IBM Systems Director Service and Support Manager Security Considerations

November 2010

Version 1.0

Authors: Erwin Early, Sebastian Fuhrer, and Mario Lorenzo

If you have comments on this paper, please send them to sefuhrer@us.ibm.com

1 INTRODUCTION

Service and Support Manager 6.2.1 is a plug-in for IBM Systems Director 6.2.1. Service and Support Manager automatically detects serviceable hardware problems and securely collects supporting data for serviceable hardware problems that occur on your monitored endpoint systems. Electronic Service Agent is a call-home tool that is integrated with Service and Support Manager. Electronic Service Agent securely transmits serviceable hardware problems and associated support files, as well as system inventory and system status updates, Performance Management data, and quality software data to IBM support.

Service and Support Manager includes the following features:

- Once installed Service and Support Manager will start to monitor all eligible endpoint systems within your IBM Systems Director environment for serviceable hardware problems.
- Upon activation, Service and Support Manager will use the embedded Electronic Service Agent tool to transmit serviceable hardware problems and support files, inventory, system status updates, Performance Management data, and quality software data to IBM support.
- Collects and securely sends scheduled system inventory files to IBM. Inventory information is available to IBM support representatives when they are solving reported problems. The inventory data is persistent and can be viewed by authorized IBM personnel as well as by the customer through the electronic support portal. The electronic support portal is an IBM web application.
- Diagnostic data is collected and securely reported to IBM based on a problem that has been detected by Service and Support Manager. When a serviceable hardware problem is detected additional data is collected and securely transmitted to IBM support. Support files can include extended error data or problem determination data.
- Communicates with IBM support using a secure Internet connection using encryption and authentication.

1.1 Document Purpose

The purpose of this document is to provide information to the IT professional responsible for ensuring that customer data is:

- Transmitted securely between monitored endpoint systems and the IBM Systems Director management server
- Securely stored in on the IBM Systems Director management server or remote database.
- Transmitted securely by Service and Support Manager to IBM support for diagnostic purposes.
- Securely stored by IBM support after it is received.
- Accessible to only those who are authorized by the customer to view it.

This document assumes a basic understanding of both IBM Systems Director and Service and Support Manager. For a more detailed understanding of Service and Support Manager, including overviews of the product and both problem and inventory reporting, refer to section 1.4 *References*.

This document only applies to version 6.2.1 of Service and Support Manager.

1.2 Intended Audience

This document is intended for IT professionals responsible for the security and data assurance of their companies systems.

1.3 Terms

Term	Definition
Monitored endpoint system	A system that has been discovered by IBM Systems Director and is eligible for monitoring by Service and Support Manager. Service and Support Manager will automatically detect and report serviceable hardware problems to IBM support.
Electronic Service Agent	Electronic Service Agent is a call-home tool that is embedded within Service and Support Manager. Electronic Service Agent securely transmits serviceable hardware problems and associated support files, system inventory, Performance Management data, and quality software data to IBM support.
Serviceable hardware problem	Service and Support Manager monitors for many different error conditions that can occur on your monitored endpoint systems. For example, if a fan error occurs on a monitored system, Service and Support Manager will detect this error and consider it to be a serviceable hardware problem that should be reported to IBM support.

1.4 References

The information in this document is current as of the time of publication; however, as with any software product changes can and do happen over time. For the most up to date information, the reader is encouraged to use the following references:

- IBM Systems Director Service and Support Manager 6.2.1 Information Center: http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp?topic=/com.ibm.esa.director.help/esa_kickoff.html

- Preparing firewalls and proxies for IBM Systems Director http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.install.helps.doc/fqm0_t_preparing_firewalls_and_proxies.html

- Ports for IBM Systems Director Server http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.plan.helps.doc/fqm0_r_all_available_ports.html

- Planning IBM Systems Director security http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.plan.helps.doc/fqm0_t_planning_security.html

- IBM Systems Director security http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.security.helps.doc/fqm0_c_security.html

2 Service and Support Manager security

The subsequent sections of this document cover three primary aspects of security as it relates to Service and Support Manager:

1. **Secure data collection and storage:**
   This section describes how service data and information is collected and stored on the IBM Systems Director management server. This section also details how serviceable hardware problems and associated support file data, and inventory data are securely stored after they are transmitted to IBM support.

2. **Secure data transmission:**
   This section describes how SSM uses a secure connection to monitor, detect, and transmit service data and support file data from monitored end-point systems to the IBM Systems Director management server. Additionally, this section describes how the embedded Electronic Service Agent tool uses a securely encrypted connection to transmit problems and associated support files, inventory, Performance Management data, and quality software data to IBM support.

3. **Customer data and information privacy:**
   This section describes how IBM protects your private customer data, and describes who has access to your private information.

2.1.1 Secure Data collection and storage

This section describes the different kinds of service data collected by Service and Support Manager and IBM Systems Director, and describes how data is securely stored on the IBM Systems Director management server. This section also describes how IBM support continues to securely store problems and associated support file data, inventory data, system status updates, Performance Management data, and quality software data after these data types are received by IBM support.

2.1.1.1 Data collected and stored on the local IBM Systems Director management server

Service and Support Manager stores collected service data on the IBM Systems Director management server.

Note: When IBM Systems Director is initially configured, the customer can choose which database to use to store content. By default IBM Systems Director uses an Apache Derby database; however, customers can configure a custom local or remote database using an IBM DB2, Microsoft SQL Server, Microsoft SQL Server Express, or Oracle® database.

The default Apache Derby database uses a simple common ID and Password for security, and content stored within the Apache Derby database is not encrypted by default. To encrypt the password for the default database see the following topic: http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.security.helps.doc/fqm0_t_encrypting_passwords_for_database_configuration.html

To enable a more secure environment, customers may want to set up a remote database that meets their security expectations. For more information, see the following topic: http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.install.helps.doc/fqm0_t_install_config_database_application.html

The following table describes how different types of data are collected and stored by Service and Support Manager:

Type	Description	Storage
Serviceable hardware problem	When a serviceable hardware problem occurs on a monitored endpoint system, Service and Support Manager automatically detects the problem data. For more information see the following topic: http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.esa.director.help/esa_problem_flow.html	Service and Support Manager creates and maintains multiple table entries in the in the IBM Systems Director management server local database. By default this is an Apache Derby database, however, customers can configure a custom local or remote database using an IBM DB2, Microsoft SQL Server, Microsoft SQL Server Express, or Oracle® database. In addition to the tables created by Service and Support Manager in the IBM Systems Director database, the initial problem event and subsequent event log updates displayed in the IBM Systems Director event log are stored as a binary file on the local management server. These events contain notifications that detail the success and failure of the detection, collection, and transmission of serviceable hardware problems.
Support file	When a serviceable hardware problem occurs on a monitored endpoint system, Service and Support Manager automatically detects the problem and collects hardware problem data from the monitored endpoint system and stores this data in the form of a support file that can later be transmitted to the IBM service provider	All collected support file data is stored in a local repository called the Support File Cache located on the IBM Systems management server. This repository is a folder

	for diagnostic purposes. The type of data collector used and contents of the support file is determined by the operating system of the monitored endpoint system. Support files can contain detailed system information, event logs, and more. For more information on the data collectors Service and Support Manger uses, and the kinds of data these collectors collect, see the following topic: http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.esa.director.help/service_and_support_settings_data_collectors_help.html	directory created on the local management server. This location is not encrypted.
Inventory	IBM Systems Director management server establishes connections with network-level resources, such as computers, switches, or printers, that have already been discovered and collects data about the hardware and software that is currently installed on those resources such as physical, logical, and virtual hardware; software applications, operating systems, middleware, firmware, BIOS, and diagnostic information; network information; and system-contained resources. For more information about inventory, see the following topic: http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.esa.director.help/esa_inventory_flow.html	Collected inventory is stored in the IBM Systems Director management server local database. By default this is an Apache Derby database, however, customers can configure a custom local or remote database using an IBM DB2, Microsoft SQL Server, Microsoft SQL Server Express, or Oracle® database.
System status updates	In addition to inventory collected by IBM Systems Director, Service and Support Manager also collects and transmits regularly scheduled status updates to IBM support. These reports provide IBM support with high-level information on the health and status of monitored endpoint systems.	Data such as machine type, model, and host name of the monitored systems are stored in an xml file. This file is stored locally on the IBM Systems Director management server and is not encrypted.
Performance Management data	Performance Management collects system utilization, performance statistics and hardware configuration information. Service and Support Manager collects Performance Management data from eligible Power Systems™ with an AIX® operating system. For more information see the following topic: http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.esa.director.help/esa_performance_management.html	Performance Management data is collected and stored on the Power Systems endpoint. When requested or scheduled, Service and Support Manager will transmit this data to IBM support. Service and Support Manager stores this data in binary form in a temporary directory and deletes this data after 7 days. This location is not encrypted.
Quality software data	Service and Support Manager can provide software quality data to IBM support for analysis.	Quality software data consists of logs stored as text files in the following location on the

	When the transmission of software quality data is enabled, Electronic Service Agent will transmit software logs to IBM support. These software logs are a collection of informational logs gathered by IBM Systems Director when a software quality event occurs on the IBM Systems Director management server. These logs are used to improve the functionality of the overall product and aid IBM in enhancing future releases of IBM Systems Director. This service does not provide software quality data for monitored endpoint systems. For more information see the following topic http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp?topic=/com.ibm.esa.director.help/esa_quality_data.html	IBM Systems Director management server: /director/data/ffdc/logs This directory is not encrypted.

2.1.1.2 Data stored by IBM support

After data is transmitted to IBM, that data is stored in different secure locations depending on the type of data that IBM support received.

Serviceable hardware problem (problem diagnostic), support files, and quality software data are sent to a secure IBM file repository called Testcase Data Exchange (https://testcase.boulder.ibm.com/). The Testcase Data Exchange file repository uses ACL authentication and authorization to control access to data. The data on Testcase is periodically purged by IBM and therefore has a short lifetime on this repository. The average lifetime of a file residing on Testcase is two weeks. Data stored on Testcase can be accessed by authorized IBM support personnel to assist in the diagnostic and troubleshooting of hardware problems or quality issues.

Inventory data and system status updates are handled through a different file exchange mechanism. This data (which includes Software and Hardware data) is transferred as inline data via HTTP over SSL (HTTPS). This data is stored as raw bulk data into a secure IBM support Database. Access to this database system is ACL controlled and database access is restricted to authorized IBM support Personnel.

2.1.2 Secure data transmission

This section describes how Service and Support Manager uses a secure connection to monitor, detect, and transmit service data and support file data from monitored endpoint systems to the IBM Systems Director management server. This section also describes how the embedded Electronic Service Agent tool uses a securely encrypted connection to transmit problems and associated support files, inventory, system status updates, Performance Management data, and quality software data to IBM support, and how Service and Support Manger downloads configuration updates from IBM support.

2.1.2.1 Data transmitted between Service and Support Manager and IBM Systems Director monitored endpoint systems

When Service and Support Manager automatically detects a serviceable hardware problem on a monitored endpoint system, it uses different data collection services depending on the operating system of the endpoint system to collect data from the monitored endpoint system. That data is then transmitted from the monitored endpoint system to the IBM Systems Director management server where it is stored. Service and Support Manager securely transmits this data between the endpoint system and the management server using the connection already established by IBM Systems Director.

By default, IBM Systems Director Server provides a Secure Sockets Layer (SSL) certificate that supports HTTPS connections between the IBM Systems Director management server and monitored endpoints. To ensure server authentication, data privacy, and data integrity, the default certificate should be replaced with either a self-signed certificate or a certificate that is signed by a certificate authority. Additionally, the key store password also should be changed.

The usage of SSL is not required, however, it is recommended. Configuring SSL ensures data integrity and data confidentiality between the management servers and its targets. This protection is especially important if IBM Systems Director is accessed from outside networks.

Information on managing the certificate can be found in the Planning Secure Sockets Layer configuration on IBM Systems Director section of the Systems Director Information Center:
http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.plan.helps.doc/fqm0_t_planning_ssl_configuration.html

Systems Director communicates with and collects data from the managed end-points through a number of different ports and communication mechanisms as noted in the table below. If firewalls exist in the network, or if the management server uses a proxy server to access the internet, then those firewalls and proxy servers must be configured to enable the communication paths indicated. A successful installation and implementation of Systems Director, and a successful usage of Service and Support Manager, requires that the ports that will be used in the systems-management environment be identified to ensure that those ports are open before the installation of Systems Director.

Port	Protocol	Direction	Communication description
20	TCP	Inbound	FTP data communication with Blade Center I/O modules (switches and bridges)
21	TCP	Inbound	FTP communication with Blade Center I/O modules (switches and bridges)

Port	Protocol	Direction	Communication description
22	TCP	Outbound	SSH communication with Advanced management modules and management module Blade Center I/O modules Platform Agent installed on systems running Linux SSH used by IBM Power systems to communication with HMC/IVM Non-Windows Agentless-managed systems
23	TCP,UDP	Outbound	Telnet communication with: Advanced management module, management module, Remote Supervisor Adapter, and Remote Supervisor Adapter II Blade Center I/O modules Updates
69	TCP	Inbound	TFTP communication with Blade Center I/O modules (switches and bridges)
80	TCP	Outbound	HTTP communication with: IBM Systems Director Web interface Advanced management module, management module, Remote Supervisor Adapter, and remote Supervisor Adapter II Blade Center I/O modules IVM interface Update management
81	TCP	Outbound	HTTPS communication with Blade Center I/O modules (switches and bridges)
135	TCP,UDP	Outbound	(Windows only) Software installation and remote access communication with Platform Agent
137	TCP,UDP	Outbound	(Windows only) Communication with Agentless-managed systems using Microsoft Windows DCOM
138	TCP,UDP	Outbound	(Windows only) Communication with Agentless-managed systems using Windows DCOM
139	TCP,UDP	Outbound	(Windows only) Communication with Agentless-managed systems using windows Server Message Block (SMB)
161	UDP	Outbound	SNMP agent communication with: Advanced management module, management module, Remote Supervisor Adapter, and Remote Supervisor Adapter II Blade Center I/O modules Platform Agent **NOTE**: This port is used when the SNMP agent for the operating system is configured. Agentless-managed systems **NOTE**: This port is used with the SNMP agent for the operating system is configured.
162	TCP,UDP	Outbound (TCP,UDP) Inbound (TCP)	Simple Network Management Protocol (SNMP) traps communication with SNMP devices, including TCP for Tivoli NetView events. Examples of SNMP devices are advanced management module, management module, Remote Supervisor Adapter, and Remote Supervisor Adapter II.
427	TCP, UDP	Outbound and Inbound	SLP communication with Advanced management module, management module, Remote Supervisor Adapter, and Remote Supervisor Adapter II Common Agent Platform Agent IBM Director Agent 5.20 Service Location Protocol (SLP) service agent or SLP directory agent.
443	TCP	Outbound	HTTPS communication with: IBM Systems Director Web interface Advanced management module and management module HMC Web interface Updates

Port	Protocol	Direction	Communication description
445	TCP,UDP	Outbound	(Windows only) Open on Agentless and Platform-Agent managed systems for the following features: Software installation Remote access communication (Agentless-managed systems only) Inventory collection
446	TCP	Outbound	Non-SSL communication with the IBM I DRDA/DDM server job
448	TCP	Outbound	SSL communication with the IBM I DRDA/DDM server job
449	TCP	Outbound	SSL communication with the IBM I server port mapper
623	UDP	Outbound	Remote Management and Control Protocol (RMCP) unsecure communication with IPMI baseboard management controller (BMC) service processors.
664	UDP	Outbound	Remote Management and Control Protocol (RMCP) secure communication with IPMI BMC service processors
Random port in the 1024-65535 range	TCP	Inbound	Random port range for communication between IBM Systems Director Server with Intelligent Platform Management Interface (IPMI) service processors **Note**: You can specify a fixed port by modifying the asmDefinitions.properties file in the data directory. For the TCP ports listed, the initiator opens a random port in the 1024-65535 range and then connects to the listener on the port listed. The listener responds by connecting to the original random port opened by the initiator.
1433	TCP	Outbound and Inbound	Microsoft SQL Server databases
1521	TCP	Outbound and Inbound	Oracle Database databases
1527	TCP	Outbound and Inbound	Apache Derby databases
2033	TCP	Inbound	Communication with the IBM Systems Director Launched Tasks program using IBM Systems Director interprocess communication (IPC)
2044	TCP	Outbound and Inbound	Smcli command-line interface **NOTE**: This port number can be changed.
3389	TCP	Outbound and Inbound	Remote Desktop Protocol, Remote Desktop Connection, or Remote Accessor for full screen access to systems running windows.
4066	TCP	Inbound	Communication with the IBM Systems Director Launched tasks program using IBM Systems Director interprocess communication (IIPC) over SSL.
5901	TCP	Outbound and Inbound	Virtual Network Computing (VNC), used by Remote Access
5988	TCP	Inbound	(Windows and Red Hat Enterprise Linux) CIM Server unsecure port
5989	TCP	Inbound	• (Windows and Red Hat Enterprise Linux) CIM Server secure port • HMC/IVM CIMOM
6641	TCP	Inbound	SAS switches
6988	TCP	Inbound	CIM listener
6989	TCP	Inbound	CIM listener
6090	TCP	Outbound	TCP Command Mode communication between IBM Systems Director Server and advanced management module, management module, Remote Supervisor Adapter, and Remote Supervisor Adapter II

Port	Protocol	Direction	Communication description
8421	TCP	Inbound	• (All operating system platforms) HTTP communication between IBM Systems Director Server and the IBM Systems Director Web interface. • HTTP used by IBM Power Systems to communication with CIM.
8422	TCP	Inbound	• (All operating system platforms) HTTPS communication between IBM Systems Director Server and the IBM Systems Director Web interface. • HTTPS used by IBM Power Systems to communication with CIM.
8470	TCP	Outbound	Non-SSL communication with the IBM I central server job
8471	TCP	Outbound	Non-SSL communication with the IBM I database server job
8472	TCP	Outbound	Non-SSL communication with the IBM I data queue server job
8473	TCP	Outbound	Non-SSL communication with the IBM I file server job
8474	TCP	Outbound	Non-SSL communication with the IBM I network print server job
8475	TCP	Outbound	Non-SSL communication with the IBM I remote command and distributed program call server job.
8476	TCP	Outbound	Non SSL communication with the IBM I signon server job
9000-9100	TCP		Communication Platform-Agent managed system running Xen
9470	TCP	Outbound	SSL communication with the IBM I central server job
9471	TCP	Outbound	SSL communication with the IBM I database server job
9472	TCP	Outbound	SSL communication with the IBM I data queue server job
9473	TCP	Outbound	SSL communication with the IBM I file server job
9474	TCP	Outbound	SSL communication with the IBM I network print server job
9475	TCP	Outbound	SSL communication with the IBM I remote command and distributed program call server job
9476	TCP	Outbound	SSL communication with the IBM I signon server job.
9510	TCP	Inbound, Outbound	Communication with Common Agent and CAS Web services.
9511-9513	TCP	Inbound	Agent Manage
9514-9515	TCP		Nonstop ports that are used to make sure Common Agent are restarted automatically if it fails. **Note**: Ports must be available, but not firewall accessible
10000			Events from storage devices
13991	UDP	Inbound	Receives events sent by advanced management module, management module, Remote Supervisor Adapter, and Remote Supervisor Adapter II
14247	UDP	Inbound	IBM Systems Director interprocess communication (IPC) with IBM Director Agent 5.20
14248	UDB	Outbound	IBM Systems Director interprocess communication (IPC) with IBM Director Agent 5.20
14251	UDP	Inbound	IBM Systems Director Server interprocess communication (IPC) support
15988	TCP	Inbound	(Red Hat Enterprise Linux, SUSE Linux) CIM Server unsecure port
15989	TCP	Inbound	(Red Hat Enterprise Linux, SUSE Linux) CIM Server secure port.
20000	TCP	Inbound	• CAS Events • Communication with VMWARE
50000	TCP	Inbound, Outbound	IBM Db2 Universal Databse databases
61616	TCP	Inbound, Outbound	JMS communication with IBM Systems Director Server unsecure port
61617	TCP	Inbound, Outbound	JMS communication with IBM Systems Director secure port.

Keep in mind that this list of ports can change over time. See the following location for the most up to date information:

http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.plan.helps.doc/fqm0_r_all_available_ports.html

2.1.2.2 Data transmitted between Service and Support Manager and IBM Support

Electronic Service Agent™ is a call-home tool integrated with Service and Support Manager. Service and Support Manager uses Electronic Service Agent to transmit serviceable hardware problems and associated support files, system inventory, system status updates, Performance Management data, and quality software data to IBM® support.

The following security precautions are used when data is transmitted to IBM support:

1. **Client system authentication:**
   The first time that the IBM Systems Director management server connects to IBM support, the machine will be registered with IBM support as an authorized client of electronic services. On subsequent transmission requests, Service and Support Manager and Electronic Service Agent authenticate to IBM support with credentials that were obtained during registration and stored locally in the form of an Id and password. IBM uses a proprietary protocol for authentication and identity verification.

2. **Communication encryption:**
   Serviceable hardware problems and associated support files, system inventory, system status updates, Performance Management data, and quality software data are all sent using the security of Hypertext Transfer Protocol Secure (HTTPS). HTTPS is achieved by encapsulating the HTTP application protocol within either the Transport Layer Security (TLSv1) cryptographic protocol or the Secure Socket Layer (SSLv3) cryptographic protocol. When transmitting large files, transactions are sent using File Transfer Protocol over SSL (FTPS). Service and Support Manager uses the embedded Electronic Service Agent tool to initiate all transactions; IBM support never initiates a connection to Service and Support Manager.

2.1.2.3 Configuration data downloaded from IBM Support

In addition to data that is transmitted securely to IBM support, Service and Support Manager also downloads configuration updates. Service and Support Manager requests updated configuration data from IBM support on a regularly scheduled basis. This data is downloaded using a standard HTTP connection. This data does not contain customer sensitive information. Downloaded configuration data consists of:

- Updated hardware error codes that Service and Support Manager uses to determine if a hardware problem is serviceable.

- Updates to IBM support servers that Service and Support connects to. This is the same information displayed in the table below (section 2.1.2.4) that contains host names, IP addresses, and ports.

2.1.2.4 Internet connections used to transmit data to IBM support and download data from IBM support.

Configuration of Service and Support Manager includes the ability to indicate whether a direct connection or connection through a proxy server should be used. It should be noted that Service and Support Manager uses the IBM Systems Director management system's connectivity environment, including connections established by the Update Manager component of IBM Systems Director.

The following connections are used to transmit serviceable hardware problems and associated support files, system inventory, system status updates, Performance Management data, and quality software data to IBM support using HTTPS or FTPS, and are used by Service and Support Manager to download configuration data updates using HTTP.

Note: The HTTP connections listed below are only used by Service and Support Manager to download configuration updates, and are never used to transmit secure service data.

Required internet connections

DNS name	IP address	Port(s)	Protocol(s)
Update manager			
www.ibm.com	129.42.56.216, 129.42.58.216, 129.42.60.216	80	http
www-03.ibm.com	204.146.30.17	80	http
download3.boulder.ibm.com	170.225.15.76	80	http
download3.mul.ie.ibm.com	129.35.224.114	80	http
download4.boulder.ibm.com	170.225.15.107	80	http
download4.mul.ie.ibm.com	129.35.224.107	80	http
delivery04-bld.dhe.ibm.com	170.225.15.104, 129.35.224.104	80	http
delivery04-mul.dhe.ibm.com	129.35.224.115, 170.225.15.115	80	http
delivery04.dhe.ibm.com	129.35.224.105, 170.225.15.105	80	http
Service and Support Manager			
eccgw01.boulder.ibm.com	207.25.252.197	443	https
eccgw02.rochester.ibm.com	129.42.160.51	443	https

Required internet connections			
DNS name	**IP address**	**Port(s)**	**Protocol(s)**
www-945.ibm.com	129.42.26.224, 129.42.34.224, 129.42.42.224	443	https
www6.software.ibm.com	170.225.15.41	443	https
www.ecurep.ibm.com	192.109.81.20	443	https
testcase.boulder.ibm.com	170.225.15.31	21	ftps

NOTE: IP addresses are subject to change, so ensure that you use DNS names whenever possible. For the most up to date list see:
http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.install.helps.doc/fqm0_t_preparing_firewalls_and_proxies.html

2.1.3 Customer data and information privacy

Service information provided to IBM support remains private and secure. Only authorized IBM support personnel and those people specifically authorized by the customer have access to this information. Customers provide contact information to Service and Support Manager and authorize Service and Support Manager to securely transmit their contact information to IBM support. Information is also gathered from phone calls with groups within IBM. These IBM groups have electronic access to the information so that they can prepare for and perform advanced problem determination.

Service information collected by Service and Support Manager includes the following:

- Support contact information, including names, phone numbers, and e-mail addresses. The contact information is customer-provided. The customer has direct control of the level of information provided.
- Software listings
- Hardware inventory
- System configuration information
- Network information such as IP Addresses and hostnames

Service information does not include the following:

- Collection or transmission of any of the customer's financial, statistical, or personnel information
- Business data

2.1.3.1 Access to stored customer inventory data

Inventory reported to IBM support is available for customers to view from the **IBM Electronic Support** Website. Customers can use the **My Systems** page to view inventory collected across all their systems (This tool requires an IBM ID to be associated with Service and Support Manager and the embedded Electronic Service Agent tool).
Note: It may take up to 24 hours from the time inventory is reported for it to appear on the IBM Electronic Services Website.

For more information, visit the **IBM Electronic Support** portal:
http://www.ibm.com/supportportal

Once you have navigated to the Website, click **About this site / Tours** to view documentation on setting up notifications, viewing systems, and searching for inventory.

An IBM ID is required to view your stored inventory data. Your IBM ID is your single point of access to IBM web applications that use IBM Registration. You need just one IBM ID and one password to access any IBM Registration based application. Furthermore, your information is centralized so you can update it in a convenient and secure location. The benefits of having an IBM Registration ID will increase over time as more and more IBM applications migrate to IBM Registration. For more information on IBM IDs, see the following topic:
https://www.ibm.com/account/profile/us?page=regfaqhelp

Service and Support Manager allows customers to provide up to two separate customer IBM IDs. Service and Support Manager stores the IBM IDs on the IBM Systems Director management server as an xml file in the following location: /director/data/esa/config. This location is not encrypted. Service and Support Manager associates an IBM ID with the IBM Systems Director management server that contains both Service and Support Manager and the embedded Electronic Service Agent tool. This provides customers with that IBM ID access to view their system inventory that is transmitted automatically by Electronic Service Agent.

2.1.3.2 IBM Systems Director user interface security

Service and Support Manager uses the default IBM Systems Director user groups to limit or restrict access to some tasks. Access to particular resources or tasks is governed by restrictions based on the user ID or user group membership and the roles that are defined for each user. Service and Support Manager requires either `smadmin` or `smmgr` user authority in order to manage monitored systems, contact information, and settings. User groups with less authority than `smadmin` or `smmgr` allow a user to view some information, but most actions and tasks will be disabled, and settings and contact information will not be accessible. For more information about IBM Systems Director users and groups, see the following link:
http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.security.helps.doc/fqm0_c_user_accounts.html

The Power Architecture and Power.org wordmarks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

Linux is a trademark of Linus Torvalds in the United States, other countries or both.

Microsoft, and Windows are registered trademarks of the Microsoft Corporation.

Copying or downloading the images contained in this document is expressly prohibited without the written consent of IBM.

IBM Corporation
Systems and Technology Group
Route 100
Somers, New York 10589

Produced in the United States of America
September 2010

The IBM home page on the Internet can be found at: http://www.ibm.com.

The IBM Power Systems home page on the Internet can be found at: http://www.ibm.com/systems/power/

XBW03012-USEN-00