HP Universal CMDB

Software Version: 10.01, CP 12.00

Discovery and Integration Content Guide - Supported Content (Revised Edition)

Document Release Date: October 2013

Software Release Date: November 2012

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

Java and Oracle are registered trademarks of Oracle Corporation and/or its affiliates.

Microsoft®, Windows®, Windows NT®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

- This product includes software developed by the Apache Software Foundation (http://www.apache.org/).
- This product includes OpenLDAP code from OpenLDAP Foundation (http://www.openldap.org/foundation/).
- This product includes GNU code from Free Software Foundation, Inc. (http://www.fsf.org/).
- This product includes JiBX code from Dennis M. Sosnoski.
- This product includes the XPP3 XMLPull parser included in the distribution and used throughout JiBX, from Extreme! Lab, Indiana University.
- This product includes the Office Look and Feels License from Robert Futrell (http://sourceforge.net/projects/officelnfs).
- This product includes JEP - Java Expression Parser code from Netaphor Software, Inc. (http://www.netaphor.com/home.asp).

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Supported Content

Chapter 1

Discovered Applications

Note: Additional supported content is publicly available to download through the HP Live Network (https://hpln.hp.com). Follow the **Discovery and Dependency Mapping** quick link. You will need an HP Passport user name and password.

Vendor	Product	Versions	Credentials	Discovers...
Amazon	Amazon Web Services		AWS	EC2 and RDS topologies.
Apache	Http Server	1.3, 2.0, 2.2	Shell	Apache Http server Listening ports, Virtual hosts, configuration files, Web application, Apache Modules (including mod_proxy and mod_proxy_balancer.
Apache	Tomcat	5, 5.5, 6.0	Shell	Tomcat Server, Web applications, configuration files, virtual servers, listening ports, Tomcat Cluster, Tomcat Service.
BMC	Atrium CMDB	2.0, 2.1, 7.5.x, 7.6.x and earlier, 8.1	Remedy	Pushes configuration items (CIs) from HP UCMDB to the Atrium CMDB server using mapping xml files. **Note**: Synchronized Content, not discovery of application topology.
BMC	Remedy ARS	7.0, 7.1, 7.5, 7.6	Remedy	Pushes CIs from HP UCMDB to Remedy ARS using mapping xml files. **Note**: Synchronized Content, not discovery of application topology.
CA Technologies	CA CMDB	12.0, 12.5	CA CMDB protocol	Pushes CIs from HP UCMDB to the CA CMDB server using mapping xml files.

Vendor	Product	Versions	Credentials	Discovers...
Cisco	CSS	6.10, 7.4	SNMP	Mapping of Virtual IPs to real IP addresses of servers configured for load balancing; configuration files, load balancing algorithms, and end user IP addresses. **Note**: Cisco WebNS is the software version running on the 11000 and 11500 series CSS.
Citrix	XEN	3.4	SSH, Telnet	Bridge, CPU, Execution Environment, File System, File System Export, Interface, Layer2Connection, Node, Physical Port, Virtualization Layer Software, Xen domain config.
EMC	EMC AutoStart	5.x	Shell	ClusterResourceConfig, ClusterResourceGroup, ClusterResourceGroupConfig, ClusterSoftware, Containment, EMC AutoStart Cluster, IpAddress, Node.
EMC	EMC Control Center (ECC)	6.0.1	Oracle DB	Synchronized Configuration Items (CIs) currently include Storage Arrays, Fibre Channel Switches, Hosts (Servers), Storage Fabrics, Storage Zones, Logical Volumes, Host Bus Adapters, Storage Controllers, and Fibre Channel Ports. Integration also synchronizes physical relationships between various hardware and logical relationships between Logical Volumes, Storage Zones, Storage Fabrics, and hardware devices to enable end-to-end mapping of the storage infrastructure in UCMDB. **Note**: Synchronized content is discovered, not the application topology.

Vendor	Product	Versions	Credentials	Discovers...
F5	BIG-IP LTM	4.6, 9.1, 10.2.2	SNMP	Mapping of Virtual IPs to real IP addresses of servers configured for load balancing; configuration files, load balancing algorithms, and end user IP addresses.
HP	Network Node Manager (NNM)	8.1, 8.11, 9.0, 9.1	NNM API	Discovered nodes, IPs, networks, interfaces and Layer 2 connection information to create a Layer 2 topology in UCMDB.
HP	NonStop	H06.x	SSH	Database, Database Instance, HP NonStop, NonStop SQL/MX.
HP	nPartitions	A.03xx, A.04xx, A.05xx	SSH, Telnet	CPU, Fibre Channel HBA, File System, HP Complex, HP nPar Config, HP vPar Config, I/O Chassis, CellBoard, Interface, nodes, Physical Volume, SCSI Adapter, Volume Group
HP	ServiceGuard	11.1x	Shell	SG cluster software, SG packages, SG resources, cluster members
HP	SIM	5.1, 5.2, 5.3, 6.0, 6.1, 6.2, 6.3, 7.0, 7.1	HP SIM	Synchronized configuration items (CIs) include nodes such as Windows, and UNIX servers, network devices, printers, clusters, cellular/partitioned systems, blade enclosures, and racks. Some server components, for example, CPU, are also synchronized. The integration also synchronizes relationships between blade servers and blade enclosures, virtual machines, physical servers, and so on. **Note**: Synchronized Content, not discovery of application topology.

Vendor	Product	Versions	Credentials	Discovers...
HP	Storage Essentials (SE)	6.0.0; 6.3 9.4, 9.41, 9.5	SQL	Synchronized Configuration Items (CIs) including Storage Arrays, Fibre Channel Switches, Hosts (Servers), Storage Fabrics, Storage Zones, Logical Volumes, Host Bus Adapters, Storage Controllers, and Fibre Channel Ports. The integration also synchronizes physical relationships between various hardware and logical relationships between Logical Volumes, Storage Zones, Storage Fabrics, and hardware devices to enable end-to-end mapping of the storage infrastructure in UCMDB.
IBM	AS/400	V4R2M0, V3R2M1, V3R2M0, V4R5M0, V5R3, V6R1	AS400	AS400Agent, Interface, IpSubnet, Node.
IBM	DB2 Universal Database (UDB)	8.2, 9.1, 9.5, 9.7	SQL	DB2 databases, including instances, tablespaces, users, processes, jobs (backup routines, log routines, and so on), any database objects. Discovery through: • direct connection to DB2 database, • SQL queries • HP DFM z/OS Mainframe **Note**: Discovery Agent, 9.2, 9.5 are recent versions.

Vendor	Product	Versions	Credentials	Discovers...
IBM	HACMP	5.4	SSH, Telnet	Topology (configured networks, node interfaces–both public TCP/IP and serial heartbeat, and service IPs) and Application Resources (configured resource groups, application servers, and volume groups).
IBM	HMC	3.x, 5.x, 6.x, 7.x	SSH, Telnet	CPU, I/O Slot, IBM Frame, IBM HMC, IBM LPar Profile, IBM Processor Pool, Interface, Node, Virtualization Layer Software, SCSI Adapter, Physical Port, Physical Volume, Fibre Channel HBA, File System, SEA Adapter.
IBM	HTTP Server	5, 6.1, 7	Shell	IBM Http Server's WebSphere plug-in configuration by parsing the IHS plug-in configuration file.
IBM	MQ Series (aka WebSphere MQ)	5.31, 6, 7.1	Shell	MQ subsystems at the system configuration level; DFM does not monitor or discover which active jobs or applications are running through the queues. Discovery includes Queue Managers, System Parameters, Queue-Sharing Groups, related DB2 Data-Sharing Groups, Cross Coupling Facility groups/members, Channel Initiator, Sender Channel, Server Channel, Receiver Channel, Requester Channel, Client Connection Channel, Server Connection Channel, Cluster Sender Channel, Cluster Receiver Channel, Alias Queue, Model Queue, Local Queue, Transmission Queue, Remote Queue, MQ Process, and MQ Cluster.
IBM	Websphere Application Server	5.x, 6.1, 7.0	Shell	J2EE Server, J2EE application, JDBC datasource, Database, EJB Module, Web Module, J2EE Domain and JMS resources

Vendor	Product	Versions	Credentials	Discovers...
JBoss	Application Server	3.x, 4.x , 5.x	JMX	JBoss J2EE application server, EJB Module, Entity Bean, J2EE Application, J2EE Domain, JDBC Data Source, JMS Destination, JMS Server, JVM, Message Driven Bean, Servlet, Session Bean, Web module.
JBoss	Application Server	3.x, 4.x, 5.x	Shell	JBoss J2EE application server, EJB Module, Entity Bean, J2EE Application, J2EE Domain, JDBC Data Source, JMS Destination, JMS Server, JVM, Message Driven Bean, Servlet, Session Bean, Web module.
Microsoft	Active Directory	2000, 2003, 2008	LDAP	Forest, Sites, Sitelinks, Domain controllers, Networks, and so on.
Microsoft	Cluster Services	Windows Server 2003, Windows Server 2008	Shell	Cluster software, configuration files, cluster members, MCS Resource Groups, MCS Resources.
Microsoft	Exchange Server	2003	WMI	Administrative Group, Directory Service Access DC, Exchange Folder, Exchange Folder Tree, Exchange Links, Exchange Message Queue, Exchange System, Routing Group.
Microsoft	Exchange Server	2003, 2007, 2010	LDAP	Forest, Sites, Exchange folders, folder trees, Administrative groups, Connectors.
Microsoft	Exchange Server	2007, 2010	NTCMD, PowerShell	Exchange Server, Exchange roles, Administrative group, Exchange Organization, Exchange Clustered Mailbox, Exchange Database Availability Group.
Microsoft	Hyper-V	Windows 2008, Windows 2008 R2	NTCMD, WMI	Resource pools, virtual switches, virtual NICs, virtual machines, and configuration files.

Vendor	Product	Versions	Credentials	Discovers...
Microsoft	IIS	5, 6, 7	Shell	Discover the IIS Web Server, IIS Web Site, IIS virtual Dir, IIS Application pool, web services and configuration files.
Microsoft	Message Queue	3.0, 4.0, 5.2	LDAP, NTCMD	MSMQ Manager, MSMQ Routing Link, MSMQ Manager, MSMQ Queue, MSMQ Rule, MSMQ Trigger.
Microsoft	Network Load Balancer	2003, 2008	NTCMD	NLB Cluster, NLB Cluster Software and Node.
Microsoft	SharePoint	2007, 2010	NTCMD	Windows, SQL Server, IIS Application Pool, IIS Web Server, IIS Web Service, IIS Web Site, SharePoint Farm.
Microsoft	SQL Server	7, 2000, 2005, 2008	SQL	Discovery of MS SQL databases, including instances, tablespaces, users, processes, jobs (backup routines, log routines, and so on), any database objects, MS SQL clustering, and log file shipping tasks.
NetApp	Data ONTAP	7.2.x, 7.3.x	NetApp	Node, LogicalVolume, Logical Volume Snapshot, FileSystem, FileSystemExport, IpAddress, Interface, CPU, Memory.
Nortel	Alteon	2424, 2208	SNMP	Mapping of Virtual IPs to real IP addresses of servers configured for load balancing; configuration files, load balancing algorithms, and end user IP addresses.
Oracle	Application Server	10g	Shell	OC4J groups, OC4J instances and its URLs.
Oracle	Database	9,10g,11g	Shell	Oracle database, TNS Listener software.
Oracle	Database	8, 9, 10g, 11g	SQL	Oracle databases, including SIDs, TNS names, instances, tablespaces, users, processes, jobs (backup routines, ONP, jobs, log routines, and so on), and any database objects.

Vendor	Product	Versions	Credentials	Discovers...
Oracle	LDOM	1.0-1.3	SSH, Telnet	LDOM Networking and Storage topologies.
Oracle	Oracle VM Server for SPARC	2.0-2.1	SSH, Telnet	LDOM Networking and Storage topologies.
Oracle	RAC	9,10g,11g	Shell	Oracle RAC.
Oracle	RAC	10g	SQL	Oracle RAC.
Oracle	E-Business Suite	11i, 12	SQL	Oracle E-Business applications, such as Oracle Financials; infrastructure components, Web servers, application servers, individual components, and configuration files.
Oracle	MySQL Database	3.x, 4.x, 5.0, 5.1, 6.0	Shell	Support MySQL Master-Master and Master-Slave configuration. Discover MySQL Database, configuration files, Replication job
Oracle	Siebel CRM	7.5, 7.7, 8.0, 8.1	Shell	Discovery of Siebel Enterprise, including Siebel applications (CallCenter, Financial, and so on), Siebel infrastructure components, Siebel Web servers, application servers, gateway servers, individual Siebel, components and configuration files.
Oracle	WebLogic	8.x, 9.x, 10.x, 11g, 11gR1 PS1, 11gR1 PS2, 11gR1 PS3	Shell or JMX	Weblogic J2EE Server, J2EE application, JDBC datasource, Database, EJB Module, Web Module and JMS resources, J2EE Domain, J2EE Cluster.
SAP	CCMS Agent	6.40-7.30	Shell	CCMS instance (RunningSoftware), SAP Gateway, SAP System, IpServiceEndpoint.

Vendor	Product	Versions	Credentials	Discovers...
SAP	Hana DB	1,0, 1.5	Shell	ConfigurationDocument, Database Schema, DB Data File, DB User, DbLogFile, DbTraceFile, HanaDatabase, IpAddress, IpServiceEndpoint, Node, RunningSoftware.
SAP	Host Agent	7.00-7.30	Shell	HostAgent instance (RunningSoftware), SAP Gateway, SAP System, IpServiceEndpoint.
SAP	IGS	7.1	Shell	IGS instance (RunningSoftware), SAP Gateway, SAP System, IpServiceEndpoint.
SAP	MaxDB	7.x	Shell	ConfigurationDocument, DB Data File, Db User, Database Schema, IpAddress, IpServiceEndpoint, MaxDB, Node, SQL Backup.
SAP	NetWeaver	2.x, 4, 7	JMX; SAP JCo	SAP ABAP Application Server, SAP Clients, SAP Gateway, SAP System, SAP Work Process, JDBC Data Sources, Databases, Hosts in deployment with IPs, SAP J2EE Application Server, SAP J2EE Dispatcher, SAP J2EE Server Process, SAP J2EE Central Services, J2EE domain, EJBs, EJB Modules, Entity Beans, Stateful/Stateless Session Beans, Web Module, SAP Business Process, SAP Business Scenario, SAP Process Step, SAP Project, SAP Transaction, SAP Application Components, SAP Transports, SAP ITS AGate, SAP ITS WGate.
SAP	SAP Solution Manager	6.4, 7.0	SAP JCo	SAP ABAP Application Server, SAP Clients, SAP System, JDBC Data Sources, Databases, SAP J2EE Application Server, SAP J2EE Dispatcher, SAP J2EE Central Services, J2EE domain.
SAP	SMD Agent	7.00-7.30	SSH, Telnet, NTCMD	SapSmdAgent, SAP Sytem

Vendor	Product	Versions	Credentials	Discovers...
SAP	TREX/BIA	7.00-7.30	SSH, Telnet, NTCMD	SapTrexInstance, SapTrexSystem, SAP System
SAP	Virus Scan Server	1.7	Shell	SAPVirusScanServer, SAP Gateway, SAP System, IpServiceEndpoint.
SAP	Web Dispatcher	6.40, 7.00-7.30	SSH, Telnet, NTCMD	SapWebDispatcher, SAP System
Sun	MySQL Database Server	4.x and above	Shell	MySQL databases and MySQL replication topology.
Sun	Solaris Cluster	3.2	SSH, Telnet	Cluster Software, Configuration file, Execution Environment, Node, Sun Cluster, Sun Cluster Resource, Sun Resource Group.
Sun	Solaris Zones	5.1	Shell	Containers, zones, and share resources.
Sybase	Adaptive Server Enterprise	10.x, 11.x, 12.x, 15.0, 15.5	SQL	Sybase databases, including instances, tablespaces, users, processes, jobs (backup routines, log routines, and so on), and any database objects.
Symantec	Veritas Cluster Server (VCS) for UNIX	2.x, 3.x, 4.x, 5.x	Shell	Cluster Software, configuration files, cluster members, VCS Resource Groups, VCS Resources.
TIBCO	ActiveMatrix BusinessWorks	5.7, 5.8	SSH, Telnet, TIBCO	TibcoAdapter, TibcoAdministrationDomain, TibcoApplication, TibcoBusinessWorks, TibcoEmsServer, JMS Destination, JMS Server
TIBCO	Enterprise Message Server	6.0	SSH, Telnet, TIBCO	TibcoEmsServer, JMS Destination, JMS Server
Tomcat	Apache	5.x, 6.x	Shell	Tomcat Server instances, Web applications, configuration files, virtual servers, listening ports.

Vendor	Product	Versions	Credentials	Discovers...
Troux	Troux	9.0x		
VMware	ESX	2.5, 3, 4, 4.1, 5.0	Shell	
VMware	ESX & ESXi	2.5, 3, 3i, 3.5, 4, 4.1, 5.0	VIM	ESX servers, cluster groups, virtual resource groups.
VMware	vCenter (formerly Virtual Center)	2.01, 2.5, 4, 4.1, 5.0	VIM and WMI	Virtual Center Server, License Server, ESX servers, cluster groups, virtual resource groups.
VMware	vCloud Director	1.5	vCloud	VMware vCloud Director and vCloud Resources (Organization, Catalog, Media, vApp, and so on).

Chapter 2

Discovered Operating Systems

Vendor	Product	Versions	Credentials	Content
IBM	AIX	5.x, 6.x, 7.1	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users
HP	HP-UX	10.xx, 11.xx	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (Daemons), Files, Local Users, HP-UX Clusters
IBM	OS/390		SNMP	Simple mainframe discovery identifies Sysplex, LPARs, and IPs
IBM	z/OS	1.8, 1.9, 1.10, 1.11, 1.12	EView	CPU, Dasd3390, InstalledSoftware, Interface, IpAddress, IpServiceEndpoint, Mainframe CPC, MainframeMajorNode, MainframePageDataset, MainframeSubsystem, MainframeSysplex, MainframeXcfGroup, MainframeXcfMember, Node, Volume Group, zOS
OpenBSD	OpenBSD	4.5	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Services (daemons), Files, Local Users
Oracle	Oracle Linux	5.7 and later	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users
RedHat	RedHat Enterprise Linux	3, 4, 5, 5.1, 5.2, 5.3, 5.4, 5.5, 6.0	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users
Sun	Solaris	5.9, 5.10	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users
SUSE	SUSE Linux Enterprise	11 and later	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users
Microsoft	Windows	All Versions later than Windows 2000	NTCMD, PowerShell, WMI	OS, Memory, Disks, CPU, Processes, Software, Services, Files, Local Users

Chapter 3

Supported Agents

The following agents are supported:

Agent	Description
SNMP Agent	Provides information about the operating systems, device types, installed software, and other system resources information. SNMP agents can usually be extended to support new MIBs, exposing more data for management purposes.
WMI Agent	Microsoft's remote management agent, which is usually available for access by a remote administrator. The WMI agent is also extensible by adding WMI providers to the generic agent.
Telnet/SSH Agent (or daemon)	Used mostly on UNIX systems to connect remotely to a machine and to launch various commands to obtain data.
Universal Discovery Agent	A remote administration technology similar in functionality to Telnet/SSH that enables launching any console command on Windows/UNIX/Mac OS X machines. The Universal Discovery Agent (UD Agent) implements a Web Services interface that is secured by the HTTPS protocol to secure communication between the Data Flow Probe and the UD Agent. Additionally, an RSA 2048-bit key is implemented together with 3DES 168-bit encryption.
HPCmd	A remote administration technology similar in functionality to Telnet/SSH that enables launching any console command on Windows machines. HPCmd relies on Administrative Shares & Remove Service Administration APIs to function correctly. The **HPCmdSvc.exe** file is signed by an HP digital certificate. To validate that **HPCmdSvc.exe** is provided by HP, right-click the **HPCmdSvc.exe** file, select **Properties** and view the digital signatures.
Application specific	Depends on the remote application to function as an agent and respond appropriately to the Probe's remote queries, for example, database discoveries, Web server discoveries, and SAP and Siebel discoveries.

Chapter 4

Universal Discovery Agent, Software Utilization Plug-In, Scanner and Software Library Support

Support for the Universal Discovery Agent, Software Utilization Plug-in, Scanner, and the Software Application Index (SAI) Library are as follows:

Windows

Operating System	Version	Platform	Agent	Utilization Plug-in	Scanner	SAI
XP	Home, Professional	x86	x	x	x	x
	Professional	x64	x	x	x	
	Professional	ia64			x	
Server	2003, 2003 R2, 2008, 2008 R2	x86, x64	x	x	x	x
	2003	ia64			x	
	2008	ia64			x	
Vista	Business, Enterprise, Ultimate	x86, x64	x	x	x	x
Windows 7	Professional, Enterprise, Ultimate	x86, x64	x	x	x	x

Linux

Operating System	Version	Platform	Agent	Utilization Plug-in	Scanner	SAI
Red Hat Enterprise AS/ES/WS	3, 4	x86, x64	x	x	x	x
Red Hat Enterprise Server/Desktop	5, 6		x	x	x	x
Novell SUSE Enterprise Server/Desktop	9, 10, 11		x	x	x	x
Oracle	4, 5, 6		x	x	x	x
CentOS	5, 6		x	x	x	x
Ubuntu Server/Desktop	10,11				x	x

IBM

Operating System	Version	Platform	Agent	Utilization Plug-in	Scanner	SAI
IBM AIX	5L 5.3, 6.1, 7.1	POWER	x	x	x	x

Oracle Solaris

Operating System	Version	Platform	Agent	Utilization-Plug-in	Scanner	SAI
Oracle Solaris	9, 10, 11	x86, 64, SPARC	x	x	x	x

HP UNIX

Operating System	Version	Platform	Agent	Utilization-Plug-in	Scanner	SAI
11.11	11i	HPPA	x	x	x	x
11.23	11i v2	HPPA,ia64	x	x	x	x
11.31	11i v3	HPPA, ia64	x	x	x	x

Apple Mac

Operating System	Version	Platform	Agent	Utilization Plug-in	Scanner	SAI
OS X	10.4, 10.5,10.6, 10.7	x86	x	x	x	x

Chapter 5

Supported Protocols

This section describes the credentials for the supported protocols for the Discovery and Integration Content Pack. For information about setting up protocol credentials in UCMDB, see the section about setting up the Data Flow Probe in the *HP Universal CMDB Data Flow Management Guide*.

Note: Credential attributes must not contain non-English letters.

AS400 Protocol

Parameter	Description
User	The user used on the AS400 system to execute the discovery commands.
Password	The password for the user account on the AS400 system used to execute the discovery commands.

AWS Protocol

Parameter	Description
User Name	Access Key ID. An alphanumeric text string that uniquely identifies the owner of the account.
User Password	Secret Access Key, performing the role of a password.

CA CMDB Protocol

Parameter	Description
User Name	The username used by CA CMDB's GRLoader to connect to CA CMDB remotely.
User Password	The password used by CA CMDB's GRLoader to connect to CA CMDB remotely.

Generic DB Protocol (SQL)

Parameter	Description
Database Type	The database type. Select the appropriate type from the box. The following database types are supported: • DB2 • Microsoft SQL Server • Microsoft SQL Server (NTLM) • Microsoft SQL Server (NTLM v2) • MySQL • Oracle • Sybase
Port Number	The port number on which the database server listens. • If you enter a port number, DFM tries to connect to a SQL database using this port number. • **For an Oracle database**: If there are many Oracle databases in the environment and you do not want to have to create a new credential for each separate database port, you leave the Port Number field empty. When accessing an Oracle database, DFM refers to the **portNumberToPortName.xml** file and retrieves the correct port number for each specific Oracle database port. **Note**: You can leave the port number empty on condition that: • All Oracle database instances are added to the **portNumberToPortName.xml** file. For details, see the section about the portNumberToPortName.xml File in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document. • The same user name and password is needed to access all Oracle database instances.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the database.
User Name	The name of the user needed to connect to the database.

Parameter	Description
Password	The password of the user needed to connect to the database.
Instance Name	The name of the database instance, that is, the Oracle system identification or the DB2 database name. When connecting to any database, you can leave this field empty. In this case, DFM takes the SID from the Triggered CI data value: **${DB.name:NA}**.
Encryption method	• **None**. • **SSL**. For Oracle only.
Trust Store File Path	Enter the full path to the SSL trust store file. To use the trust store file, do one of the following: • Enter the name (including the extension) and place the file in the following resources folder: **C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\** • Insert the trust store file full path.
Trust Store Password	The SSL trust store password.

Generic Protocol

This protocol is intended for integrations that do not need a specific protocol. It is recommended to use this protocol for all out-of-the-box integrations, as they require a user name and password only.

Parameter	Description
Description	Description of the credentials.
User Name	The name of the user needed for authentication.
User Password	The password of the user needed for authentication.

HP Asset Manager Protocol

Parameter	Description
Asset Manager User Name	The name of the Asset Manager user.
Asset Manager Password	The password of the Asset Manager user.
DB User Name	The name of the Asset Manager database user.
DB Password	The password of the Asset Manager database user.

HP SIM Protocol

Parameter	Description
Port Number	The port at which the SIM MXPartner WebService API listens for SOAP requests. The defaults are **280** for HTTP and **50001** for HTTPS.
SIM Database Instance	• **Microsoft SQL Server**: Enter the instance name only for non-default instances of Microsoft SQL Server. • **Oracle**: Enter the SID.
SIM Database Name	(Microsoft SQL Server only) Enter the name of the database.
SIM Database Password	The password of the database user (Microsoft SQL Server) or schema name (Oracle) for the SIM database.
SIM Database Port	The listener port for the database.
SIM Database Type	The SIM Database type: • MSSQL • MSSQL_NTLM • Oracle
SIM Database User Name	The database user (Microsoft SQL Server) or schema name (Oracle) with permissions to access the database.
SIM Webservice Protocol	Choose between **HTTP** or **HTTPS**.
User Name	The name of the user needed to connect to the application.
User Password	The password of the user needed to connect to the application.

HTTP Protocol

Parameter	Description
User Name	The name of a user needed to perform BASIC authentication with the remote webserver.
User Password	The password of the user needed to perform BASIC authentication with the remote webserver.

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the remote webserver. **Default:** 40,000
Protocol	The protocol used to connect to the http server: HTTP or HTTPS. **Default:** HTTP
Port number	The number of a port to connect to the remote http server. **Default (HTTP):** 80 **Default (HTTPS):** 443
Host	The host this credential applies to. It may be empty if the credentials apply to any host.
Realm	The realm this credential applies to. It may be empty if the credentials apply to any host.
Trust Store Password	The password to access the Trust Store file.
Trust Store Path	The full path to the Trust Store file containing the trusted certificates.

JBoss Protocol

Parameter	Description
Port Number	The port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the JBoss application server.
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.

LDAP Protocol

Parameter	Description
Port Number	The port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the LDAP application server.

Parameter	Description
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.
Protocol	Choose which security model to use to access the service: - **LDAP**. Discovery uses an unprotected connection. - **LDAPS**. Discovery uses an SSL connection.
LDAP Authentication Method	**Simple**. The supported authentication method.
Trust Store File Path	The file containing trusted certificates. To import certificates into the Trust Store file: - Create a new Trust Store or use the default Java Trust Store: `<java-home>/lib/security/cacerts` - Enter the full path to the LDAP Trust Store file.
Trust Store Password	The LDAP Trust Store password used to access the Trust Store file. This password is set during the creation of a new Trust Store. If the password has not been changed from the default, use **changeit** to access the default Java Trust Store.

NetApp Protocol

Parameter	Description
NetApp ONTAPI Protocol	The protocol type. **Default:** https
Port Number	The port number. **Default:** 443
User Name	The name of the user needed to connect to the application.
User Password	The password of the user needed to connect to the application.

NetApp SANscreen/OnCommand Protocol

Parameter	Description
Password	The password of the user needed to connect to the application.
Port Number	The number of the port used to connect to the SANscreen Webservice API. **Default**: 80
User Name	The name of the user needed to connect to the application.
Webservice Protocol	Protocol used to connect to the SANscreen Webservice API; HTTP or HTTPS. **Default**: HTTP

NNM Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Data Flow Probe stops trying to connect to the NNMi server.
NNM Password	The password for the specified NNMi Web service (for example, `Openview`).
NNM User name	The user name for connecting to the NNMi console. This user must have the NNMi Administrator or Web Service Client role.

Parameter	Description
NNM Webservice Port	The port for connecting to the NNMi console. This field is pre-filled with the port that the JBoss application server uses for communicating with the NNMi console, as specified in the following file: - **Windows:** `%NnmDataDir%\shared\nnm\conf\nnm.ports.properties` - **UNIX:** `$NnmDataDir/shared/nnm/conf/nnm.ports.properties` For non-SSL connections, use the value of jboss.http.port, which is `80` or `8004` by default (depending on the presence of another Web server when NNMi was installed). For SSL connections, use the value of **jboss.https.port**, which is `443` by default.
NNM Webservice Protocol	The protocol for the NNMi Web service (the default is **http**).
UCMDB Password	The password for the UCMDB Web service (the default is **admin**).
UCMDB Username	A valid UCMDB Web service account name with the UCMDB Administrator role (the default is **admin**).
UCMDB Webservice Port	The port for connecting to the UCMDB Web service. If you are using the default UCMDB configuration, use port **8080** (for non-SSL connections to UCMDB).
UCMDB Webservice Protocol	The protocol for the UCMDB Web service (the default is **http**).

NTCMD Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the NTCMD server.
User Name	The name of the user needed to connect to the host as administrator.
Password	The password of the user needed to connect to the host as administrator.

Parameter	Description
Windows Domain	The Windows domain in which the credentials are defined. If this field is left empty or is not a valid domain, the NTCMD protocol assumes the user is defined locally on the host.
Run remote commands impersonated	If selected, the discovery commands are executed remotely under the **User Name** of this credential. If not selected, the discovery commands are, instead, executed remotely under the **LocalService** account.
Remote Share Path	Used where **Admin$** does not exist on the Windows machine being connected to. Type here the name of the SHARE concatenated with full path to the Windows directory of the machine being connected to. For example: **Share$\Windows**
Share Local Path	The full path to the Windows directory of the machine being connected to. For example: **C:\Windows**

See also: the section about the Extended Shell Interface in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document.

Note:

- You can use the HPCmd Utility to establish shell connection to remote Windows machines in order to execute commands for extracting important configuration information for population in the UCMDB. For details about this utility, see the section about HPCmd in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document.

- This protocol uses the DCOM protocol for connecting to remote machines. The DCOM protocol requires that the following ports are open: 135, 137, 138, and 139. In addition the DCOM protocol uses arbitrary ports between 1024 and 65535, but there are ways to restrict the port range used by WMI/DCOM/RPC. In addition, for information about for configuring DCOM to work with firewalls, see http://support.microsoft.com/kb/154596/en-us. For all versions of Windows after NT, port 445 (name: microsoft-ds) is the preferred port for resource sharing, including Windows file sharing and other services. It uses the TCP Protocol and replaces ports 137-139.

PowerShell Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the destination machine.
User Name	The name of the user that can connect to the remote machine by PowerShell.
User Password	The password of the user that can connect to the remote machine by PowerShell.
Windows Domain	The Windows domain on which the credentials are defined. If this field is empty, PowerShell assumes that the user is defined locally on the host.

Remedy Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Data Flow Probe stops trying to connect to the Remedy application server.
Remedy Password	Enter the password of the user account that enables access to Remedy/Atrium through the Java API.
Remedy Username	Enter the user name that enables access to Remedy/Atrium through the Java API.

SAP Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the SAP console.

Parameter	Description
User Name	The name of the user needed to log in to the SAP system. The user should have the following permissions: **Authorization Object: S_RFC** Authorization: For the **S_RFC** object, obtain privileges: RFC1, SALX, SBDC, SDIF, SDIFRUNTIME, SDTX, SLST, SRFC, STUB, STUD, SUTL, SXMB, SXMI, SYST, SYSU, SEU_COMPONENT. **Authorization Object: S_XMI_PROD** Authorization: EXTCOMPANY=MERCURY; EXTPRODUCT=DARM; INTERFACE=XAL **Authorization Object:S_TABU_DIS** Authorization: DICBERCLS=SS; DICBERCLS=SC
Password	The password of the user needed to log in to the SAP system.
SAP Client Number	It is recommended to use the default value (**800**).
SAP Instance Number	By default, set to **00**.
SAP Router String	A route string describes the connection required between two hosts using one or more SAProuter programs. Each of these SAProuter programs checks its Route Permission Table (http://help.sap.com/saphelp_nw04/helpdata /en/4f/992dfe446d11d189700000e8322d00/content.htm) to see whether the connection between its predecessor and successor is allowed. If it is, SAProuter sets it up.

SAP JMX Protocol

Parameter	Description
Port Number	The SAP JMX port number. The SAP JMX Port structure is usually `5<System Number>04`. For example, if the system number is `00`, the port is `50004`. Leave this field empty to try to connect to the discovered SAP JMX port; SAP JMX port numbers are defined in the **portNumberToPortName.xml** configuration file. For details, see the section about the portNumberToPortName.xml File in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the SAP JMX console.
User Name	The name of the user needed to connect to the application as administrator.
Password	The password of the user needed to connect to the application as administrator.

Siebel Gateway Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the Siebel Gateway console.
User Name	The name of the user needed to log on to the Siebel enterprise.
Password	The password of the user needed to log on to the Siebel enterprise.
Siebel Site Name	The name of the Siebel Enterprise.

Parameter	Description
Path to Siebel Client	The location on the Probe machine of the Siebel driver folder, where you copied `srvrmgr`. For details, see the section about Siebel in the *HP Universal CMDB Discovery and Integration Content Guide - Discovery Modules* document. • If there are several protocol entries with different `srvrmgr` versions, the entry with the newer version should appear before the entry with the older version. For example, to discover Siebel 7.5.3. and Siebel 7.7, define the protocol parameters for Siebel 7.7 and then the protocol parameters for Siebel 7.5.3. • **Siebel discovery**. If the Data Flow Probe is installed on a 64-bit machine on a Windows platform, place the **ntdll.dll**, **MSVCR70.DLL**, and **msvcp70.dll** drivers together with the Siebel drivers in the Siebel driver folder on the Probe machine. These drivers usually exist on a 32-bit machine and can be copied to the 64-bit machine.
Port number	The port to use during connection to the Siebel Gateway. **Default:** empty.

SNMP Protocol

Parameters

Parameter	Description
Port Number	(For SNMP versions v1, v2, and v3) The port number on which the SNMP agent listens.
Connection Timeout	Timeout(in milliseconds) after which the Probe stops trying to connect to the SNMP agent.
Retry Count	The number of times the Probe tries to connect to the SNMP agent. If the number is exceeded, the Probe stops attempting to make the connection.
Versions 1, 2	**Community**. Enter the authentication password you used when connecting to the SNMP service community (which you defined when configuring the SNMP service—for example, a community for read-only or read/write). **GET Request Operation Type**. The type of GET operation used to execute SNMP queries; either GET-NEXT or GET-BULK. **Default:** GET-NEXT.

Parameter	Description
Version 3	**Authentication Method**: Select one of the following options for securing the access to management information: • **noAuthNoPriv.** Using this option provides no security, confidentiality, or privacy at all. It can be useful for certain applications, such as development and debugging, to turn security off. This option requires only a user name for authentication (similar to requirements for v1 and v2). • **authNoPriv.** The user logging on to the management application is authenticated by the SNMP v3 entity before the entity allows the user to access any of the values in the MIB objects on the agent. Using this option requires a user name, password, and the authentication algorithm (HMAC-MD5 or HMAC-SHA algorithms). • **authPriv.** The user logging on to the management application is authenticated by the SNMP v3 entity before the entity allows the user to access any of the values in the MIB objects on the agent. In addition, all of the requests and responses from the management application to the SNMP v3 entity are encrypted, so that all the data is completely secure. This option requires a user name, password, and an authentication algorithm (HMAC-MD5 or HMAC-SHA). **User Name**: The name of the user authorized to log on to the management application. **Password**: The password used to log on to the management application. **Authentication Algorithm**: The MD5 and SHA algorithms are supported. **Privacy Key**: The secret key used to encrypt the scoped PDU portion in an SNMP v3 message. **Privacy Algorithm**: The DES, 3DES, AES-128, AES-192 and AES-256 algorithms are supported.

Note:

1. By default, SNMP queries are executed with a timeout of 3000 milliseconds. This value is defined in the snmpGlobalRequestTimeout parameter in the globalSettings.xml configuration file.

2. Due to control restrictions for some countries, the JDK has a deliberate, built-in key size restriction. If required (for example, if SNMP agents use 256-bit AES encryption), the restriction can be removed as follows:

   a. Download the .zip file from http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html.

   b. Extract **local_policy.jar** and **US_export_policy.jar** from the .zip file.

   c. Copy these files and replace the files that arrived with the probe installation in the **${PROBE_INSTALL}\bin\jre\lib\security\** folder.

   d. Restart the probe.

1. By default, SNMP queries are executed with a timeout of 3000 milliseconds. This value is defined in the snmpGlobalRequestTimeout parameter in the globalSettings.xml configuration file.

2. Due to control restrictions for some countries, the JDK has a deliberate, built-in key size restriction. If required (for example, if SNMP agents use 256-bit AES encryption), the restriction can be removed as follows:

   a. Download the .zip file from http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html.

   b. Extract **local_policy.jar** and **US_export_policy.jar** from the .zip file.

   c. Copy these files and replace the files that arrived with the probe installation in the **${PROBE_INSTALL}\bin\jre\lib\security\** folder.

   d. Restart the probe.

Troubleshooting and Limitations

Problem. Failure to collect information from SNMP devices.

- **Solution 1:** Verify that you can actually access information from your Network Management station by using a utility that can verify the connectivity with the SNMP agent. An example of such a utility is **GetIf**.

- **Solution 2:**: Verify that the connection data to the SNMP protocol has been defined correctly.

- **Solution 3:** Verify that you have the necessary access rights to retrieve data from the MIB objects on the SNMP agent.

SSH Protocol

Parameters

Parameter	Description
Port Number	By default an SSH agent uses port 22. If you are using a different port for SSH, enter that port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the remote machine. For the UNIX platform: If your server is slow, it is recommended to change Timeout to 40000.
Handshake Hello Timeout	The handshake timeout (in milliseconds).
Version	**SSH2**. Connect through SSH-2 only. **SSH1**. Connect through SSH-1 only. **SSH2 or SSH1**. Connect through SSH-2 and in case of error (if SSH-2 is not supported by the server), try to connect through SSH-1.
Shell Command Separator	The character that separates different commands in a shell (to enable the execution of several commands in the same line). For example, in UNIX, the default shell command separator is a semicolon (**;**). In Windows, the shell command separator is an ampersand (**&**).
Authentication Method	Choose one of the following authentication options to access SSH: • **password**. Enter a user name and password. • **publickey**. Enter the user name and path to the key file that authenticates the client. See also: "How to Create an SSH Connection Based on Public/Private Keys Pair" in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document. • **keyboard-interactive**. Enter questions and answers. For details, see "Prompts and Responses" on the next page below.
User Name	The name of the user needed to connect to the host through the SSH network protocol.
Password	The password of the user needed to connect to the host.

Parameter	Description
Key File Path	(Enabled when the `publickey` authentication method is selected.) Location of the authentication key. (In certain environments, the full key path is required to connect to an SSH agent.) See also: "How to Create an SSH Connection Based on Public/Private Keys Pair" in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document.
Prompts and Responses	(Enabled when the `keyboard-interactive` authentication method is selected.) A method whereby the server sends one or more prompts to enter information and the client displays them and sends back responses keyed-in by the user. The following is an example of prompts and expected responses: **Prompt**: Please enter your user name. **Response**: Shelly-Ann **Prompt**: What is your age? **Response**: 21 **Prompt**: This computer is HP property. Press y to enter. **Response**: y To create these prompts and responses, enter the following strings in the fields, separated by commas: **Prompts**: user,age,enter **Response**: Shelly-Ann,21,y You can enter the full string as it appears in the SSH prompt, or you can enter a key word, for example, **user**. DFM maps this word to the correct prompt.
Sudo paths	The full paths to the **sudo** command. Paths are separated by commas.

Parameter	Description
Sudo commands	A list of commands that can be executed with the **sudo** command. Commands are separated by commas. For all commands to be executed with **sudo**, add an asterisk (*****) to this field. This field accepts a **sudo** command that prompts for the user's password. There is both pattern matching and pattern completion using Python/Jython regular expressions. For example,for the expressions: • **/usr/sbin/uname** • **uname -a** • **uname -r** • **/mypath/my_other_path/uname -my args -my other args** the pattern match would be: **.*uname** This matches anything before **uname**, and any arguments **uname** has. The list of commands that can be executed with **sudo** is dependant on the configuration of **sudo** commands on the discovered destination. Therefore, an asterisk (*) in this field means that all commands configured on the discovered destination should be run with **sudo**. **Note:** To enable a non-root user to deploy the UD Agent on a UNIX system, ensure that the list of commands includes the **agentinstall.sh** and **nohup** commands.
***SU username**	The name of the user to use with the **su** command.
***SU password**	The password to use for the **su** command.
Sudo/SU Policy	• **su.** Use the **su** command. • **sudo.** Use the **sudo** command. • **sudo or su.** Use the **sudo** command. In case of failure, use the **su** command.

*To configure SU support options, right click **SSH protocol** and select **Edit using previous interface**.

> **Note:** The SSH1 protocol does not support public keys of the SSH2 protocol. Therefore, it is not advisable to set the alternative version (“SSH2 or SSH1”) if Authentication Method is configured to use publickey. In such a case, you should configure using the exact SSH protocol.

Troubleshooting

Problem. Failure to connect to the TTY (SSH/Telnet) agent.

- **Solution**. To troubleshoot connectivity problems with the TTY (SSH/Telnet) agent, use a utility that can verify the connectivity with the TTY (SSH/Telnet) agent. An example of such a utility is the client tool PuTTY.

Problem. Discovery job(s) fail with error message “Time out exception”.

- **Solution 1**. Increase the value of the **shellGlobalCommandTimeout** parameter in **globalSettings.xml**.
- **Solution 2**. Check the shell of the discovery user on the discovered destination. The command line for the ksh(korn shell) has a limit of 256 characters. Some discovery commands exceed that limit and can cause a “Time out exception” error message. In this case (a) Change the default shell for the discovery user from ksh to bash; or (b) Consult with the system administrator to determine if it is possible to increase the maximum command line size for korn shell on the problematic destination.

> **Note:** If you use the SSH or Telnet credentials for discovery, we recommend that you add the following folders to the system path:
>
> - /sbin
> - /usr/sbin
> - /usr/local/sbin

For details on configuring F-Secure when discovering Windows machines on which the F-Secure application is running on an SSH server, see the section about Windows Processes in the *HP Universal CMDB Discovery and Integration Content Guide - Discovery Modules*document.

For additional information about the SSH protocol, see the sections about the Extended Shell Interface and SSH Connection in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document:

Telnet Protocol

Parameters

Parameter	Description
Port Number	The port number. By default a Telnet agent uses port 23. If you are using a different port for Telnet in your environment, enter the required port number.

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the remote machine. **For UNIX platforms**: If your server is slow, it is recommended to change Connection Timeout to 40000.
Authentication Method	Choose one of the following authentication options to access Telnet: • **password**. Enter a user name and password. • **keyboard-interactive**. Enter questions and answers. For details, see "Prompts and Responses" below below.
User Name	The name of the user needed to connect to the host.
Password	The password of the user needed to connect to the host.
Prompts and Responses	(Enabled when the `keyboard-interactive` authentication method is selected.) A method whereby the server sends one or more prompts to enter information and the client displays them and sends back responses keyed-in by the user. The following is an example of prompts and expected responses: **Prompt**: Please enter your user name. **Response**: Shelly-Ann **Prompt**: What is your age? **Response**: 21 **Prompt**: This computer is HP property. Press y to enter. **Response**: y To create these prompts and responses, enter the following strings in the fields, separated by commas: **Prompts**: user,age,enter **Response**: Shelly-Ann,21,y You can enter the full string as it appears in the Telnet prompt, or you can enter a key word, for example, **user**. DFM maps this word to the correct prompt.
Sudo paths	The full paths to the **sudo** command. Paths are separated by commas.

Parameter	Description
Sudo commands	A list of commands that can be executed with the **sudo** command. Commands are separated by commas. For all commands to be executed with **sudo**, add an asterisk (*) to this field. This field accepts a **sudo** command that prompts for the user's password. There is both pattern matching and pattern completion using Python/Jython regular expressions. For example,for the expressions: • **/usr/sbin/uname** • **uname -a** • **uname -r** • **/mypath/my_other_path/uname -my args -my other args** The pattern match would be: • **.*uname** This matches anything before **uname**, and any arguments **uname** has. **Note:** The list of commands that can be executed with **sudo** is dependant on the configuration of **sudo** commands on the discovered destination. Therefore, an asterisk (*) in this field means that all commands configured on the discovered destination should be run with **sudo**.
***SU username**	The name of the user to use with the **su** command.
***SU password**	The password to use with the **su** command.
Sudo/SU policy	• **su.** Use the **su** command. • **sudo.** Use the **sudo** command. • **sudo or su.** Use the **sudo** command. In case of failure, use the **su** command. This is the default.

*To configure SU support options, right click **Telnet protocol** and select **Edit using previous interface**.

Troubleshooting and Limitations

Problem. Failure to connect to the TTY (SSH/Telnet) agent.

- **Solution**. To troubleshoot connectivity problems with the TTY (SSH/Telnet) agent, use a utility that can verify the connectivity with the TTY (SSH/Telnet) agent. An example of such a utility is the client tool PuTTY.

Limitation. The Telnet protocol does not support discovery of Windows Telnet servers.

Problem. Discovery job(s) fail with error message “Time out exception”.

- **Solution 1**. Increase the value of the **shellGlobalCommandTimeout** parameter in **globalSettings.xml**.
- **Solution 2**. Check the shell of the discovery user on the discovered destination. The command line for the ksh(korn shell) has a limit of 256 characters. Some discovery commands exceed that limit and can cause a “Time out exception” error message. In this case (a) Change the default shell for the discovery user from ksh to bash; or (b) Consult with the system administrator to determine if it is possible to increase the maximum command line size for korn shell on the problematic destination.

Note: If you use the SSH or Telnet credentials for discovery, we recommend that you add the following folders to the system path:

- /sbin
- /usr/sbin
- /usr/local/sbin

TIBCO Protocol

Parameter	Description
User Name	The name of the user needed to log into the TIBCO system.
Password	The password of the user needed to log into the TIBCO system.

UDDI Registry Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the UDDI Registry.
UDDI Registry URL	The URL where the UDDI Registry is located.

Universal Discovery Protocol

See also the section about the Extended Shell Interface in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document.

Parameter	Description
UD SHA1 ID	A hash of UD credential's certificates. Enables you to visually distinguish between UD credentials that have different certificates (different hash) and those that have similar certificates (similar hash). **Note:** This value is generated automatically and cannot be modified.
Port Number	The port number on which the UD Agent listens. Select one of the following ports: • **2738** • **7738**
Connection Timeout	The amount of time (in milliseconds) after which the Probe stops trying to connect to the UD Agent.
Sudo paths	The full paths to the **sudo** command. Paths are separated by commas.

Parameter	Description
Sudo commands	A list of commands that can be executed with the **sudo** command. Commands are separated by commas. For all commands to be executed with **sudo**, add an asterisk (*****) to this field. This field accepts a **sudo** command that prompts for the user's password. There is both pattern matching and pattern completion using Python/Jython regular expressions. For example,for the expressions: • **/usr/sbin/uname** • **uname -a** • **uname -r** • **/mypath/my_other_path/uname -my args -my other args** the pattern match would be: **.*uname** This matches anything before **uname**, and any arguments **uname** has. The list of commands that can be executed with **sudo** is dependant on the configuration of **sudo** commands on the discovered destination. Therefore, an asterisk (*) in this field means that all commands configured on the discovered destination should be run with **sudo**. **Note:** To enable a non-root user to deploy the UD Agent on a UNIX environment, ensure that the list of commands includes the **agentinstall.sh** and **nohup** commands.

vCloud Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the vCloud application server.
User Name	The name of the user needed to connect to the application.
User Password	The password of the user needed to connect to the application.
vCloud Organization	The organization the user belongs to. When connecting with the global vCloud Administrator, set this to **System**.

VMware Infrastructure Management (VIM) Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to VMware Infrastructure.
Port Number	DFM uses the number defined here when processing one of the `Network – VMware` jobs: If the port number is left empty, DFM performs a WMI query to extract the port number from the registry. DFM queries **HKLM\SOFTWARE\VMware, Inc.\VMware VirtualCenter** and searches for the **HttpsProxyPort** or **HttpProxyPort** attributes: • If the **HttpsProxyPort** attribute is found, DFM uses its value for the port and sets the prefix to **HTTPS**. • If the **HttpProxyPort** attribute is found, DFM uses its value for the port and sets the prefix to **HTTP**.
Use SSL	**true**: DFM uses a Secure Sockets Layer (SSL) protocol to access VMware Infrastructure, and the prefix is set to **HTTPS**. **false**: DFM uses the http protocol.
User Name	The name of the user needed to connect to VMware Infrastructure.
Password	The password of the user needed to connect to VMware Infrastructure.

WebLogic Protocol

Parameter	Description
Port Number	If you enter a port number, DFM tries to connect to WebLogic using this port number. However, say you know that there are many WebLogic machines in the environment and do not want to have to create a new credential for each machine. You leave the Port Number field empty. When accessing a WebLogic machine, DFM refers to the WebLogic port (defined in **portNumberToPortName.xml**) already found on this machine (by TCP scanning). **Note**: You can leave the port number empty on condition that: • All WebLogic ports are added to the **portNumberToPortName.xml** file. For details, see the section about the portNumberToPortName.xml File in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document. • The same user name and password is needed to access all WebLogic instances.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the WebLogic application server.
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.
Protocol	An application-level protocol that determines whether DFM should connect to the server securely. Enter **http** or **https**.
Trust Store File Path	Enter the full path to the SSL trust store file. To use the trust store file, do one of the following: • Enter the name (including the extension) and place the file in the following resources folder: **C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\weblogic\<WebLogic version>**. • Insert the trust store file full path.
Trust Store Password	The SSL trust store password.

Parameter	Description
Key Store File Path	Enter the full path to the SSL keystore file. To use the keystore file, do one of the following: • Enter the name (including the extension) and place the file in the following resources folder: **C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\weblogic\<WebLogic version>**. • Insert the keystore file full path.
Key Store Password	The password for the keystore file.

WebSphere Protocol

Parameter	Description
Port Number	The protocol port number as provided by the WebSphere system administrator. You can also retrieve the protocol port number by connecting to the Administrative Console using the user name and password provided by the WebSphere system administrator. In your browser, enter the following URL: **http:/<host>:9060/admin**, where: • **<host>** is the IP address of the host running the WebSphere protocol • **9060** is the port used to connect to the WebSphere console Access **Servers > Application Servers > Ports > SOAP_CONNECTOR_ADDRESS** to retrieve the required port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the WebSphere server.
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.

Parameter	Description
Trust Store File Path	The name of the SSL trust store file. To use the trust store file, do one of the following: • Enter the name (including the extension) and place the file in the following resources folder: **C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\websphere**. • Insert the trust store file full path.
Trust Store Password	The SSL trust store password.
Key Store File Path	The name of the SSL keystore file. To use the keystore file, do one of the following: • Enter the name (including the extension) and place the file in the following resources folder: **C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryResources\j2ee\websphere**. • Insert the keystore file full path.
Key Store Password	The password for the keystore file.

WMI Protocol

Parameter	Description
User Name	The name of the user needed to connect to the host.
Password	The password of the user needed to connect to the host.
Windows Domain	The Windows domain in which the credentials are defined. If this field is left empty or is not a valid domain, the WMI protocol assumes the user is defined locally on the host.

- For improved performance, it is recommended to use domain accounts rather than local accounts, with the WMI protocol.

- This protocol uses the DCOM protocol for connecting to remote machines. The DCOM protocol requires that the following ports are open: 135, 137, 138, and 139. In addition the DCOM protocol uses arbitrary ports between 1024 and 65535, but there are ways to restrict the port range used by WMI/DCOM/RPC. In addition, for information about for configuring

DCOM to work with firewalls, see http://support.microsoft.com/kb/154596/en-us.

Chapter 6

Default Ports for Supported Protocols

The following table lists the default ports for each supported protocol.

Protocol	Default Port
HP SIM	50001, 280
HTTP	80
JBoss	1099
LDAP	389
NNM	80
NTCMD	135, 137, 138, 139
PowerShell	80, 443, 5985, 5986 **Note:** The ports depend on the Microsoft Windows operating system configuration
SAP	• 3200 • 3300-3303 • 33xx, where xx is the SAP server instance number **Note:** To enable UCMDB to identify other port numbers mapped to SAP instances, you must configure the **portNumberToPortName.xml** file. For more details, see "How to Define a New Port" in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document.
SAP JMX	• 50004, 50104, 50204, 50304, 50404 • 5xx04, where xx is the SAP J2EE server instance number **Note:** To enable UCMDB to identify other port numbers mapped to SAP instances, you must configure the **portNumberToPortName.xml** file. For more details, see "How to Define a New Port" in the *HP Universal CMDB Discovery and Integration Content Guide - General Reference* document.
Siebel Gateway	2320
SNMP	161
SQL	1521, 1433, 6789, 3306, 2048

Protocol	Default Port
SSH	22
Telnet	23
UDDI	80, 443
VMWare VIM	80, 443
WebLogic	7001, 7002
WebSphere	8880
WMI	135, 137, 138, 139

Chapter 7

Discovery Modules and Jobs

The following is a list of discovery modules and the discovery jobs they contain.

Module	Discovery Jobs
Cloud and Virtualization > Cloud > Amazon Web Services	• AWS by Web Services
Cloud and Virtualization > Cloud > VMware vCloud	• vCloud Director by vCloud API • vCloud Director URL by vCloud API
Cloud and Virtualization > Virtualization > HP nPartitions	• HP nPars and vPars by Shell
Cloud and Virtualization > Virtualization > Hyper-V	• Hyper-V Topology by Shell • Hyper-V Topology by WMI
Cloud and Virtualization > Virtualization > IBM HMC	• IBM HMC by SHELL • IBM LPAR And VIO Server Topology by Shell
Cloud and Virtualization > Virtualization > Oracle VM Server for SPARC	• Oracle VM Server for SPARC Technology by Shell
Cloud and Virtualization > Virtualization > Solaris Zones	• Solaris Zones by TTY
Cloud and Virtualization > Virtualization > VMware	• VMware vCenter Connection by WMI and VIM • VMware vCenter Topology by VIM • VMware ESX Connection by VIM • VMware ESX Topology by VIM • Manual VMware VIM Connection • VMware vMotion Monitor by VIM

Module	Discovery Jobs
Cloud and Virtualization > Virtualization > Xen and KVM	- Xen and KVM by Shell
Clustering and Load Balancing > Failover Clusters > EMC AutoStart	- EMC AutoStart By Shell
Clustering and Load Balancing > Failover Clusters > HACMP	- HACMP Topology Discovery - HACMP Application Discovery
Clustering and Load Balancing > Failover Clusters > Microsoft Cluster	- MS Cluster by NTCMD or UDA
Clustering and Load Balancing > Failover Clusters > ServiceGuard	- Service Guard Cluster Topology by TTY
Clustering and Load Balancing > Failover Clusters >Solaris Cluster	- Sun Cluster by Shell
Clustering and Load Balancing > Failover Clusters > Veritas	- Veritas Cluster by Shell
Clustering and Load Balancing > Load Balancers > Alteon LB	- Alteon application switch by SNMP
Clustering and Load Balancing > Load Balancers > Cisco CSS	- Cisco CSS by SNMP
Clustering and Load Balancing > Load Balancers > F5 Big IP	- F5 BIG-IP LTM by SNMP
Clustering and Load Balancing > Load Balancers > Microsoft NLB	- MS NLB by NTCMD or UDA
Database > Connections using Host Credentials	- DB Connections by Shell - DB Connections by WMI
Database > DB2	- Databases TCP Ports - DB2 Universal Database Connection by SQL - DB2 Topology by SQL
Database > DB2	- HP NonStop Topology by Shell
Database > HanaDb	- HanaDb by Shell

Module	Discovery Jobs
Database > MS-SQL	• Databases TCP Ports • MSSQL Server Connection by SQL • MSSQL Topology by SQL
Database > MaxDb	• MaxDb by Shell
Database > MySQL	• Databases TCP Ports • MySQL Connection by SQL • MySQL by Shell
Database > Oracle	• Databases TCP Ports • Oracle Database Connection by SQL • Oracle Topology by SQL • Oracle Config Files by SQL • Oracle Listeners by Shell • Oracle RAC Topology by Shell
Database > Sybase	• Databases TCP Ports • Sybase Database Connection by SQL • Sybase Topology by SQL
Discovery-based Product Integrations > CiscoWorks LAN Management Solution	• CiscoWorks LMS Database Ports
Enterprise Applications > Active Directory	• Active Directory Topology by LDAP • Active Directory Connection by LDAP

Module	Discovery Jobs
Enterprise Applications > Microsoft Exchange	• Microsoft Exchange Topology by WMI • Microsoft Exchange Connection by NTCMD or UDA • Microsoft Exchange Topology by NTCMD or UDA • Microsoft Exchange Connection by WMI • Microsoft Exchange Topology by LDAP • Microsoft Exchange Topology by PowerShell
Enterprise Applications > Microsoft SharePoint	• Microsoft SharePoint Topology
Enterprise Applications > Oracle E-Business Suite	• Oracle Applications by SQL
Enterprise Applications > SAP	• SAP ABAP Connection by SAP JCO • SAP ABAP Topology by SAP JCO • SAP Applications by SAP JCO • SAP ITS by NTCMD or UDA • SAP Java Topology by SAP JMX • SAP Solution Manager by SAP JCO • SAP Solution Manager Topology by SAP JCO • SAP System by Shell • SAP Profiles by Shell • SAP TCP Ports

Module	Discovery Jobs
Enterprise Applications > Siebel	• Siebel Application Servers • Siebel DB by NTCMD or UDA • Siebel DB by TTY • Siebel Application Server Configuration • Siebel Gateway Connection • Siebel Web Applications by NTCMD or UDA • Siebel Web Applications by TTY
Hosts and Resources > Basic Applications	• Host Applications by Power Shell • Host Applications by Shell • Host Applications by SNMP • Host Applications by WMI
Hosts and Resources > IBM i (iSeries) > IBM i By Eview	• IBM i Connection • IBM i Objects • IBM i Resources
Hosts and Resources > Inventory Discovery > Basic Inventory	• Host Resources by Power Shell • Host Resources by Shell • Host Resources by SNMP • Host Resources by WMI
Hosts and Resources > Inventory Discovery > Inventory by Scanner	• Call Home Processing • Inventory Discovery by Manual Scanner Deployment • Inventory Discovery by Scanner

Module	Discovery Jobs
Hosts and Resources > Mainframe > Mainframe by EView Agent	• DB2 by EView • CICS by EView • EView Connection • LPAR Resources by EView • IMS by EView • MQ by EView
Hosts and Resources > Mainframe > Mainframe by SNMP	• Mainframe TCP by SNMP • Mainframe topology by SNMP
Hosts and Resources > Storage > NetApp Filer	• NetApp Filer by WebServices
Hosts and Resources > Storage > SMI-S	• Storage Devices Connection by SMI-S • Storage Devices Topology by SMI-S
Middleware > Java EE Application Servers > Apache Tomcat	• Apache Tomcat by Shell
Middleware > Java EE Application Servers > Glassfish	• JEE Glassfish by Shell
Middleware > Java EE Application Servers > JBoss	• JEE JBoss by Shell • JEE TCP Ports • JEE JBoss by JMX • JEE JBoss Connections by JMX
Middleware > Java EE Application Servers > Oracle iAS	• Oracle Application Server • WebServices by URL

Module	Discovery Jobs
Middleware > Java EE Application Servers > WebLogic	• JEE TCP Ports • JEE Weblogic by JMX • JEE Weblogic by Shell • JEE Weblogic Connections by JMX • WebServices by URL
Middleware > Java EE Application Servers > WebSphere	• JEE TCP Ports • JEE WebSphere by Shell • JEE WebSphere by Shell or JMX • JEE WebSphere Connections by JMX
Middleware > Messaging Servers > Microsoft MQ	• Active Directory Connection by LDAP • Microsoft Message Queue Topology by LDAP • Microsoft Message Queue Topology by NTCMD or UDA
Middleware > Messaging Servers > TIBCO	• TIBCO BusinessWorks by Shell • TIBCO EMS by Shell
Middleware > Messaging Servers > WebSphere MQ	• MQ by Shell
Middleware > Web Servers > Basic	• Webserver by Shell • WebServer Detection using TCP Ports • WebSphere to Webserver Dependency
Middleware > Web Servers > IIS	• IIS Applications by NTCMD or UDA • WebServices by URL

Module	Discovery Jobs
Middleware > Web Services > UDDI Registry	• WebService Connections by UDDI Registry • WebServices by UDDI Registry • WebServices by URL
Network Infrastructure > Basic	• Arp Table by SNMP • Cisco HSRP by SNMP • Class B IPs by ICMP • Class C IPs by ICMP • Client Connection by SNMP • DNS Resolver • IP MAC Harvesting by SNMP • Range IPs by ICMP • Range IPs by nmap
Network Infrastructure > DNS	• DNS Zone by DNS • DNS Zone by nslookup • Hosts by Shell using nslookup on DNS Server
Network Infrastructure > Host Connection	• Host Connection by PowerShell • Host Connection by Shell • Host Connection by SNMP • Host Connection by WMI • Host Connection by AS400
Network Infrastructure > JIT Discovery	• JIT Passive Discovery

Module	Discovery Jobs
Network Infrastructure > Layer2	• Host Networking by SNMP • Layer2 Saved Files • Layer2 Topology Bridge-based by SNMP • Layer2 Topology VLAN-based by SNMP • Merge VLANs by Ports • VLAN ports by SNMP • VLANs by SNMP
Network Infrastructure > No-Credentials Discovery	• Host Fingerprint using nmap • Hosts using nslookup on Probe • Microsoft Windows Domains • Microsoft Windows Domains Topology
Network Infrastructure > TCP Connectivity > Active Discovery	• TCP Data by Shell • TCP Data by SNMP
Network Infrastructure > TCP Connectivity > Passive Discovery	• Collect Network Data by NetFlow • Network Connectivity Data Analyzer
Tools and Samples > Deprecated Jobs	• IHS Websphere Plugin by Shell • IP Traffic by Network Data • Potential Servers by Network Data • Server Ports by Network Data • Servers by Network Data
Tools and Samples > Discovery Samples	• Dynamic Credential Sample

Module	Discovery Jobs
Tools and Samples > Discovery Tools	• File Monitor by Shell • Link DB Datafiles And Clustered FS • Merge Clustered Software • TCP Ports
Tools and Samples > Getting Started Guide	• SQL Discovery Tutorial
Tools and Samples > UD Agent Management	• Install UD Agent • Uninstall UD Agent • Update UD Agent

Chapter 8

Supported Integrations

- Aperture VISTA
- Atrium to UCMDB
- CA CMDB
- CiscoWorks LMS
- Data Dependency and Mapping Inventory
- Data Push into Atrium
- EMC Control Center (ECC)
- HP Asset Manager
- HP Configuration Manager
- HP ServiceCenter/Service Manager
- HP Systems Insight Manager (HP SIM)
- IDS Scheer ARIS
- Microsoft SCCM/SMS
- NetApp SANscreen/OnCommand Insight
- Network Node Manager (NNMi)
- ServiceNow
- Storage Essentials (SE)
- Troux
- UCMDB to XML Adapter

Chapter 9

Support for HP UCMDB Integration Service on Linux

The following table lists the integration adapters that support the HP UCMDB Integration Service on the Linux platform.

Adapter	Population	Federation	Data Push
AM	Not supported	Not supported	Not supported
SM 6.2x\7.0x\7.1x-9.2x	-	Not supported	Not supported
SM 9.x	Supported	Supported	Supported
UCMDB 9.x\10.x	Supported	Supported	-
CM policy\kpi adapters	-	Supported	-
DDMi	Not supported	Supported	-
Generic Push adapters	-	-	Not supported
SMS/SCCM	Not supported	Supported	-
Service now	-	-	Not supported
EMC Control Center	Supported	-	-
Storage Essentials	Supported	-	-
NNMi	Supported	-	Supported
SIM	Supported	-	-

Chapter 10

Localization

This section details localized versions of operating systems and applications which are supported by UCMDB.

Operating Systems

Discovery of host resources, Universal Discovery Agent installation (including the Software Utilization Plug-In) and inventory discovery using Inventory Scanners, is supported for the following localized versions of **Windows**:

- Chinese
- Dutch
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Spanish

Applications

Vendor	Product	Versions	Supported Localized Versions
Microsoft	Active Directory	2003, 2008	Japanese
Microsoft	Cluster Services	2003R2, 2008R2	Japanese
Microsoft	Hyper-V	2008, 2008R2	Japanese