SIEMENS

Title:	**HiPath 4000 Assistant V4**
Subtitle:	**Security Checklist**
Document type:	
ID:	
File name:	**HP4kM V4 Security Checklist.doc**
Version:	**1.2**
Issue Date:	**2009-04-06**
State:	**Released**
Responsible:	***Corresponding Project Lead*** Martina Prikop ***Corresponding System Test Manager*** Anton Sudi
Department:	iSec 22

History of Change

Version	Date	Changes	Author(s)
0.1	2007-08-28	Draft for review	Werner Kühnert
0.2	2007-09-05	Reviewed, added chapter 6.3	Petr Jelen
1.0	2007-06-06	Released	Werner Kühnert
1.1	2008-10-08	Minor fixes	Petr Jelen
1.2	2008-10-08	Minor fixes	H. Holzastner

List of Authors

Team Member	Department	Function	Chapter
Werner Kühnert	iSec 22		
Petr Jelen	iSec 22		6.3
H. Holzastner	iSec 22		

Table of Content

1 GENERAL INFORMATION

This Security Checklist is provided in order to create the prerequisites in the service to install all Siemens and certified 3rd party components of HiPath 4000 Assistant V5 corresponding to the current security requirements.

This Security Checklist supports the service technicians and re-sellers and consulting in the examination and setting of the required security measures in the software and at the hardware for HiPath 4000 Assistant V5.

The current security settings are to be confirmed by the customer by means of signature in the delivery of HiPath 4000 Assistant V5.

The Security Checklist includes information on settings of:

- Hardware,
- operating system,
- HiPath 4000 Assistant,
- extending software,
- 3rd party software.

Deviations of the security settings on customer wish are to be documented.

2 Customer Data and Signatures

Please provide information on the customer here.

Customer	
Name	
Address	
Contact Person Product	
Contact Person Security	

Please provide information on the Siemens service technician here.

Siemens	
Service Technician	
Address	
Phone	
Email	

Please provide information on all performed security checks here.

Performed Security Checks		
Date	**Signature Customer**	**Signature Siemens Service Technician**

3 Hardware Settings

Hardware Settings	
Component	HiPath 4000 Assistant
Necessary Settings	There are no necessary security hardware settings known now.
Description	
Accomplished	N/A
Notes	

Accomplished	
Notes	

4 Operating System

4.1 Operating System Installation

Operating System	
Sub Component	Operating System
Settings	There are no necessary security operating system settings known now.
Description	The operating system used for HiPath 4000 Assistant V5 is SCO UnixWare 7.1.4, Maintenance pack 3 The Operating system has been installed automatically.
Accomplished	N/A
Notes	

4.2 Disable PPP

Services Settings	
Sub Component	PPP
Settings	
Description	1. procadmin –t –d pppd 2. ppptalk stop To disable PPP permanently the file /etc/rc2.d/S71ppp has to be renamed or removed. Please note, that no PPP connection to the system will be possible after you disable PPP. LAN connectivity is not affected.
Accomplished	
Notes	

4.3 Disable PPTP

Services Settings	
Sub Component	PPTP
Settings	
Description	3. procadmin –t –d pptpc 4. /etc/init.d/pptp stop To disable PPP permanently the file /etc/rc2.d/S72pptp has to be renamed or removed.
Accomplished	
Notes	

4.4 Close unused IP ports

By default all unused IP ports should be closed.

Port 21 ftp	
Settings	1. Edit the file /etc/inetd.conf and comment out all lines containing ftp 2. execute “sacadm –k –p inetd” and then “sacadm –s –p inetd” to activate the changes made in the file /etc/inetd.conf
Explanation	Port 21 is used for ftp service. If the system does not use this service the port does not have to be opened because both authentication and data are transferred in plaintext.
Description	Evaluate if ftp is required by any 3rd party component. It is recommended to disable ftp at all and use scp instead.
Additional Information	
Accomplished	
Notes	
Port 23 telnet	
Settings	In order to change the default configuration, edit the host access configuration files: /etc/inet/hosts.allow (daemon,client) pairs that are granted access. /etc/inet/hosts.deny (daemon,client) pairs that are denied access. See also: man hosts_access

Explanation	
Description	Access to telnet (port 23) from extern is disabled by tcp wrappers by default. It is recommended to use ssh instead.
Additional Information	
Accomplished	
Notes	
Port 512 Remote Process Execution	
Settings	1. Edit the file /etc/inetd.conf and comment out all lines containing exec. 2. execute “sacadm –k –p inetd” and “sacadm –s –p inetd” to activate the changes made to the file /etc/inetd.conf
Explanation	Port 512 is used for 3rd party components rexec access to HiPath 4000 Assistant. This solution brings a risk because arbitrary programs may be executed.
Description	rexec is disabled by default.
Additional Information	
Accomplished	
Notes	
Port 513 Remote Login	
Settings	1. Edit the file /etc/inetd.conf and comment out all lines containing login 2. execute “sacadm –k –p inetd” and “sacadm –s –p inetd” to activate the changes made to the file /etc/inetd.conf
Explanation	Port 513 is used for 3rd part components rlogin access to HiPath 4000 Assistants.
Description	rlogin is disabled by default.
Additional Information	
Accomplished	
Notes	
Port 514 Remote Shell	
Settings	1. Edit the file /etc/inetd.conf and comment out all lines containing shell 2. execute “sacadm –k –p inetd” and “sacadm –s –p inetd” to activate the changes made to the file /etc/inetd.conf

Explanation	Port 514 is used for 3rd part components remote shell access to HiPath 4000 Assistants.
Description	rsh is disabled by default.
Additional Information	
Accomplished	
Notes	

5 Extending and 3rd Party Software

This list provides an overview over Siemens HiPath extending software and 3rd party components in which a security settings must be done. It has to be outlined if the component is installed or not.

3rd Party Software			
Component	**Version**	**Installed**	**Notes**
Apache Web Server	1.3.37	YES	
Informix DB	7.25.UC1	YES	

5.1 Component Settings for Apache Web Server

Apache Web Server Settings	
Settings	Provide own key material for SSL if possible.
Explanation	Since the web-server certificate and its private key are part of the general installation CD, each customer gets the same key material. Furthermore, SSL authentication of clients is not supported, but web server authentication only. Therefore, this key material is not used for authentication. Instead, SSL is used for encryption only.
Description	Evaluate if you need to use: - a self signed certificate [skip to A] or - an imported certificate signed by CA [skip to B] or - a certificate signed by an official CA and generated via CSR [skip to C]. A. Self signed certificate 1. Generate a certificate 1) On the **Start Page** of **Access Management** navigate to **Manage Web Server Certificates → Certificates for this Web Server**. 2) Double click **Generate**. 3) Click on **New Certificate** button. 4) Enter all required data, and click on **Continue** button. 5) The program goes back to the **Activate Server Certificate** dialog. 2. Activate the generated certificated 1) Select the generated certificate in the **Overview of all**

certificates that can be activated list.

2) Click on **Continue** button.
3) Enter the Password for the private key, if required, and click on **Activate Certificate** button.
4) Click **OK** button on the showed message box.

B. Imported certificate signed by CA

1. Import a certificate
    1) On the **Start Page** of **Access Management** navigate to **Manage Web Server Certificates → Certificates for this Web Server**.
    2) Double click **Import**.
    3) Enter the appropriate file name.
    4) Enter the **Password** for the private key.
    5) Click **Import**.
    6) The program goes back to the **Activate Server Certificate** dialog.
2. Activate the imported certificated
    1) Select the imported certificate in the **Overview of all certificates that can be activated** list.
    2) Click on **Continue** button.
    3) Enter the Password for the private key, if required, and click on **Activate Certificate** button.
    4) Click **OK** button on the showed message box.

C. Certificate signed by an official CA and generated via CSR

1. Generate a certificate
    1) On the **Start Page** of **Access Management** navigate to **Manage Web Server Certificates → Certificates for this Web Server**.
    2) Double click **Generate via CSR**.
    3) Click on **Generate New Certificate Request** button.
    4) Enter all required data, and click on **Continue** button.
    5) The confirmation message is shown. Click **Continue** button.
2. Test the certificate
    1) Click the **Test** icon in the **Action** column of the table displayed in the **Generate Certificate via CSR** dialog.
    2) After successful testing **the Activate Server Certificate** dialog is opened again.
3. Export the certificate
    1) Click the **Export** icon in the **Action** column of the table

	displayed in the **Generate Certificate via CSR** dialog. 2) Copy the CSR with Copy & Paste or export CSR to file. 4. Send the exported CSR to your Certificate Authority for signing purposes. 5. Import the signed certificate 1) Click the **Import** icon in the **Action** column of the table displayed in the **Generate Certificate via CSR** dialog. 2) Copy the content of the signed certificate with Copy & Paste or import the signed certificate from file. 3) Enter the **Password** for private key and click on **Continue**. 6. Activate the signed certificate 1) Click the **Activate** icon in the **Action** column of the table displayed in the **Generate Certificate via CSR** dialog. Once you click **Activate** icon the web server is restarted automatically.
Additional Information	[Access Management, Chapter 2.11.1, pp. 2-114 – 2-145]
Accomplished	
Notes	

5.2 Component Settings for Report Generator

Component	Informix DB / Report Generator
Settings	1. Change default password for account *u_repgen*. 2a. If Report Generator is not used lock account *u_repgen*. 2b. Else install clients which run custom reports preferably on the same LAN segment as HiPath 4000 Manager Server. Distribute to the clients password of the *u_repgen* account.
Explanation	The *u_repgen* account is created on the Informix RDBMS to establish ODBC access from Report Generator which is a Siemens component. Client connects to Informix DB via ODBC. The traffic is not secure. All data including authentication are transferred as a plaintext. Clients use *u_repgen* account which is configured for read-only access.
Description	By default *u_repgen* account is locked. Open and use this account only if customized reports are used. 1. On the **Start Page** of **Access Management** navigate to **Account Management → System Account Administration**. 2. Select *u_repgen* account. 3. Enter a new password in **New password** and **Retype Password** fields.

	4. Evaluate if Report Generator is used i. If YES install clients which run creation of custom reports preferably on the same LAN segment as HiPath 4000 Manager Server. ii. If NOT lock *u_repgen* account with **Lock user account** checkbox.
Additional Information	[Access Management, Chapter 2.7.1, pp. 2-48 – 2-50; Chapter 3.3, pp. 3-8 – 3-12]
Accomplished	
Notes	

5.3 Component Settings for 3rd party components connecting to Informix DB

Component	Informix DB / 3rd party components connecting to Informix DB
Settings	1. Change default passwords for accounts *uas_read*, *uas_rdwr*. 2a. If no 3rd party component connecting to Informix DB is used lock accounts *uas_read* and/or *uas_rdwr*. 2b. Else install 3rd party component on the same LAN segment as the HiPath 4000 Manager Server. Evaluate if 3rd party component needs read-only or read-write access to data stored on Informix DB and distribute to the component supplier the password of either *uas_read* or *uas_rdwr* account.
Explanation	The *uas_read* and *uas_rdwr* accounts are created on the Informix RDBMS to establish ODBC/JDBC access from 3rd party components. 3rd party components connect to Informix DB via ODBC/JDBC. The traffic is not secure. All data including authentication are transferred as a plaintext.
Description	By default *uas_read* and *uas_rdwr* accounts are locked. Open and use these accounts only if 3rd party components are used. 1. On the **Start Page** of **Access Management** navigate to **Account Management → System Account Administration**. 2. Select *uas_read* and/or *uas_rdwr* accounts. 3. Enter a new password in **New password** and **Retype Password** fields. 4. If 3rd party components are not used lock *uas_read* and/or *uas_rdwr* accounts with **Lock user account** checkbox. 5. Distribute *uas_read* and *uas_rdwr* accounts' passwords to 3rd party components according to documentation obtained from components' suppliers.

Additional Information	[Access Management, Chapter 2.7.1, pp. 2-48 – 2-50; Chapter 3.3, pp. 3-8 – 3-12]
Accomplished	
Notes	

6 HiPath 4000 Assistant

6.1 Change predefined passwords for accounts

HiPath 4000 Manager	
Sub Component	Administrator Accounts
Settings	Change default passwords for *engr*, *rsta*, *rsca* and *cusa* accounts.
Explanation	During the installation all accounts are created with default passwords which are generally known. Thus, all passwords need to be changed upon first usage of the corresponding account.
Description	The user is asked to change the password during the first log in with *engr* account. For each of the three other accounts separately: 1. On the **Start Page** of **Access Management** navigate to **Account Management → System Account Administration**. *2.* Select an account. 3. Enter a new password in **New password** and **Retype Password** fields. 4. Evaluate if all the accounts are necessary for administration. If not lock unused accounts. For information on these accounts see [Access Management, Chapter 1.2.1, pp. 1-5 – 1-6].
Additional Information	[Access Management, Chapter 2.7.1, pp. 2-48 – 2-50; Chapter 3.3, pp. 3-8 – 3-12]
Accomplished	
Notes	

6.2 Change predefined passwords for NSL accounts

HiPath 4000 Manager	
Sub Component	Administrator Accounts
Settings	Change default passwords for NSL accounts – *nsl-syst, nsl-engr, nsl-rsta, nsl-rsca, nsl-cusa and nsl-cust accounts.*
Explanation	NSL accounts are used for secure user-independent access. E.g. communication between Manager and Assistant. During the installation all NSL accounts are created with default empty password. Thus, all

	passwords need to be changed to prevent unauthorized access to system.
Description	NSL accounts are not used for interactive login to system. For each of these accounts do separately: 1. On the **Start Page** of **Access Management** navigate to **Account Management** → **System Account Administration**. *2.* Select an account. 3. Enter a new password in **New password** and **Retype Password** fields.
Additional Information	[Access Management, Chapter 2.7.1; Chapter 3.3]
Accomplished	
Notes	NSL accounts are usually used for connection from Manager to asigned Assistant. When you change NSL passwords on Assistant, don't forget to change corresponding passwords on Manager in **System Management** → **HiPath 4000 /Hicom 300 Administration** → corresponding Assistant → enable **Access Management** checkbox and select **Access Management** tabsheet → **Set Passwords for Network Single Logon**

6.3 Create administrator accounts and assign privileges

HiPath 4000 Manager	
Sub Component	Administrator Accounts
Settings	Create administrator accounts for customer administrators if needed and assign appropriate access rights.
Explanation	You can create individual administrator accounts and assign them appropriate access rights. This enable to manage user access to HiPath 4000 Management and accommodate users with sufficient rights.
Description	1. On the **Start Page** of **Access Management** navigate to **Account Management** → **User Account Administration**. 2. For each new user account do: a. Select **User** → **Add …** in menu. b. Enter user name and description. c. Set password and/or password properties. 3. On the **Start Page** of **Access Management** navigate to **Account Management** → **Access Right Configuration**. 4. For each new user account do:

	a. Select user in **Users** list. b. Select access rights in **Access Rights Groups** list to be assigned to the selected user. c. Select **Assign** in context menu. d. Check in the **Users** list that the access rights were assigned.
Additional Information	[Access Management, Chapter 2.6, pp. 2-28 – 2-43; Chapter 3.3, pp. 3-8 – 3-12]
Accomplished	
Notes	

6.4 Turn off unused applications

HiPath 4000 Manager	
Sub Component	Application control
Settings	Disable applications which are not used by the customer or service.
Explanation	You can create individual administrator accounts and assign them appropriate access rights. This enable to manage user access to HiPath 4000 Management and accommodate users with sufficient rights.
Description	1. On the Start Page of **Base Administration** navigate to **Application Control**. 2. Uncheck the applications, which are not used, for sure. 3. Click Submit when you are finished with the selection. The unchecked applications will be disabled. You can enable them later, if necessary.
Additional Information	
Accomplished	
Notes	

7 Security Patches

Security patches will be added to new HD’s. No dedicated installation is required.

Bibliography

/Access Management/	HiPath 4000 Management V5 Access Management (Assistant/Manager) Help. Siemens AG. 2008.
/Installation Manual/	HiPath 4000 Manager V5 Installation and Service Manual. Siemens AG. 2008.
/Installation Guide/	HiPath 4000 Manager V5 Installation Guide. Siemens AG. 2008.
/Unix Base Administration/	HiPath 4000 Management V5 Unix Base Administration Help. Siemens AG. 2008.

Abbreviations / Definitions / Glossary / Terminology

Abbreviation	Definition
BIOS	Basic Input-Output System
CA	Certification Authority
CMOS	Complementary Metal Oxide Semiconductor
CSR	Certificate Signing Request
DB	Database
DTB	HiPath Display Telephone Book
FTP	File Transfer Protocol
HP FM	HiPath Fault Management
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
JDBC	Java Database Connectivity
LAN	Local Area Network
N/A	Not Applicable
ODBC	Open Database Connectivity
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RDBMS	Relational Database Management System
RMI	Remote Method Invocation
SLES9	SuSE Linux Enterprise Server 9
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Smart Switch Over
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Appendix A: Used TCP/IP Ports

HiPath 4000 Assistant V5 portlist is published in an independent document.

Appendix B: Installed Services

See [Installation Manual, Chapter 3.11, p. 3-24] for verifying successful starting of processes and components.