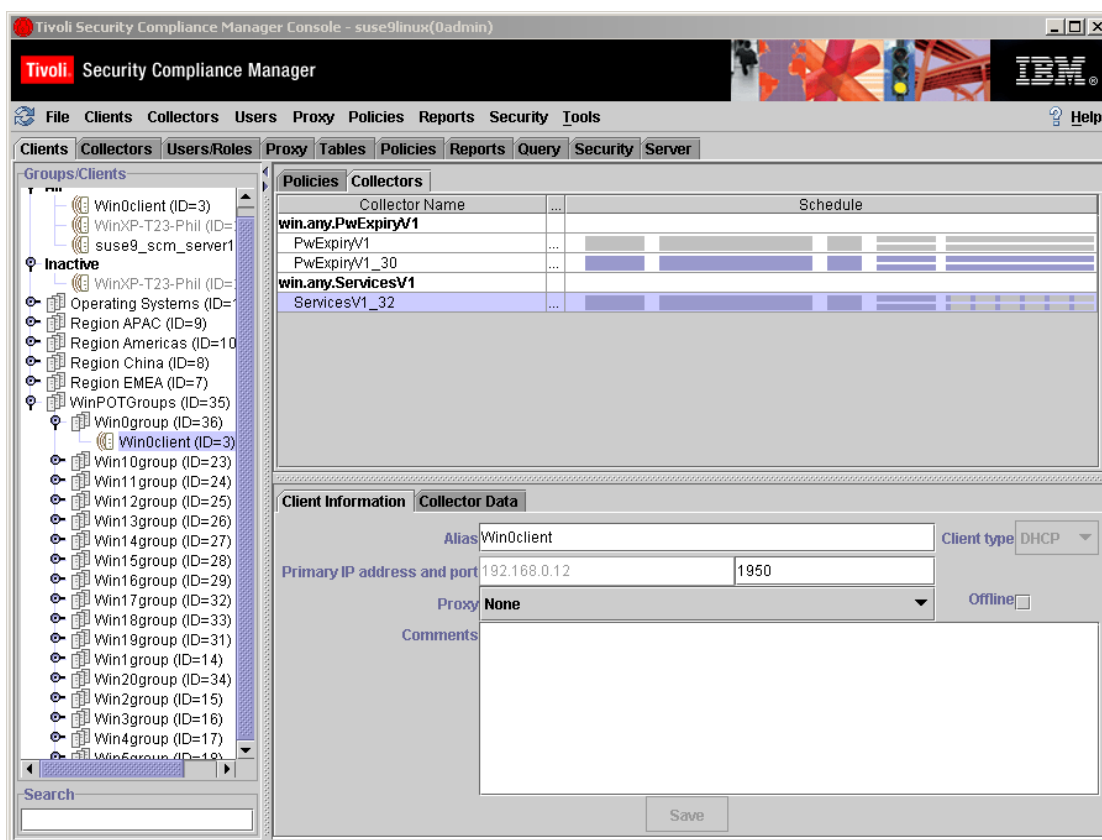
11.1 SQL Reports

- 1) You can use the **Reports** facility to display and save the result of SQL queries, and to send the report to a designated email address.

NOTE THAT THESE EXERCISES REQUIRE YOU TO RUN THE APPROPRIATE WINDOWS COLLECTOR

(Hint: For Windows Services Collector, see the graphic below – you need to right-click on the Collector below and choose 'Run Collector' – it is best to run all the collectors listed below first to try out some of the reports later on in this lab) –

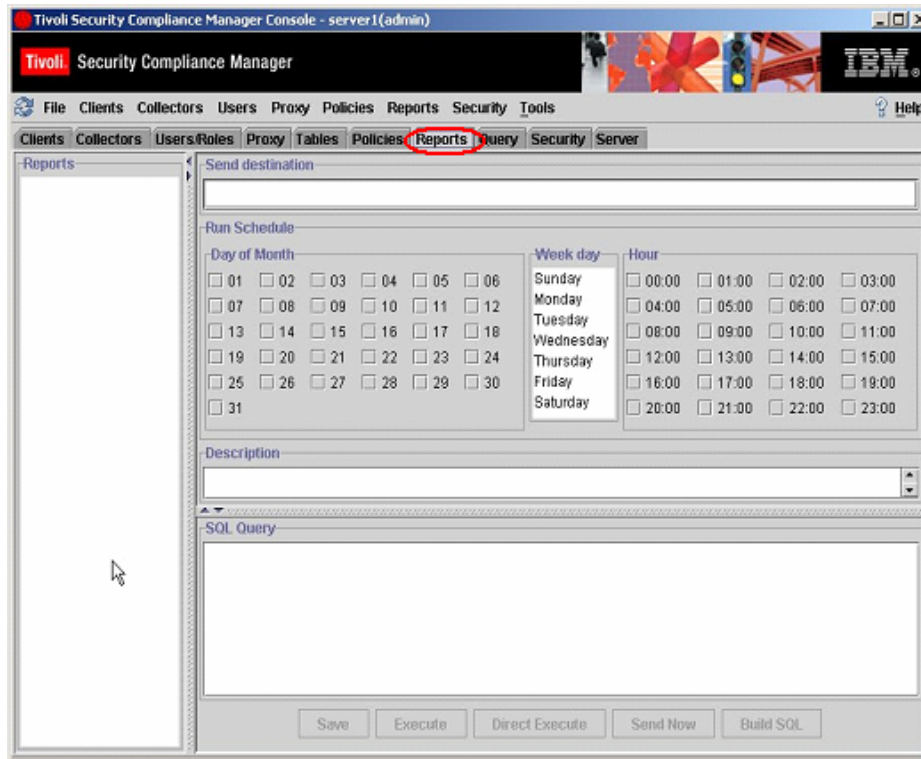
- 2) Go to the **Clients** tab, from the **Collectors** view, run the policy's collector instance (**ServicesV1_32**), as shown below, if this was not run previously successfully. Use right click on the collector instance and the **Run Collector** as done previously for the other collectors



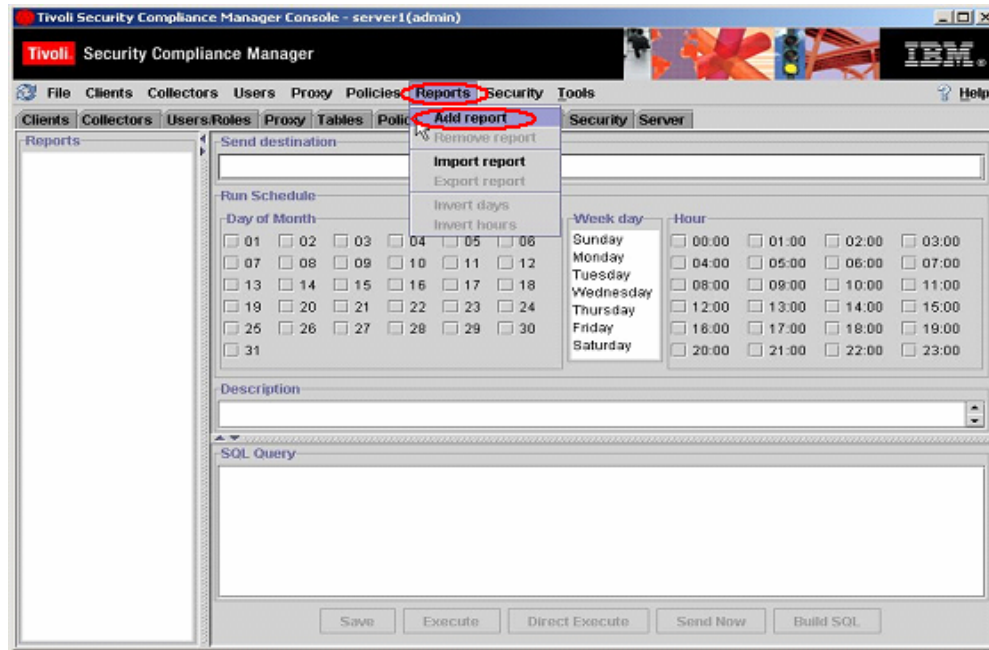
Adding a Report

- 3) Click on the **Reports** tab on the Administration Console.

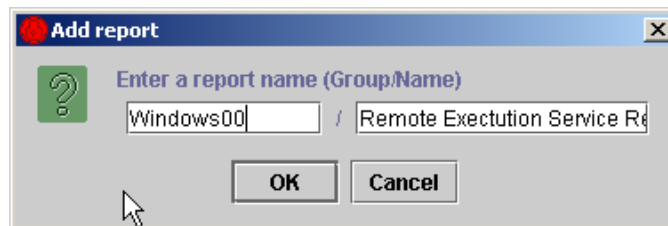
Selecting the **Reports** tab will display the Reports panel.



- 4) Click on **Reports** from the main menu bar to display the Reports submenu, and then click **Add Report**.



- 5) The **Add Report** dialogue box will open. The report must be given a name and placed into a report group. If the group specified does not exist, it will be created. Enter **Windows00** for the Group name and **Remote Execution Related Services Report** as the report name.



You should now see the Group and Report names appear in the **Reports** panel on the left.

The screenshot shows the Tivoli Security Compliance Manager Console window. The title bar reads "Tivoli Security Compliance Manager Console - suse9linux(0admin)". The main menu bar includes "File", "Clients", "Collectors", "Users", "Proxy", "Policies", "Reports", "Security", and "Tools". Below this is a sub-menu bar with "Clients", "Collectors", "Users/Roles", "Proxy", "Tables", "Policies", "Reports", "Query", "Security", and "Server". The "Reports" panel on the left shows a tree view with "Windows00" expanded, containing "Remote Execution" and "Windows". The main configuration area has several sections: "Send destination" with a text input field; "Run Schedule" with a "Day of Month" grid (01-31), a "Week day" dropdown (Sunday-Saturday), and an "Hour" grid (00:00-23:00); "Description" with a large text area; and "SQL Query" with a large text area. At the bottom are buttons for "Save", "Execute", "Direct Execute", "Send Now", and "Build SQL".

11.1.1 Configuring a Report

Configuring a report consists of the following steps:

- entering an email address to send the report to
- specifying when the report will run using the Run Schedule section
- entering a description of what is being reported on
- building a SQL query that will be used to extract the required data from the collector or system tables in the database

- 6) In the **Send To** field enter the email addresses to which your reports are to be sent. For this exercise you will not be emailing the report although you can add the user, **scmuser @ myorg.com**

Select values for the Day of Month, Week day and Hour. For this lab it will not matter what values are selected as you will run the schedule immediately, however entries for these three attributes must be entered in order for the report to run.

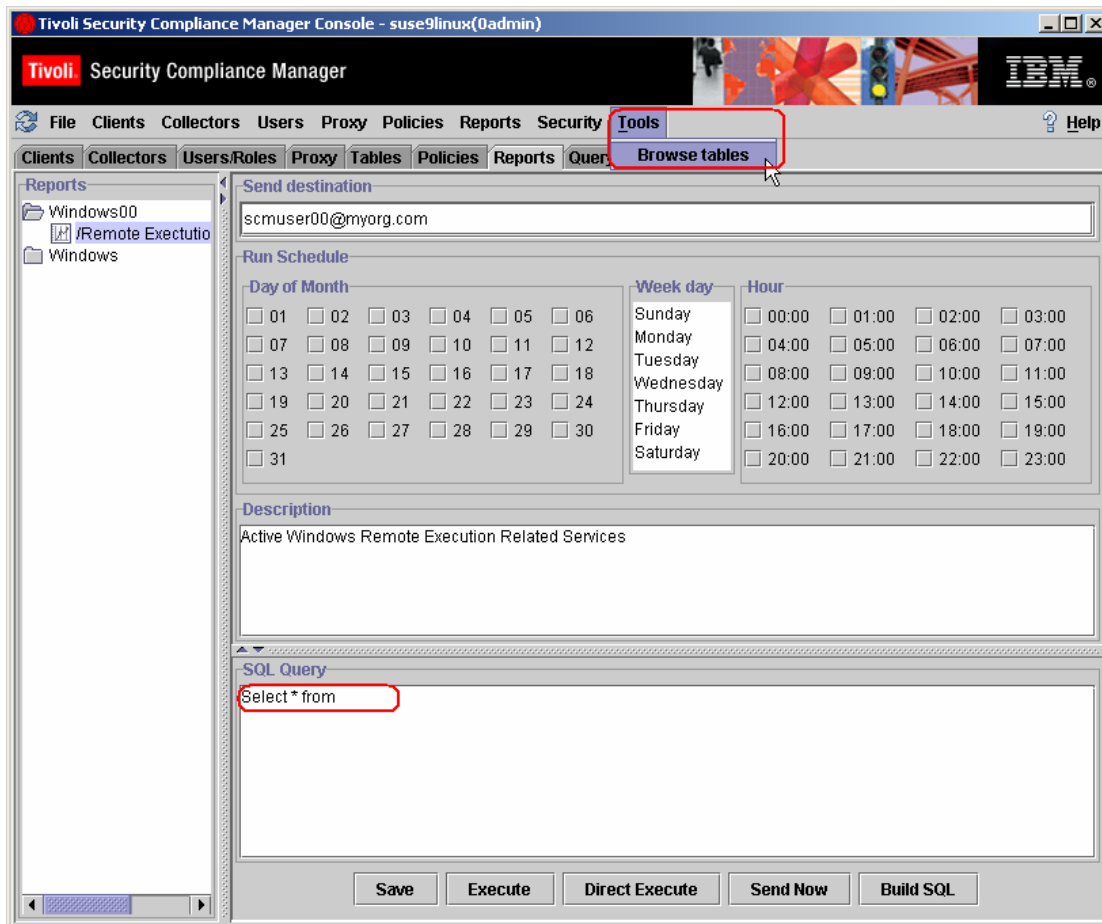
- 7) Enter a description for the report in the **Description** field. Enter '**Active Windows Remote Execution Related Services**' report and press **Save**

The screenshot shows the Tivoli Security Compliance Manager Console window. The title bar reads "Tivoli Security Compliance Manager Console - suse9linux(0admin)". The main menu includes File, Clients, Collectors, Users, Proxy, Policies, Reports, Security, and Tools. A sub-menu bar below it includes Clients, Collectors, Users/Roles, Proxy, Tables, Policies, Reports, Query, Security, and Server. On the left, a tree view shows "Reports" expanded, with sub-items "Windows00", "Remote Execution", and "Windows". The main area is divided into several sections: "Send destination" with a text field containing "scmuser@myorg.com"; "Run Schedule" with three columns of checkboxes for "Day of Month" (01-31), "Week day" (Sunday-Saturday), and "Hour" (00:00-23:00); "Description" with a text field containing "Active Windows Remote Execution Related Services"; and "SQL Query" with a large empty text area. At the bottom, there are five buttons: "Save" (highlighted with a red rectangle), "Execute", "Direct Execute", "Send Now", and "Build SQL".

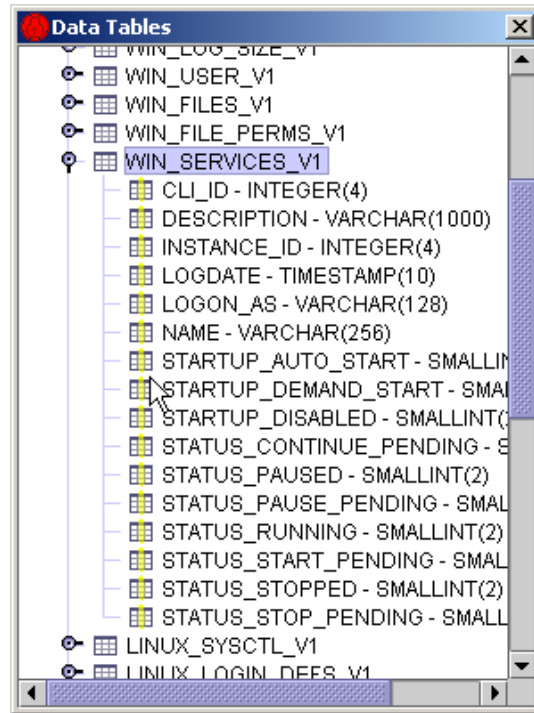
- 8) The report you are going to create will include the Windows information gathered by the **win.any.Services_v1** collector. To do this first enter the following into **the SQL Query** field:

```
select * from
```

- 9) Next, click on **Tools** on the Main menu bar and select **Browse Tables**.



A new window will be pop up displaying the data table for each collector that has been added to the server.



10) Drag and drop **WIN_SERVICES_V1** into the **SQL Query** field. You will notice that the SQL query is updated with the table name for that collector. Expand the **WIN_SERVICES_V1** table to reveal the attributes of the table. Now type the word **'where'** after the table name just dragged across (you don't need to close the Data Tables window just yet)

11) Now drag and drop the attributes **STATUS_RUNNING** and **NAME** into the **SQL Query** box

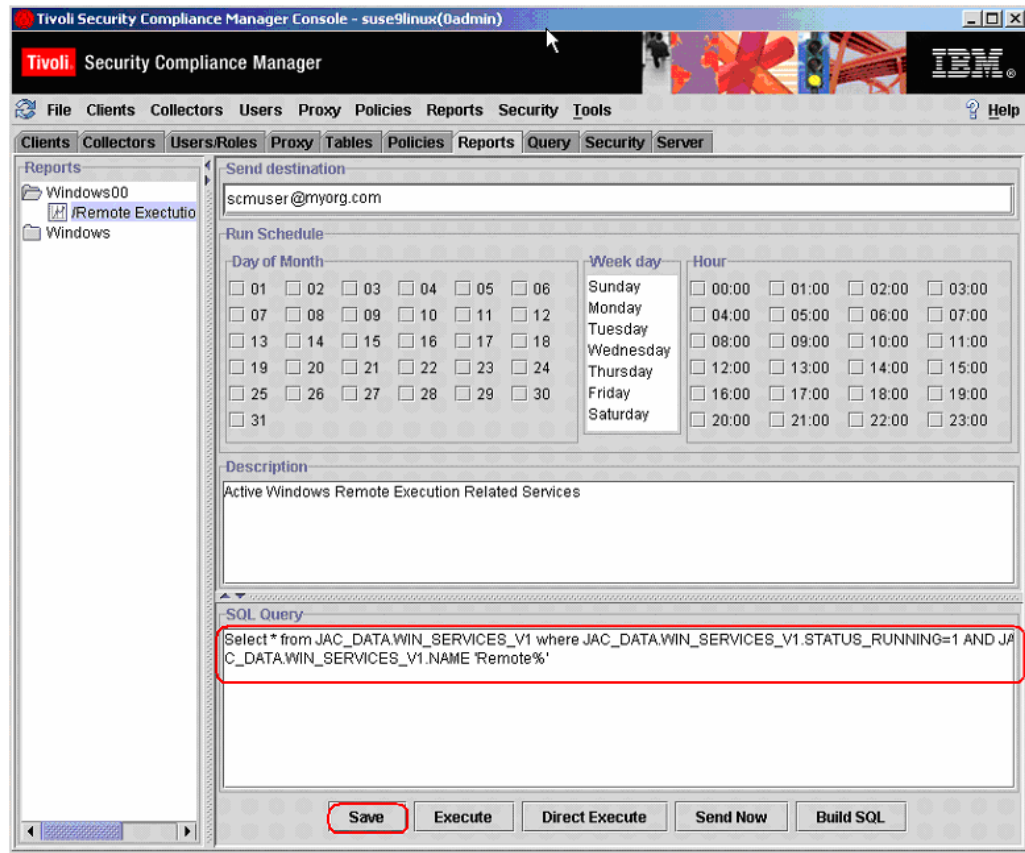
12) Complete the SQL Query so it now looks like this:

```
select * from JAC_DATA.WIN_SERVICES_V1 where  
JAC_DATA.WIN_SERVICES_V1.STATUS_RUNNING=1 AND  
JAC_DATA.WIN_SERVICES_V1.NAME LIKE 'Remote%'
```

Where ('1' means the Remote services are running)

13) Close the **Data Tables** windows. Keep the query as is or to make it more specific by entering the criteria for retrieving only the information from certain systems.

It could have been simpler just to type this query directly into the SQL Query field, but using the drag and drop method will ensure that you have the schema, table and attribute names entered correctly.



14) Select **Save** to save the report definition.

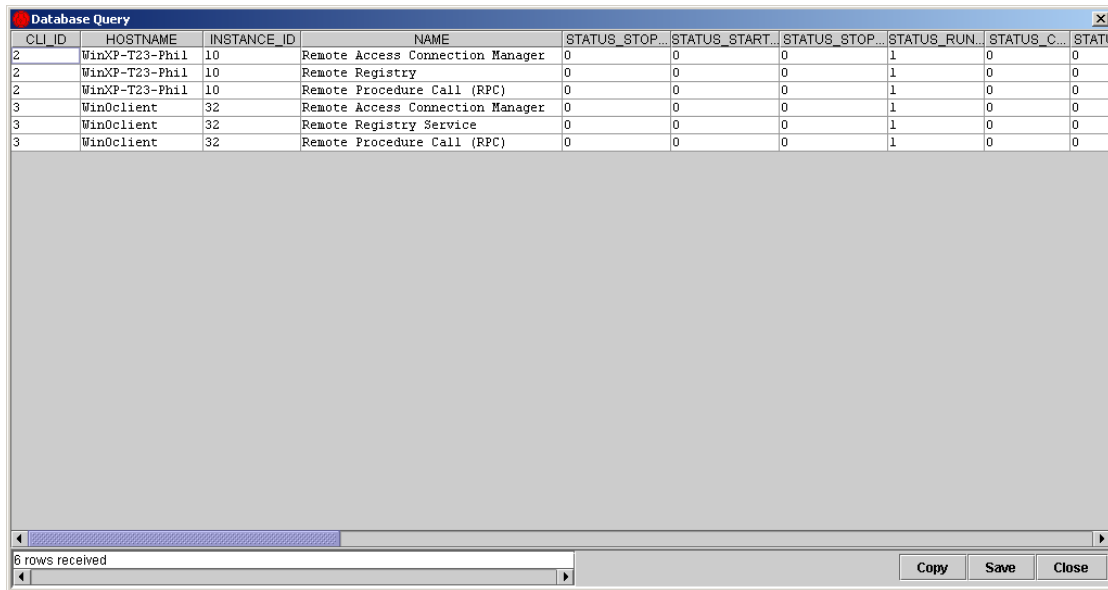
It is also possible to build the SQL query by clicking on the **Build SQL** button and defining the tables, criteria, search conditions via a series of steps which will automatically create the query for you (as you did in the Policy lab). You may wish to experiment with the Query builder more after you complete this exercise.

11.1.2 Execute a report

Clicking on any of the three buttons below the **SQL Query**; i.e. **Execute**, **Direct Execute** and **Send Now**, will run the SQL query and create a report, however, each has a slightly different function:

- The **Execute** button will create a report using the saved report configuration.
- The **Direct Execute** button will create a report using the current report configuration which is displayed in the query window, but may have not been saved.
- The **Send Now** button will create a report using the current configuration i.e. that which is displayed and send it to the email address entered in the Send to field.

- 15) Click on the **Direct Execute** button. The output of the report created will be displayed in the Database Query window.

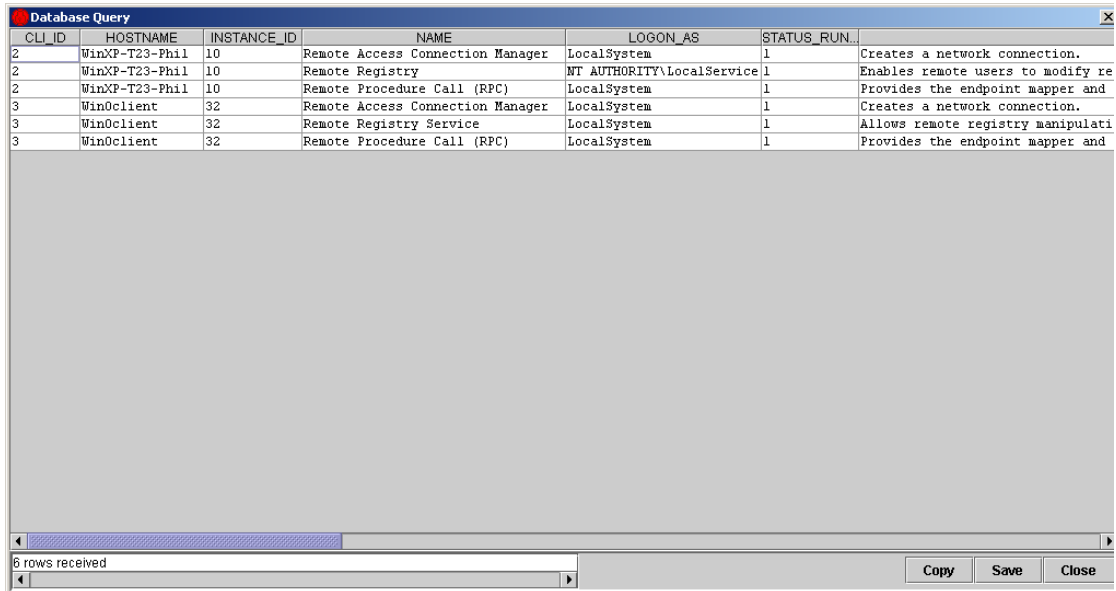


CLI_ID	HOSTNAME	INSTANCE_ID	NAME	STATUS_STOP...	STATUS_START...	STATUS_STOP...	STATUS_RUN...	STATUS_C...	STATI
2	WinXP-T23-Phil	10	Remote Access Connection Manager	0	0	0	1	0	0
2	WinXP-T23-Phil	10	Remote Registry	0	0	0	1	0	0
2	WinXP-T23-Phil	10	Remote Procedure Call (RPC)	0	0	0	1	0	0
3	WinOclient	32	Remote Access Connection Manager	0	0	0	1	0	0
3	WinOclient	32	Remote Registry Service	0	0	0	1	0	0
3	WinOclient	32	Remote Procedure Call (RPC)	0	0	0	1	0	0

6 rows received

Copy Save Close

- 16) You can re-order the columns in the report by clicking on the name of the column you wish to reposition, and dragging it to the required position. You now can either **Copy** the report to the Clipboard, for importing into another application or **Save** the report as a text file.



CLI_ID	HOSTNAME	INSTANCE_ID	NAME	LOGON_AS	STATUS_RUN..	
2	WinXP-T23-Phil	10	Remote Access Connection Manager	LocalSystem	1	Creates a network connection.
2	WinXP-T23-Phil	10	Remote Registry	NT AUTHORITY\LocalService	1	Enables remote users to modify re
2	WinXP-T23-Phil	10	Remote Procedure Call (RPC)	LocalSystem	1	Provides the endpoint mapper and
3	WinOclient	32	Remote Access Connection Manager	LocalSystem	1	Creates a network connection.
3	WinOclient	32	Remote Registry Service	LocalSystem	1	Allows remote registry manipulati
3	WinOclient	32	Remote Procedure Call (RPC)	LocalSystem	1	Provides the endpoint mapper and

6 rows received

Copy Save Close

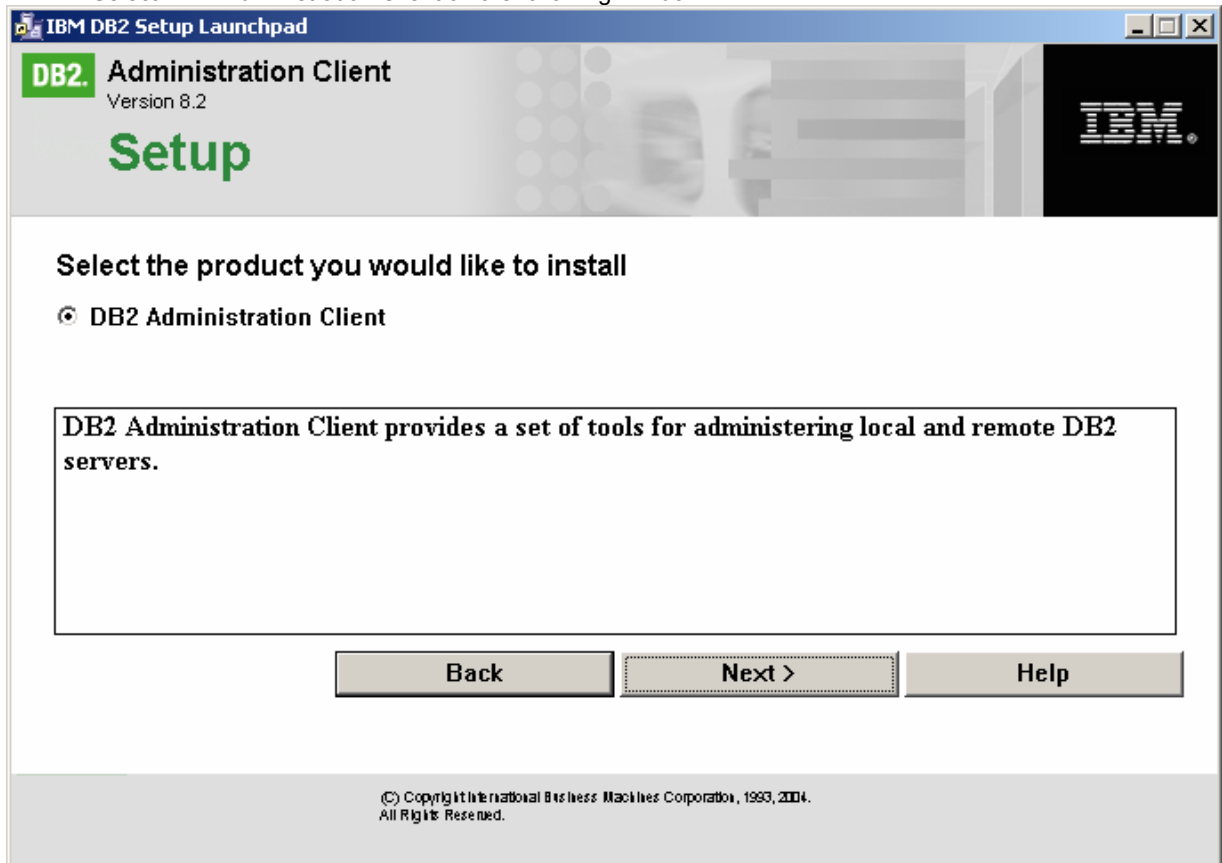
If you use **Send Now** the report is generated and sent to the email address specified.

12 Preparing the W2K client for ITSCM Operational Reporting

12.1 W2K: Installation DB2 UDB Administration Client V8.2

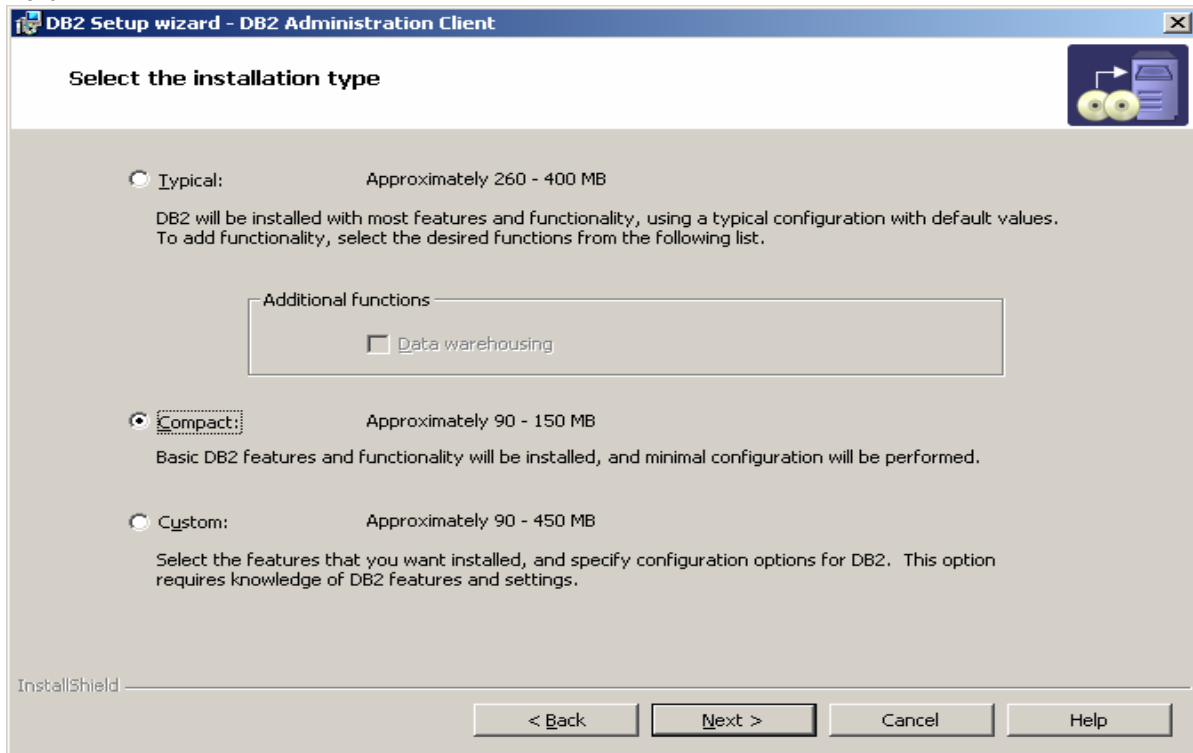
This session has used a DB2 UDB Administration Client V8.2 for Windows 98, NT, 2000, 2003, XP and ME 32-bit. (Please remember: V 8.2 corresponds to V 8.1 Fixpack 7a)

- Call setup.exe from the code directory
- Select Install product , Next
- Select: DB2 Administration Client on the following Window

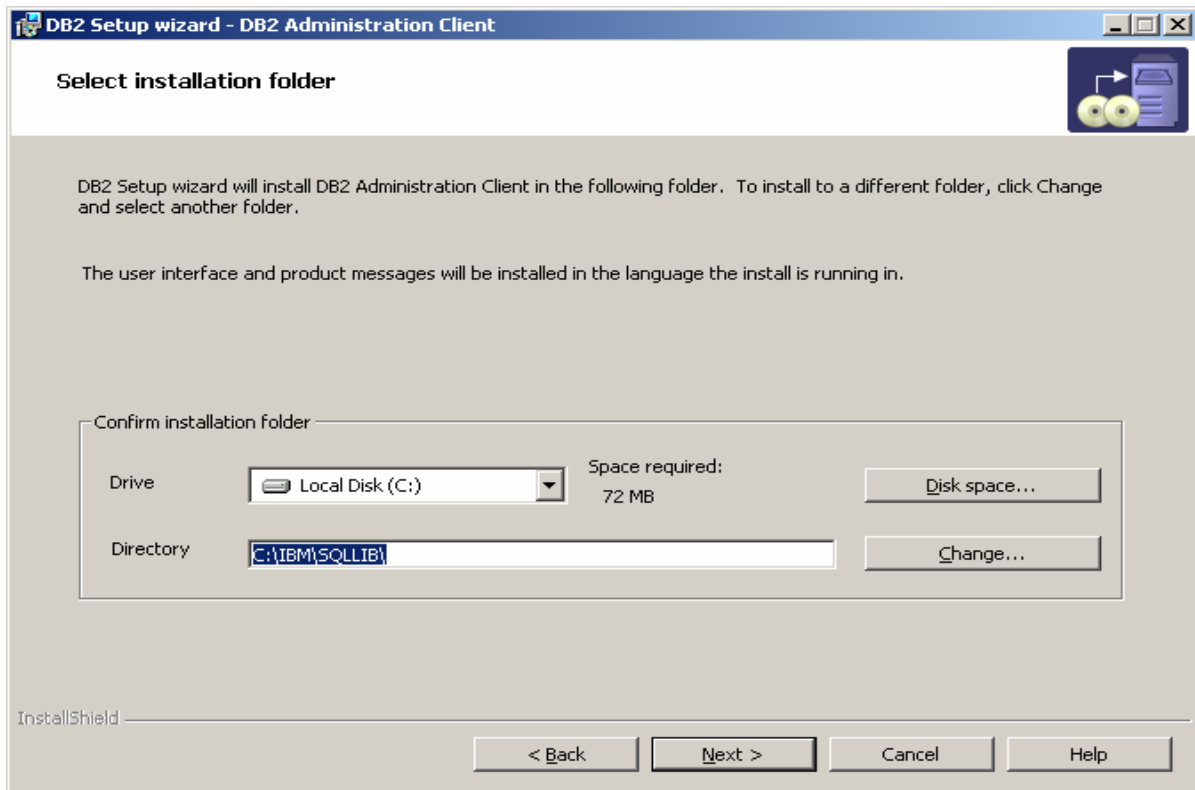


- Select Next on the Welcome screen
- Accept the licence agreement, Next

Select Installation Type: Compact (this Installs only the base code and command line utilities),
Next



- Select the Installation folder, Next



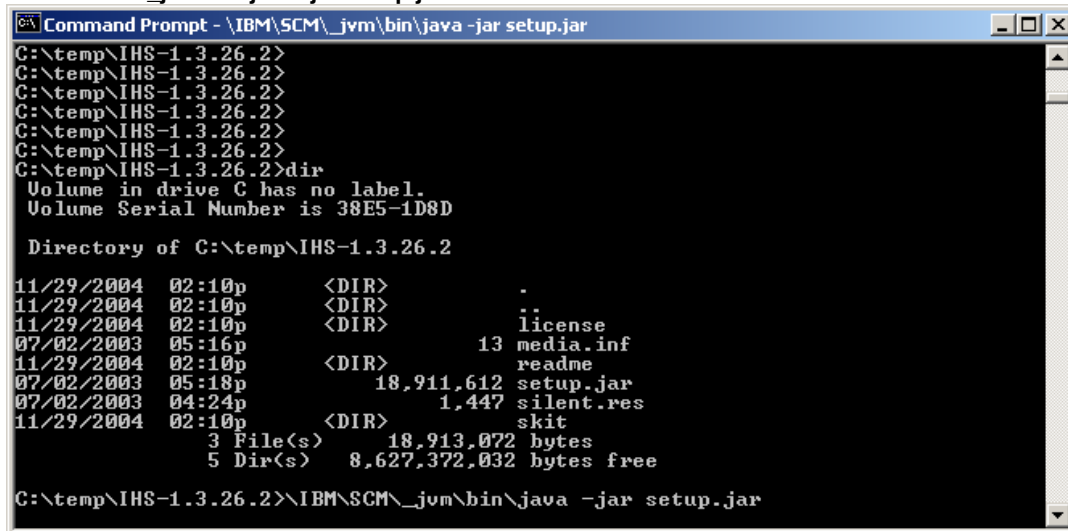
- don't select NetBIOS on the next screen
- Confirm the Installation parameters, Next
 - Product to install: DB2 Administration Client
 - Installation type: Compact
 - Selected features:
 - APPC
 - NetBIOS
 - Named Pipes
 - TCP/IP
 - System Bind Files
 - MDAC 2.7
 - ODBC Support
 - Target directory: C:\IBM\SQLLIB
 - Space required: 72 MB
 - New instances:
 - Instance name: DB2

12.2 W2K: Installation of IBM HTTP server 1.3.26.2

I used the HTTP Server code from the WAS 5.0 distribution for Windows. Because there is no setup.exe, I started the installation using the already installed java 1.3.1 JRE:

Alternatively the IBM HTTP server is available free of charge from WWW.IBM.COM with a full set of instructions.

C:\IBM\SCM\jvm\bin\java -jar setup.jar



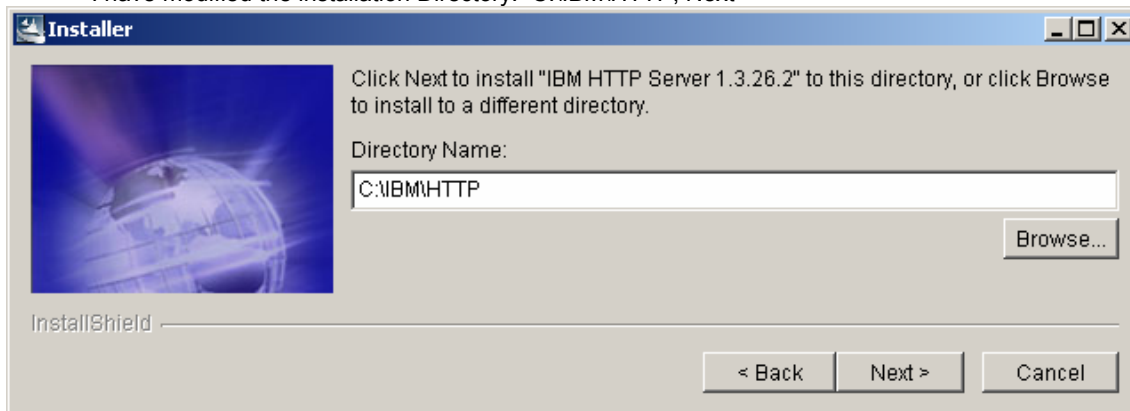
```
Command Prompt - \IBM\SCM\jvm\bin\java -jar setup.jar
C:\temp\IHS-1.3.26.2>
C:\temp\IHS-1.3.26.2>
C:\temp\IHS-1.3.26.2>
C:\temp\IHS-1.3.26.2>
C:\temp\IHS-1.3.26.2>
C:\temp\IHS-1.3.26.2>
C:\temp\IHS-1.3.26.2>
C:\temp\IHS-1.3.26.2>dir
Volume in drive C has no label.
Volume Serial Number is 38E5-1D8D

Directory of C:\temp\IHS-1.3.26.2

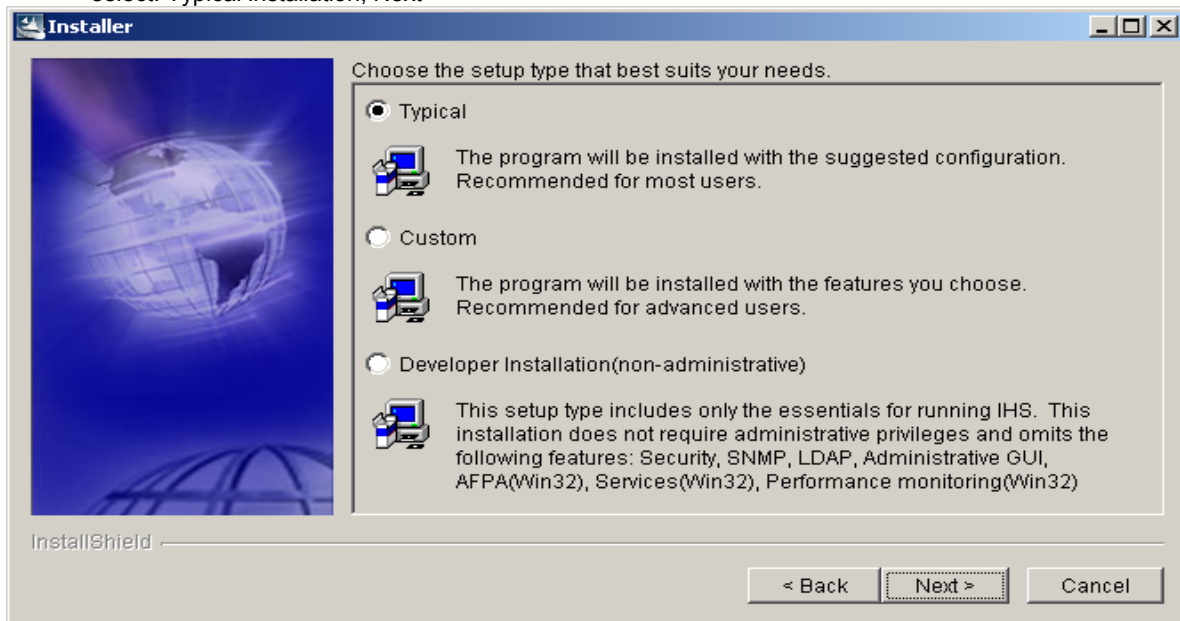
11/29/2004  02:10p      <DIR>          .
11/29/2004  02:10p      <DIR>          ..
11/29/2004  02:10p      <DIR>          license
07/02/2003  05:16p             13 media.inf
11/29/2004  02:10p      <DIR>          readme
07/02/2003  05:18p      18,911,612 setup.jar
07/02/2003  04:24p           1,447 silent.res
11/29/2004  02:10p      <DIR>          skit
               3 File(s)      18,913,072 bytes
               5 Dir(s)      8,627,372,032 bytes free

C:\temp\IHS-1.3.26.2>\IBM\SCM\jvm\bin\java -jar setup.jar
```

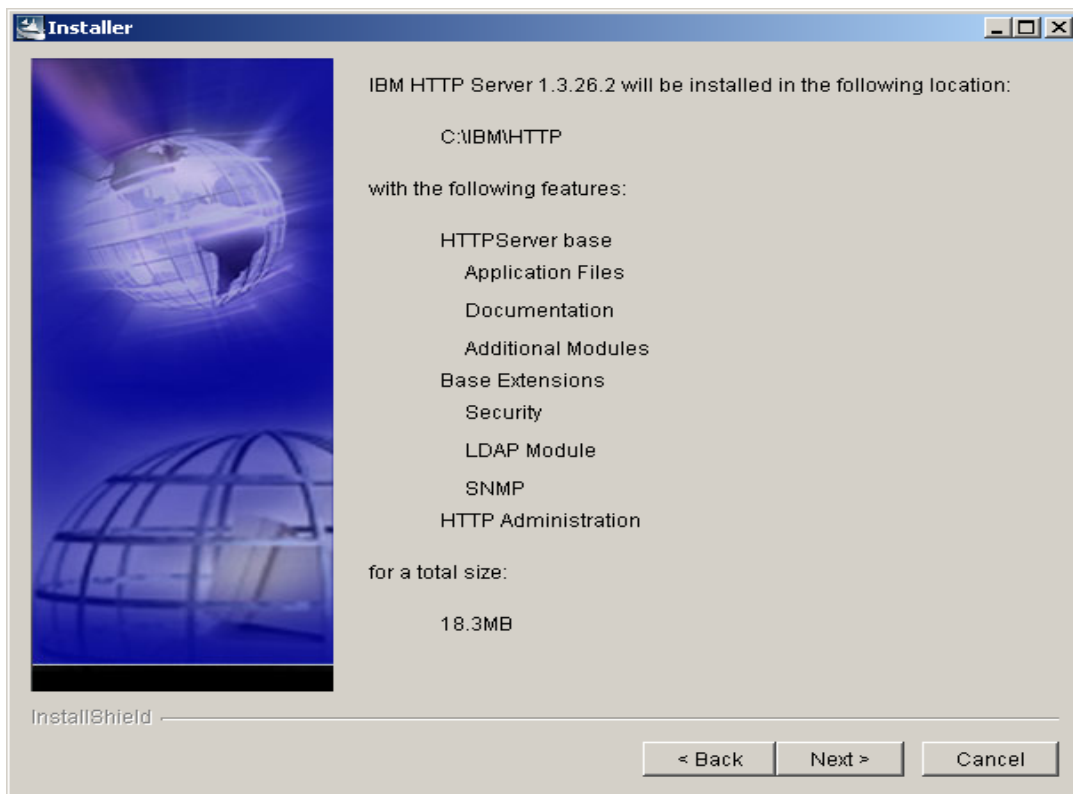
- Select the language used for this wizard : English
- Click Next on the Welcome screen, Next
- Accept the licence agreement, Next
- I have modified the installation Directory: C:\IBM\HTTP, Next



- select: Typical installation, Next



- Specify user and password: Administrator / PASSWORD, Next
- Confirm the Installation parameters, Next, Finished!



12.3 W2K: Install Crystal 9 Enterprise

For a complete Installation description see:
Crystal Enterprise™ 9 Installation Guide, “Full stand-alone installation” on page 11

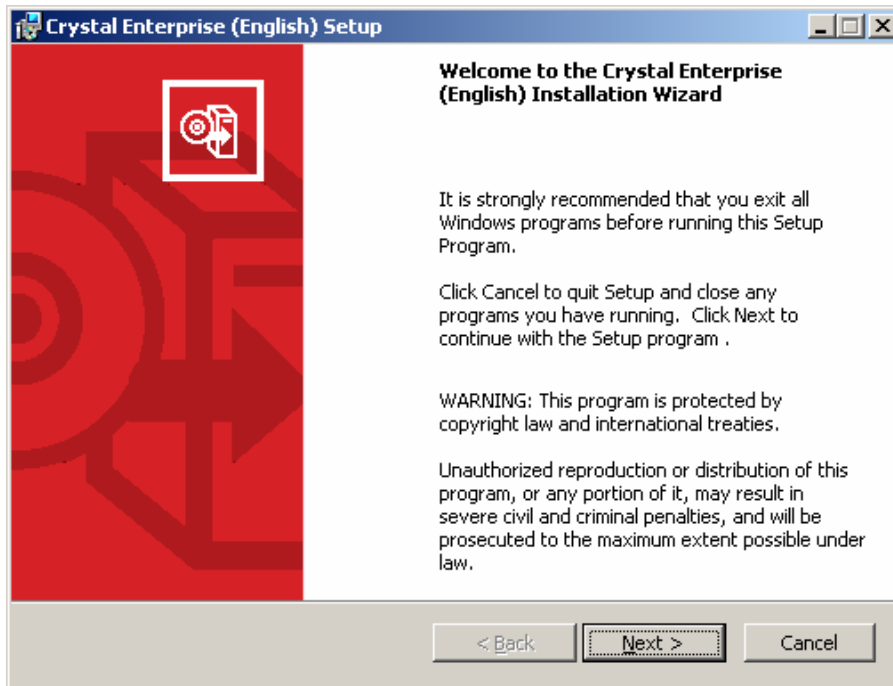
In this scenario, I installed Crystal Enterprise on a single machine that is already running as web server. This provides the quickest way to install Crystal Enterprise.

12.3.1 Create Windows account for MSDE:

User: as
Password: PASSWORD
Groups: administrators

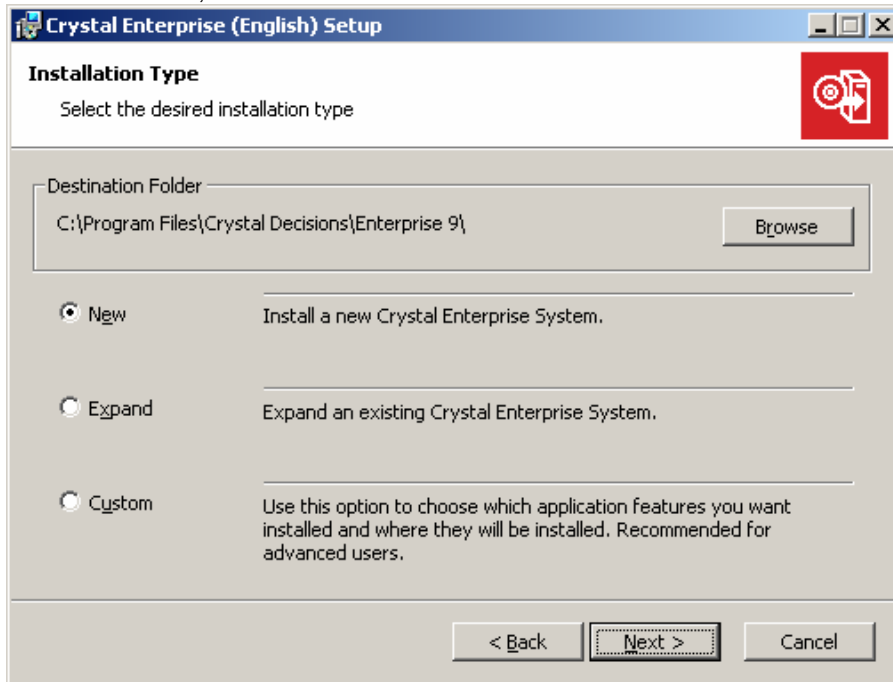
12.3.2 Install the Server

Run **setup.exe** from the win32 directory of your product distribution. Proceed through the Setup program's dialog boxes and follow the instructions displayed on your screen until you reach the Installation Type dialog box:

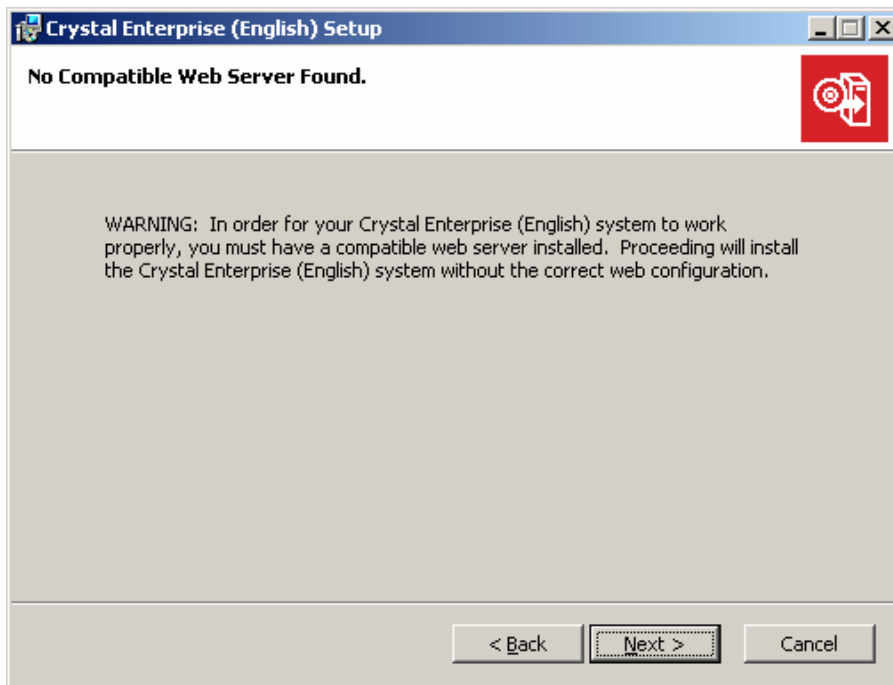


- Accept the licence agreement

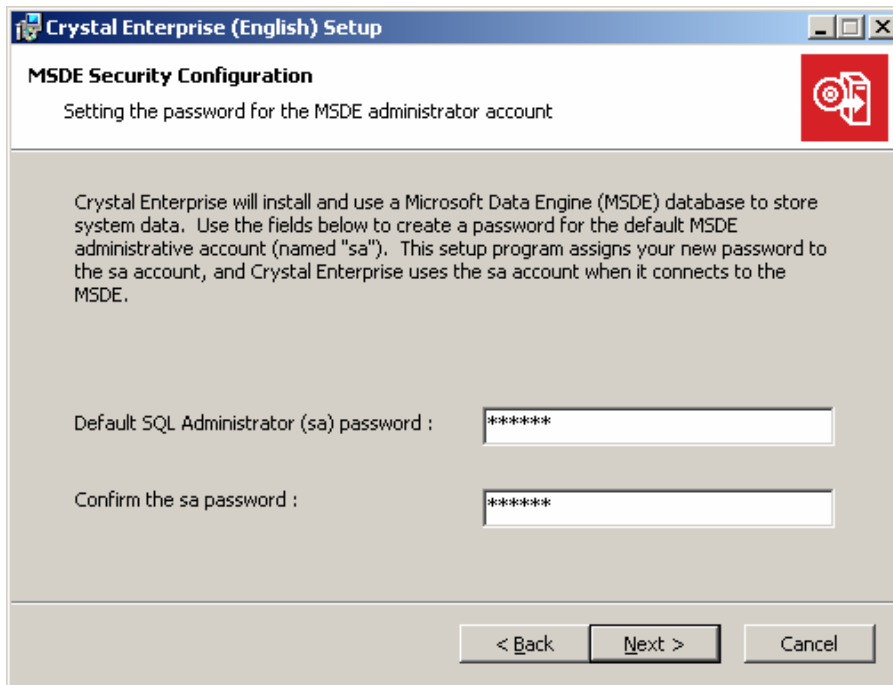
- Click **New**; then click **Next**.



The setup program checks to see whether or not the Microsoft Data Engine (MSDE) or Microsoft SQL Server is already installed on the local machine.



If the setup program does not detect an existing database, use the “MSDE Security Configuration” dialog box to create a password for the default SQL administrator account that will be installed along with the MSDE.



Crystal Enterprise (English) Setup

MSDE Security Configuration

Setting the password for the MSDE administrator account

Crystal Enterprise will install and use a Microsoft Data Engine (MSDE) database to store system data. Use the fields below to create a password for the default MSDE administrative account (named "sa"). This setup program assigns your new password to the sa account, and Crystal Enterprise uses the sa account when it connects to the MSDE.

Default SQL Administrator (sa) password : *****

Confirm the sa password : *****

< Back Next > Cancel

When you reach the Start Installation dialog box, click Next.

The installation of files begins immediately. During the installation process, you may be prompted to restart the local machine. When the installation program has finished copying files, you are given the opportunity to register your product.

12.4 Installation and Configuration of ITSCM Operational Reports

For details see:

Tivoli® Security Compliance Manager Release Notes Version 5.1 : Chapter 6. Operational reports

http://publib.boulder.ibm.com/tividd/td/ITSCM/GI11-4695-00/en_US/PDF/scm51_relnotes.pdf

12.4.1 Obtain and prepare the Operational Report Files

To install the operational reports:

1. Obtain the scm_op_report.zip file from the Tivoli Security Compliance Manager Web site:
<http://www.ibm.com/software/tivoli/products/security-compliance-mgr/>
2. Copy the ZIP file to the Microsoft® Windows 2000 system where you installed the Crystal Enterprise 9 server.
3. Unpack the ZIP file into a temporary directory.
4. If you plan to use the **Collector Run Information operational report**:
 - Locate the SQL archive (SAR) file in the temporary directory for the Collector Run Information report that corresponds to the version of DB2 being used and the operating system of the DB2 system. sar/db2_8.1/sles/scm_col_run.sar DB2 8.1 on SUSE LINUX systems
 - Copy the appropriate file to a temporary directory on the system running the DB2 database server.
 - Connect to the database using a user with administrator permissions.
 - Verify that the user has the appropriate DBADM privileges by entering the following command at a DB2 command prompt:
 - o get authorizations
 - o If DBADM authorizations have not been granted, run the following command at a DB2 command prompt:
 - o grant DBADM on database to USER db2admin where db2admin is the DB2 user ID.
 - Import the SQL archive file to the DB2 database server by running the following command at a DB2 command prompt:
 - o put routine from temp_directory_on_DB2_server/scm_col_run.sar
 - To verify that the stored procedure is returning data, enter the following command at a DB2 command prompt: CALL JAC_SYS.COL_REPORT()

db2 => get authorizations

```
Administrative Authorizations for Current User
.....
Direct SYSADM authority           = NO
Direct DBADM authority           = YES
Direct CREATETAB authority       = YES
.....
db2 =>
```

db2 => put routine from /home/db2inst1/scm_col_run.sar

```
SQL0443N  Routine "**OUTLINE_SAR" (specific name "") has returned an error
SQLSTATE with diagnostic text "-970,55009,
```

```
/home/db2inst1/sqllib/function/routine/sqlproc".  SQLSTATE=38000
```

```
db2 => CALL JAC_SYS.COL_REPORT()
```

```
SQL0440N  No authorized routine named "JAC_SYS.COL_REPORT" of type "PROCEDURE"  
having compatible arguments was found.  SQLSTATE=42884
```

Note:

The last two db2 commands create error messages. Further investigations are needed.

12.4.2 Configure the CE 9 CGI Web Connector for IBM HTTP Server

For details see the document entitled

How to configure the CGI Web Connector with IBM HTTP Server on the Business Objects Web site.

This document might be available at:

http://support.businessobjects.com/communityCS/TechnicalPapers/ce9_ihs_cgi_web_connector.pdf.asp

Copying the Web Connector file

Before you can configure the CGI Web Connector, copy the file Wcscgi.cgi, which is located in C:\Program Files\Crystal Decisions\Enterprise 9\win32_x86, to the cgi-bin directory of the IHS web server.

To ensure that you are using the correct cgi-bin directory, consult your IHS Administrator. The default cgi-bin directory is: C:\Program Files\IBM HTTP Server\cgi-bin.:

12.4.3 Create IBM HTTP Administrator account

```
C:\IBM\HTTP>htpasswd -cm confladmin.passwd admin
```

```
New password: ***** # PASSWORD
```

```
Re-type new password: ***** # PASSWORD
```

```
Adding password for user admin
```

Ensure that you have enabled an Administration account for the IBM HTTP Server.

Connect to the IBM Administration Server

To connect to the IBM Administration Server:

Type the following URL in the address bar of new browser window:

<http://localhost:8008>

Confirm the server name

Confirm that the server name is correct in the IHS configuration

expand **Basic Settings** and then expand **Core Settings**. (In our example, the host is crystal)

crystal

12.4.4 Create directory aliases

Next, add three directory aliases by completing the following steps:

1. On the IBM Administration Server web page, expand the Mappings folder, and then expand the Aliases folder.

Add

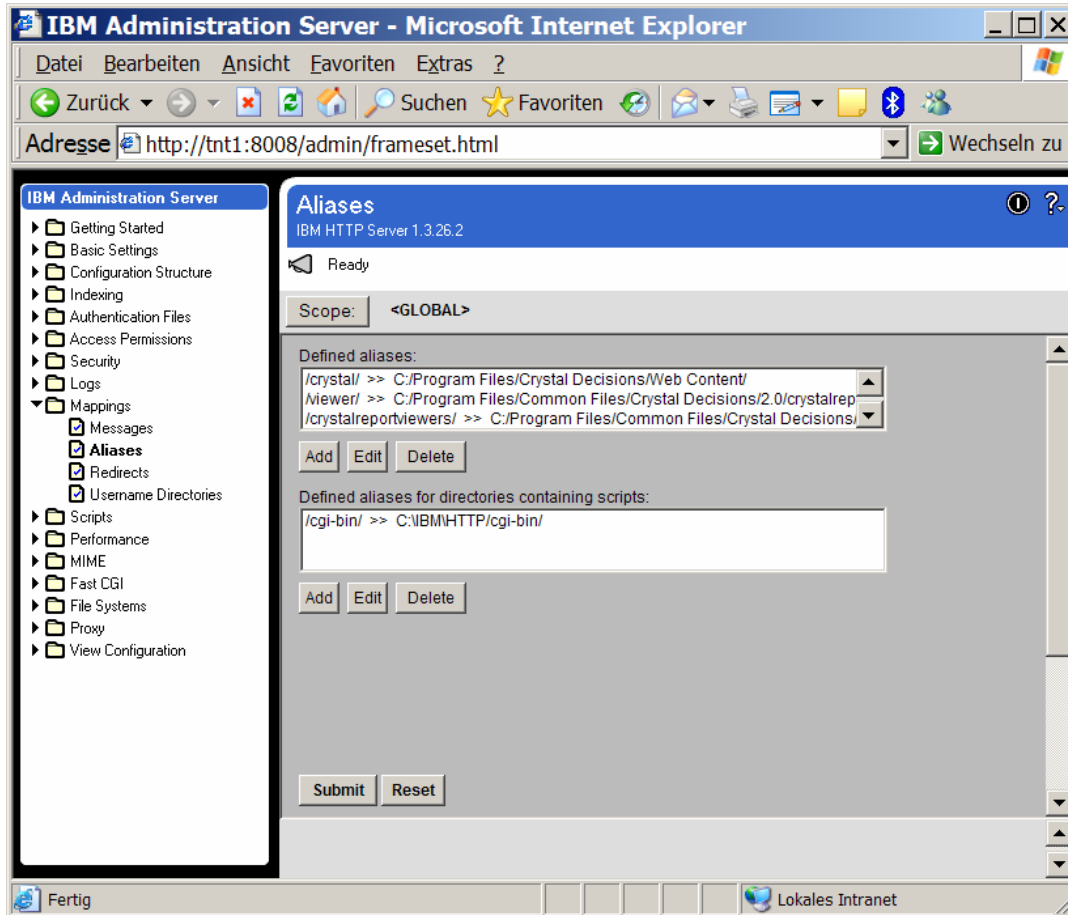
/crystal/ C:/Program Files/Crystal Decisions/Web Content/

/viewer/ C:/Program Files/Common Files/Crystal

Decisions/2.0/crystalreportviewers/

/crystalreportviewers/ C:/Program Files/Common Files/Crystal

Decisions/2.0/crystalreportviewers/

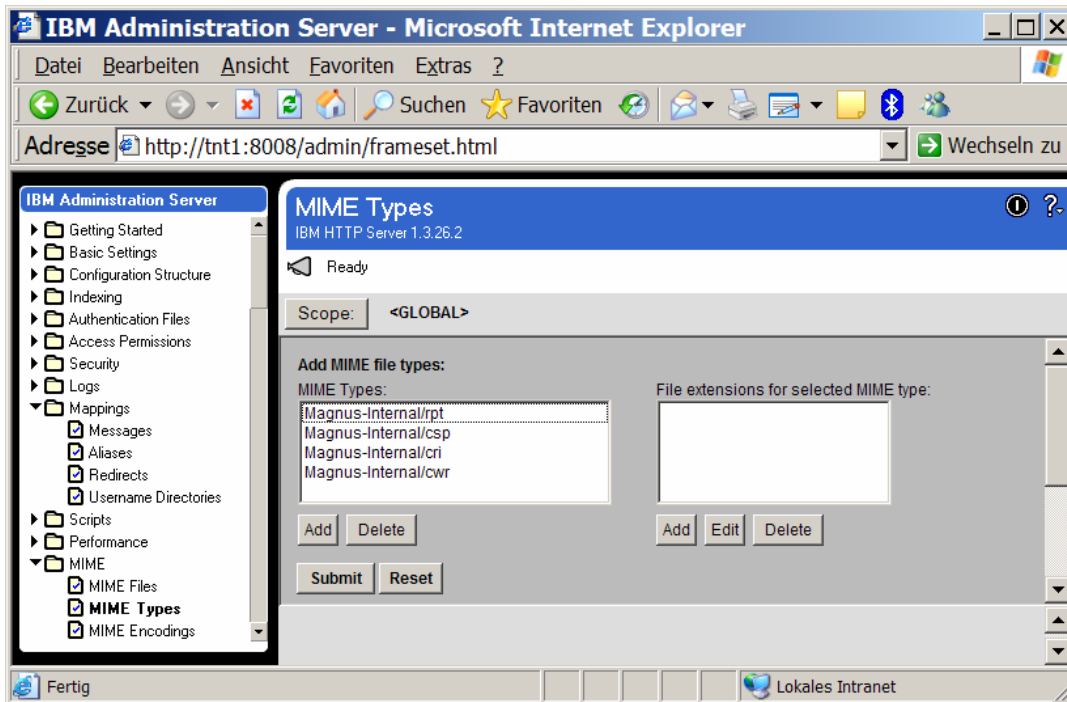


Click Submit

12.4.5 Add MIME types

Add four Multi-Purpose Internet Mail Extensions (MIME) by completing the following steps:
Expand the MIME folder, and then expand the MIME Types folder.

MIME types and extensions:	MIME Type
Magnus-Internal/rpt"	.rpt
File Extension Magnus-Internal/csp	.csp
Magnus-Internal/cri	.cri
Magnus-Internal/cwr	.cwr

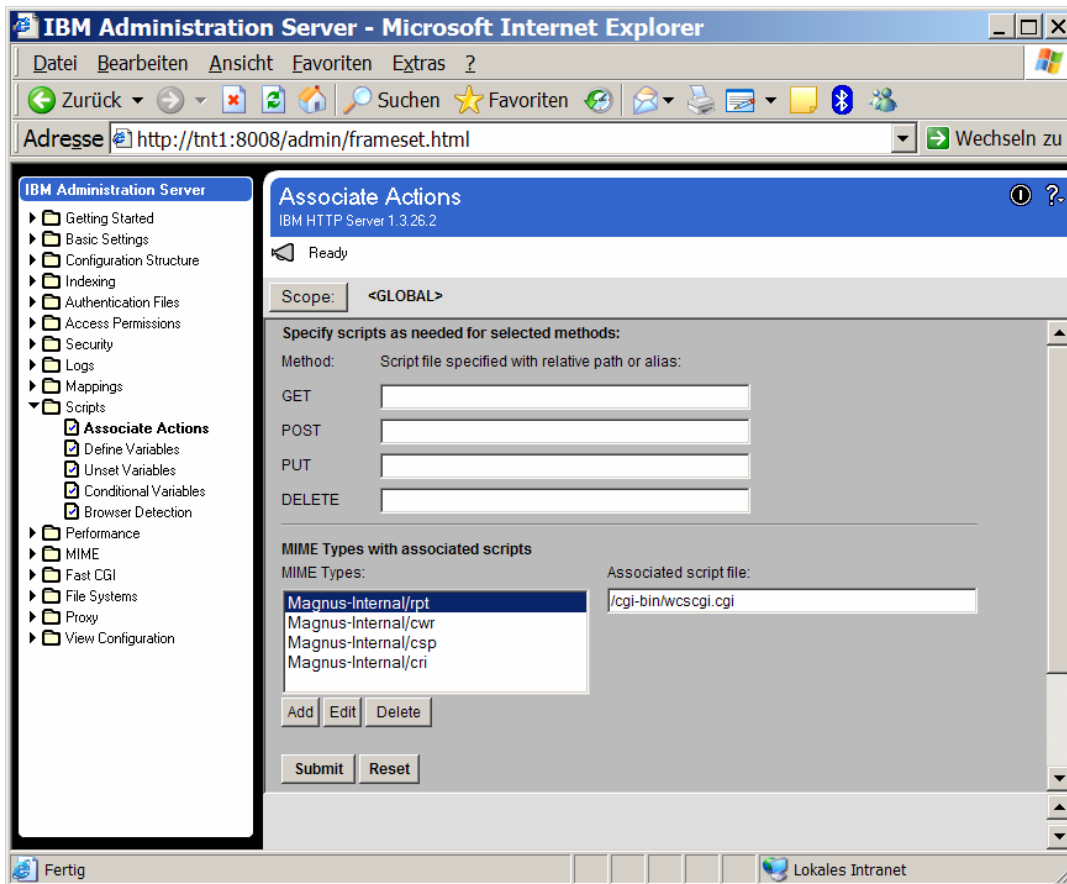


Click Submit

12.4.6 Associate MIME types with scripts

Set up the CGI Web Connector to handle requests for resources of the previous MIME types.

1. On the IBM Administration Server web page, expand the Scripts folder, and then expand the Associate Actions folder.
2. Click the Add button below the Mime Types box.
3. Click Magnus-Internal/rpt in the Select from the following MIME types known to the server list.
4. In the Enter or edit script file specified with relative path or alias: box, type `"/cgi-bin/wscsgi.cgi"` (no quotes).
5. Click Apply.
6. Repeat steps 1 to 4 for each of the MIME types added in the previous section.



7. Click Submit.

12.4.7 Edit the Crystal Enterprise HTML pages

Modify three Crystal Enterprise 9.0 HTML pages as follows:

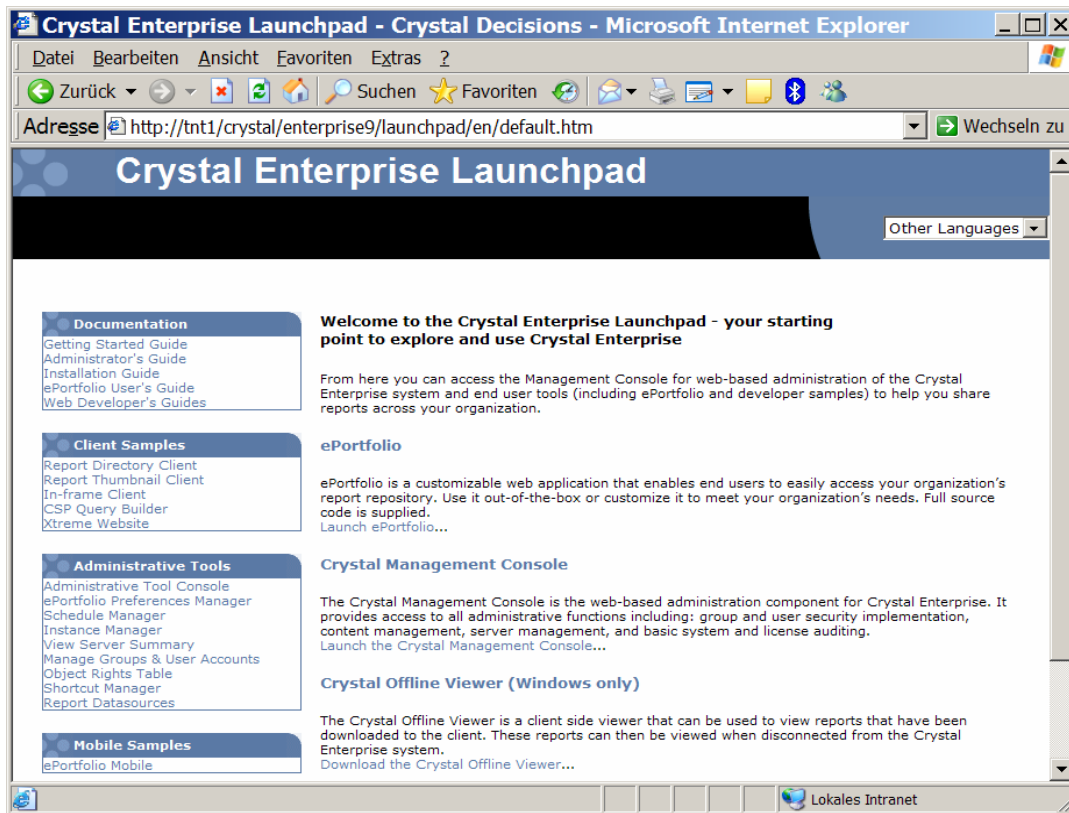
1. Go to C:\Program Files\Crystal Decisions\Web Content\Enterprise 9\ ePortfolio, and rename the file Default.htm to Default.txt.
2. Locate the following lines of code in the file Default.txt:

```
<HTML> <HEAD>  
<SCRIPT language="javascript"> location.replace ( "redirect.csp" ); </SCRIPT>  
</HEAD> </HTML>
```
3. Change "redirect.csp" to "en/default.htm".
4. Save the file.
CAUTION Before completing the next step, make backup copies of Default.htm in these directories:
C:\Program Files\Crystal Decisions\Web Content\Enterprise9\Websamples
C:\Program Files\ Crystal Decisions\Web Content\Enterprise9\Help
5. Rename Default.txt back to Default.htm and copy it to the following directories: C:\Program Files\Crystal Decisions\Web Content\Enterprise9\Websamples C:\Program Files\ Crystal Decisions\Web Content\Enterprise9\Help
6. If the CGI Web Connector is connecting to the Web Component Server (WCS) on a different server, proceed to the section Set the environment variables.
7. If the CGI Web Connector is connecting to the WCS on the same computer, proceed to the section Testing the Configuration.

12.4.8 Testing the Configuration

Finally test the configuration:

1. In a web browser, navigate to the following URL address (substituting the name of your server) to start the Crystal Launchpad:
<http://<YourServerName>/crystal/enterprise9>



2. Click each link on the Crystal Launchpad to ensure that it works as expected.

e-Portfolio:

<http://suse8linux1/cgi-bin/wcscgi.cgi/crystal/enterprise9/ePortfolio/de/default.htm>

Note:

If the **ePortfolio** link is not available, first check the configuration of the http server.
Verify the last lines in **httpd.conf**

```
.....  
AddType Magnus-Internal/rpt .rpt  
AddType Magnus-Internal/csp .csp  
AddType Magnus-Internal/cri .cri  
AddType Magnus-Internal/cwr .cwr  
Action Magnus-Internal/rpt /cgi-bin/wcscgi.cgi  
Action Magnus-Internal/cwr /cgi-bin/wcscgi.cgi  
Action Magnus-Internal/csp /cgi-bin/wcscgi.cgi  
Action Magnus-Internal/cri /cgi-bin/wcscgi.cgi
```

12.4.9 Create an Open Database Connectivity (ODBC) data source

Create an Open Database Connectivity (ODBC) data source on the Crystal Enterprise 9 server system called SCM_DB to the Tivoli Security Compliance Manager database.

a. From the Windows desktop, click

Start → Settings → Control Panel → Administrative Tools → Data Sources (ODBC).

b. Click the **System DSN** tab.

c. Click **Add** and create a DB2 data source with a name of SCM_DB.

CLI/ODBC Settings - SCM_DB

Data Source | Advanced Settings

Data source name: SCM_DB

Description: TSCM Database

Connect to data source to retrieve configuration information

User ID: db2inst1

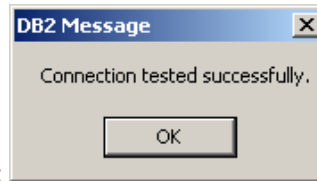
Password: xxxxxx

☒ Save password

Connect

Bind CLI/ODBC support utilities

OK Cancel Apply Help



The Connection Test should be successfully:

12.5 Make the Tivoli Security Compliance Manager operational reports available

Make the Tivoli Security Compliance Manager operational reports available on the Crystal Enterprise 9 server using the publish.bat file that is provided in the ZIP file.

The batch file syntax is:

**publish.bat *rpt_directory* *host_name* *aps_user_name* *aps_password*
db2_user_id *db2_password* *log_file_path***

where: *rpt_directory* Directory from the unpacked ZIP file that contains the reports (.rpt and .xml files)

host_name Name of the Crystal Enterprise 9 server system.

aps_user_name User name for the Crystal Automated Process Scheduler database.

aps_password Password associated with the *aps_user_name* specified.

db2_user_id User ID for accessing the DB2 database server.

db2_password Password associated with the *db2_user_id* specified.

log_file_path Directory to contain messages produced by the publish.bat file

For example:

**publish.bat c:\temp\reports myserver.mycompany.com Administrator my8pw db2admin
myDB2pw c:\logs**

Verify that no errors were logged in the *log_file_path* directory.

I used the command:

**publish C:\temp\scm_op_report\reports suse8linux1 Administrator "" db2inst1
PASSWORD C:\temp\logs**

Note:

CE9 has the following default Security Authentication settings:

Default Authentication: Enterprise

Password: none

Other Authentication: Windows NT

Password: WINDOWS-Password

Because the CE9 APS is using the authentication method Enterprise, the password in the example above is blank (""). For problem determination use the logfile mentioned above,

13 Verify the Operational Reports

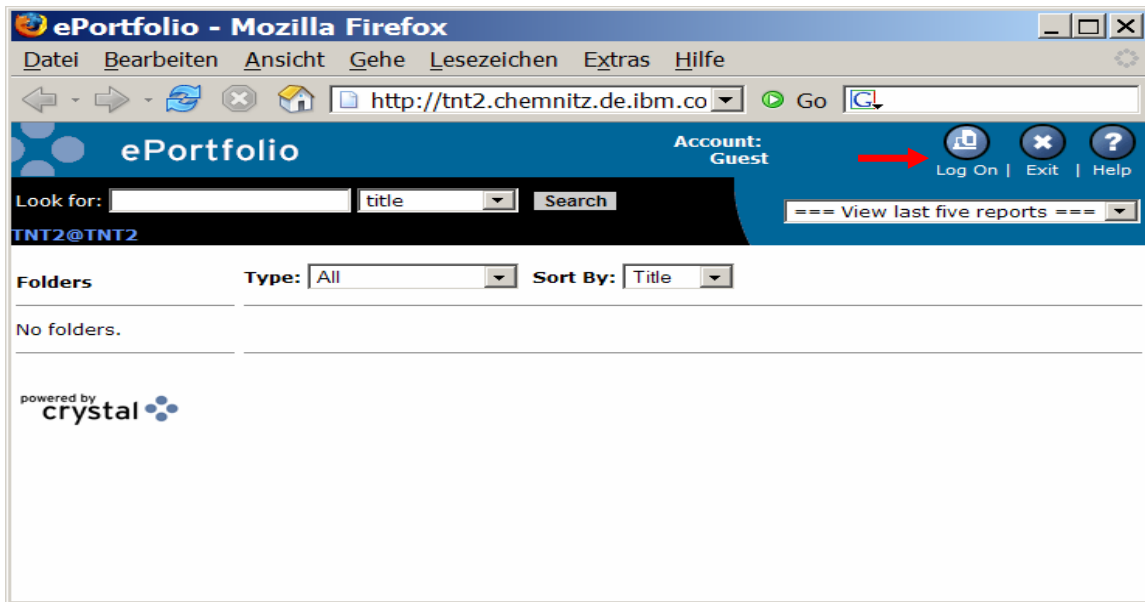
13.1 Reporting Interface

The operational reports are available via Web-browser: Call the following URL:

http://YOUR_HOST/crystal/enterprise9/launchpad/en/default.htm



On the next page: Select **ePortfolio**:



On the next page: Select **Log On**

On the next page: Login with:
Authentication: Windows NT
User: Administrator / PASSWORD

ePortfolio - Logon - Mozilla Firefox

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

Go

ePortfolio

Cancel | Help

Log On

Existing User

APS Name: TNT1

User Name:

Password:

Authentication: Enterprise

Enterprise

LDAP

Windows NT

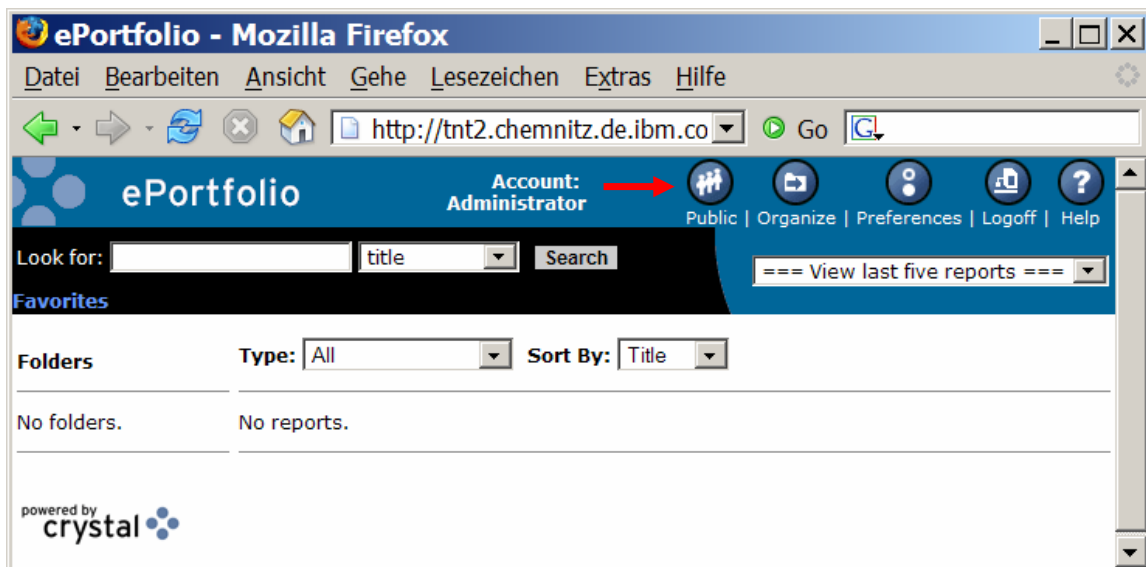
powered by crystal

Note:

CE9 has the following security authentication options

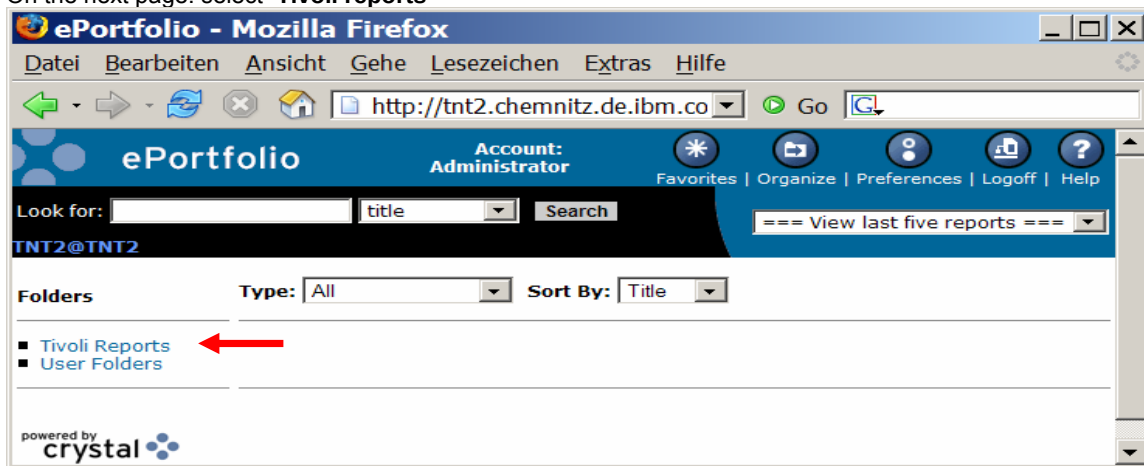
- Enterprise: User Administrator, no password (default)
- LDAP
- Windows NT: User Administrator, Windows password

On the next page: Select **Public**

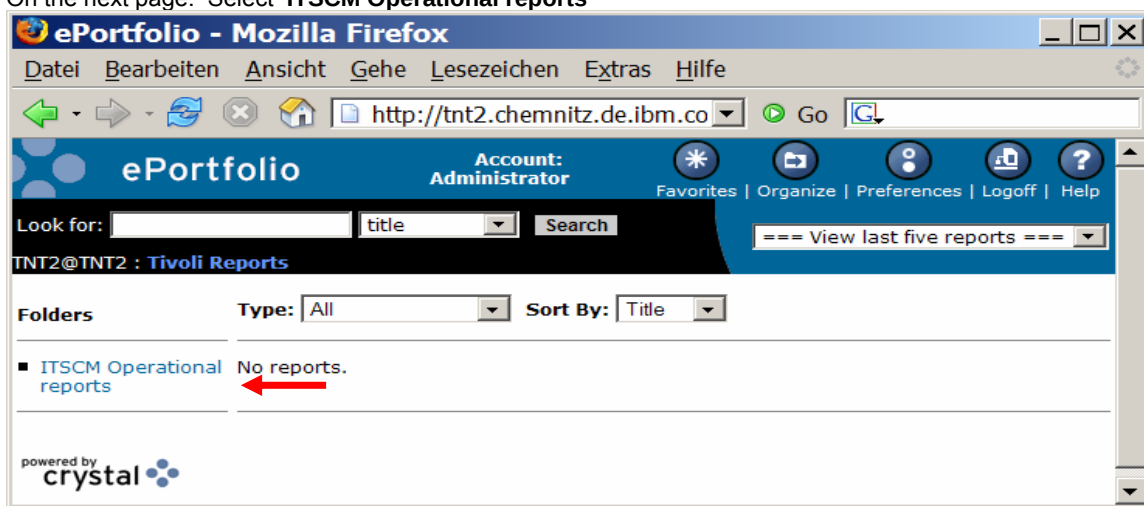


the next page: Select **Public**

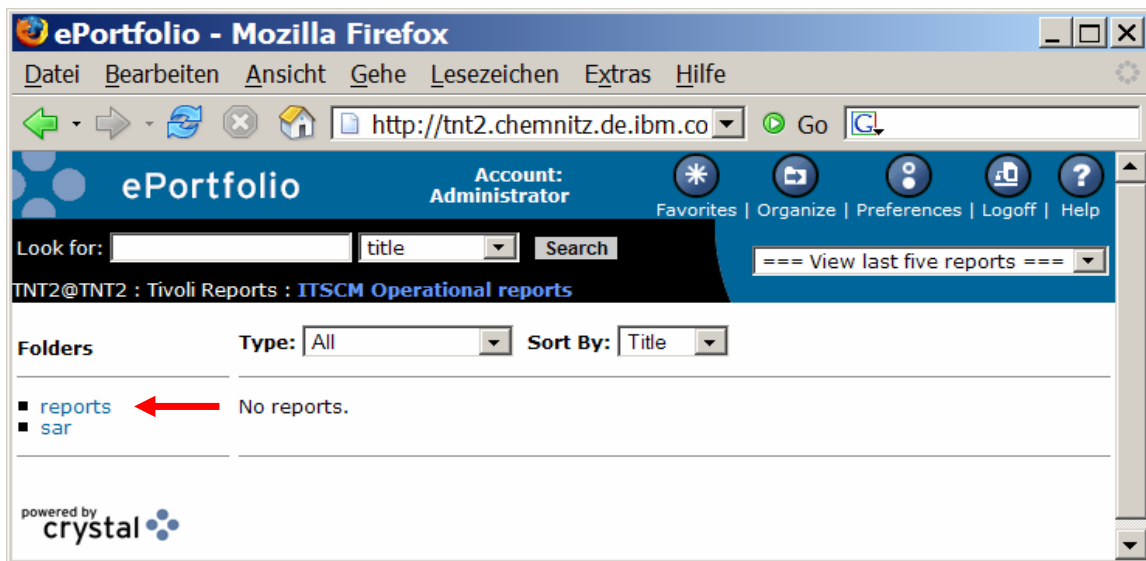
On the next page: select **Tivoli reports**



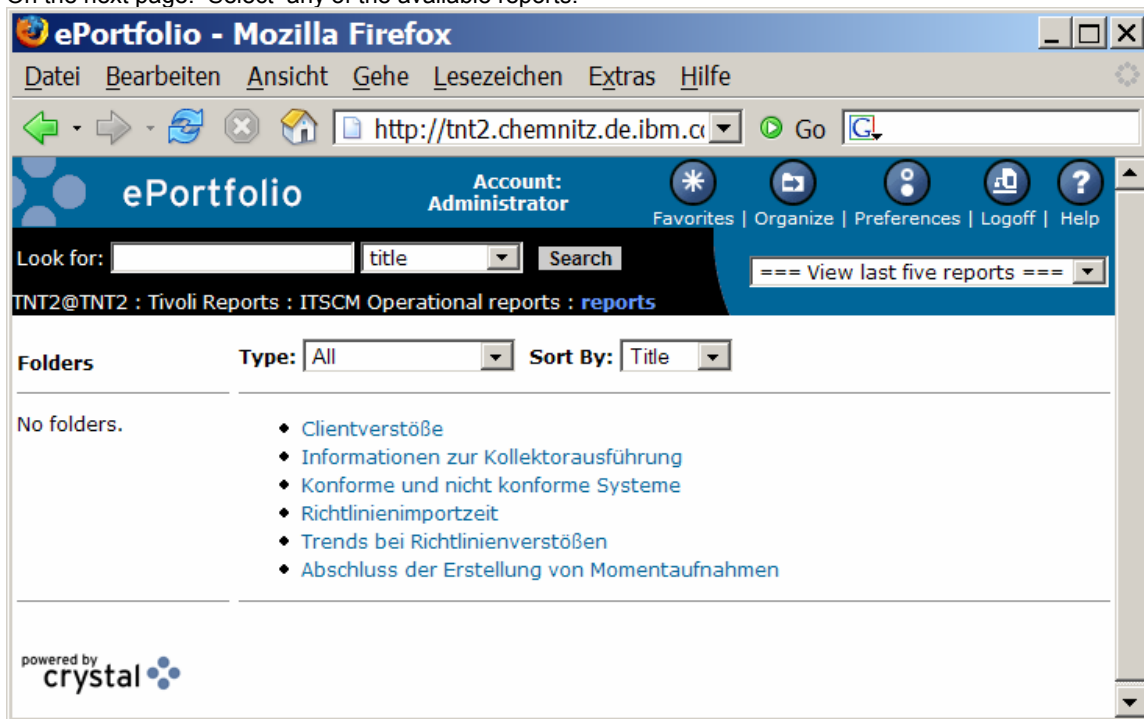
On the next page: Select **ITSCM Operational reports**



On the next page: Select **reports**



On the next page: Select any of the available reports:



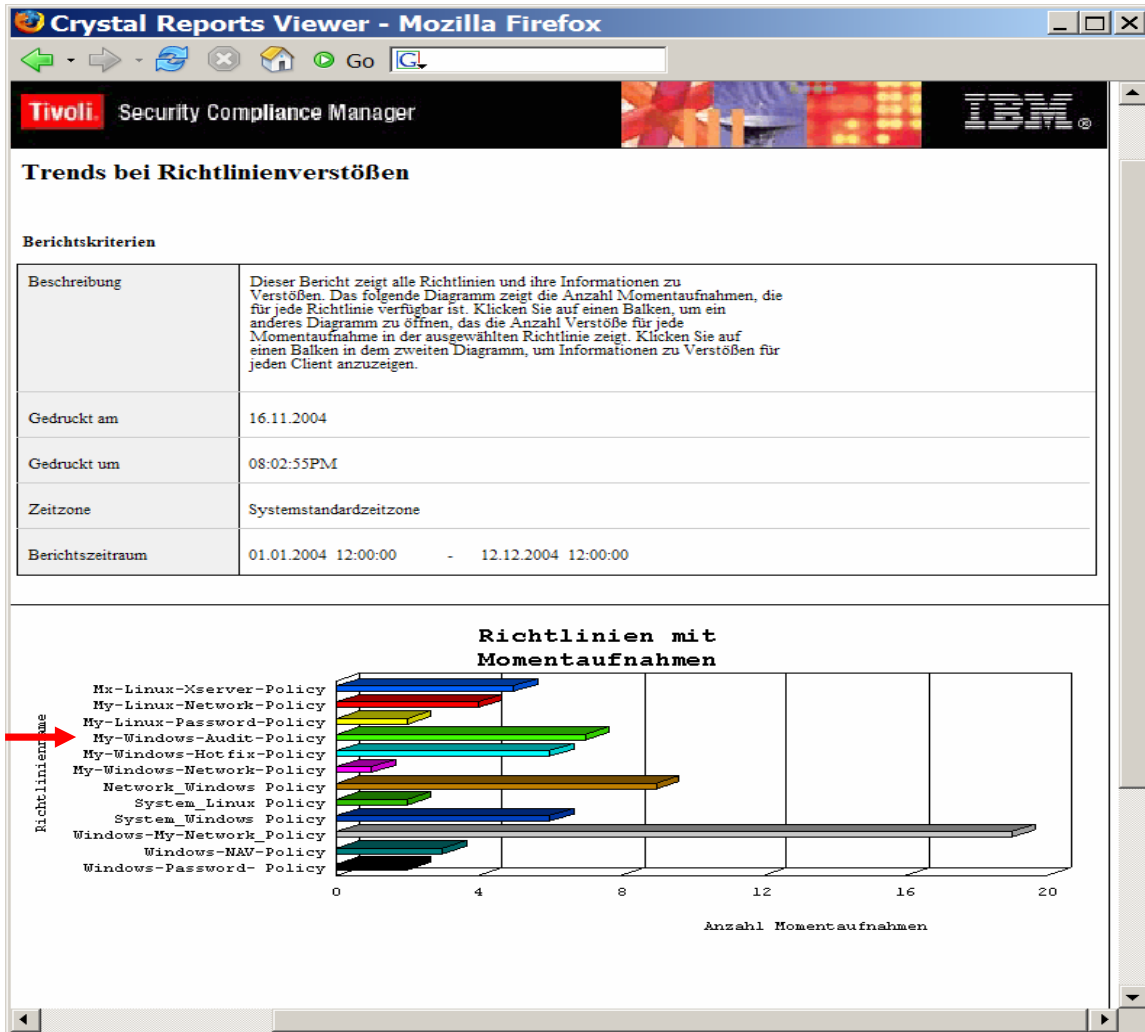
13.2 Sample Operational Reports

The following pages show two examples for **ITSCM Operational reports**:

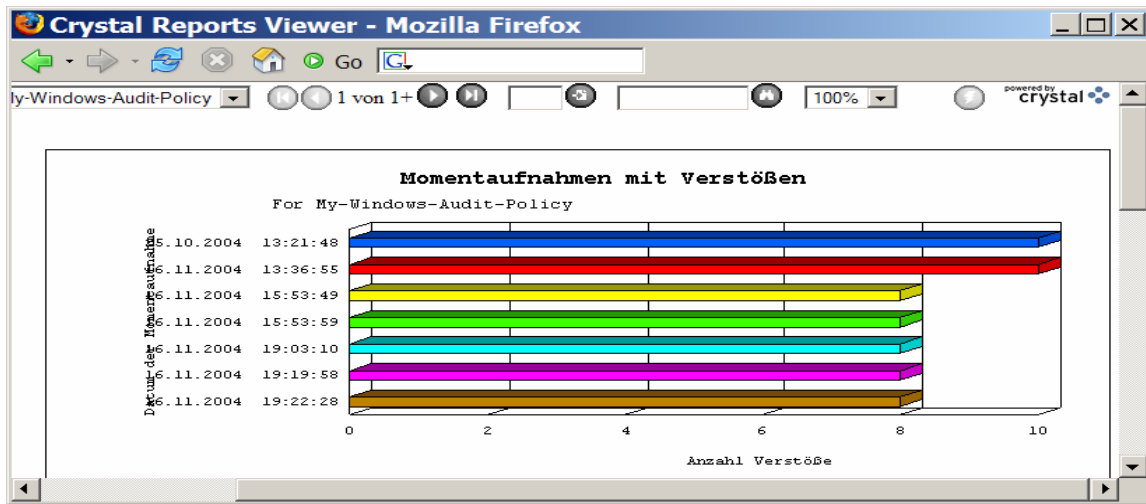
- Policy Violations Trends (Trends bei Richtlinienverstößen)
- Client Violations (Clientverstöße)

Note:

The Browser Mozilla 1.7.2 and Firefox 1.0 cannot handle a selection box to specify the date range of the report.
Use Internet Explorer or edit the date line.



Drill Down to: My-Windows-Audit-Policy



13.2.2 Sample - Report: Client Violations

The screenshot shows a web browser window titled "Crystal Reports Viewer - Mozilla Firefox". The address bar is empty. The main content area displays a message in German: "Für den angeforderten Bericht sind weitere Informationen erforderlich." (For the requested report, further information is required). Below this, there is a section titled "Crystal-Parameterfeld(er)" (Crystal-Parameter field(s)). Under this section, there is a "Policy" header. The text below the header reads: "Geben Sie den Namen der Richtlinie ein, für die die letzte Momentaufnahme und Verstöße angezeigt werden sollen; andernfalls werden Informationen zu allen Richtlinien angezeigt." (Enter the name of the policy for which the last snapshot and violations should be displayed; otherwise, information for all policies will be displayed). There is a dropdown menu with "Alle Richtlinien" (All policies) selected, followed by an asterisk and a text input field. At the bottom right of the form, there is an "OK" button, which is highlighted by a red arrow.

Crystal Reports Viewer - Mozilla Firefox

Für den angeforderten Bericht sind weitere Informationen erforderlich.

Crystal-Parameterfeld(er)

Policy

Geben Sie den Namen der Richtlinie ein, für die die letzte Momentaufnahme und Verstöße angezeigt werden sollen; andernfalls werden Informationen zu allen Richtlinien angezeigt.

Alle Richtlinien *

OK

select: ok

Crystal Reports Viewer - Mozilla Firefox

ptbericht 1 von 2+ 100% powered by crystal

Tivoli Security Compliance Manager

Clientverstöße

Berichtskriterien

Beschreibung	Dieser Bericht zeigt die Richtlinien und ihre letzten Momentaufnahmen an, einschließlich der Details zu Verstößen für jeden Client.
Gedruckt am	16.11.2004
Gedruckt um	08:05:57PM
Zeitzone	Systemstandardzeitzone

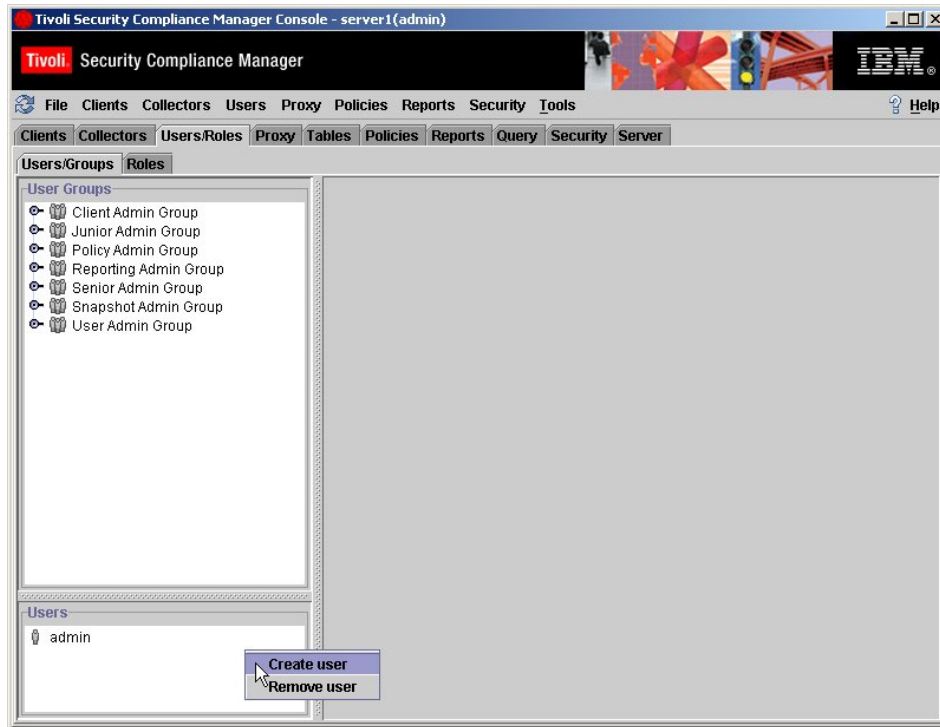
Richtlinienname	Name der Konformitätsabfrage	Nachricht für Verstoß	Erstellungszeit der Momentaufnahme
Client: lx2		DHCP:	
System_Linux Policy	Login Success or Failure for 'authpriv'	Incorrect syslog.conf setting authpriv- Priority: NULL, Action: NULL	16.11.2004 09:31:46
Mx-Linux-Xserver-Policy	forbidden-Xserver-running	X-Server is not allowed but running on 9.153.73.31	16.11.2004 19:00:02
My-Linux-Password-Policy	Minimum Password Length	Incorrect minimum password length: 5	16.11.2004 19:02:45
My-Linux-Network-Policy	Forbidden process finger	Process tcpd in.fingerd -w is not allowed but running on 9.153.73.31	16.11.2004 15:49:46
My-Linux-Network-Policy	Forbidden process rexec	Process tcpd in.rexecd is not allowed but running on 9.153.73.31	16.11.2004 15:49:46
My-Linux-Network-Policy	Forbidden process talk	Process tcpd in.talkd is not allowed but running on 9.153.73.31	16.11.2004 15:49:46
My-Linux-Network-Policy	Forbidden process rlogin	Process tcpd in.rlogind is not allowed but running on 9.153.73.31	16.11.2004 15:49:46
Gesamtanzahl Verstöße			7

14 Configuration of Security Compliance Manager Users, Groups and Roles

This section will take you through the creation of users and creating roles and templates for roles of the user groups. This is a very flexible administrator user setup for rights and permissions globally or for a restricted set of group of resources.

14.1 Creating Users

To create Tivoli Security Compliance Manager users, navigate to the **Users/Roles** tab then to the **Users/Groups** tab. In the lower left window pane, right click in the Users area to create a new user.



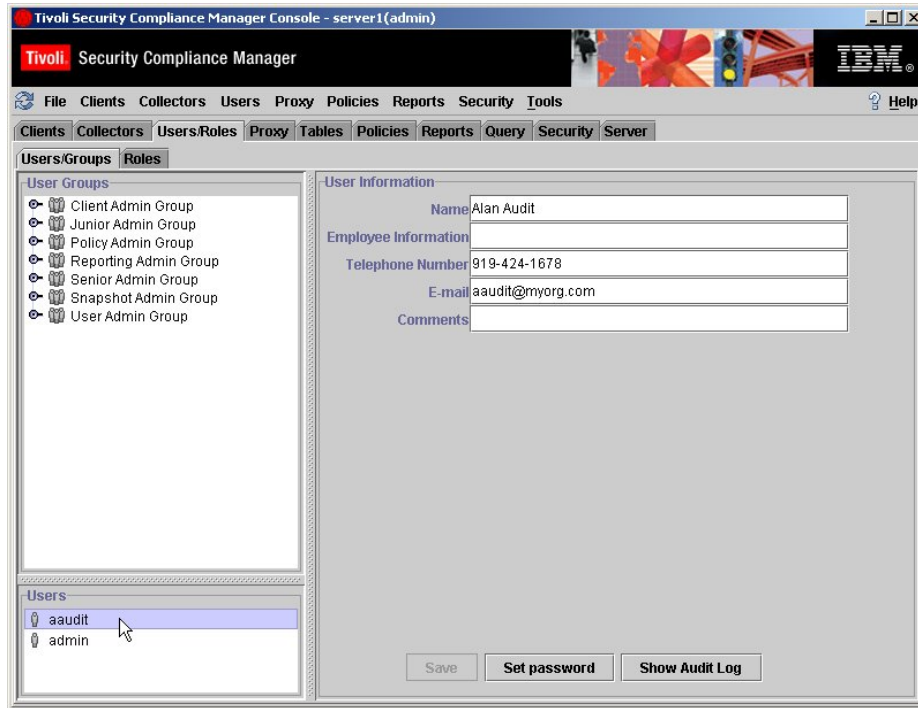
A popup will appear to enter the information about the user. Create a new user called **Alan Audit**.

The "Create User" dialog box is shown. It has a title bar "Create User" and a close button. On the left is a green question mark icon. The form contains the following fields:

- User ID: aaudit
- Full Name: Alan Audit
- Employee Information: (empty field)
- Telephone Number: 919-424-1678
- E-mail address: aaudit@myorg.com

At the bottom are "OK" and "Cancel" buttons.

After the user is created, you can then assign a password if you want them to logon to the Security Compliance Manager Administration Console.



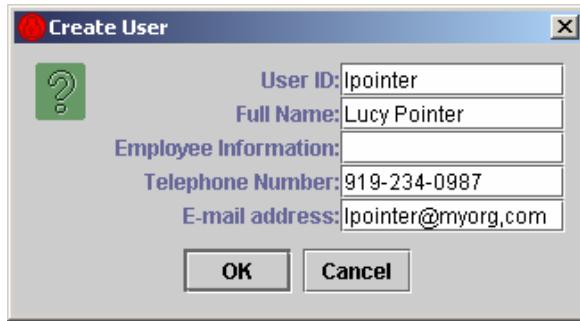
Click on the **Set Password** button. A popup window is presented to enter the new password.



Use the password, **passw0rd** or one of choice (keeping track of it,) for your new user.

Until the new user has been given some authority, do not logon using the new user ID.

Create another user of your choice. You will use these users in the next sections.



Create User

User ID:

Full Name:

Employee Information:

Telephone Number:

E-mail address:

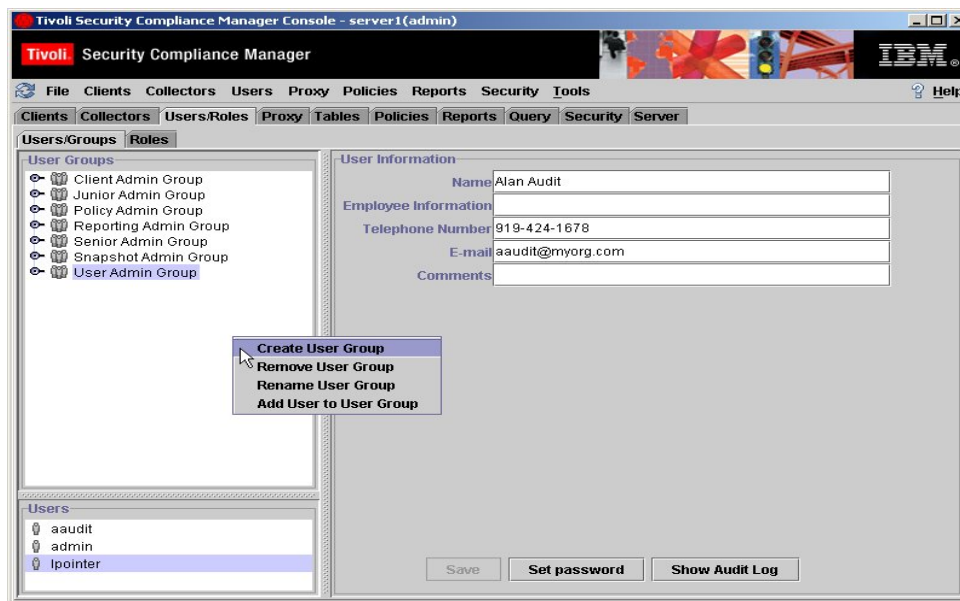
14.2 Creating Groups

Groups are logical containers of users. Security Compliance Manager provides some default user groups for different types of resource access.

In this lab you will create your own user groups. Users can be in more than one group but user Groups cannot be nested.

Roles, which you will create next after Groups, are assigned to groups to set the permissions that define the capabilities that members have when they logon to the Administration Console.

To create groups, navigate to the **Users/Roles** tab, then to the **Users/Groups** tab. In the upper left window, right click in the Groups area to create a new group.



Tivoli Security Compliance Manager Console - server1(admin)

Tivoli Security Compliance Manager

File Clients Collectors Users Proxy Policies Reports Security Tools

Clients Collectors Users/Roles Proxy Tables Policies Reports Query Security Server

Users/Groups Roles

User Groups

- Client Admin Group
- Junior Admin Group
- Policy Admin Group
- Reporting Admin Group
- Senior Admin Group
- Snapshot Admin Group
- User Admin Group

User Information

Name:

Employee Information:

Telephone Number:

E-mail:

Comments:

Users

- aaudit
- admin
- lpointer

Create User Group

- Remove User Group
- Rename User Group
- Add User to User Group

For example: Create the following groups:

lab-Auditors

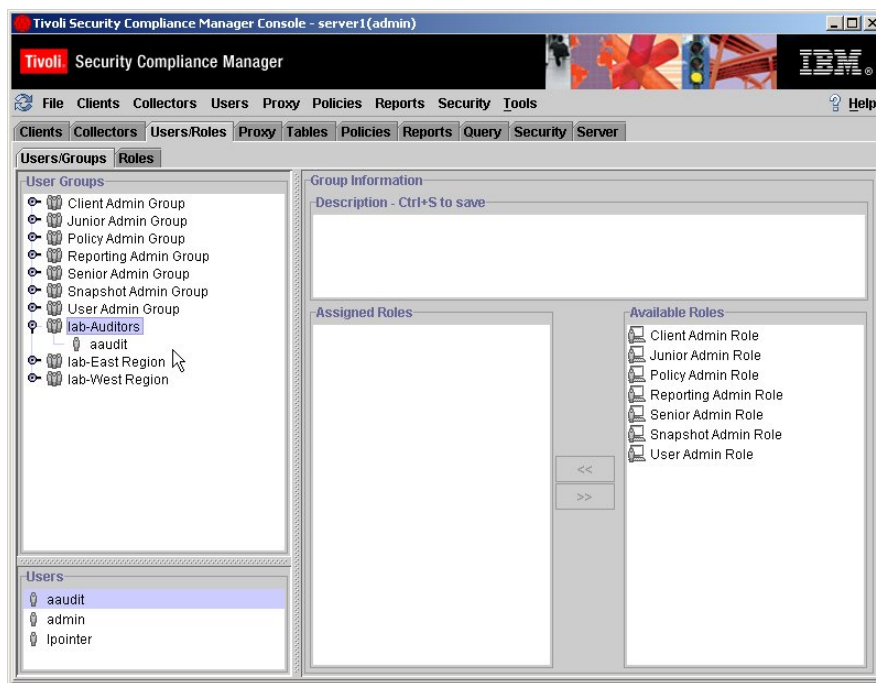
lab-East Region
lab-West Region



Next you will add your users to the new groups. To add a user to a group, first select the user name, and then select the group name. Then right click in the Groups window to get the **Add User to User Group** menu item.

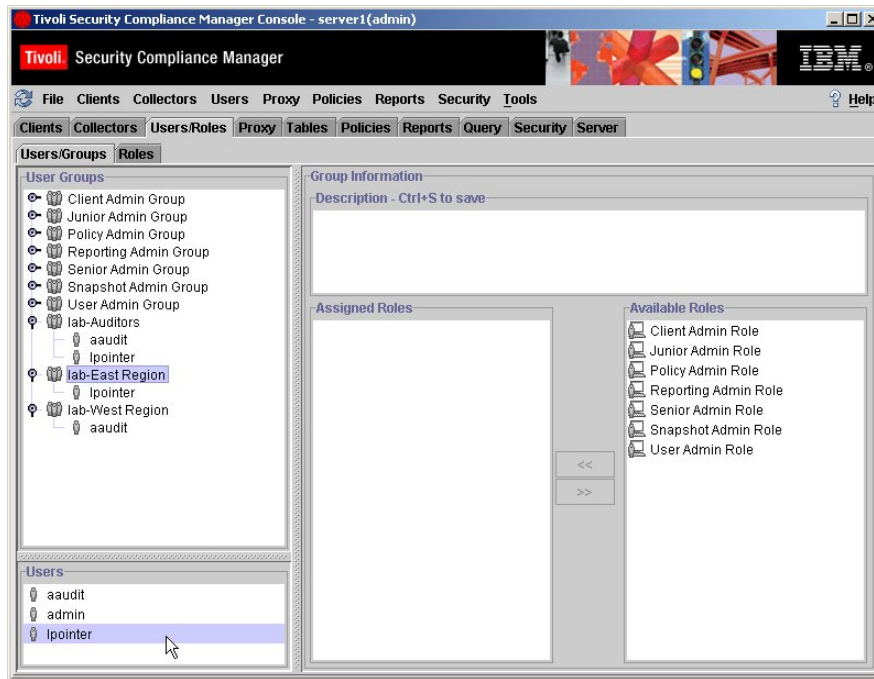
Select **aaudit** so the name is highlighted. Then select **lab-auditors** so the name is highlighted. Right click to get the menu.

Select **Add User to User Group** and **aaudit** should appear as a member of the group.



A user can be a member of one or more groups.

Next add user **aaudit** to the **lab-West Region**. Then add **lpointer** to the **lab-Auditors** group and the **lab-East Region**.

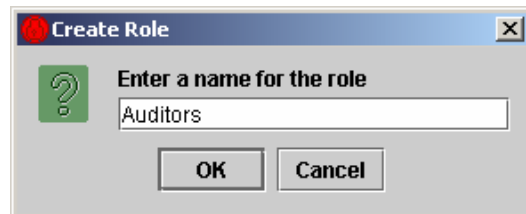


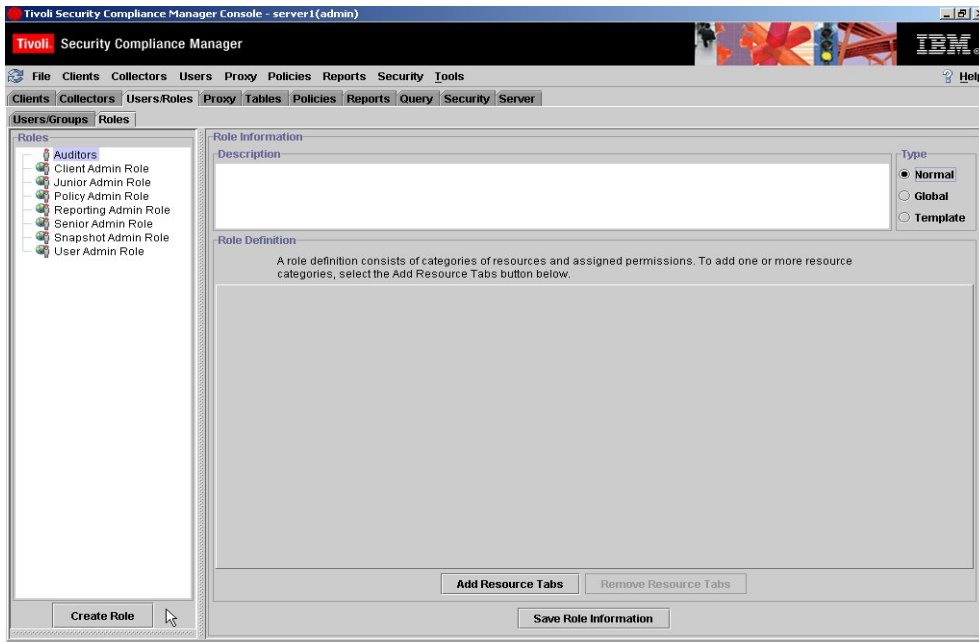
When completed, your groups should look similar to the screen above.

14.3 Creating Templates

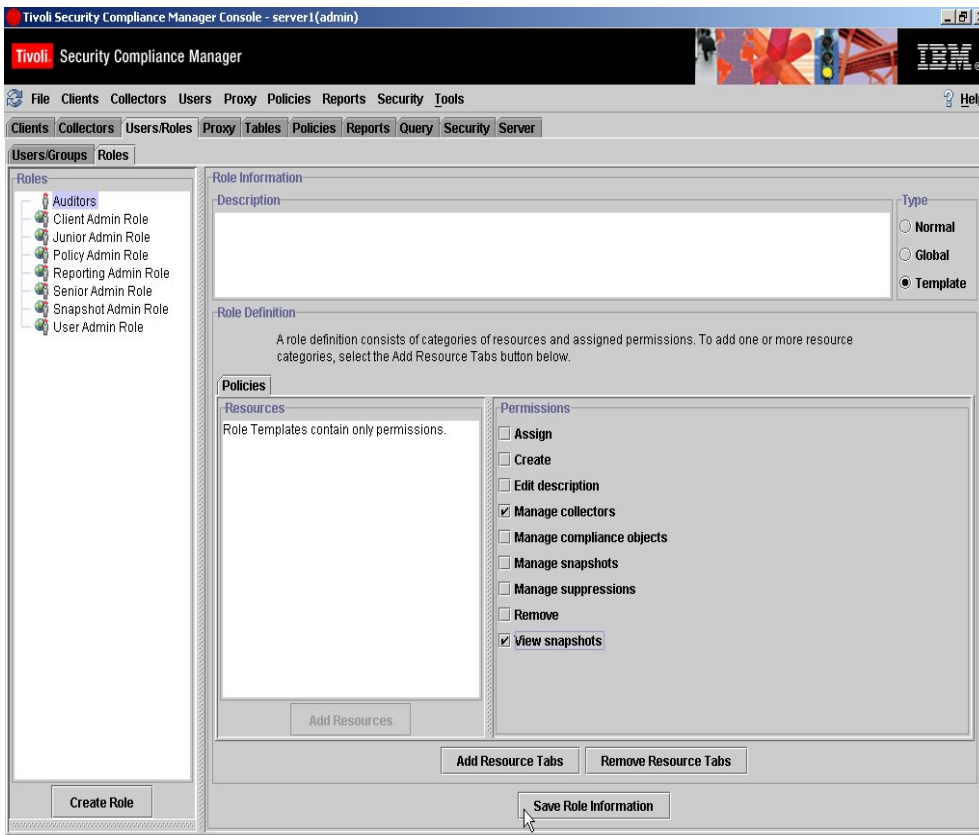
A Template role defines a set of permissions that apply to the specified resource categories. Roles can inherit permission of a template role and further restrict access to resources.

Create a template role called **Auditors**. Select the **Roles** tab and click on the **Create Role** button at the bottom of the left Roles frame.

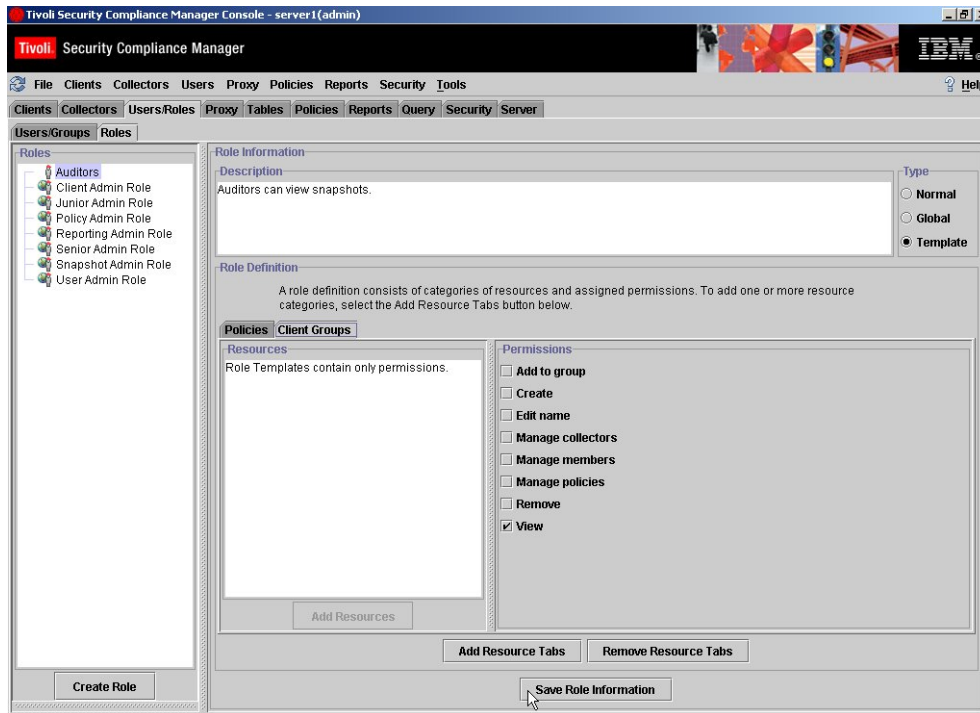




Configure the template role **Auditors** as follows:



1. Enter a description of **Auditors can view snapshots**.
2. Make the Role type a **Template**.
3. Add the resource tab of **Policies** in the role definition.
4. Select **Manage Collectors** and **View snapshots** from the Permissions list in the role definition for Policies.

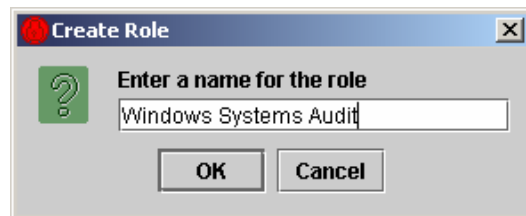


5. Add the resource tab of **Client Groups** in the role definition.
6. Select **View** from the Permissions list in the role definition for Client Groups
7. Save the role using the **Save Role Information** button.

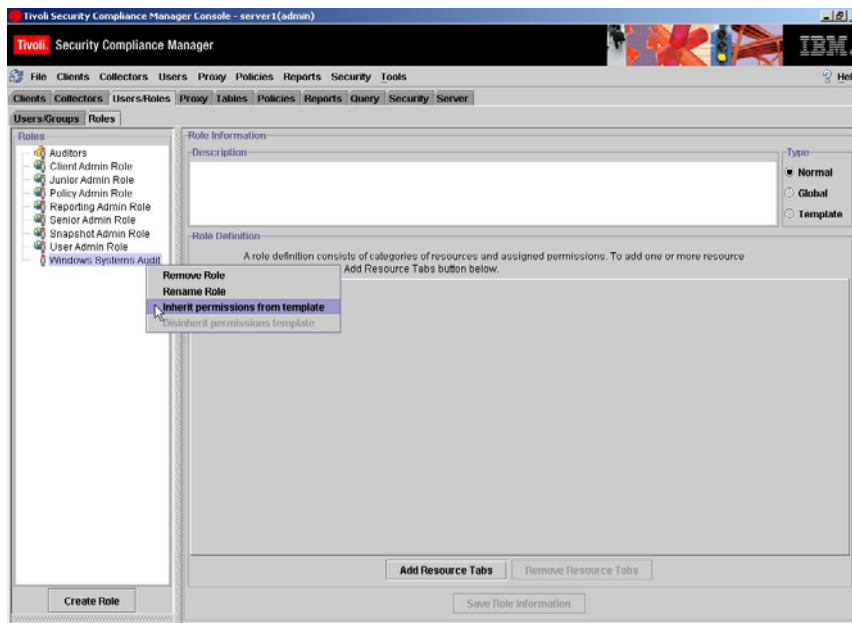
14.4 Creating Roles

Next, you will create a role that will inherit the Auditors template you just created.

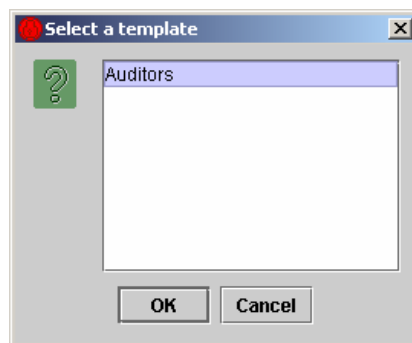
Create another new role called Windows Systems Audit. Select **Normal** for its type.



Save the role. Next, highlight the role **Windows Systems Audit** and right click on it to get the menu item **Inherit Permissions from Template**.



Next, select the **Auditors** template role.

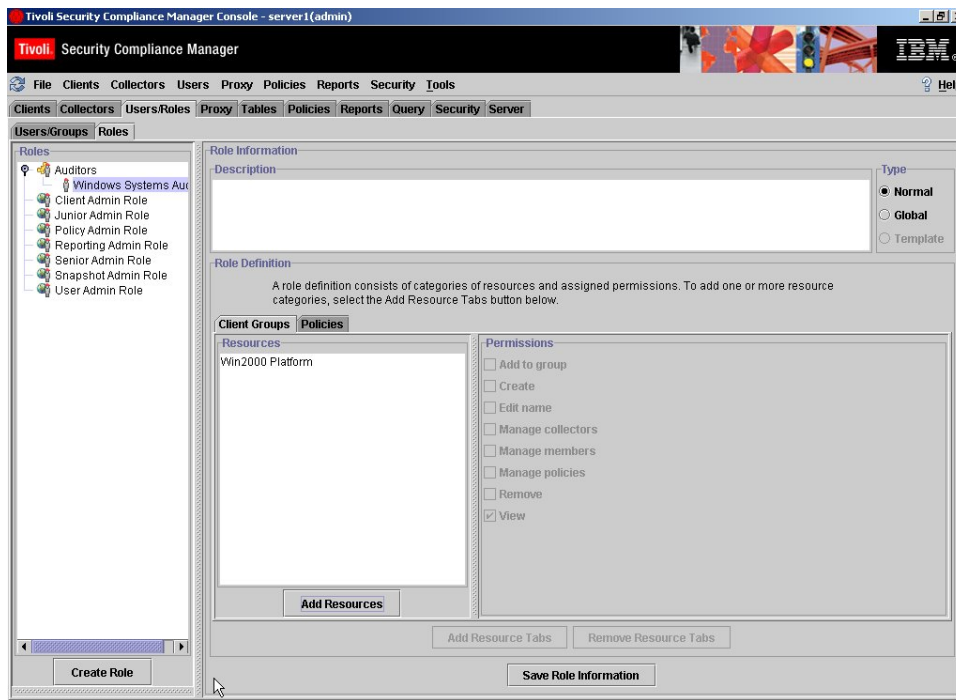


Next, examine the **Windows Systems Audit Role**. You can see that it has inherited the **Policy** Resource tab and the Permission of **View Snapshot** and the **Client Groups** Resource tab with the Permission of **View**.

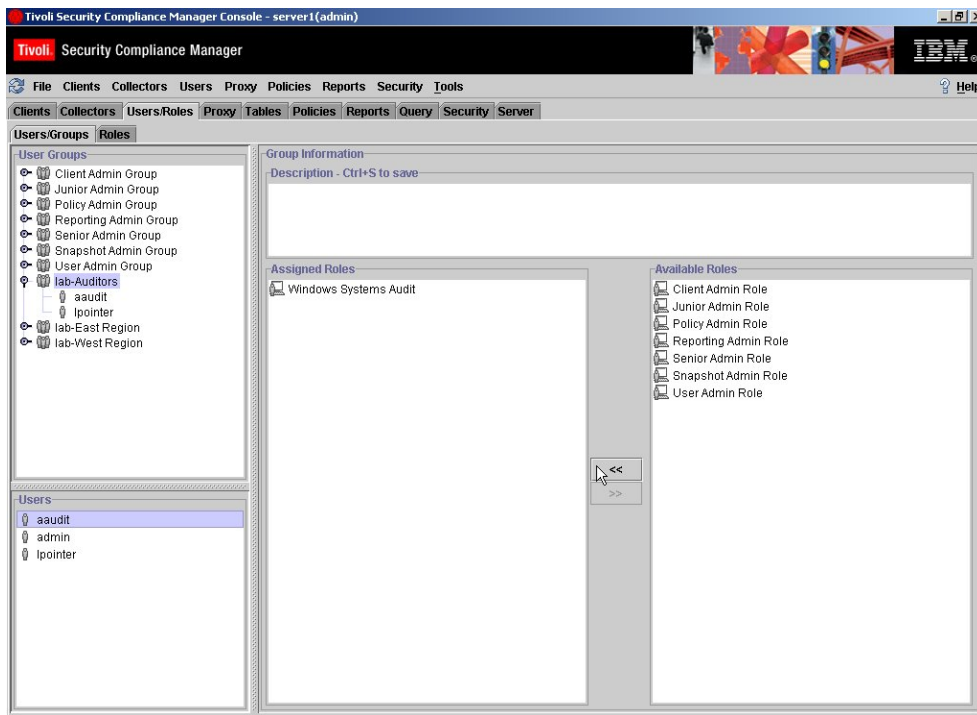
You can further restrict this role by adding specific resources such as specific policies or client groups. With the **Policies** tab selected, add a specific policy by selecting the **Add Resources** button and selecting the **Check PW Expiry** policy from the popup window. Also, add the **Network_Windows Policy**.

Also, you need to specify the **Client** group of **Win2000 Platform** to allow view access to clients in that group.

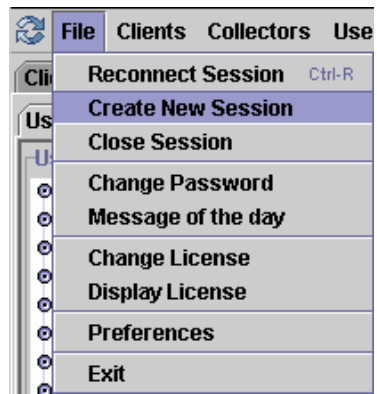
Your final configuration should look like this.



Test the role by assigning it to the group, lab-Auditors.



Open another Administration Console window and log in as Alan Audit (**aaudit/passw0rd**).



Logon as **Alan Audit**. Using the Administration Console, navigate through the console functions to see which functions are restricted to this user.

15 IBM Integrated Security Solution for Cisco Networks (IISCN)

15.1 System Overview

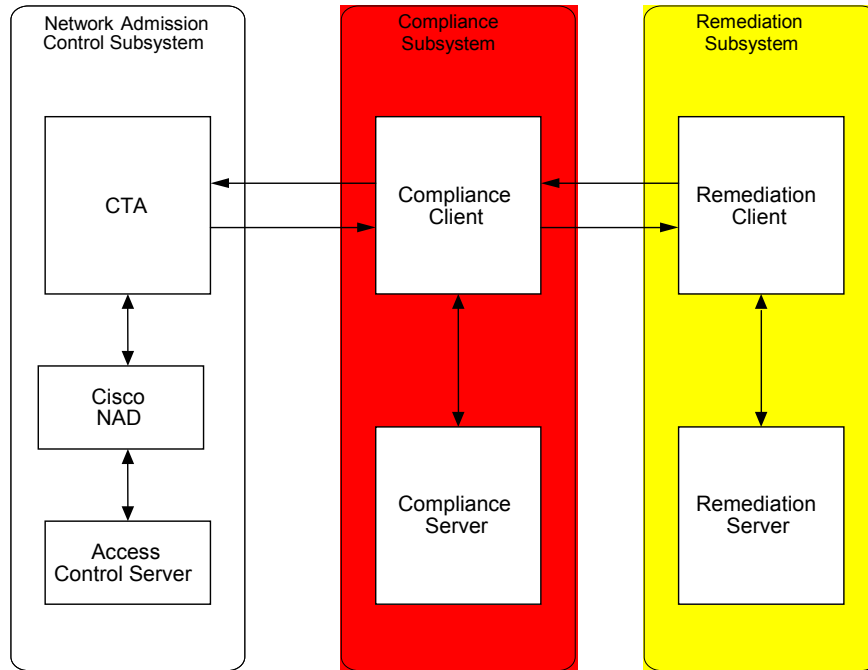
The IISCN Solution is an integration of three major sub-systems with components specifically developed for IISCN. Each of the three sub-systems must be installed individually. The IISCN integration components are then installed to provide the interfaces between the major sub-systems.

The function of IISCN is to detect the state of network attached devices, compare the detected state with a defined set of policies to establish device postures, dynamically reconfigure the network based on detected device postures, and change the state of devices to be in compliance with policies.

The IISCN solution, as delivered includes a set of Policies and Workflows that address certain well-known conditions such as OS Levels, HotFixes, Security and Policy Settings. These included Policies and Workflows can be configured to address new instances of these well-known conditions.

In addition, IISCN is an extensible platform that provides the ability to create new Policies that can detect various combinations of state on devices and Workflows that can change various states on the devices.

The Subsystems



TCR Solution Block Diagram

15.1.1 Network Admission Control - Cisco NAC

Cisco's Network Admission Control (NAC) program is a methodology rather than an actual product. NAC involves three components_ the Cisco Trust Agent (CTA), a Cisco Network Access Device (NAD) running a NAC-enabled version of Cisco's IOS, and a Cisco Secure Access Control Server (ACS) running version 3.3 or above of the software.

The primary function of Cisco NAC in TCR version 1.0 is to communicate with the compliance components on a client and either allow network access for compliant clients or restrict network access for non-compliant clients.

The CTA runs on the client and communicates with Posture Plug-Ins to determine the status of the client. The CTA reports this status to the NAD upon request. The NAD then reports this data to the ACS where the client's Posture is determined. Based on the client's posture, the NAD will either allow it access to the network or will quarantine it.

Information on [Cisco NAC](#) is available at:

15.1.2 Compliance – Tivoli Security Compliance Manager 5.1

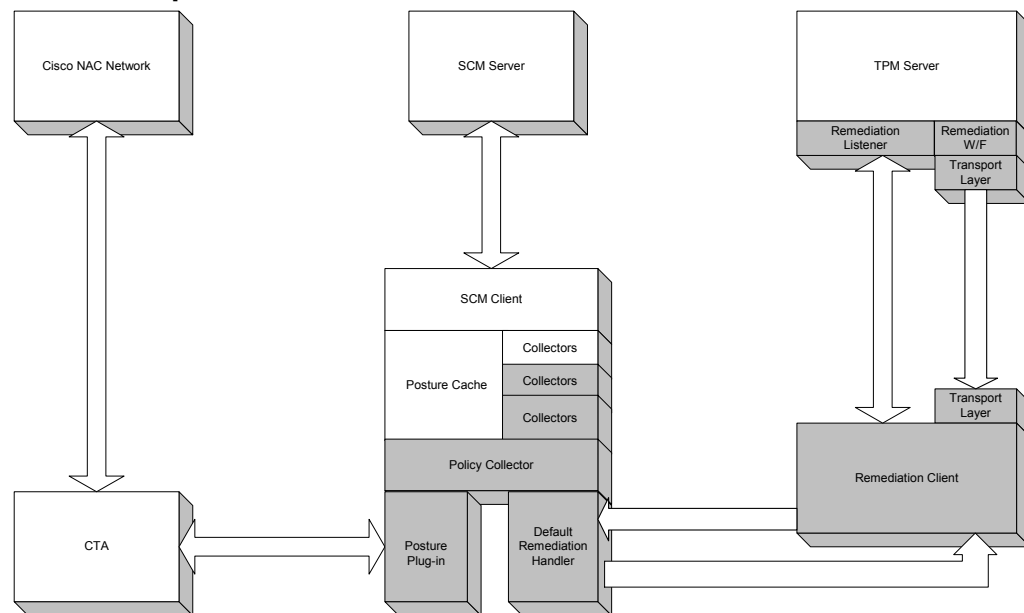
Tivoli Security Compliance Manager is a policy compliance solution that supports the definition of complex policies that specify conditions that should exist on a client. In addition, the client component of ITSCM can detect the state of these conditions and report the collected current state information back to the server. The set of conditions that can be checked for is limited by a library of collectors, each of which collects data from a specific source. Collectors can be developed as new sources of information or new conditional states are added to the client.

15.1.3 Remediation – Tivoli Provisioning Manager 2.1

Tivoli Provisioning Manager is an object and workflow-based solution that supports the definition of abstracted objects and workflows that perform specific actions on applicable clients using the abstracted objects. TPM requires a transport layer for copying objects to clients and executing commands on clients. Access to this transport layer is provided to the workflows. A TPM administrator can pre-define all of the objects and workflows necessary to remediate a non-compliant condition on a client.

Tivoli Intelligent Orchestrator 2.1 can also be used as the platform for remediation. All of the IISCN components that run on TPM 2.1 will also run on TIO 2.1.

IISCN Components



15.1.4 Tivoli Security Compliance Manager Client for NAC

The standard ITSCM Solution delivers an ITSCM Client that runs on the clients to collect compliance information and report it back to the ITSCM Server. For TCR, a special extension of the ITSCM Client is delivered. This client is adapted to communicate with the Cisco Trust Agent and supports the Posture Plug-In interface required by Cisco to report posture data during the NAC process.

15.1.5 Default Remediation Handler

The ITSCM Client includes a Default Remediation Handler (DRH) that will provide a graphical interface for displaying the compliance posture and data and a method for reinitiating the compliance scanning process. The DRH supports the passing of non-compliance data and remediation request data to the Remediation Client. Finally, it provides an interface for notification of activity and completion of Remediation Requests.

15.1.6 ITSCM Collectors for NAC

The standard ITSCM Collectors (base collectors) simply cache data and return it to the Server when appropriate. For TCR, a new set of collectors is delivered. These “posture collectors” allow the Posture Plug-in to report Compliance data to the CTA.

15.1.7 Remediation Client

The TCR Remediation client is a TCR-specific component that handles the interface between the ITSCM Client for NAC and the TPM server. It is a single interface point that parses the compliance data reported by the ITSCM Client for NAC and creates a Remediation Request that is then passed to the Remediation Listener.

15.1.8 Remediation Listener

The Remediation Listener is a process that runs on the TPM Server and accepts Remediation Requests from Remediation Clients. If properly formed, the Remediation Requests are parsed and the appropriate data in the requests is passed to a Remediation Workflow which invokes the actual actions that perform the remediation on the client.

15.1.9 Remediation Workflows

The Remediation Workflows are TPM Workflows developed specifically for TCR to initiate the actual remediation actions on the client. They perform actions on the client such as copying files, executing commands, and issuing messages.

15.1.10 The Transport Layer (TRAPI)

The transport layer provides a means for communications between the client and the TPM Server. During the remediation process, the TPM Server may send files, commands, messages and other information to the client using the transport layer.

For Phase 1, the transport layer used is openssh, delivered via the open-source cygwin client.

Formatted: Heading 3,Heading 3 Char

Formatted: Heading 3,Heading 3 Char

16 Installing the Cisco NAC Components

The following Cisco components must be installed:

- o ACS Server
- o IOS NAD
- o CTA

16.1 ACS Server

Install the ACS 3.3 software and configure it according to the [Cisco NAC Deployment Guide](#).

Copy the [avplist5.txt](#) file to the c:\temp directory on the ACS server.

Add the Tivoli Security Compliance Manager attributes to ACS by running the command:

C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -addavp c:\temp\avplist5.txt

Restart the ACS server.

Restart the CSAuth and CSAdmin services.

After that is done, the ACS server should be aware of the IBM ITSCM attributes. To verify this, run the command:

csutil -dumpAVP avpdump.txt

where avpdump.txt is the file where the attributes are written. The Tivoli Security Compliance Manager attributes should be viewable in this file.

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

16.2 IOS NAD

Ensure that your model and software version supports NAC. Follow the directions in the [Cisco NAC Deployment Guide](#) to setup the NAD.

16.3 Cisco Trust Agent (CTA)

ATTENTION: Ensure that you have the proper operating system version installed. The TCR Client requires Microsoft Windows 2000 with both Service Pack 2 and the .NET framework installed, or Microsoft Windows XP Professional with the .NET framework installed.

1. Install the Cisco Trust Agent client software according to the [Cisco NAC DeploymentGuide](#).
2. Install the ACS Server's CA certificate on this client:
 - a) Copy the ACS Server's [ca.cer file](#) to the c:\certs directory on the client.
 - b) Open a command prompt and go to the following directory:
C:\Program Files\Cisco Systems\CiscoTrustAgent directory
 - c) Install the ACS certificate using the following command:

ctacert /add c:\certs\ca.cer /store "Root"

17 Installing and configuring the Tivoli Security Compliance Manager components for IISCN

17.1 Tivoli Security Compliance Manager Server

1. Install the IBM Tivoli Security Compliance Manager server as described [previously in this document](#) or in the IBM Tivoli Security Compliance Manager Installation Guide: All Components. This book is available on the Web at:

<http://publib.boulder.ibm.com/tividd/td/IBMTivoliSecurityComplianceManager5.1.html>

2. Install fix pack 5.1.0-TIV-SCM-FP0009, or later, on the server.

ATTENTION: If you are using an existing Tivoli Security Compliance Manager server, you might have some collectors already installed. Unregister and uninstall any collectors that might conflict with the collectors provided with TCR.

3. Import the SCMNACPolicy_V1.11_Win2000.pol and SCMNACPolicy_V1.11_WinXP.pol files delivered with fix pack 5.1.0-TIV-SCM-FP0009, or later, Described earlier in [section 4.1](#) or using the Tivoli Security Compliance Manager administration console. Information on importing policies can be found in the IBM Tivoli Security Compliance Manager Administration Guide, available on the Web at:

<http://publib.boulder.ibm.com/tividd/td/IBMTivoliSecurityComplianceManager5.1.html>

4. [Register all the com.* and nac.* collectors](#) using the administration console. If the SCM Server has been configured to take advantage of the added security of digitally signing collector code, then authorise all collectors before registering. Refer to the collector [authorisation section 4.2](#) in the Doc or the ITSCM User Guide for further details.
5. Create client groups for the Windows 2000 client systems and the Windows XP client systems using the administration console. Add the appropriate policies to each client group.

For example, you can create a group called Windows2000 to represent clients running Windows 2000 and add the SCMNACPolicy_V1.11_Win2000 policy to that client group. Similarly, you can create a WindowsXP client group and add the SCMNACPolicy_V1.11_WinXP policy.

17.2 Tivoli Security Compliance Manager Client

1. Install the IBM Tivoli [Security Compliance Manager client](#) as described in the IBM Tivoli Security Compliance Manager Installation Guide: All Components. This book is available on the Web at:

<http://publib.boulder.ibm.com/tividd/td/IBMTivoliSecurityComplianceManager5.1.html>

Specify the IP address or Server host name of the Tivoli Security Compliance Manager server and use the default port numbers.

Note: It is preferable to use the Host Name and keep a local "Host File" to resolve IP address as this makes all the VMware images more portable with only the host file requiring updates on all systems.

Indicate that the client uses DHCP and specify the Windows system ID as the alias for the system. This alias can be changed when registering the client to the server or used automatically if the ITSCM Server has been set to auto-register DHCP clients.

Note: It is preferable that the alias name indicates the OS installed for easy administration of clients to groups.

2. Install fix pack 5.1.0-TIV-SCM-FP0009, or later, on the client system. When prompted, indicate that you want to install the files for the IBM Integrated Security Solution for Cisco Networks.
3. Copy the following files to the **C:\Program Files\IBM\SCM\client** directory on the client system:
[SCMNACPolicy_Basic_Win2000.cpf](#)
[SCMNACPolicy_Basic_WinXP.cpf](#)
[SCMNACPolicy_Boot_Win2000.cpf](#)
[SCMNACPolicy_Boot_WinXP.cpf](#)
4. Add the **C:\Program Files\IBM\SCM\client** directory to the beginning of the system path using the Windows Control Panel:

Start -> Settings -> Control Panel -> System -> Advanced -> Environment Variables
5. Stop the client either using the Services window of the Windows Control Panel or by entering the following command in a command window:

net stop "SCM Client"
6. Open a command window and go to the **C:\Program Files\IBM\SCM\client** directory.
7. Run the following command, specifying the name of the appropriate cpf files:

installcpf <policy>

where <policy> is one of the following:

SCMNACPolicy_Basic_Win2000.cpf
SCMNACPolicy_Basic_WinXP.cpf
SCMNACPolicy_Boot_Win2000.cpf
SCMNACPolicy_Boot_WinXP.cpf

The Boot versions of the policies check for nothing at all, and are provided to bootstrap a client to the point where the production policy for the deployment can be installed automatically. The Basic versions include checks for Windows password length and minimum age.

These policies are provided to serve as a template for creating deployment

specific policies such that the required values in the collector parameters of the collectors can be modified as applicable.

8. Optional. Install the sample HTML pages by extracting the contents of the [acme2.zip](#) file to the %SCM_HOME% directory.
9. Optional. Enable verbose client logging by modifying the client preferences file, client.pref, and change debug=false to debug=true.
10. Enable the Tivoli Security Compliance Manager client component, which runs as a Windows service, to interact with the desktop.
 1. Open the Services window from the Windows Control Panel.
Start -> Settings -> Control Panel -> Administrative Tools -> Services
 2. Double-click **SCM Client** to open the Properties window.
 3. Click the **Log On** tab.
 4. Select both "Log on as Local System Account" and "Allow service to interact with desktop".
 5. Click **OK**.
 6. Right-click SCM Client and click Start to start the client component.
(You also can start the client using the **net use "SCM Client"** command.)

ATTENTION: If the service is not set to interact with the desktop, the remediation handler GUI does not work as expected.

18 Installing and configuring the Tivoli Provisioning Manager components

18.1 Tivoli Provisioning Manager server

1. Install the Tivoli Provisioning Manager 2.1 software as described in the IBM Tivoli Provisioning Manager 2.1 Installation Guide for Windows. This document is available on the Web at:

<http://publib.boulder.ibm.com/tividd/td/IBMTivoliProvisioningManager2.1.html>

2. Install Tivoli Provisioning Manager Fix Pack 1 on the system.
3. Reinitialize the DataCenter to remove all sample data and create the Tivoli Provisioning Manager server as a DataCenter object.
 - o Copy the [tcrdcm.xml](#) file to the %TIO_HOME%\xml directory.
 - o Change all occurrences of the IP address "9.2.16.131" in the tcrdcm.xml file to the IP address of your Tivoli Provisioning Manager server. Change the server name of "elix0r2" to the host name of your server. The sub-network name will be in the form of <IP_address>/32.
 - o Optional. Copy the tcr.remediation.server.workflows.tcdriver file to the %TIO_HOME%\drivers directory. Any tcdrivers in this directory are loaded by the reinit process.
 - o Open a command window and change to the %TIO_HOME%\xml directory.
 - o Run the following command:

```
..\tools\reinit.cmd .\tcrdcm.xml
```

NOTE: The reinit process takes a long time, so be patient.

4. Install the transport layer (cygwin for Phase 1) according to the instructions in the IBM Tivoli Provisioning Manager 2.1 Installation Guide for Windows.
5. Configure the system for SSH and generate keys for the tioadmin user according to the instructions in the installation guide.
6. Extract the files in the tcr.remediation.server.helpers.zip archive file to the %TIO_HOME%\bin\TCR directory on the server. If the directory does not exist, create it.
7. Mark the executable files in the %TIO_HOME%\bin\TCR directory as being executable. For example:
chmod a+x *.exe

18.2 Remediation Workflows

ATTENTION: If you took the optional step of copying the `tcr.remediation.server.workflows.tcdriver` to the `%TIO_HOME%\drivers` directory before reinitializing the Data Center Model, your workflows have already been installed. You can skip this step and go on to installing the Remediation Listener.

ATTENTION: If you are installing an upgrade to a set of workflows on the server, you **MUST** remove the *previous* version of the workflows using the *previous* version of the `tcr.remediation.server.workflows.tcdriver` file. **DO NOT** copy the new version of this file over the previous version or you will not be able to remove the previous versions of the workflows without reinitializing the DCM.

1. Open a command prompt and go to the `%TIO_HOME%\drivers` directory.
2. Run the following command (all on one line) to remove the previous workflows:

```
..ltoolslsc-driver-manager.cmd forceUninstallDriver  
tcr.remediation.server.workflows.tcdriver
```

3. Copy the new `tcr.remediation.server.workflows` file into the current directory.
4. Run the following command to install the remediation workflows:

```
..ltoolslsc-driver-manager forceInstallDriver  
tcr.remediation.server.workflows.tcdriver
```

18.3 Remediation Listener

Install the Remediation Listener. This installs as a separate Enterprise Application under WebSphere.

1. Copy the `tcr.remediation.server.ear` file to the `%WEBSPPHERE_HOME%\AppServer\InstallableApps` directory.
2. From the WebSphere Application console, select Enterprise Applications and then Install New Application.
3. Select the `tcr.remediation.server.ear` file in the `%WEBSPPHERE_HOME%\AppServer\InstallableApps` directory and install it using all the default settings.
4. Edit the `tc-rs-config.properties` file in the `%WEBSPPHERE_HOME%\AppServer\installedApps\<server_name>\tcr.remediation.server.ear\tcr.remediation.server.war\WEB-INF\tcr-rs-config.properties` as follows:
 - a) `"tiouserid=<TIO_UID>"`, the user ID under which TIO runs, usually `"tioappadmin"`
 - b) `"tiopasswd=<TIO_PWD>"`, the password associated with the `tiouserid`
 - c) `"tiohostname=<TIO_HOST>"`, the fully qualified host name of the TIO system
 - d) `"tioport=<TIO_PORT>"`, the port used by TIO to serve WS requests, usually 9080

Do not change any other values.

5. Start the `tcr.remediation.server` application.

19 Installation and configuration of IISCN Components

19.1.1 Tivoli Security Compliance Manager Posture Plug-in

The Tivoli Security Compliance Manager Posture Plug-in is automatically installed and is activated the next time the Cisco Trust Agent is activated.

19.1.2 Remediation Client

1. Install cygwin on the client and setup the cygwin client for SSH following the directions in the [Remclientsetup.doc](#) file.
2. Create a new directory on the client system as workspace for the IBM Integrated Security Solution for Cisco Networks components, for example:

C:\Program Files\IBM\SCM\client\TCR

3. Extract all the files from the tcr.remediation.client.helpers.zip archive into this new directory.
4. Copy the [tcr.cacerts](#) file containing the demo root certificate authority (CA) key for the IBM Integrated Security Solution for Cisco Networks into this same directory.

ATTENTION: The attached tcr.cacerts file is a demonstration version that is compatible with the demonstration certificate provided with WebSphere. This certificate can be used for non-production environments, but do not use it in a production environment. In a production environment, you must create a Java keystore containing the CA certificate of the WebSphere Application Server that is hosting Tivoli Provisioning Manager and the Remediation Listener applications.

5. Copy the [trapi.properties](#) and [tcr.properties](#) file into this new directory.
6. Edit the trapi.properties file and change the following settings to match the client environment:
 - tcr.remediation.common.trapi.ssh.endpoint.accountname=<local admin Account name – Administrator by default>
 - tcr.remediation.common.trapi.ssh.endpoint.password=<Password for the local admin account>
 - tcr.remediation.common.trapi.ssh.endpoint.authorizedkeysfile=<path to authorized_keys file EG: /c:/cygwin/home/Administrator/.ssh/authorized_keys>
 - tcr.remediation.common.trapi.ssh.endpoint.hostkeyfile.1=<path to endpoint host key file EG: /c:/cygwin/home/Administrator/.ssh/ssh_host_dsa_key.pub>
 - tcr.remediation.common.trapi.ssh.server.knownhostsfile.1=<path to known_hosts file EG: /c:/cygwin/home/Administrator/.ssh/known_hosts>

Leave everything else in the file unchanged.

7. Edit the handlers.properties file in the %SCM_HOME%\client directory and add the following line:

tcr.remediation.client.workspace=<TCRWORKSPACE>

where <TCRWORKSPACE> is the directory you created above.

ATTENTION: The path to the TCR Workspace must use the UNIX forward slash (/) directory separator, not the Windows backslash character (\). For example:

`tcr.remediation.client.workspace=/c:/program files/ibm/scm/client/tcr`

8. The log4j open source library must be installed. To install it:
 - a. Obtain the logging-log4j-1.2.9.zip file (or a later 1.2.x version) from <http://logging.apache.org/site/binindex.html>
 - b. Unpack the ZIP file into a temporary directory.
 - c. Copy the logging-log4j-1.2.9/dist/lib/log4j-1.2.9.jar file to the %SCM_HOME%\jars directory on the client system.
9. Restart the Tivoli Security Compliance Manager client.

19.2 Configuration Setup

19.2.1 Policy Creation and Assignment

Policies can be created using the Tivoli Security Compliance Manager Administration console. See the IBM Tivoli Security Compliance Manager Administration Guide for detailed instructions. The guide is available on the Web at:
<http://publib.boulder.ibm.com/tividd/td/IBMTivoliSecurityComplianceManager5.1.html>

Policies include a list of collectors, which is generated by building SQL statements that select data from the tables maintained by the individual collectors. To create policies using the TCR “Posture Collectors”, include table names that have the word “Posture” in the table name. This generates collector lists using the Posture Collectors.

After the collector list has been generated, edit the collector parameters of the Posture Collectors to specify the required values for the various collectors and the appropriate TCR Workflows to be called to remediate compliance violations.

The SCMNACPolicy_V1.1_Win2000.pol and SCMNACPolicy_V1.1_WinXP.pol policies that are delivered with TCR can be used as a template from which to develop your own production policies. The required values in the delivered policies might not be correct for your environment, and the software artefacts needed to remediate the various required versions must also be provided on your remediation server if the deployment is to succeed. However, the workflow names defined in the delivered policies are the correct names for remediating each type of violation. Use the delivered policies as a learning tool to discover which workflows are used for remediation of various conditions.

For Phase 1, clients are assigned policies according to their operating system type so define a single policy for each OS type of the clients.

Create a client group for each OS type and assign the clients to the client groups as appropriate. Then assign a policy to each client group. This way all clients of the same OS type will inherit the same policy.

19.2.2 Remediation Capability

Any compliance violation has the potential to be remediated by the remediation server. In order to support automated remediation, the software objects used to remediate conditions must be installed and registered on the remediation server.

Installation of the objects is a simple matter of copying the files in question to a predetermined directory on the server. Any files used to remediate clients, such as client policy files (.cpf), self-installing updates, hot fixes, Service Packs, and so on, should be copied to this directory on the server.

ATTENTION: The names of the software artefacts that are registered for use by TCR is EXTREMELY IMPORTANT. If the objects are not named correctly, the TCR workflows will not be able to find them in the DCM. Refer to the [tcrprovisioning.doc](#) document for an in-depth discussion of creating new artefacts.

Registration of the objects is a matter of adding them as software objects to the TIO DCM. This is done using the TIO WebUI. For more information on the TIO WebUI, visit the following Web site:

<http://www-106.ibm.com/software/sysmgmt/products/support/IBMTivoliIntelligentThinkDynamicOrchestrator.html>

19.2.3 Network Configuration

The accompanying document, [Cisco NAC Installation/Configuration Example for TCR](#) should be read before configuring the network. While it is targeted at a particular environment, if the names, addresses and device types are ignored, the actual step-by-step process is well documented and should be understood before configuration is attempted. The steps to configure the network are all described in detail in this document. If you understand this process after reading the document, it will greatly enhance the chances that your NAC deployment will be successful.

19.2.4 ACS Server

19.2.4.1 NAC Database

An External Database must be configured for Network Admission control. This database will provide the definition of the credentials, policies, and rules to be applied to NAC.

19.2.4.2 Mandatory Credentials

Mandatory credentials include sets of attributes that must be registered by CTA Plug-ins so that they can then return values for these attributes during runtime. IBM registers two attributes in Phase 1, Policy_Version and Violation_Count.

19.2.4.3 Local Policy

A local policy consists of rules that will be evaluated by the ACS Server based on information returned by the CTA Agent.

19.2.4.4 Local Rules

Each local rule allows for the checking of one or more attributes from the mandatory credentials. Combined with Boolean operations and hard-coded values, the attributes values returned by the

plug-ins can be checked and compared against known values. A compliance posture and return token which will be activated if a rule is matched are also assigned here.

19.2.4.5 Downloadable ACLs

Downloadable IP ACLs are the mechanism by which quarantines are created and enforced. The ACLs used are standard Cisco IOS ACLs.

19.2.4.6 Groups

Groups are an abstraction used to assign Downloadable ACLs to multiple clients.

19.2.4.7 User Group Mappings

User Group Mappings allow the postures defined in the NAC External Database Policies to be applied to users.

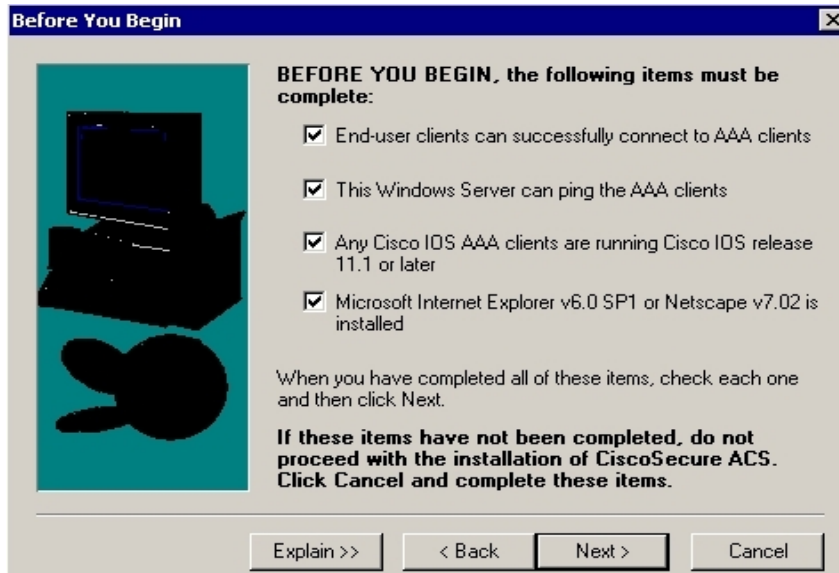
19.2.5 IOS NAD

The IOS NAD must be configured to enable NAC and to use the ACS Server as its AAA Server.

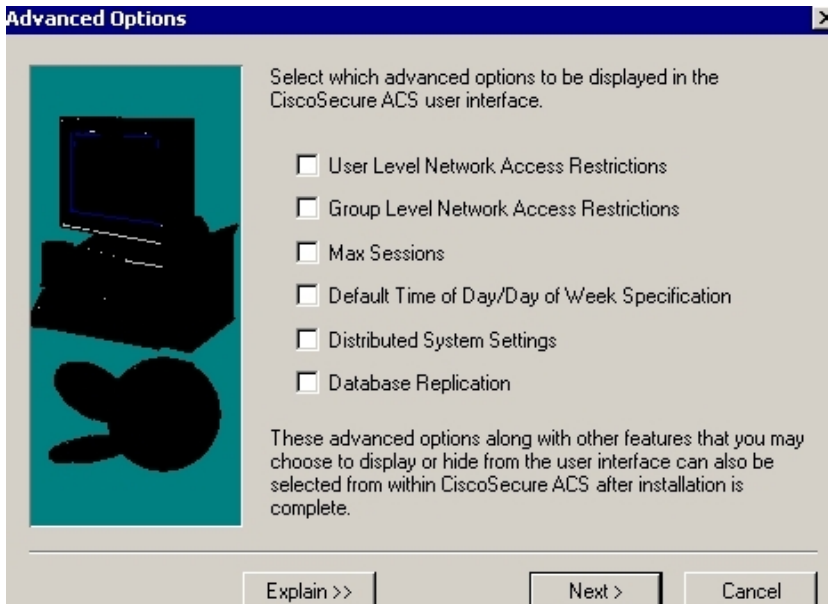
20 Cisco NAC Installation/Configuration example for TCR

20.1 Install and Configure ACS 3.3

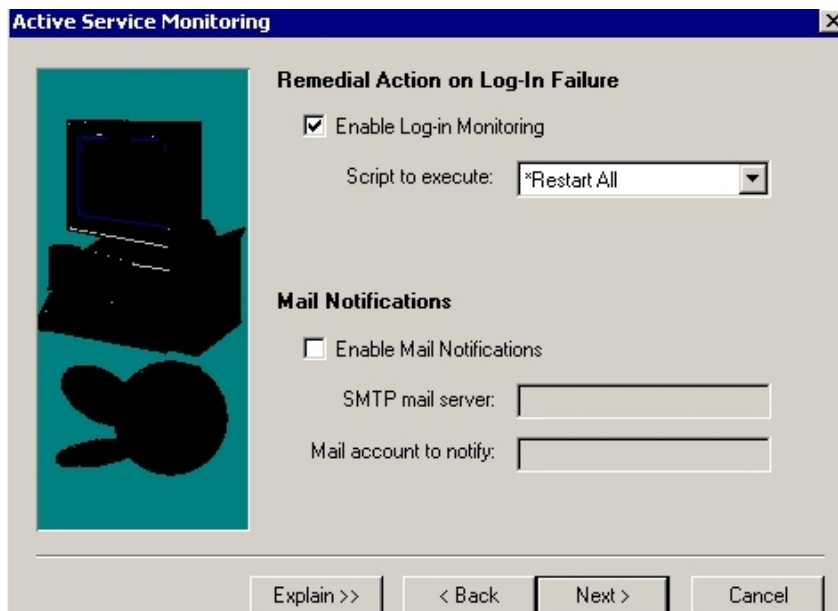
Start the ACS installation. On the 'Before You Begin' panel, check all items.



On the 'Advanced Options' panel you may select items or leave unchecked..



Accept defaults on 'Active Service Monitoring' panel.



Active Service Monitoring

Remedial Action on Log-In Failure

☒ Enable Log-in Monitoring

Script to execute: *Restart All

Mail Notifications

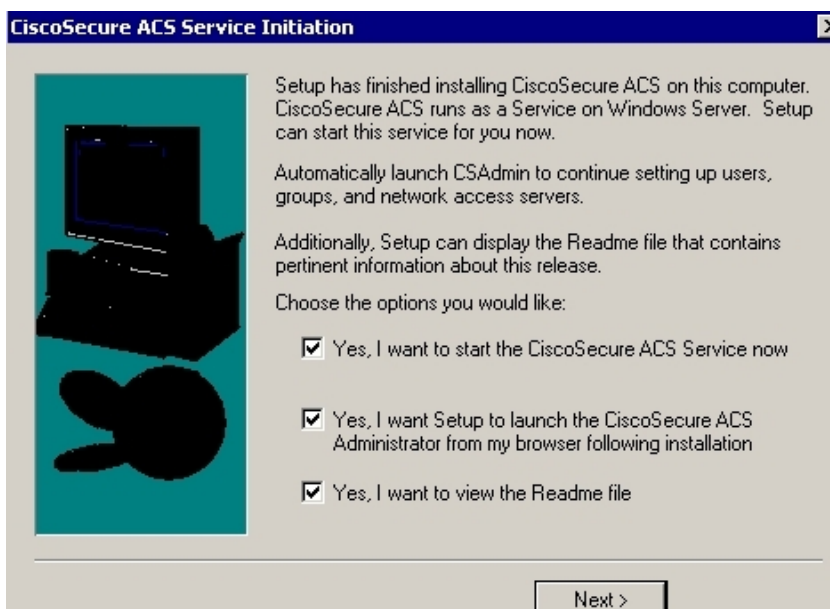
☐ Enable Mail Notifications

SMTP mail server:

Mail account to notify:

Explain >> < Back Next > Cancel

Accept defaults on 'Service Initiation' panel.



CiscoSecure ACS Service Initiation

Setup has finished installing CiscoSecure ACS on this computer. CiscoSecure ACS runs as a Service on Windows Server. Setup can start this service for you now.

Automatically launch CSAdmin to continue setting up users, groups, and network access servers.

Additionally, Setup can display the Readme file that contains pertinent information about this release.

Choose the options you would like:

☒ Yes, I want to start the CiscoSecure ACS Service now

☒ Yes, I want Setup to launch the CiscoSecure ACS Administrator from my browser following installation

☒ Yes, I want to view the Readme file

Next >

The home page for the ACS server should be displayed in the browser.



Under 'Interface Configuration' -> '**Advanced Options**', make sure 'Group-Level Downloadable ACLs' is checked, and click 'Submit'.

Interface Configuration

Edit

Advanced Options ?

NOTE: These options will hide sections from the interface only if those sections are not in use.

☐ Per-user TACACS+/RADIUS Attributes

☐ User-Level Shared Network Access Restrictions

☒ User-Level Network Access Restrictions

☐ User-Level Downloadable ACLs

☒ Default Time-of-Day / Day-of-Week Specification

☐ Group-Level Shared Network Access Restrictions

☒ Group-Level Network Access Restrictions

☒ Group-Level Downloadable ACLs

☐ Group-Level Password Aging

☒ Network Access Filtering

☒ Max Sessions

If you will be accessing the ACS server from a browser that is not running on the same system as the ACS server, then you need to **configure an administrator**.
'Administration Control' -> 'Add Administrator'. Fill in the admin name and password, then click 'Grant All', then 'Submit'.

Add Administrator

Administrator Details ?

Administrator Name

Password

Confirm Password

Administrator Privileges ?

Next, **add the IOS NAD** by going to 'Network Configuration' and clicking the 'Add Entry' button under 'AAA Clients'.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

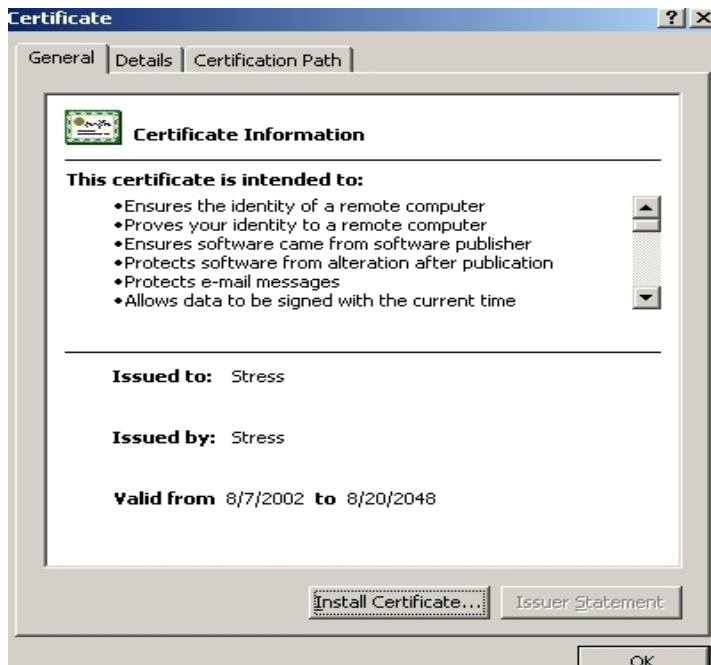
Type in the information for the NAD and click 'Submit and Restart'.

Add AAA Client

AAA Client Hostname	Cisco1751
AAA Client IP Address	192.168.1.1
Key	radiuskey
Authenticate Using	RADIUS (Cisco IOS/PIX)
☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
☐ Log Update/Watchdog Packets from this AAA Client	
☐ Log RADIUS Tunneling Packets from this AAA Client	
☐ Replace RADIUS Port info with Username from this AAA Client	

20.2 Install the ACS Certificate.

Copy the certificate files – ca.cer, server.cer, and server.pvk - into the directory C:\certs. Run ca.cer. When the following window appears, click on 'Install Certificate'. Accept all defaults and click OK to close.



On the ACS main page, select 'System Configuration' -> 'ACS Certificate Setup' -> 'Install ACS Certificate'. Fill in the appropriate information for the certificate and key files, and enter '1111' for the private key password. Click 'Submit'. For now **ignore the prompt to restart ACS**.

Install ACS Certificate

Install new certificate

?

☒ Read certificate from file

Certificate file

☐ Use certificate from storage

Certificate CN

Private key file

Private key password

Installed Certificate Information	
Issued to:	Server
Issued by:	Stress
Valid from:	August 07 2002 at 07:13:53
Valid to:	August 20 2048 at 00:45:37
Validity:	OK

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

Go to 'System Configuration' -> 'ACS Certificate Setup' -> 'ACS Certification Authority Setup'. Fill in the full path to the ca.cer file, and click Submit. **Do not restart.**

ACS Certification Authority Setup

CA Operations	
Add new CA certificate to local certificate storage	
CA certificate file	C:\certs\ca.cer

Go to 'System Configuration' -> 'ACS Certificate Setup' -> 'Edit Certificate Trust List'. Scroll down and select 'Stress'. Now restart as directed.

☐	SecureSign RootCA1 (Japan Certification Services, Inc. SecureSign F
☐	SecureSign RootCA2 (Japan Certification Services, Inc. SecureSign F
☐	SecureSign RootCA3 (Japan Certification Services, Inc. SecureSign F
☒	Stress
☐	Swisskey Root CA
☐	TC TrustCenter Class 1 CA

20.2.1.1 Add the IBM ITSCM attributes

To add the IBM ITSCM attributes to ACS by running the command:

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -addavp C:\temp\avplist2.txt
```

Where avplist2.txt is a file containing the IBM ITSCM attribute information.

Restart the ACS server after doing this – the services **CSAuth** and **CSAdmin** must be restarted.

Once this is done, ACS should be aware of the IBM ITSCM attributes.

To verify this, run the command: `csutil -dumpAVP avpdump.txt`

where avpdump.txt is the file that the attributes will be written to. The IBM ITSCM attributes should be viewable in this file.

These attributes should also be viewable in the logging attributes list, which will be used in the [‘Configure Logging’](#) section of this document.

The attributes are also utilized as part of the ACS policy rules checking. The values of the attributes are checked against those specified in the policy rules, and the appropriate token, ie, ‘Healthy’, ‘Quarantine’, etc, is returned to the client. ACS Policy rules are described in the [Configure External User Database](#) section.

20.3 Configure Logging

Select the **System Configuration** button on the left side.

Step 1 Click the logging link.

Step 2 Click **CSV Passed Authentications**.

Use	Local Logging Configuration
☒	CSV Failed Attempts
☒	CSV Passed Authentications
☒	CSV RADIUS Accounting
☒	CSV TACACS+ Accounting
☒	CSV TACACS+ Administration
☒	CSV VoIP Accounting

The logging page displays. In the ‘Attributes’ column you should see some IBM ITSCM attributes. Move these to the ‘Logged Attributes’ column and be sure that the ‘Log to CSV Passed Authentications report’ button is checked, then click Submit.

Edit

CSV Passed Authentications File Configuration

Enable Logging


☒ Log to CSV Passed Authentications report

Select Columns To Log


Attributes

AAA Server
Priv-Int
Proxy-IP-Address
ExtDB Info
Source-NAS
Filter Information
Network Device Group
Access Device
PEAP/EAP-FAST-Clear
Global Message Id
Logged Remotely
Real Name
Description
User Field 3
User Field 4
User Field 5
Class
Reason

Logged Attributes

Message-Type
User-Name
Group-Name
Caller-ID
NAS-Port
NAS-IP-Address
cisco-av-pair
Cisco:PA:PA-Name
Cisco:PA:PA-Version
Cisco:PA:OS-Type
Cisco:PA:OS-Version
Cisco:PA:User-Name
Cisco:Host:ServiceP
Cisco:Host:HotFixes
Cisco:Host:HostFDDI
Cisco:HIP:CSAVersi
Cisco:HIP:CSADoper
Cisco:HIP:CSAMCN

Up

Down

Submit

Reset Columns

Cancel

20.4 Configure Downloadable ACLs

Configure an ACL for each client condition so that ACS will return the appropriate downloadable ACL to the NAD for the specified postures. Use the following to configure the group settings.

Name	Healthy	Checkup	Unknown	Infected	Quarantine
Description	Permit all	Permit all	Allow to internet only	Deny all	Limited access for updates
ACL Content Name	permitall	permitall	Unknown	infected	quarantine
ACL Definition	permit ip any any	permit ip any any	deny ip 192.168.0.0 0.0.255.255 permit ip any any	deny ip any any	permit tcp any host 192.168.1.4 eq www

Complete these steps.

Step 1 From the ACS server, select the **Shared Profile Components** button on the left side.

Step 2 Select **Downloadable IP ACLs** from the Shared Profile Components menu.

Step 3 The following screen appears, click **Add**.

Step 4

Shared Profile Components

Select

Downloadable IP ACLs	
Name	Description
None Defined	

Step 4
Enter the downloadable ACL attributes specified in the table for our example.

Enter the **Name** and **Description** and click **Add**.

Enter the specified ACL syntax.

Click **Submit** after each downloadable ACL entry. Then Submit.

Repeat the above steps for each entry.

20.5 Configure Groups

Rename existing group numbers with a name to identify the posture (i.e. Healthy, Checkup, Quarantine, and Unknown). Then assign attributes for each group type, such as a downloadable ACL and actions presented to the client (message to display, URL redirect, timeouts). Use the following to configure the group settings for this example.

Group	Name	Downloadable IP ACL	Posture-token string
10	Healthy	Healthy	posture-token=Healthy
11	Checkup	Checkup	posture-token= Checkup
12	Quarantine	Quarantine	posture-token= Quarantine status-query=30 revalidation-timeout=300
13	Infected	Infected	posture-token=Infected
14	Unknown	Unknown	posture-token= Unknown

Complete these steps.

Step 1 From the ACS server, select **Group Setup** from the ACS admin screen.

Step 2 Select the group number that corresponds to the following conditions, click **Rename Group**, enter name and then click **Submit**.

Step 3 For each group perform the following:

- Select **Edit Settings**.

- Scroll down to the Downloadable ACLs window. Check the **Assign IP ACL** box and select the proper access list for the group condition.
- Then scroll down to the Cisco IOS/PIX RADIUS Attributes section and select (check) 009/001] cisco-av-pair. Enter the “**posture-token=string**” for the appropriate posture token (healthy, checkup, etc).

Group Setup

Click **Submit**.

After the last group entry click **Submit + Restart**

20.6 Configure a Clientless User

Configure a user ID named “clientless”. ACS will use this ID to specify what is returned to a host with no posture agent loaded.

Complete these steps.

From the ACS server, select **User Setup** from the left side of the ACS administration screen.

Enter a new user named **clientless** and click **Add/Edit**.

The user setup page appears.

Scroll down to user Setup and enter the same password that will be entered into the NAD for a clientless user. In our example **cisco123** and re-enter to confirm.

Scroll down to “Group to which the user is assigned” and select **Unknown**.

Click **Submit**.

20.7 Configure Global Authentication for EAP

Enable EAP-GTC and NAC.

Complete these steps.

- From the ACS server, select **System**

User Setup

The screenshot shows the 'User Setup' window with the following fields and options:

- Password Authentication:** A dropdown menu set to 'CiscoSecure Database'.
- CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.):** A text area.
- Password:** A text field with masked characters.
- Confirm Password:** A text field with masked characters.
- ☐ **Separate (CHAP/MS-CHAP/ARAP):** An unchecked checkbox.
- Password:** A text field.
- Confirm Password:** A text field.
- When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.** A descriptive text block.
- Group to which the user is assigned:** A dropdown menu set to 'Unknown'.

Configuration from the left side of the ACS administration screen.

- Select **Global Authentication Setup** from the System Configuration menu.
- Select (check) **Allow EAP-GTC**.
- Select (check) **Allow CNAC**.
- Click **Submit**.

20.8 Configure External User Database

Create an External User database to specify a set of mandatory credentials that ACS will look for.

In our example our network hosts are running the IBM ITSCM client application (agent). Therefore you must create a database to specify the mandatory credentials, a set of rules, and the actions that are returned by ACS.

Complete these steps.

20.8.1.1 Create the NAC Database

From the ACS server, select **External User Database** from the left side of the ACS administration screen.

At the External User Database menu, select **Database Configuration>Network Admission Control**.

Select **Create New Configuration**.

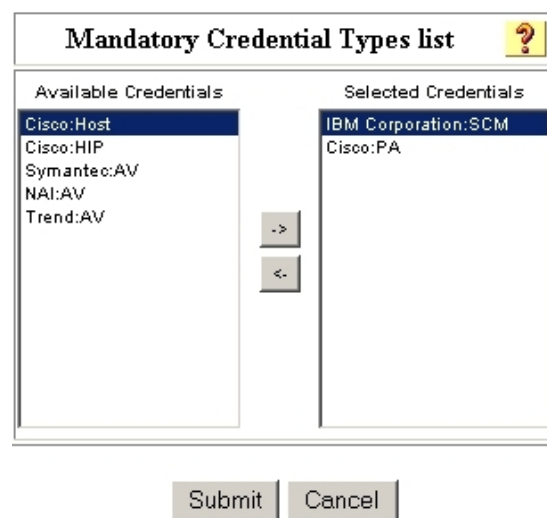
Enter the name for this iteration of the NAC database.

Click **Submit**.

Make sure the database name appears in the External Database Configuration window. Click **Configure**.

You will be presented with two windows; one asking for any mandatory credential types and another where you will configure the local (or external) rules for the credential validation policies. Click **Edit List**.

The 'Mandatory Credential Types List' window appears. Move the IBM and Cisco:PA credentials from Available to Selected Credentials.



Click **Submit**.

The Credential Type Configuration page displays with your settings. Scroll down to the bottom and click **Save Configuration**.

You are returned back to the External User Database main screen.

Then proceed to the next step.

20.8.1.2 Create the Local Policy

You should be at the External User Database main screen.

Step 1 Click Network Admission Control.

Step 2 In the External User Database Configuration window select the database and click **Configure**.

- Step 3** Under the Credential Validation Policies click **Local Policies**.
- Step 4** Click **New Local Policy**. The local policy Configuration screen displays.

Local Policy Configuration

Name:

Description:

Policy Rule List ?

Configurable Rules

No Rules

New Rule Up Down

Default Rule

Result Credential Type	Token	Action
CiscoPA	Unknown	

Submit Cancel

- Step 5** Enter the Rule name and a description.
- Step 6** Click **New Rule**.
- Step 7** A rule configuration screen displays.
- Step 8** Select the specified attribute, operator and value for the rule from the job aid table.
- Step 9** Once complete click **Submit**.
- Step 10** Repeat steps until all the rules for this policy has been created.

A simple rule set that checks the Policy Version attribute value for different platforms may look like the following:

Local Policy Configuration

Name:

Description:

Policy Rule List 

Configurable Rules

1	☐	Cisco:PA:OS-Type contains Windows 2000 IBM Corporation:SCM:Policy Version != SCM:NACPolicy V1.0 Win2000
		Result Credential Type Token Action
		IBM Corporation:SCM Quarantine PolicyVersion=V1.0Wi
2	☐	Cisco:PA:OS-Type contains Windows XP IBM Corporation:SCM:Policy Version != SCM:NACPolicy V1.0 WinXP
		Result Credential Type Token Action
		IBM Corporation:SCM Healthy PolicyVersion=V1.0Wi

Default Rule

Result Credential Type	Token	Action
IBM Corporation:SCM	Healthy	Default Rule

20.8.1.3 Configure User Group Mappings

Map a Posture Token to an ACS User Group. Also create posture agent messages to display to the users.

It is assumed that you are at the External User Database Configuration page. If not, select the following **External User Databases>Database Group Mappings**.

Token	User group	PA User Message
IBM ITSCM Database		
Healthy	Healthy	Welcome healthy user.
Checkup	Checkup	Checkup needed.
Quarantine	Quarantine	You are placed in quarantine.
Infected	Infected	You are identified as infected.
Unknown	Unknown	

Complete these steps.

- Step 1** From the External User Databases page click **Database Group Mapping**.
- Step 2** Click the CNAC database for this group mapping (i.e. IBM).
- Step 3** Select the User Group.
- Step 4** Enter the message that displays to users
- Step 5** Repeat steps 3 and 4 for each token.
- Step 6** Click Submit.

20.8.1.4 Configure Unknown User Policy

In this task map a Posture Token to an ACS User Group. Also create posture agent messages to display to the users.

It is assumed that you are at the External User Database Configuration page. If not, select the following **External User Databases>Network Admission Control**.

Complete these steps

From External User Databases click **Unknown User Policy**.

- Step 1** Make sure that the Check Box is checked. NAC will not work if this is not done. Then move the IBM Database to the Selected Databases column.
- Step 2** Click **Submit**.

21 IOS NAD Configuration for NAC

This will configure the basic settings to allow an administrator access to the necessary screens in order to configure NAC on the Cisco Router.

- Configure basic ACS administrator access for NAC

21.1.1 Setup

Before starting, verify the following:

- Step 1** Router is powered on.
- Step 2** Connect the serial cable to the router console port.
- Step 3** Configure your router with basic settings and assign the interfaces to match our topology.

Complete these steps.

21.1.1.1.1 *Access the Router*

From the ACS access **Hyperterminal**.

Enter the enable mode.

21.1.1.2 Configure AAA

In global config enter the following:

```
aaa new-model
aaa authentication eou default group radius
aaa authorization auth-proxy default group radius
ip admission inactivity-timer 10
```

21.1.1.3 Configure Radius Server

```
radius-server host 192.168.1.2
radius-server key radiuskey
ip radius source-interface FastEthernet0/0
```

21.1.1.4 Configure the Interface ACL facing the hosts

```
access-list 101 permit udp any host 192.168.150.1
```

Specify an ip admission Posture ACL

```
ip admission name NAC eapoudp
```

21.1.1.5 Configure Clientless Hosts

```
identity profile eapoudp
device authorize ip-address 192.168.150.2 policy NAC-CL
```

```

exit
identity policy NAC-CL
    access-group NACacl
Cisco1751(config-identity-policy)# exit
Cisco1751(config)#
ip access-list extended NACacl
permit ip any any
eou clientless username clientless
eou clientless password cisco123
eou allow clientless
eou timeout hold-period 60
eou timeout status-query 30
eou timeout revalidation 600

```

21.1.1.6 NAC Interface Configuration

```
interface x
```

If 1 port Ethernet card (WIC-1ENET) is used to interface the client, x is the Ethernet interfacing the host PC, like ethernet 0/0.

If 4 port Ethernet card (WIC-4ESW) is used to interface the client, x is the vlan interfacing the host PC, like vlan 2..

```
Cisco1751(config-if)# ip access-group 101 in
```

```
Cisco1751(config-if)# ip admission NAC
```

21.1.1.7 Enable Logging

```
eou logging
```

```
Cisco1751(config)# logging host 192.168.1.5
```

21.1.1.8 Install CTA

These steps you through installing Cisco Trust Agent (CTA) on a host PC.

- Step 1** Access one of the client machines, i.e. a system on the 192.168.150.0 network.
- Step 2** Run the CTA setup program. This might be **CTAsetup-1.053.exe**.
- Step 3** A CTA installation wizard appears stating it is installing. Click **Next**.
- Step 4** Accept the license agreement.
- Step 5** Accept the defaults by clicking **Next**.
- Step 6** A CTA pop up window appears stating the install is successful. Click **Ok** then **Finish**.
- Step 7** If you would like to verify CTA is running, go to Services and you should see CTA running. Click **Settings>Control Panel>Administrative tools>Services**.
- Step 8** Install the certificate that allows authorization to the ACS. The file ca.cer that was used on the server must exist locally on the client, in this case in the \Certs directory. Run the command


```
ctacert /add C:\Certs\ca.cer /store "Root"
```


You should see a prompt stating that the certification install was successful.
- Step 9** Copy the file %allusersprofile%\Applications\Cisco Systems\CiscoTrustAgent\ctalogd.tmp to ctalogd.ini.

22 Setup IBM ITSCM NAC Plug-in and Client

Complete these steps to install IBM ITSCM plugin to the host and interface with Cisco CTA.

- Step 1** Confirm CTA is installed on the host PC
- Step 2** Copy the following two posture plugin files into the “Program Files\Common Files\Cisco Systems\CiscoTrustAgent\Plugins\Install” folder:
 - Ibmnac6.dll
 - Ibmnac6.inf
- Step 3** Restart the CTA services.
- Step 4** Verify ACS and the router allows admission to healthy hosts while denying admission to non-compliant hosts.

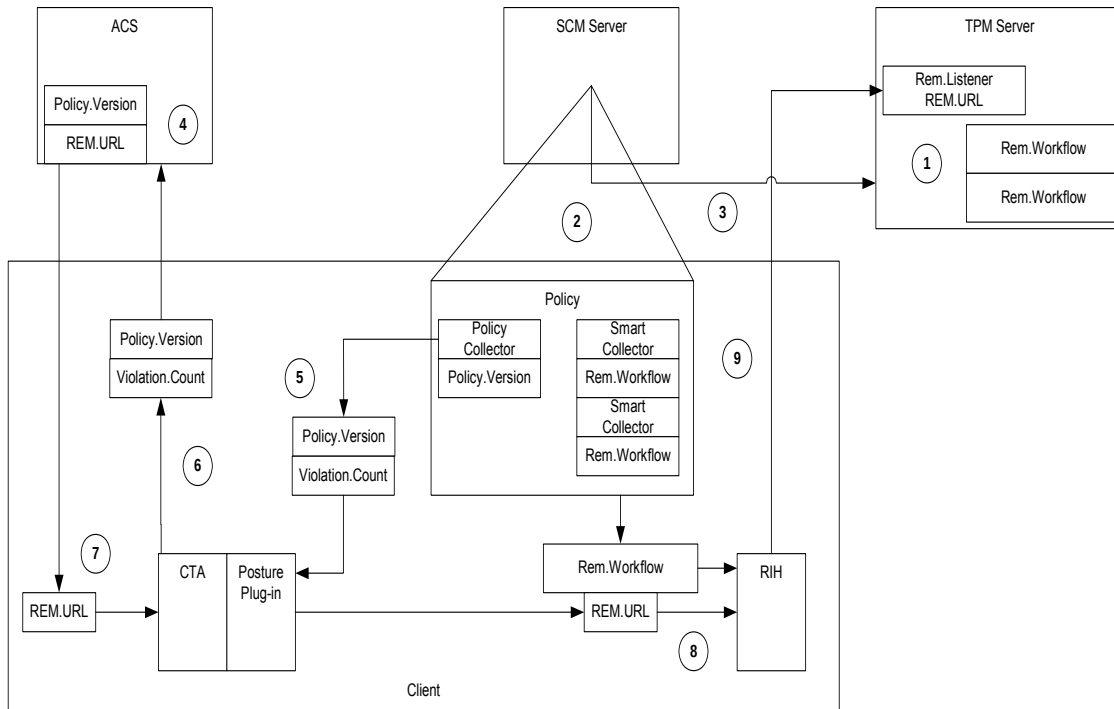
22.1 Putting it All Together - Creating and deploying a new TCR object

In order to create a new TCR object, you must first have a means to remediate violations and a way to detect violations. Remediation, using the TPM Server, is accomplished using Remediation workflows, so you must either identify an existing workflow capable of remediating the violation or provide a new workflow for remediation.

Detection is controlled using compliance policies defined at the ITSCM Server, which in turn use collectors to detect state on the client. You must identify a collector that can detect violations.

Once a suitable Remediation Workflow and Compliance Collector are identified, policies must be changed on the ITSCM Server and the ACM Server and a new policy remediation object must be created on the TPM Server to effect the change.

The following is a diagram and description of the steps required to configure the various sub-systems with information to handle the new TCR Object and the process by which this information will take effect.



1. TPM Server

A Remediation Workflow that will remediate violations must be provided and the name must be noted for entry in the ITSCM Policy. If the Remediation Workflow will use any files to be copied and/or executed on the client, these must be loaded onto the TPM Server and registered with the TPM Data Center Model.

The Remediation URL of the Remediation Listener that will provide access to this workflow must be noted for entry in the ACM Local Server Policy.

2. Compliance Policy

A Compliance Policy must be created or updated on the ITSCM Server. The policy must include a collector of appropriate type to detect violations. The collectors parameters must be configured with the values that will be checked against when making violation compliance decisions and the name of the Remediation Workflow that will remediate violations when detected as noted in (1) above.

Each Policy must include a Policy Collector. This collector must have its collector parameters updated for Policy_Version. The new value must be noted for entry in the ACM Server Local Policy.

The new Compliance Policy must have an object created that will be loaded onto clients by the TPM Server. To create such objects, the appropriate policy must be exported on the ITSCM Server and then converted into a "Client Policy File" (.cpf) using the createcpf utility on the ITSCM Server. The .cpf file is the object that will be loaded onto clients to remediate policy version.

3. TPM Server

The new Compliance Policy object (.cpf file) must be loaded and registered with the TPM DCM so that it can be loaded onto clients.

A well-known workflow for remediating policy objects should be provided with TCR. It should be noted here.

4. ACS Local Policy

The ACS Server's Local Policy for NAC must be updated with the new Policy_Version as noted at the ITSCM Server in (2) above.

The ACS Server's Local Policy for NAC must contain the Remediation URL of the Remediation Listener as noted in (1) above. In most cases this will already be correct in the policy, but it is noted here for first time installations.

1. Client to CTA

When a client is next queried by the CTA, the policy version reported on the client will be the one the client has been running.

2. CTA to ACS

The CTA will report this and it will not match the new Policy_Version defined on the ACS Server.

3. ACS to CTA

The ACS will send a quarantine notification with the Remediation URL of the Remediation Listener back to the CTA, and the client will be quarantined for Remediation.

4. Policy Collector to Remediation Handler

Upon notification from the CTA, the Policy Collector will pass the Remediation URL and a remediation request containing the name of the well-known workflow for remediating policy objects to the Remediation Initiation Handler.

5. Remediation Handler to Remediation Listener

The Remediation Handler will contact the TPM server asking for a policy update and the appropriate workflow will load the new policy object onto the client.

Formatted: Bullets and Numbering

Once this process has completed, the new policy object will include collectors to scan for the new TCR Object. These will run and a violation should now be detected. The violation will be remediated as in steps 5 – 9 above, and the healthy client will then be admitted onto the network.

22.2 Example Scenarios

22.2.1 HotFix

A new hotfix is available. All clients are to be updated with the new hotfix before admission to the corporate network.

1. TPM Server

- a. An executable to install the hotfix must be loaded onto the TPM Server and registered as a Software Patch using the TPM Web UI. It should be assigned a device driver type of TCRMSPatchInstall.
- b. Note the URL of the Remediation Listener

2. ITSCM Server

- a. Identify a Policy or Policies applicable to the clients that require the patch, or create a new one.
- b. Add a Compliance Object to the policy and name it appropriately. Assign it a PostureHotFix Collector.

- c. Set the PostureHotFixcollector parameters to indicate the HotFix ID, and to use TCRMSPatchInstall as the workflow. If a HotFix Collector already exists in the policy, simply add the new hotfix number to the list of values in the hotfix parameter.
- d. Update the collector parameters of the Policy Collector to change the Policy_Version parameter to a new value. Note this value for the ACS Server.
- e. Save the Policy.

3. ACS Server

- a. Select External Databases, Network Admission Control and select the correct instance and local policy for IBM ITSCM.
- b. In the local policy, change the rules that apply to the clients to specify the new Policy_Version noted in 2-d above.
- c. Save the changes.

22.2.2 Password Length

1. TPM Server

- a. Note the URL of the Remediation Listener

2. ITSCM Server

- a. Identify a Policy or Policies applicable to the clients that require the patch, or create a new one.
- b. Add a Compliance Object to the policy and name it appropriately. Assign it a PostureNetAccounts Collector.
- c. Set the PostureNetAccounts collector parameters to indicate the new password length, and to use TCRMinPasswordLen as the workflow. If a NetAccounts collector already exists in the policy, edit its parameters to specify the new password length and workflow name.
- d. Update the collector parameters of the Policy Collector to change the Policy_Version parameter to a new value. Note this value for the ACS Server.
- e. Save the Policy.

3. ACS Server

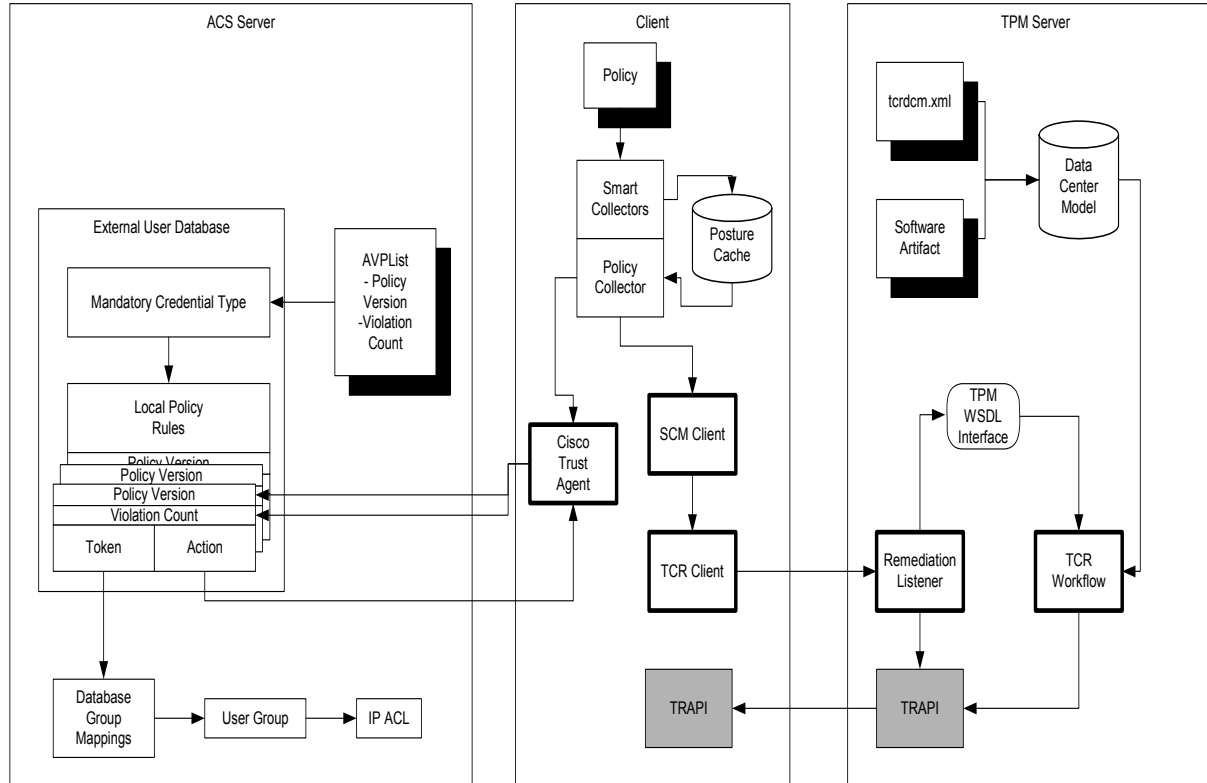
- a. Select External Databases, Network Admission Control and select the correct instance and local policy for IBM ITSCM.
- b. In the local policy, change the rules that apply to the clients to specify the new Policy_Version noted in 2-d above.
- c. Save the changes.

23 Troubleshooting the Deployment

Before troubleshooting a NAC deployment, it is extremely important to understand how NAC works and the sequence of events for a full NAC/Quarantine/Remediation/Compliance process. The previous section, **Putting it All Together - Creating and deploying a new TCR object**, provides a description of this process and should be read and understood before troubleshooting.

TCR-Specific Objects Attributes and Relationships

In order to debug a TCR Deployment, it is essential to understand the TCR objects, their function, their relationships, and the way in which attributes are configured within the objects to form relationships with other TCR objects. In the following Diagram, the Shadowed Boxes represent files or content that is imported to change the behaviour of the deployment. The heavily-lined boxes are software that is installed as part of the deployment. The grey boxes represent the TRAPI layer. The deployment description below refers to this diagram.



Deployment Description

In the preceding diagram, the first thing that would be done in the deployment would be to install the Software (Cisco Trust Agent, ITSCM Client, TCR Client, Remediation Listeners, TCR Workflows as well as TRAPI). Once the software is installed and configured to be able to communicate, the importable objects are imported to extend the solution. Finally, the installed and imported components must be configured to make the system perform in the desired manner.

Installed Software

Client

- **Cisco Trust Agent**
The Cisco Trust agent must be version 1.0.53 or above and must have the ACS Server's CA Certificate installed.
- **ITSCM Client**
The ITSCM Client must have ITSCM 5.1 Client + ITSCM Fix Pack 2 installed
- **TCR Client**
The TCR Client software is delivered and installed with the ITSCM Client software

TPM Server

- **Remediation Listener**
The Remediation Server is delivered as tcr.remediation.server.ear and is installed as an Enterprise App on WebSphere
- **TCR Workflows**
The TCR Workflows are delivered in the tcr.remediation.server.workflows.tcdriver file and are installed as standard TPM Workflows.

Imported Items

Client

- **ITSCM Policy**
Policy files are created on the ITSCM Server and exported for transfer and installation on clients. The ITSCM Policy contains all of the collectors and collector-specific parameters for a client.
- **TPM Server**
- **tcrdcm.xml**
This file is used to reinitialize the TPM Data Center Model. It should be edited to change the server name and IP Address to match the local deployment.
- **Software Artifacts**
These are files that will be used to perform the remediation actions on the clients. Examples are self-installing updates, exported ITSCM Policy files, etc. Anything that might be copied to a client to correct or update something must be registered with the TPM Data Center Model first so it can be accessed by the TCR Workflows.
- **ACS Server**
- **AVPList**
The AVPList.txt file provided by IBM must be registered with the ACS Server in order for the Mandatory Credentials for IBM ITSCM to be available to ACS policies. The provided file should register a Credential for IBM:ITSCM with two attributes: Policy_Version and Violation_Count.

Configuration

Client

- The client is configured with the address and port# of the ITSCM Server. It is setup as a DHCP type ITSCM Client and is assigned an alias.
- The client.pref file can be edited and the debugging levels changed.

TPM Server

- The Data Center Model is populated with items from the tcrdcm.xml file when the data center is reinitialized.

ACS Server

- The NAC External Database must be configured with local policies and rules to detect the registered attributes from the ITSCM Client and to determine a client's posture based on the values passed in the registered attributes.
- Each local rule can have a token and an action.
 - o The Token mapped to a User Group using the External Database Group Mapping feature.

- o Each User Group is assigned a downloadable IP ACL, which determines how the network will behave when a client is found to be in a certain state. Once a client's posture token has been determined, the client will become a member of the User Group that is mapped to the Posture Token. Each User Group can be assigned a Downloadable IP ACL which will determine how the network will treat clients that are assigned to the group.
- o The Actions defined for each local rule will be passed back to the client as the argument to a pnotify message. This argument is then processed by the client.

24 Hints, Tips, and Tools

24.1 General Notes

Before installing any of the SCM components it is important to check the latest information from the README.TXT that is shipped with the code, and the latest product Release notes. This is particularly important as the supported set of platforms for each SCM component, i.e. Server, Client, Admin GUI and Admin CLI are different.

24.2 DB2 Installation

On a Windows platform, ensure that you reboot the system after completing the DB2 installation, as you will probably get a jdbc error when trying to access the SCM Admin GUI for the first time.

During the installation of DB2 selecting the default installation options will be sufficient for an SCM installation. You do not need to create a DB2 instance as the installation of the SCM server will do this automatically. It is suggested to use the default user names (and groups in a UNIX installation) for all DB2 services. It would probably be a good idea to use the same password for all these services also.

24.3 SCM Server Installation

Before installing the SCM server component you need the following information:

- Name of an email server, and an email address to which server notices will be sent
- Server and client ports, the defaults are 1955 and 1950 respectively, it is recommended to use these defaults, unless they are already in use
- Passwords to be used for the master and server keystores. Note: During installation you will have the opportunity to stashing the server keystore password for automatic startup by checking a selection box. It is recommended that you check this box, as this will instruct the installation program to register the SCM server process as a Windows service, otherwise you will need to run the jacservic command to start and stop the SCM server service.
- The user id and password (with administration access) for communicating with the DB2 database
- For remote databases or Windows installations, you will need the location of the jar or zip containing the JDBC driver and the URL for database connectivity, for Windows this is c:\program files\sqllib\java\db2java.zip
 - i. By default SCM will install to /opt/IBM/SCM on AIX, and should not be installed on the root file system, therefore if /opt is on the root file system you will need to do one of the following:
 - ii. Create a separate file system for /opt
 - iii. Create a separate file system for /opt/IBM or /opt/IBM/SCM
 - iv. Create a symbolic link from /opt to /usr/opt
 - v. Create a symbolic link from /opt/IBM or /opt/IBM/SCM to some other file system

Execute one of the following to start the server installation wizard:

- For windows execute scm_win32.exe from the code source
- For AIX execute ./scm_aix.bin as the root user.
- For Solaris execute ./scm_solarisSparc.bin as the root user

When installing the SCM server on Solaris ensure that the file system used for temporary disk space, typically /var, is large enough for the installation, otherwise the installation

program will not be able to run. If the default file system for temporary disk space is less than 45 MB, you should specify another location on a file system with adequate disk space for temporary installation data to be stored, you can do this by specifying the temp directory, i.e.

`./scm_solarisSparc.bin`

- For Linux execute `./scm_linux.bin` as the root user
- When presented with the installation directory, `C:\Tivoli\SCM`, either accept this default or change. If more than one SCM component is to be installed on the same machine, you must use the *same* base install directory for each one.
- Ensure that the IBM SCM Server is selected to be installed, by default the SCM client is selected
- On the Server E-mail configuration page enter the Email server name and an email address to send server messages to. You cannot leave these fields blank, however, as long as the email address is in the correct format, i.e. `name@domain`, you can proceed.
- Enter the port numbers for the Server and client, or accept the defaults.
- Enter passwords for the master keystore password and the server keystore password
- Specify whether the database is local or remote
- In the Database configuration enter the database user id and password that SCM will use to connect to DB2
- Enter the location of the JDBC driver, usually `c:\program files\sqllib\java\db2java.zip`
- If you are using a local database you do not need to make any changes to the field labeled "URL to use for database connectivity". If the database is remote add the URL to this field
- If you are using a remote database you will be prompted on the next page to check that the JAC database has been created and that DB2 has been enabled to use the JDBC interface.
- Enter a user name and password for the SCM administrator
- Before installation begins you will be presented with some information about the configuration, i.e. the location SCM will be installed to and the components to be installed – i.e. the SCM server, and the SCM Database Configuration which is automatically selected for installation

24.4 Installing the SCM Client

SCM client – this component can be installed on AIX, Solaris, Windows 2000 Server, Windows Advanced Server, Windows 200 Professional, Windows XP Professional, Windows NT 4.0 Server and Workstation, Windows 2003 (Standard and Enterprise), Redhat Linux, Redhat Enterprise Linux, SUSE Linux, SUSE Enterprise Linux server.

Before installing, you should have the following information:

- The port numbers the client and server will be communicating over, this should be the same port numbers selected during the server installation.
- The communication mode – Push or pull. In push mode the client initiates communication with the server, in push mode the Server initiates communication with the client
- As with the Server installation, if the platform you are installing on is HP-UX (or Solaris?), you will need obtain the Java Runtime environment for that platform as it is not supplied with the SCM code

To begin the installation of the SCM client execute one of the following:

- For windows execute `scm_win32.exe` from the code source

- For AIX execute `./scm_aix.bin`.
- For Solaris execute `./scm_solarisSparc`.
- For Linux execute `./scm_linux.bin`.
- For HP-UX execute `./scm_hp11x.bin`.

Here is the procedure for installing the SCM client:

- i. When presented with the installation directory, `C:\Tivoli\SCM`, either accept this default or change. If this client is on the same machine as the Server, it must be installed in the same location as the server was.
- ii. Ensure the SCM client has been selected for installation, it should as it is the default
- iii. Enter the port number the client will be listening on, this should be the same port value specified for the client during the server installation
- iv. Select whether the Client will be running in Push or Pull mode. In Push mode communication can be initiated by either the client or server, in Pull mode the server will initiate communication. Why?
- v. If you select the Push mode, you will be prompted to enter the server name (or server IP address) and port number the server will be listening on. The port number should be the same as that specified for the server during the server installation. Also you will have the option of specifying whether the client uses DHCP to obtain its IP address, if this check box is selected you will need to enter a name that the server can use as a client for your DHCP client.

Note: If you select Push mode, then check the box to specify that the client uses DHCP, and then go back a couple of pages to change your option from Push to Pull mode, you will be prompted to enter a DHCP alias name, this is a bug in the beta code build, the workaround to this is to go back to the page where you select Push or Pull mode and select Push mode, click next for the next page and *unselect* the DHCP option, then go back one page and change your selection to Pull mode and continue.

24.5 Installing the SCM Administration Utilities

This component provides you with the SCM command line interface and if installed on a Windows platform it will also install the SCM Admin GUI. The admin GUI does not need to be installed on a machine with any other SCM components, the machine it is installed on will need TCP/IP connectivity to the SCM server machine.

24.6 Post Installation

After you have installed the server, the client, and the administration console or command line interface or both, be sure to install the Tivoli Security Compliance Manager collectors and policies from the product CD into a directory that the server can read and write to. See the *IBM Tivoli Security Compliance Manager Administration Guide* for more information about using the collectors.

After you have installed Tivoli Security Compliance Manager, it is important to review log space in DB2 to determine if you have adequate space for Tivoli Security Compliance Manager logging requirements. You must have administrator authority for DB2 to issue the following commands, which will enable you to review the logging requirements and make changes, if necessary.

The values in the following commands are the minimum size needed for a reasonably loaded system. If you are using a more heavily loaded system, you might need to increase the log file size and or the number of log files.

- i. To see the current DB2 settings, issue the command:

```
db2 get db cfg for JAC
```

- ii. To set the log file to 1000 4K pages, issue the command:

```
db2 update db config for JAC using LOGFILSIZ 1000
```

- iii. To set DB2 to use 10 circular log files, issue the command:

```
db2 update db config for JAC using LOGPRIMARY 10
```

- iv. After you make these changes, stop and then restart the server.

24.7 Installing an Email server

You would only need to install an email server if you are working on a demo/POC environment where you do not have access to a corporate email system. The ArGoSoft SMTP/POP3 mail server is a freeware product that is quick to install and configure, however it runs only on Windows platforms.

24.8 Configuration

There are two main configuration files which you can edit in order to modify SCM:

- client.pref (default path /opt/IBM/SCM/client/client.pref or C:\Tivoli\SCM\client\client.pref)
- server.ini (default path /opt/IBM/SCM/server/server.ini)

```
[JAC]
# Hostname or IP address of the server you wish to contact
jac_host=9.173.178.14

# Port number on the JAC server
jac_port=1955

# Port number the JAC server uses to contact the client with to execute commands
# Use -1 to allow RMI to choose
export_port=1950

# Type of client to act as
# PULL: Server contacts client first - Use for firewalls
# PUSH: Client contacts server first - More efficient
client_type=pull

# Print debug messages to STDOUT
debug=false

# Base directory of the client
base_directory=C:\Tivoli\SCM\client

# Once the number of messages in the queue > MAX_MESSAGES, the flush the queue
immediately
max_messages=100

# Don't allow more than MAX_QUEUE_SIZE messages in the queue
max_queue_size=200

# Time in milliseconds messages in the client queue are sent to the server
flusher_sleep_time=6000

# Time in milliseconds the client pings the server
pinger_sleep_time=60000
dhcp=false
#alias=dhcp9207.pic.uk.ibm.com
```

Figure 4, client.pref

The main settings you may need to modify are:

- `jac_host` this can either be the SCM server's name, or IP address. If the client is acting only as a proxy relay, the `jac_host` will be set to `localhost`, i.e. `jac-host=localhost`
- `export_port` this is the port that this client will be listening on, the default is 1950, but may be changed, need to be consistent with the definition for the client in the GUI
- `client_type` this is either pull or push. If you want to change the type of the client you will need to edit this value as well as the client setting from the GUI or CLI.
- `flusher_sleep_time` the SCM client stores data to be sent to the SCM server as messages in a queue, this value specifies the interval in milliseconds between sending each message. Typically in test scenarios you may want to decrease this value.
- `pinger_sleep_time` this is the time interval between client "pings" to the SCM server. The default is 60000 ms, i.e 10 minutes, again in a test environment you may want to decrease this value.
- `dhcp=false` this value can be either true or false. The omission of this value or commenting it out with a preceding `#` character is the same as setting the value to false.

Note: If a client is configured as a DHCP client in the client.prefs file, the IP address of the client machine can be changed without the client losing its registration to the SCM server. Note this feature is intended for use by client machines picking up an IP address from a DHCP server, however, it is functionally independent of DHCP, i.e. a machine with a static IP address can be registered as a DHCP client without any functional problems.

```
# #####
# General JAC parameters
# #####
# jac.debug - shows debug information
# jac.server.resolve.clients - if false JAC assumes UnicastRemoteObject.getClientHost returns an IP address.
#                               Set this to true if it returns a hostname instead
# jac.server.process_threads - Number of processing threads in the JAC server
# jac.server.no_activity_timeout - milliseconds before the server will consider a client inactive
# jac.server.dump_file - File used to store messages queued when the server shutdown
# jac.adminserver.separate_db_connection - if true each admin server object has it's own database connection
# jac.run_cleaners - if true, start the table cleaner thread
# jac.run_scheduled_queries - if true, start the scheduled queries thread
# jac.cleaner.sleep_time - milliseconds between table cleanings

bootstrap.services.filename=./services
jac.debug=false
jac.base_directory=C:\Tivoli\SCM\server\
jac.server.resolve_clients=false
jac.server.max_process_threads=20
jac.server.process_threads=5
jac.server.no_activity_timeout=300000
jac.server.dump_file=./server.dump
jac.cleaner.sleep_time=3600000
jac.data.tablespace=JAC_DTS
jac.index.tablespace=JAC_DTS
jac.data.noindex=false
jac.server.queue.high_wm=10000
jac.server.queue.low_wm=9500
jac.server.queue.scratch_directory=scratch/
jac.adminserver.max_token_age=30000
jac.server.exceptions_directory=exceptions/
client.pull.secret=secret
server.inactive_timeout=900000
db.serverpoolsize=5
db.adminpoolsize=5
jac.security.authenticator=com.ibm.jac.server.JACAuthenticator
#jac.security.authenticator=com.ibm.jac.server.CWAAuthenticator
```

```

#authenticator.cwa.ldaphost=
#authenticator.cwa.defaultdomain=

# DHCP Client Auto Registration - Uncomment to enable
#jac.dhcp_auto_register=true

# #####
# Mail parameters used by JAC when sending mail
# #####
# mail.smtp.host - Hostname of the SMTP server to send mail. Can be localhost if you has sendmail running loc
# mail.mailid - Specifies who to send mail as. This will be the "From" for JAC mailings

mail.smtp.host=secureway6.pic.uk.ibm.com
mail.mailid=user1@secureway6.pic.uk.ibm.com

# #####
# RMI parameters
# #####
# rmi.port - port the server listens for remote calls on
# rmi.debug - turns on RMI debugging. LOTS OF OUTPUT!

rmi.port=1955
rmi.debug=false
client.pull.listener.port=1950
export_port=1951

# #####
# Database parameters
# #####
# db.is_remote - if false connect to the database using the CLI. Otherwise use the network driver
# db.userid - userid to log onto the database
# db.password - database password for db.userid
# db.local.url - JDBC url of your local database
# db.remote.url - JDBC url of your remote database
# db.local.jdbc.driver - fully qualified class of the local JDBC driver. Make sure this is in your classpath
# db.remote.jdbc.driver - fully qualified class of the remote JDBC driver. Make sure this is in your classpath

db.is_remote=false
db.userid=db2admin
db.password=IyMjcGFzc3dvcmQ=
db.local.url=jdbc:db2:JAC
db.remote.url=jdbc:db2://localhost/JAC_REM
db.local.jdbc.driver=COM.ibm.db2.jdbc.app.DB2Driver
db.remote.jdbc.driver=COM.ibm.db2.jdbc.net.DB2Driver
db.enable.batch=false
db.default.max_age=720

# #####
# Security
# #####

keystore.directory=C:\Tivoli\SCM\server\keystores
provider.keystores=ibm.jks
provider.certs=ibm
provider.keystore.ibm.password=IyMjMTIzNDU2
server.keystore=server.jks
server.keystore.password=IyMjcGFzc3dvcmQ=
server.sslkey=sslcert
server.authkey=authcert
authorizer.max.keys=4
licensecert.password=IyMjbGljZW5zZW50cmQ=
auditcert.password=IyMjYXVkaXRjZXJ0

# SSL session cache size for push clients
server.session.cache.size=5000

# SSL session cache size for pull clients
client.session.cache.size=1000

# #####
# ACO Security Manager settings
# #####

aco.objectList=com.ibm.jac.server.JACClientImpl,com.ibm.jac.server.JACGroupImpl,com.ibm.jac.server.JACCollecto
aco.disableAccessChecks=false
bootstrap.services.filename=C:\Tivoli\SCM\server\services
jac.server_directory=C:\Tivoli\SCM\server\
db.jdbc_jar=D:\Program Files\IBM\SQLLIB\java\db2java.zip

```

Figure 5, server.ini

This configuration file is provided with comments for each setting, note that it has important information such as the location of password keystores, databases and the SMTP mail server, DB2 access information and debug settings.

Note the `jac_dhcp_auto_register` setting, this needs to be set to true if you want DHCP clients to get automatically registered at the SCM server.

24.9 Implementing a Proxy Agent

The basic steps to installing a proxy agent are as follows

- i. Install the SCM client on the machine where you want to run the proxy agent
- ii. During installation ensure that the client type is defined as PULL
- iii. Use the SCM GUI or CLI to Register this client on the SCM server
- iv. Add the `com.ibm.jac.server.JACProxy.jar` collector to the client. If this collector has not been installed into SCM yet, you would have to install, authorise and register it before this step
- v. Edit the proxy collector – do this from the Clients view, by right clicking on the collector field and selecting Edit Collector from the drop down menu. You will need to add INBOUND and OUTBOUND IP and port values for the proxy, e.g.

192.100.120.54/32:1960	INBOUND
192.100.120.2/16:1950	OUTBOUND
- vi. where in this case 32 and 16 specify net masks to apply to the IP address to define the range of address to accept/broadcast to, i.e. $32 = 4 \times 8$ (4 IP octets) therefore the mask applies to the whole IP address so that only traffic from the single IP address is accepted, so in this case only traffic from the SCM server, which has an address of 192.100.120.24, the proxy will be listening on port 1960. For the outbound traffic we have specified a netmask of 16, i.e. two octets, which means the traffic from the proxy agent, will be broadcast to IPs in the 192.100.X.X address range, the clients will all be listening on port 1950.
- vii. Select the proxy tab on the Admin GUI and right click in the lower panel and select Create Proxy from the menu.
- viii. Enter a meaningful name for the Proxy
- ix. Enter the IP address of the machine the proxy agent resides on
- x. Next, install and register the clients that will connect to the SCM server via the proxy. These clients need to be PULL clients also; Push clients are not supported for proxy operation. Existing clients may need their `client.pref` files modifying as well as configuration from the GUI
- xi. From the Client panel, click on the client name you wish to connect to the proxy. From the client configuration section click on the arrow by the Proxy field open a list with the names of available proxies, select the proxy and then click on the Save button.
- xii. Right click on the `com.ibm.jac.server.JACProxy` collector field (whilst still in the Clients panel), and select Run Collector now from the menu.

The client should connect to the SCM server via the proxy at the next “heartbeat”, if this does not occur try restarting the clients and server

24.10ACS Server

On the ACS Server web GUI, go to the reports section and look at the Passed Authentications and Failed Attempts reports.

The Failed Attempts report shows you instances where the NAC process was not completed successfully for some reason. The Authentication Failure Code column will give you an indication of what failed. Use this report to find details on why NAC challenges are not completing. This will typically lead you to something not right in your Cisco NAC setup, between the CTA, IOS NAD, and ACS Server.

The Passed Authentications report shows you NAC challenges that were completed successfully, even if the result was that the client was quarantined. If entries are being added to this report, your basic Cisco NAC Setup is probably okay and the hosts are being quarantined due to their compliance postures. At any rate, you can see the values passed up from the ITSCM Posture Plug-in for each host in this report.

24.11Cisco Trust Agent

On the client, the CTA handles all communications with the Cisco network. The accompanying file, ppta.exe, can be used to query the CTA to see what information it will be passing to the network. This file should be placed into the %CTA_HOME% directory and executed from there. When run, it will pop up a window. Click on the Update List button to display all of the registered Posture-Plugins on the system. You should see the IBM ITSCM plugin displayed in the list. Select the IBM plugin and click on the Posture Button. The attributes and values that will be passed to the network by the IBM plugin are displayed in the lower window. Make sure that these values are the expected values.

24.12IBM Tivoli Security Compliance Manager Client

- When the ITSCM Client is started, the ITSCM Policy Collector should listen for TCP connections on port 40500. If a **netstat -an** command is run in a command window and the line:
TCP 127.0.0.1:40500 0.0.0.0:0 LISTENING
Does **not** appear in the list of connections, then the ITSCM Client Policy Collector is not running correctly.
- If the client is listening on port 40500, you can telnet to the client and issue the same commands that the CTA would issue. In a command line window, issue the command
telnet localhost 40500
to establish a connection with the client.
These commands will allow you to see what is being passed back to the network, look at the complete posture cache and test calls to the Remediation handler.
The commands 'pquery' and 'pstatuschange' have no arguments.
 - pquery will display the current value of all defined posture attributes.
 - pstatuschange will display either true or false, which is how the network will determine whether the client's status has changed since the last pquery.The commands 'print' and 'runall' will display and refresh the posture cache.
 - print will show the full contents of the posture cache and is useful to see what the client sees as the state of your system.
 - Runall will run all of the collectors again and refresh the posture cache with fresh information.The command 'pnotify <REM_URL>' will fire up the remediation handler, with <REM_URL> being the URL of the remediation listener that will be called to handle the remediation request.

- Client Logging can be turned on by setting the property 'debug' to 'true' in the %SCM_HOME%\client\client.pref file. Once turned on, a file called 'client.log' will be created and updated in the %SCM_HOME%\client directory.

24.13 Remediation Client

- When the ITSCM Client is started, it will automatically start the remediation client's RemediationInitiationHandler. The remediation client will maintain a log file in the %SCM_HOME%\client directory called tcr.remediation.client.log. Log settings for the remediation client's logs can be changed by editing the file 'log4j.properties' in the tcr.remediation.client.jar file in the %SCM_HOME%\jars directory.

24.14 IBM Tivoli Provisioning Manager Server

- On the TPM Server web GUI, you can go to the System Config/Workflow Management tab and from there select Deployment Requests. This will bring up a report of all current deployment requests that have been or are being processed by the TPM Server.
 - o A typical TCR Remediation Thread will begin and end with deployment requests called TCRRegisterDevice and TCRUnregisterDevice. Any workflows called between these will be a remediation workflow, or various workflows to copy files to the client or execute commands on the client. So, a typical remediation would include a TCRRegisterDevice followed by remediation workflow such as "MSPatchInstall" followed by several file copying workflows, followed by several command execution workflows, followed by a TCRUnregisterDevice workflow. By following these steps in a remediation thread you can determine how far along the remediation got and potentially find error information back for each deployment request.
- In the %WEBSPPHERE_HOME%\appserver\logs\server1 directory, the ServerOut.log file will contain all of the logging information for both the TPM application and the tcr.remediation.server application.

25 Appendix 1

25.1 Reference Information

- IBM Tivoli Security Compliance Manager Overview
<http://www-306.ibm.com/software/tivoli/products/security-compliance-mgr/>
- IBM Tivoli Security Compliance Manager 5.1 Utilities
<http://www.ibm.com/support/docview.wss?uid=swg24007082>
- IBM Redbooks:
 - IBM Tivoli Security Compliance Manager SG24-6450-00
 - Building a Compliance based Network Admission Control and Remediation Solution SG22-6678-00
- IBM Tivoli Security Compliance Manager Product Documentation
<http://publib.boulder.ibm.com/tividd/td/IBMTivoliSecurityComplianceManager5.1.html>
- Automation package for IBM Integrated Security Solution for Cisco Networks
<http://www-18.lotus.com/wps/portal/automation/>