Universal CMDB

Software Version: Content Pack 19.00 (CP19)

Discovery and Integrations Content Guide - Supported Content

Document Release Date: February 2017 (Second Edition)
Software Release Date: March 2016

Hewlett Packard
Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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: https://softwaresupport.hp.com/.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HP Software Support site or click **Create an Account** 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 HPE sales representative for details.

Document Changes

Version	Changes
CP19 (2nd Edition, February 7, 2017)	Added clarification about the Red Hat Enterprise Linux versions supported. For details, see the "Discovered Operating Systems" section.

Support

Visit the HP Software Support site at: https://softwaresupport.hp.com.

This website 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 website 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 to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: https://softwaresupport.hp.com/web/softwaresupport/access-levels.

HP Software Solutions Now accesses the HPSW Solution and Integration Portal website. 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 website is http://h20230.www2.hp.com/sc/solutions/index.jsp.

Contents

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, 2.4	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.x, 7.x, 8.x, 9.0	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.x, 9.x	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.

Vendor	Product	Versions	Credentials	Discovers...
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.
Cisco	CSS	6.1, 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, 4, 4.1, 4.2, 5.6, 5.6 FP1, 5.6 SP2, 6.0, 6.0.2, 6.1, 6.2, 6.5	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.

Vendor	Product	Versions	Credentials	Discovers...
EMC	EMC Control Center (ECC)	6.0, 6.1	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.
F5	BIG-IP LTM	4.6, 9.1, 10.2.2, 10.2.3, 10.2.4, 11, 11.1.0, 11.2.1, 11.3.0, 11.4.0	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	IVM	B.06.10.05	SSH	Virtualization Layer Software, Node, HP IVM Config, Interface
HP	Network Node Manager (NNM)	8.1, 8.11, 9.0, 9.1, 10.00, 10.10	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.

Vendor	Product	Versions	Credentials	Discovers...
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, 7.2, 7.3, 7.4, 7.5	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, 9.6, 9.7	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 (renamed to iSeries/IBM i)	V3R2M0, V3R2M1, V4R2M0, V4R5M0, V5R3, V5R4MO, V6R1	AS400	AS400Agent, Interface, IpSubnet, Node.
IBM	DB2 Universal Database (UDB)	8.2, 9.1, 9.5, 9.7, 9.8, 10.1, 10.5	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	FSM	1.x	SSH	Chassis, Composition, Containment, IBM FSM, IBM Frame, Interface, IpAddress, Management, Node, Realization, Storage Array, and Switch.
IBM	HACMP	5.3, 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, 4.x, 5.x, 6.x, 7.x, 8	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, 8.0, 8.5, 8.5.5	Shell	IBM Http Server's WebSphere plug-in configuration by parsing the IHS plug-in configuration file.
IBM	IVM		SSH, Telnet	CPU, I/O Slot, IBM Frame, IBM IVM, IBM Processor Pool, Node, Virtualization Layer Software

Vendor	Product	Versions	Credentials	Discovers...
IBM	MQ Series (aka WebSphere MQ)	5.x, 6.x, 7.0.1, 7.1, 7.5, 8.0	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	Security Access Manager for Web	8.x	HTTP	Security Access Manager for Web.
IBM	Security Access Manager for Web	6- 8.x	Shell	Security Access Manager for Web.
IBM	WebSphere Application Server	5.x, 6.1, 7.0, 8.0, 8.5, 8.5.5	Shell	J2EE Server, J2EE application, JDBC datasource, Database, EJB Module, Web Module, J2EE Domain and JMS resources
JBoss	Application Server	4.x, 5.x, 6.x, 7.x, 8.x, 9.x, 10.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.

Vendor	Product	Versions	Credentials	Discovers...
JBoss	Application Server	4.x, 5.x, 6.x, 7.x, 8.x, 9.x, 10.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, 2008 R2, 2012, 2012 R2	LDAP	Forest, Sites, Sitelinks, Domain controllers, Networks, and so on.
Microsoft	App- V	4.5, 5.0	None	Detects virtual applications that run under supported application virtualization technologies.
Microsoft	Cluster Services	Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2	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, 2013, 2016	LDAP	Forest, Sites, Exchange folders, folder trees, Administrative groups, Connectors.
Microsoft	Exchange Server	2007, 2010, 2013, 2016	NTCMD, PowerShell	Exchange Server, Exchange roles, Administrative group, Exchange Organization, Exchange Clustered Mailbox, Exchange Database Availability Group.

Vendor	Product	Versions	Credentials	Discovers...
Microsoft	Hyper-V	Windows 2008, Windows 2008 R2, Windows Server 2012, Windows Server 2012 R2	NTCMD, WMI	Resource pools, virtual switches, virtual NICs, virtual machines, and configuration files.
Microsoft	IIS	5, 6, 7, 7.5, 8, 8.5	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	2000, 2003, 2008, 2012, 2012 R2	NTCMD	NLB Cluster, NLB Cluster Software and Node.
Microsoft	SharePoint	2007, 2010, 2013	NTCMD	Windows, SQL Server, IIS Application Pool, IIS Web Server, IIS Web Service, IIS Web Site, SharePoint Farm.
Microsoft	SQL Server	2000, 2005, 2008, 2008 R2, 2012, 2012 SP2, 2014	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, 8.x	NetApp	Node, LogicalVolume, Logical Volume Snapshot, FileSystem, FileSystemExport, IpAddress, Interface, CPU, Memory.

Vendor	Product	Versions	Credentials	Discovers...
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, 11g	Shell	OC4J groups, OC4J instances and its URLs.
Oracle	Database	9, 10g, 11g, 12c, 12c R1	Shell	Oracle database, TNS Listener software.
Oracle	Database	8, 9, 10g, 11g, 12c, 12c R1	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.
Oracle	LDOM	1.0-1.3	SSH, Telnet	LDOM Networking and Storage topologies.
Oracle	Oracle VM for x86	3.2.1	SSH	Virtualization topology, Virtual Machines, Server Pools, Hypervisors
Oracle	Oracle VM Server for SPARC	2.0-2.1	SSH, Telnet	LDOM Networking and Storage topologies.
Oracle	RAC	9, 10g, 11g, 12c, 12c R1	Shell	Oracle RAC.
Oracle	RAC	10g, 11g , 12c, 12c R1	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.

Vendor	Product	Versions	Credentials	Discovers...
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, 8.2	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	9.x, 10.x, 11g, 11gR1 SP1, 11gR1 SP2, 11gR1 SP3, 12c	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.
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.

Vendor	Product	Versions	Credentials	Discovers...
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, 7.0, 7.3	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, 7.1	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
SAP	TREX/BIA	7.00-7.30	SSH, Telnet, NTCMD	SapTrexInstance, SapTrexSystem, SAP System

Vendor	Product	Versions	Credentials	Discovers...
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	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, 16	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
Troux	Troux	9.0x		
VMware	ESX	2.5, 3, 4, 4.1, 5.0	Shell	
VMware	ESX & ESXi	4.1, 5.0, 5.1, 5.5, 6.x	CIM	ESX servers, Virtual Machines

Vendor	Product	Versions	Credentials	Discovers...
VMware	ESX & ESXi	2.5, 3, 3i, 3.5, 4, 4.1, 5.0, 5.1, 5.5, 6.0	VIM	ESX servers, cluster groups, virtual resource groups.
VMware	vCenter (formerly Virtual Center)	2.01, 2.5, 4, 4.1, 5.0, 5.1, 5.5, 6.0	VIM and WMI	Virtual Center Server, License Server, ESX servers, cluster groups, virtual resource groups.
VMware	vCloud Director	1.5 - 5.1.2	vCloud	VMware vCloud Director and vCloud Resources (Organization, Catalog, Media, vApp, and so on).

ASM Content Support Matrix

The list below shows the Automated Service Modeling (ASM) supportability on the following technologies:

- Supports the following J2EE servers:
  - WebSphere
  - JBoss
  - WebLogic
- Supports WebSphere MQ when it is integrated with one of the following servers:
  - WebSphere
  - Weblogic
- Supports the following Database servers:
  - Oracle single instance and RAC
  - SQL Server single instance and cluster
  - DB2 single instance (does not support DB2 cluster and mainframe).
  - MySQL
  - PostgreSQL
- Supports IIS as the ASP or .NET application server.
- Supports the following Web Servers:

  - Apache
  - IBM HTTP Server
  - IIS
  - Tomcat
- Supports the following access management products:
  - IBM WebSEAL
  - Oracle Access Manager
- Supports the following load balancers (need to run bottom-up discovery first):
  - F5
  - Cisco ACE
  - Alteon LB
  - Citrix NetScaler
  - A10 vThunder
- Supports the following cluster:
  - Microsoft cluster
- Supports the following enterprise applications:
  - HP Universal CMDB
  - HP Service Manager

Supported Protocols

ASM can run discoveries through the following protocols:

- NTCMD
- SSH
- Universal Discovery Protocol

Chapter 2: Discovered Operating Systems

Vendor	Product	Versions	Credentials	Content
Apple	OS X	10.5,10.6, 10.7, 10.8, 10.9, 10.10, 10.11	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users
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
Linux	CentOS	5, 6, 7	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users

Vendor	Product	Versions	Credentials	Content
Linux	Ubuntu Server/Desktop	10, 11, 12, 13, 14, 15	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users
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
Red Hat	Red Hat Enterprise Linux	3, 4, 5, 6, 7	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users
Sun	Solaris	5.9, 5.10, 11	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users
SUSE	SUSE Linux Enterprise	10 and later	SSH, Telnet	OS, Memory, Disks, CPU, Processes, Software (packages), Services (daemons), Files, Local Users

Vendor	Product	Versions	Credentials	Content
Microsoft	Windows	• Windows XP Home, Professional • Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 • Windows Vista Business, Enterprise, Ultimate • Windows 7 Professional, Enterprise, Ultimate • Windows 8, Windows 8.1, Windows 8 Pro, Windows 8 Enterprise • Windows 10 Home, Windows 10 Pro, Windows 10 Enterprise	NTCMD, PowerShell, WMI	OS, Memory, Disks, CPU, Processes, Software, Services, Files, Local Users

Chapter 3: Universal Discovery IPv6 Support

This section is an overview of Universal Discovery jobs, adapters, and protocols that support IPv6.

Note: Content not mentioned in this list supports IPv4 only.

Discovery Jobs

The following discovery jobs support IPv6.

Module	Discovery Job	Works Over IPv6	Discovers IPv6 Data
Clustering and Load Balancing Failover Clusters > Microsoft Cluster	MS Cluster by NTCMD or UDA	✓	✓
Databases > DB2	Databases TCP Ports	✓	✓
Databases > DB2	DB2 Topology by SQL	✓	✓
Databases > DB2	DB2 Universal Database Connection by SQL	✓	✓
Databases > MS-SQL	Databases TCP Ports	✓	✓
Databases > MS-SQL	MSSQL Server Connection by SQL	✓	✓
Databases > MS-SQL	MSSQL Topology by SQL	✓	✓
Databases > MySQL	MySQL Connection by SQL	✓	✓
Databases > Oracle	Databases TCP Ports	✓	✓
Databases > Oracle	Oracle Config Files by SQL	✓	✓
Databases > Oracle	Oracle Database Connection by SQL	✓	✓
Databases > Oracle	Oracle Topology by SQL	✓	✓
Databases > Sybase	Databases TCP Ports	✓	✓
Database > Sybase	Sybase Database Connection by SQL	✓	✓

Module	Discovery Job	Works Over IPv6	Discovers IPv6 Data
Databases> Sybase	Sybase Topology by SQL	✓	✓
Enterprise Applications > Microsoft Exchange	Microsoft Exchange Topology by PowerShell	✓	✓
Enterprise Applications > Microsoft SharePoint	Microsoft SharePoint Topology	✓	✓
Enterprise Applications > Oracle E-Business Suite	Oracle Applications by SQL	✓	✓
Hosts and Resources > Basic Applications	Host Applications by PowerShell	✓	✓
Hosts and Resources > Basic Applications	Host Applications by Shell	✓	✓
Hosts and Resources > Basic Applications	Host Applications by SNMP	✓	✓
Hosts and Resources > Basic Applications	Host Applications by WMI	✓	✓
Hosts and Resources > Inventory Discovery > Basic Inventory	Host Resources by PowerShell	✓	✓
Hosts and Resources > Inventory Discovery > Basic Inventory	Host Resources by Shell	✓	✓
Hosts and Resources > Inventory Discovery > Basic Inventory	Host Resources by SNMP	✓	✓
Hosts and Resources > Inventory Discovery > Basic Inventory	Host Resources by WMI	✓	✓
Network Infrastructure > Host Connection	Host Connection by PowerShell	✓	✓
Network Infrastructure > Host Connection	Host Connection by Shell	✓	✓
Network Infrastructure > Host Connection	Host Connection by SNMP	✓	✓
Network Infrastructure > Host Connection	Host Connection by WMI	✓	✓
Tools and Samples > SSL Certificates	SSL Certificates Discovery by HTTPS	✓	✓
Tools and Samples > UD Agent Management	Install UD Agent	✓	✓

Module	Discovery Job	Works Over IPv6	Discovers IPv6 Data
Tools and Samples > UD Agent Management	Uninstall UD Agent	✓	✓
Tools and Samples > UD Agent Management	Update UD Agent	✓	✓

Integrations

The following integration adapters support IPv6.

Integration	Works Over IPv6	Discovers IPv6 Data
ALMAdapter	✓	✓
BSM 9.x	✓	
BSM Kpi Adapter	✓	✓
CiscoWorks Net Devices	✓	✓
CM KPI Adapter	✓	✓
CM New Policy Adapter	✓	✓
CM Policy Adapter	✓	✓
DDMI	✓	
EMC Control Center	✓	N/A
Enterprise Collaboration	✓	✓
Generic Database Adapter (GDBA)	✓	N/A
Import topology from CSV file	✓	N/A
Import topology from Database	✓	N/A
Import topology from Properties file	✓	N/A
Operation Orchestration Automation Flow Adapter	✓	✓
Pull Topology from NNMi		✓
Push Adapter	✓	N/A
Push DB Example	✓	N/A
Storage Essentials	✓	N/A

Integration	Works Over IPv6	Discovers IPv6 Data
System Center Configuration Manager	✓	
UCMDB 10.x	✓	✓
UCMDB 9.x	✓	✓

Protocols

The following protocols support IPv6.

- HTTP
- NTCMD
- PowerShell
- SQL (Generic DB)
- SNMP
- SSH
- Telnet
- Universal Discovery Agent
- WMI

Chapter 4: 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 5: Universal Discovery Agent, Software Utilization Plug-In, Scanner, Scanner Scheduler, and SAI Support

The Universal Discovery Agent, Software Utilization Plug-in, Scanner, Scanner Scheduler, and the Software Application Library (SAI) are installed on the discovered machines. These components are supported for machines running on the following operating systems and platforms:

Windows

Operating System	Version	Platform	Agent	Utilization Plug-in	Scanner/Scanner Scheduler	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	
	2012	x64	x	x	x	x
Vista	Business, Enterprise, Ultimate	x86, x64	x	x	x	x
Windows 7	Professional, Enterprise, Ultimate	x86, x64	x	x	x	x
Windows 8	Windows 8, Windows 8 Pro, Windows 8 Enterprise	x86, x64	x	x	x	x
Windows 10	Windows 10 Home, Windows 10 Pro, Windows 10 Enterprise	x86, x64	x	x	x	x

Linux

Operating System	Version	Platform	Agent	Utilization Plug-in	Scanner/Scanner Scheduler	SAI
Red Hat Enterprise AS/ES/WS	3, 4	x86, x64	x	x	x	x
Red Hat Enterprise Server/Desktop	5, 6, 7		x	x	x	x
Novell SUSE Enterprise Server/Desktop	9, 10, 11, 12		x	x	x	x
Oracle	4, 5, 6, 7		x	x	x	x
CentOS	5, 6, 7		x	x	x	x
Ubuntu Server/Desktop	10, 11, 12, 13, 14, 15		x	x	x	x

IBM

Operating System	Version	Platform	Agent	Utilization Plug-in	Scanner/Scanner Scheduler	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/ Scanner Scheduler	SAI
Oracle Solaris	9	x64, SPARC	x	x	x	x
	10, 11	x86, x64, SPARC	x	x	x	x

HP UNIX

Operating System	Version	Platform	Agent	Utilization-Plug-in	Scanner/Scanner Scheduler	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/Scanner Scheduler	SAI
OS X	10.5,10.6, 10.7, 10.8, 10.9, 10.10, 10.11	x86	x	x	x	x

Chapter 6: Store and Forward Server Support

The Store and Forward server is supported on the following operating systems and platforms:

Windows

Operating System	Version	Platform
Server	2008	x64
Server	2008 R2	
Server	2012	

Linux

Operating System	Version	Platform
Red Hat Enterprise Linux Server/Desktop	5	x86-64
Red Hat Enterprise Linux Server/Workstation	6	
Oracle Linux	4,5,6	

Chapter 7: 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
Username	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.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.

Parameter	Description
External Vault	Select this radio button if you prefer to use an external credential vault. - **Type.** The external vault type. Currently only CyberArk is supported. - **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

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.

AWS Protocol

Parameter	Description
Username	Access Key ID. An alphanumeric text string that uniquely identifies the owner of the account.
Password	Secret Access Key, performing the role of a password.
Http Proxy Host	The hostname, or address, of the proxy server.

Parameter	Description
Http Proxy Port	The port number of the proxy server.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the database.

Note: The **Http Proxy Host** and **Http Proxy Port** parameters only appear in the Edit Protocol Parameter dialog box. To open this dialog box, right-click the protocol that you created, and then select **Edit using previous interface**.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

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.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

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 • PostgreSQL • SAP Hana Database • SAP MaxDB
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 *UCMDB Discovery and Integrations 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.

Parameter	Description
Username	The name of the user needed to connect to the database.
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**. No encryption method will be used. • **SSL**. For Oracle and Sybase 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.

Note: This protocol supports IPv6.

For Oracle database connection jobs, you can use certificate-based authentication. To do this, right-click the entry for the connection credentials, select the **Edit using previous interface** option, and then configure the following settings:

- **Key Store File**: Specify the full path to the Java SSL KeyStore.
- **Key Store Format Type**: Select the KeyStore format type.
- **Key Store Password**: Specify the KeyStore password.
- **Oracle Authentication Services**: Enable or disable SSL as an Oracle authentication service.
  - **None**: Disable
  - **TCPS**: Enable
- **Trust Store Format Type**: Specify the TrustStore format type.

If the setting in **Key Store Format Type** or **Trust Store Format Type** is not JKS, the following jar files of Oracle public key infrastructure (PKI) need be manually copied to the **%DataFlowProbe%\content\lib** folder:

- oraclepki.jar
- osdt_cert.jar
- osdt_core.jar

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	**Description**
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

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**
Username	The name of the user needed for authentication.
Password	The password of the user needed for authentication.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	**Description**
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

HP Network Automation Java Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the database.
Port Number	The port number on which the HP NA server listens for Java API connections. If no value is assigned, the default value is 1099.
User Name	The name of the user, which is needed to connect to HP NA.
User Password	The password of the user, which is needed to connect to HP NA.

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 Username	The database user (Microsoft SQL Server) or schema name (Oracle) with permissions to access the database.
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 Webservice Protocol	Choose between **HTTP** or **HTTPS**.
Username	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

HTTP Protocol

Parameter	Description
Username	The name of a user needed to perform BASIC authentication with the remote webserver.
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
Port number	The number of a port to connect to the remote http server. **Default (HTTP):** 80 **Default (HTTPS):** 443
Protocol	The protocol used to connect to the http server: HTTP or HTTPS. **Default:** HTTP
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.

Note: This protocol supports IPv6.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.

Parameter	Description
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

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
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the remote webserver.
Username	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. - **Username.** See description above. - **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. - **Type.** The external vault type. Currently only CyberArk is supported. - **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

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.
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.
Username	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.
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 *UCMDB Discovery and Integrations Content Guide - General Reference* document.

Note:

- This protocol supports IPv6, with the following limitations:
  - Windows XP: Does not work over IPv6
  - Windows Server 2003/2003 R2: Registry on the target system being discovered needs to be modified as described in this Microsoft support article: http://support.microsoft.com/kb/281308
- 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 *UCMDB Discovery and Integrations 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.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

PowerCmd Protocol

The PowerCmd protocol is for the Windows discovery.

The PowerCmd protocol provides a generic Windows Shell based on PowerShell. It can be used to run Windows commands like the NTCMD protocol and Universal Discovery protocol. Actually, except that the PowerCmd protocol needs the PowerShell remoting, this protocol is almost the same as the NTCMD protocol.

Parameter	Description
Allow Redirection	Allows redirection of this connection to an alternate Uniform Resource Identifier (URI). **Default:** false
Application Name	The application name. This parameter must be set in case the remote application name is different from WSMan.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the destination machine. **Default:** 30000
Connection URI	A fully qualified Connection URI. **Default:** null
Port Number	The port number. By default, a PowerShell agent uses port 5985 for a regular connection and 5986 for a secure connection. If you are using a different port for PowerShell in your environment, enter the required port number.
Use SSL	Uses the Secure Sockets Layer (SSL) protocol to establish a connection to the remote computer. By default, SSL is not used.
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.

Note: This protocol supports IPv6.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. - **Username.** See description above. - **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. - **Type.** The external vault type. Currently only CyberArk is supported. - **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

PowerCmd Protocol Troubleshooting

This section describes the troubleshooting for the PowerCmd protocol.

Before starting troubleshooting with the PowerCmd protocol, make sure that the following steps are performed:

1. Both the Data Flow Probe machine and the remote discovery machine enabled PowerShell.

   To check whether PowerShell is enabled, do the following:

   a. Open the Command Prompt window.

   b. Enter `powershell -help`. The PowerShell help information should appear. Otherwise, install PowerShell.

2. The Data Flow Probe machine can create PowerShell connection to the remote discovery machine.

   To do so,

   a. Open the Windows PowerShell window.

   b. Enter `enable-psremoting`.

   c. Type `A` and press **Enter** to continue.

   d. Enter `winrm g winrm/config/client`. The output should be like as follows:

   ```
   Client
       NetworkDelayms = 5000
       URLPrefix = wsman
       AllowUnencrypted = false
       Auth
          Basic = true
          Digest = true
          Kerberos = true
          Negotiate = true
          Certificate = true
          CredSSP = false
       DefaultPorts
          HTTP = 5985
          HTTPS = 5986
       TrustedHosts = *
   ```

   Note: * means all.

   e. Enter `New-pssession –computername yourservername –credential yourcredential` to verify whether the connection can be created successfully.

3. The Data Flow Probe machine installed .Net framework 3.5.

4. The Data Flow Probe machine can execute all PowerShell scripts.

   To do so,

   a. Run **gpedit.msc**.

   b. In the **Local Group Policy Editor** dialog box, go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows**

   PowerShell > Turn on Script Execution.

   c. Double-click **Turn on Script Execution**, and then click **Enabled**.

   d. In the **Execution Policy** list, click **Allow all scripts**.

   e. Click **OK**.

- **Problem:** A remote host cannot be connected by the PowerCmd protocol.

  Solution: Check if the PowerCmd connection can be made between Data Flow Probe and the target host. To do so,

  a. Log in to the Data Flow Probe machine.

  b. Locate the **PowerCmd.ps1** file in the **<*DataFlowProbe_Home*>\runtime\probeManager\discoveryResources** directory.

  c. Open the Command Prompt window in the same directory.

  d. At the Command Prompt, invoke the following command:

  ```
  powershell .\PowerCmd.ps1 <machine name or ip> <username> <password>
  ```

  e. The output should be like as follows:

  ```
  powershell .\PowerCmd.ps1 1.2.3.4 admin password
  Connecting to 1.2.3.4
  MAM:Remote>hostname
  myremotehost1
  MAM:Remote>
  ```

- **Problem:** The **PowerCmd.ps1** file in the **<*DataFlowProbe_Home*>\runtime\probeManager\discoveryResources** directory cannot be loaded because the execution of scripts is disabled on this system.

  Solution: By default, the PowerShell scripts are not allowed to execute on the Data Flow Probe machine if the scripts are not signed. To enable the feature, refer to Step 4.

PowerShell Protocol

Parameter	Description
Allow Redirection	Allows redirection of this connection to an alternate Uniform Resource Identifier.
Application Name	The application name. This parameter must be set in case the remote application name is different from WSMan.
Connection URI	A fully qualified Connection URI. **Default:** null
Username	The name of the user that can connect to the remote machine by PowerShell.
Password	The password of the user that can connect to the remote machine by PowerShell.
Port Number	The port number. By default a PowerShell agent uses port 5985 for a regular connection and 5986 for a secure connection. If you are using a different port for PowerShell in your environment, enter the required port number.
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.
Use SSL	Uses the Secure Sockets Layer (SSL) protocol to establish a connection to the remote computer. By default, SSL is not used.

Note: This protocol supports IPv6.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

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.
Password	Enter the password of the user account that enables access to Remedy/Atrium through the Java API.
Username	Enter the user name that enables access to Remedy/Atrium through the Java API.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. - **Username.** See description above. - **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. - **Type.** The external vault type. Currently only CyberArk is supported. - **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

Salesforce Rest Protocol

Parameter	Description
Consumer Key	The Consumer Key of the Connected App that you create in Salesforce. For details on how to create Connected App, see the section of the *UCMDB Discovery and Integrations Content Guide - Third Party Integrations*.
Consumer Secret	The Consumer Secret of the Connected App that you create in Salesforce. For details on how to create Connected App, see the section of the *UCMDB Discovery and Integrations Content Guide - Third Party Integrations*.

Parameter	Description
Http Proxy	If a proxy is required to access the Salesforce site from Data Flow Probe, the proxy's URL needs to be filled here. For example, **http://example.com:8080**.
Is Sandbox	Indicates whether the BMC Remedyforce is a Sandbox or production environment. **Default:** false
Security Token	A Security token is used along with the user name and password. You can retrieve the token through **Setup > My Personal Information > Reset My Security Token** in Salesforce. The token will be sent via email.
User Name	The name of the user needed to access the Salesforce data.
User Password	The password of the user needed to access the Salesforce data.

SAP Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the SAP console.
JCo version	The version of the JCo connector. Default value : 2.x
User Name	The name of the user needed to log on 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 on to the SAP system.
SAP Client Number	It is recommended to use the default value (**800**).

Parameter	Description
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 *UCMDB Discovery and Integrations 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 *UCMDB Discovery and Integrations 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

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). **Username**: 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:

- This protocol supports IPv6.
- 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.
- 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.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

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 UNIX, the default shell command separator is a semicolon (**;**). • For Windows, the shell command separator is an ampersand (**&**). • For Cygwin, select **auto detect**.

Parameter	Description
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 *UCMDB Discovery and Integrations Content Guide - General Reference* document. • **keyboard-interactive**. Enter questions and answers. For details, see "SSH Protocol" on the previous page below.
Username	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.
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 *UCMDB Discovery and Integrations Content Guide - General Reference* document.

Parameter	Description
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.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.

Parameter	Description
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

Privileged Mode Properties

Policy	Select one of the following options: • **Privileged Mode.** Enables you to run commands in a privileged shell environment, after entering a privileged shell. • **Sudo-like.** Enables you to run commands in privileged command execution mode by using a specified prefix before the target command. • **Privileged Mode or Sudo-like.** A combination of both of the above options.

Mode	Based on your Policy selection, select the **Mode**. For **Privileged Mode**, select one of the following options: - **Su.** DFM executes the **su** command and enters the password at the prompt to enter the privileged shell, then executes the required command, and then executes **exit** to exit the privileged shell. - **Enable.** DFM executes the **enable <level>** command and enters the password at the prompt to enter the privileged shell, then executes the required command, and then executes the **disable <previous_level>** command to exit the privileged shell (where **<level>** represents the selected privileged mode level and **<previous_level>** represents the original level before running the **enable** command). - **Custom.** DFM executes the user-defined Enter command and enters the password at the prompt to enter the privileged shell, then executes the required command, and then executes the user-defined Exit command to exit the privileged shell. For **Sudo-like**, select one of the following options: - **Sudo.** DFM executes the **sudo** command followed by the required command and then enters the password at the prompt. - **Custom.** DFM executes the user-defined Command line followed by the required command and then enters the password at the prompt. For **Privileged Mode or Sudo-like**, select an option in each panel.
<Privileged Mode/Su>	When you select **Privileged Mode** as the policy and **Su** as the mode, the following fields are relevant: - **Username.** Enter the user name for the su command. - **Password.** Enter the password for the su command. - **Command List.** See "Command List".
<Privileged Mode/Enable>	When you select **Privileged Mode** as the policy and **Enable** as the mode, the following fields are relevant: - **Level.** Enter the privileged mode level for the enable command. **Note:** Entering an empty value selects the highest level, 15. - **Password.** Enter the password for the enable command. - **Command List.** See "Command List".

<Privileged Mode/Custom>	When you select **Privileged Mode** as the policy and **Custom** as the mode, the following fields are relevant: • **Enter Command.** Command used to enter privileged command execution mode. For example: ◦ for enable: **enable 10** ◦ for su: **su root** • **Exit Command.** Command used to exit privileged command execution mode. For example: ◦ for enable: **disable 5** ◦ for su: **exit** • **Password Prompt.** The prompt string that appears after entering the privileged command execution mode. For example: ◦ for both enable and su: **Password:** • **Password.** Enter the password to use when the password prompt appears. • **Command List.** See "Command List".
<Sudo-like/Sudo>	When you select **Sudo-like** as the policy and **Sudo** as the mode, the following fields are relevant: • **Sudo Paths.** Enter the full paths to the sudo command. Paths should be separated by commas. • **Command List.** See "Command List".
<Sudo-like/Custom>	When you select **Sudo-like** as the policy and **Custom** as the mode, the following fields are relevant: • **Command Line.** Enter the full command line before the target command to be executed in privileged mode. For example: ◦ for sudo: **/usr/bin/sudo** ◦ for pbrun: **/bin/pbrun** • **Command List.** See "Command List".
<Privileged Mode or Sudo-like>	When you select **Privileged Mode or Sudo-like** as the policy, you have the option to configure both types of policy. Each policy appears in a separate panel with the relevant options as described for each policy/mode selection.

Command List	Enter a list of commands that can be executed with the current policy/mode selection. Commands must be separated by commas. This field accepts a sudo command that prompts for the user's password. To select all possible commands to be executed in the current policy/mode, enter an asterisk (*) in this field. You can also select commands by pattern matching and pattern completion using Python/Jython regular expressions. For example, entering **.*uname** would select all of the following expressions: • /usr/sbin/uname • uname -a • uname -r • /mypath/my_other_path/uname -my args -my other args **Note:** • Entering an empty value in this field means that no commands can be run in privileged command execution mode. • The list of commands that can be executed with sudo (where the policy/mode selection is **Sudo-like/Sudo**) depends on the configuration of sudo commands on the discovered destination. Entering an asterisk (*) in this field means that all commands configured on the discovered destination can be run with sudo. • 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.

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:

- This protocol supports IPv6.
- 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 *UCMDB Discovery and Integrations 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 *UCMDB Discovery and Integrations 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 "Telnet Protocol" on the previous page below.
Username	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.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

Privileged Mode Properties

Policy	Select one of the following options: • **Privileged Mode.** Enables you to run commands in a privileged shell environment, after entering a privileged shell. • **Sudo-like.** Enables you to run commands in privileged command execution mode by using a specified prefix before the target command. • **Privileged Mode or Sudo-like.** A combination of both of the above options.

Mode	Based on your Policy selection, select the **Mode**. For **Privileged Mode**, select one of the following options: • **Su.** DFM executes the **su** command and enters the password at the prompt to enter the privileged shell, then executes the required command, and then executes **exit** to exit the privileged shell. • **Enable.** DFM executes the **enable <level>** command and enters the password at the prompt to enter the privileged shell, then executes the required command, and then executes the **disable <previous_level>** command to exit the privileged shell (where **<level>** represents the selected privileged mode level and **<previous_level>** represents the original level before running the **enable** command). • **Custom.** DFM executes the user-defined Enter command and enters the password at the prompt to enter the privileged shell, then executes the required command, and then executes the user-defined Exit command to exit the privileged shell. For **Sudo-like**, select one of the following options: • **Sudo.** DFM executes the **sudo** command followed by the required command and then enters the password at the prompt. • **Custom.** DFM executes the user-defined Command line followed by the required command and then enters the password at the prompt. For **Privileged Mode or Sudo-like**, select an option in each panel.
<Privileged Mode/Su>	When you select **Privileged Mode** as the policy and **Su** as the mode, the following fields are relevant: • **Username.** Enter the user name for the su command. • **Password.** Enter the password for the su command. • **Command List.** See "Command List".
<Privileged Mode/Enable>	When you select **Privileged Mode** as the policy and **Enable** as the mode, the following fields are relevant: • **Level.** Enter the privileged mode level for the enable command. **Note:** Entering an empty value selects the highest level, 15. • **Password.** Enter the password for the enable command. • **Command List.** See "Command List".

<Privileged Mode/Custom>	When you select **Privileged Mode** as the policy and **Custom** as the mode, the following fields are relevant: • **Enter Command.** Command used to enter privileged command execution mode. For example: ◦ for enable: **enable 10** ◦ for su: **su root** • **Exit Command.** Command used to exit privileged command execution mode. For example: ◦ for enable: **disable 5** ◦ for su: **exit** • **Password Prompt.** The prompt string that appears after entering the privileged command execution mode. For example: ◦ for both enable and su: **Password:** • **Password.** Enter the password to use when the password prompt appears. • **Command List.** See "Command List".
<Sudo-like/Sudo>	When you select **Sudo-like** as the policy and **Sudo** as the mode, the following fields are relevant: • **Sudo Paths.** Enter the full paths to the sudo command. Paths should be separated by commas. • **Command List.** See "Command List".
<Sudo-like/Custom>	When you select **Sudo-like** as the policy and **Custom** as the mode, the following fields are relevant: • **Command Line.** Enter the full command line before the target command to be executed in privileged mode. For example: ◦ for sudo: **/usr/bin/sudo** ◦ for pbrun: **/bin/pbrun** • **Command List.** See "Command List".
<Privileged Mode or Sudo-like>	When you select **Privileged Mode or Sudo-like** as the policy, you have the option to configure both types of policy. Each policy appears in a separate panel with the relevant options as described for each policy/mode selection.

Command List	Enter a list of commands that can be executed with the current policy/mode selection. Commands must be separated by commas. This field accepts a sudo command that prompts for the user's password. To select all possible commands to be executed in the current policy/mode, enter an asterisk (*) in this field. You can also select commands by pattern matching and pattern completion using Python/Jython regular expressions. For example, entering ***uname** would select all of the following expressions: • /usr/sbin/uname • uname -a • uname -r • /mypath/my_other_path/uname -my args -my other args **Note:** • Entering an empty value in this field means that no commands can be run in privileged command execution mode. • The list of commands that can be executed with sudo(where the policy/mode selection is **Sudo-like/Sudo**) depends on the configuration of sudo commands on the discovered destination. Entering an asterisk (*) in this field means that all commands configured on the discovered destination can be run with sudo. • 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.

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, it is recommended to add the following folders to the system path:

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

TIBCO Protocol

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

Parameter	Description
UD SHA1 ID	A hash of UD credential's certificates. Enables you to visually distinguish between UD credentials that have different

Parameter	Description
	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.
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

Parameter	Description
	on a UNIX environment, ensure that the list of commands includes the **agentinstall.sh** and **nohup** commands.

Note: This protocol supports IPv6.

See also the section about the Extended Shell Interface in the *UCMDB Discovery and Integrations Content Guide - General Reference* document.

vCloud Protocol

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

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.

Parameter	Description
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

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.

Parameter	Description
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 *UCMDB Discovery and Integrations 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**.

Parameter	Description
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.
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.

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.
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
Username	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.

Note:

- This protocol supports IPv6.
- 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 port is open: 135. 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.

Note: When the CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **Reference**) grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	Select this radio button if you prefer to use regular credential as before. • **Username.** See description above. • **Password.** See description above.
External Vault	Select this radio button if you prefer to use an external credential vault. • **Type.** The external vault type. Currently only CyberArk is supported. • **Reference.** The reference ID that will be used by UCMDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. Set the reference ID in the CyberArk Enterprise Password Vault in the following format: **<Safe Name>\<Folder Path>\<Reference ID>**. Where **<Safe Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<Reference ID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

Chapter 8: 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, 445
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 *UCMDB Discovery and Integrations 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 *UCMDB Discovery and Integrations Content Guide - General Reference* document.
Siebel Gateway	2320

Protocol	Default Port
SNMP	161
SQL	Oracle:1521 MS-SQL: 1433 MySQL: 3306 6789, 2048
SSH	22
Telnet	23
UDDI	80, 443
Universal Discovery Agent	2738, 7738
VMWare VIM	80, 443
WebLogic	7001, 7002
WebSphere	8880
WMI	135, 137, 138, 139, 445

Chapter 9: Supported Discovery Modules and Jobs

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

Note:

- For a list of jobs that support IPv6, see "Universal Discovery IPv6 Support" on page 23.
- For more information about script-based and scanner-based jobs, see the section that describes the script-based and scanner-based jobs in the *HP Universal CMDB Data Flow Management Guide*.

Module	Discovery Jobs
Cloud and Virtualization > Cloud > Amazon Web Services	• AWS by Web Services
Cloud and Virtualization > Cloud > OpenStack Web Services	• OpenStack by Web Services
Cloud and Virtualization > Cloud > VMware vCloud	• vCloud Director by vCloud API • vCloud Director URL by vCloud API
Cloud and Virtualization > Virtualization > Citrix	• Citrix Xen Connection • Citirx Xen Topology
Cloud and Virtualization > Virtualization > Docker	• Docker Discovery by Shell
Cloud and Virtualization > Virtualization > HP IVM	• HP IVM by Shell
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	• IBM Virtualization by Shell • IBM LPAR And VIO Server Topology by Shell • IBM PureFlex Topology by Shell
Cloud and Virtualization > Virtualization > Oracle VM Server for SPARC	• Oracle VM Server for SPARC Technology by Shell

Module	Discovery Jobs
Cloud and Virtualization > Virtualization > Oracle VM Server for x86	• Oracle VM for x86 by Manager Main CLI
Cloud and Virtualization > Virtualization > Solaris Zones	• Solaris Zones by TTY
Cloud and Virtualization > Virtualization > VMware	• Manual VMware VIM Connection • VMware ESX Connection by CIM • VMware ESX Connection by VIM • VMware ESX Topology by CIM • VMware ESX Topology by VIM • VMware vCenter Connection by VIM • VMware vCenter Topology by VIM • VMware vMotion Monitor by VIM
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 Application Discovery • HACMP Topology Discovery
Clustering and Load Balancing > Failover Clusters > Microsoft Cluster	• MS Cluster by NTCMD or UDA
Clustering and Load Balancing > Failover Clusters > Red Hat Cluster Suite	• Red Hat Cluster by Shell
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 > A10 vThunder	• A10 vThunder by SNMP
Clustering and Load Balancing > Load Balancers	• Alteon application switch by

Module	Discovery Jobs
> Alteon LB	SNMP
Clustering and Load Balancing > Load Balancers > Cisco ACE	- Cisco ACE by SNMP
Clustering and Load Balancing > Load Balancers > Cisco CSS	- Cisco CSS by SNMP
Clustering and Load Balancing > Load Balancers > Citrix NetScaler	- Citrix NetScaler 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 Topology by SQL - DB2 Universal Database Connection by SQL
Database > HP NonStop SQL	- HP NonStop Topology by Shell
Database > HanaDb	- HanaDb by Shell - HanaDb Connection by SQL - HanaDb Topology by SQL
Database > MS-SQL	- Databases TCP Ports - MSSQL Server Connection by SQL - MSSQL Topology by SQL
Database > MaxDb	- MaxDb by Shell - MaxDb Connection by SQL - MaxDb Topology by SQL
Database > MySQL	- Databases TCP Ports - MySQL by Shell - MySQL Connection by SQL
Database > Oracle	- Databases TCP Ports

Module	Discovery Jobs
	- Oracle Config Files by SQL - Oracle Connection by Shell - Oracle Database Connection by SQL - Oracle Database Connection by SQL- Lightweight - Oracle Listeners by Shell - Oracle RAC Topology by Shell - Oracle TNS Names by LDAP - Oracle Topology by SQL
Database > PostgreSQL	- Databases TCP Ports - PostgreSQL Connection by SQL
Database > Sybase	- Databases TCP Ports - Sybase Database Connection by SQL - Sybase Topology by SQL
Enterprise Applications > Active Directory	- Active Directory Connection by LDAP - Active Directory Topology by LDAP
Enterprise Applications > Microsoft Exchange	- Microsoft Exchange Connection by NTCMD or UDA - Microsoft Exchange Connection by WMI - Microsoft Exchange Topology by LDAP - Microsoft Exchange Topology by NTCMD or UDA - Microsoft Exchange Topology by PowerShell - Microsoft Exchange Topology by WMI
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

Module	Discovery Jobs
	JCO - SAP ABAP Topology by SAP JCO - SAP Applications by SAP JCO - SAP ITS by NTCMD or UDA - SAP Java Topology by HTTP - SAP Java Topology by SAP JMX - SAP Java Topology by WebServices - SAP Solution Manager by SAP JCO - SAP Solution Manager Topology by SAP JCO - SAP TCP Ports
Enterprise Applications > Siebel	- Siebel Application Server Configuration - Siebel Application Servers - Siebel DB by NTCMD or UDA - Siebel DB by TTY - Siebel Gateway Connection - Siebel Web Applications by NTCMD or UDA - Siebel Web Applications by TTY
Hosts and Resources > Basic Applications	- Host Applications by PowerShell - 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 PowerShell - Host Resources by Shell - Host Resources by SNMP

Module	Discovery Jobs
	- 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
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 - NetApp Filer Connection by WebServices
Hosts and Resources > Storage > SMI-S	- Storage Devices Connection by CIM - Storage Devices Topology by CIM
Mainframe > EView Agent	- CICS by EView - DB2 by EView - EView Connection - IMS by EView - LPAR Resources by EView - MQ by EView
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 JMX - JEE JBoss by Shell - JEE JBoss Connections by JMX - JEE TCP Ports
Middleware > Java EE Application Servers > Oracle iAS	- Oracle Application Server by Shell - Web Services by URL
Middleware > Java EE Application Servers > WebLogic	- JEE TCP Ports - JEE Weblogic by JMX - JEE Weblogic by Shell

Module	Discovery Jobs
	• 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 > Java EE Application Servers > WebSphere Liberty Core Server Discovery	• JEE WebSphere Liberty Core by Shell
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 > Proxy Servers > Reverse Proxy > IBM	• Webseal Connection by Shell • Webseal Connection By Web Services • Webseal Topology by Shell • Webseal Topology By Web Services
Middleware > Security Servers > Oracle Access Management	• Oracle Access Management Connection by Web Services • Oracle Access Management Policies by Web Services • Oracle Access Management Dependencies via URL
Middleware > Web Servers > Basic	• Web Server by Shell • Web Server Detection using TCP Ports • WebSphere to Web Server

Module	Discovery Jobs
	Dependency
Middleware > Web Servers > IIS	- IIS Applications by NTCMD or UDA - Web Services by URL
Middleware > Web Services > UDDI Registry	- Web Service Connections by UDDI Registry - Web Services by UDDI Registry - Web Services 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 - Manual UriEndpoint Discovery - 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
Network Infrastructure > Layer2	- Host Networking by SNMP - Layer2 Topology Bridge-based by SNMP - Layer2 Topology by Shell - Layer2 Topology CDP-LLDP-

Module	Discovery Jobs
	based by SNMP • Layer2 Topology VLAN-based by SNMP • Merge VLANs by Ports • Process Layer2 Saved Files • Report Linux with Duplicated MAC Layer2 • 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 • SAP Profiles by Shell • SAP System by Shell • Server Ports by Network Data • Servers by Network Data • VLAN ports by SNMP
Tools and Samples > Discovery Samples	• Dynamic Credential Sample
Tools and Samples > Discovery Tools	• File Monitor by Shell • Link DB Datafiles And Clustered FS • Merge Clustered Software • TCP Ports

Module	Discovery Jobs
	• Thin Clients MAC-based Detection
Tools and Samples > Getting Started Guide	• SQL Discovery Tutorial
Tools and Samples > SSL Certificates	• SSL Certificates Discovery by HTTPS
Tools and Samples > UD Agent Management	• Install UD Agent • Migrate DDMI Agent • Uninstall UD Agent • Update UD Agent

Chapter 10: Supported Integrations

Note:

- For a list of out-of-the-box integration adapters for these integrations, see "Out-of-the-Box Integration Adapters" on the next page.
- For a list of integrations that support IPv6, see "Universal Discovery IPv6 Support" on page 23.

HP Product Integrations

Integration	Population	Federation	Push
Executive Scorecard	N/A	N/A	✓
HP APM	N/A	N/A	✓
HP Asset Manager	✓	✓	✓
HP Configuration Manager	N/A	✓	N/A
HP Network Automation	✓	N/A	N/A
Network Node Manager (NNMi)	✓	N/A	✓
HP OneView	N/A	✓	N/A
HP Service Anywhere	N/A	N/A	✓
HP ServiceCenter/Service Manager	✓	✓	✓
HP UCMDB	✓	✓	✓
BSM	✓	✓	✓
Data Dependency and Mapping Inventory (DDMI)	✓	N/A	N/A
HP Systems Insight Manager (HP SIM)	✓	N/A	N/A
Storage Essentials (SE)	✓	N/A	N/A
HP Storage Operations Manager (SOM)	✓	N/A	N/A

Third Party Integrations

Integration	Population	Federation	Push
Aperture VISTA	✓	N/A	N/A
BMC	✓	N/A	✓
CA CMDB	N/A	N/A	✓
CiscoWorks LMS • CiscoWorks Layer 2 • CiscoWorks NetDevices	✓	N/A	N/A
EMC Control Center (ECC)	✓	N/A	N/A
IDS Scheer ARIS	✓	N/A	N/A
Microsoft System Center Configuration Manager (SCCM)/SMS	✓	✓	N/A
NetApp SANscreen/OnCommand Insight	✓	N/A	N/A
ServiceNow	N/A	N/A	✓
Troux	✓	N/A	✓

Integration Tools

Integration	Population	Push
Import topology from CSV file	✓	N/A
Import topology from Database	✓	N/A
Import topology from Excel Workbook	✓	N/A
Import topology from Properties file	✓	N/A
UCMDB to XML Adapter	N/A	✓
UCMDB API Population	✓	N/A

Out-of-the-Box Integration Adapters

> **Note:** Most of the adapters listed below are provided with the Discovery and Integrations Content Pack. Unless otherwise indicated, information on each of these adapters can be found in the relevant integration section of this guide, or by clicking the **Show Content Help**

? button for each adapter.

HP Product Adapters

Adapter Name (A-Z)	Description
AM population and federation	Used to populate and federate data from Asset Manager.
Asset Manager Push Adapter	Used to push data from UCMDB to Asset Manager.
BSM 9.x	Used to perform a population sync from BSM to UCMDB. For details, see the *RTSM Best Practices* document.
CM KPI Adapter	Used to federate KPI data from Configuration Manager.
CM New Policy Adapter	Used to federate policy data from Configuration Manager.
DDMI	Used to populate and federate data from DDMI.
NNMi: Population from NNMi	Used to populate data from NNMi.
NNMi: Push IDs into NNMi	Used to push UCMDB Node IDs to NNMi.
Service Center 6.2x	Used to federate data from HP ServiceCenter version 6.2x.
Service Manager 7.0x	Used to federate data from HP Service Manager version 7.0x.
Service Manager 7.1x - 9.2x	Used to federate data from and push data to HP Service Manager versions 7.1x-9.2x.
ServiceManagerAdapter9.x	Used to populate and federate data from and push data to Service Manager 9.3x and 9.40.
ServiceManagerEnhancedAdapter9.x	Used to populate and federate data from and push data to Service Manager 9.40. This adapter is based on the UCMDB generic adapter framework.
ServiceManagerAdapter9.41	Used to populate and federate data from and push data to Service Manager 9.41.
ServiceManagerEnhancedAdapter9.41	Used to populate and federate data from and push data to Service Manager 9.41. This adapter is based on the UCMDB generic adapter framework.

Adapter Name (A-Z)	Description
Storage Essentials	Used to populate CIs and relationships from Storage Essentials.
Storage Operations Manager	Used to populate CIs and relationships from Storage Operations Manager.
Systems Insight Manager	Used to populate CIs and relationships from HP SIM.
UCMDB 9.x	Used for populating and federating data from UCMDB 9.x. For details, see the section about integrating multiple CMDBs in the *HP Universal CMDB Data Flow Management Guide*.
UCMDB 10.x	Used for populating and federating data from UCMDB 10.x. For details, see the section about integrating multiple CMDBs in the *HP Universal CMDB Data Flow Management Guide*.
UCMDB to XML	Used to export the results (CIs and relationships) of TQL queries and convert these to XML files.

Third Party Product Adapters

Adapter Name (A-Z)	Description
Atrium to UCMDB	Used to populate CIs and relationships from Atrium.
CiscoWorks Layer 2	Used to populate server data from CiscoWorks.
CiscoWorks NetDevices	Used to populate network device data from CiscoWorks.
CA CMDB	Used to push CIs and relationships to CA CMDB.
Data Push into Atrium	Used to push CIs and relationships to BMC Atrium.
EMC Control Center	Used to populate CIs and relationships from EMC Control Center.
Import topology (CSV, Database, Excel, Properties File)	Used to import topology from a specified file type.
Microsoft SMS	Used to populate and federate data from Microsoft SMS.

Adapter Name (A-Z)	Description
Service-Now Integration	Used to push CIs and relationships to ServiceNow.
Software AG ARIS	Used to populate CIs and relationships from IDS Scheer ARIS.
Troux: Population from Troux	Used to populate CIs from Troux.
Troux: Data Push into Troux	Used to push data to Troux.

Other

Adapter Name (A-Z)	Description
UCMDB API Population	Used to define an integration that specifies the reconciliation priority for data that is added to the UCMDB using the UCMDB API. For details, see the *HP Universal CMDB Developer Reference Guide*.

Chapter 11: 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
HP Asset Manager	Not supported	Not supported	Not supported
HP Service Manager 6.2x\7.0x\7.1x-9.2x	-	Not supported	Not supported
HP Service Manager M 9.x	Supported	Supported	Supported
HP UCMDB 9.x\10.x	Supported	Supported	-
HP Configuration Manager policy\kpi adapters	-	Supported	-
HP Discovery and Dependency Mapping Inventory	Not supported	Supported	-
Generic Push adapters	-	-	Not supported
Microsoft System Center Configuration Manager/Systems Management Server	Not supported	Supported	-
ServiceNow	-	-	Not supported
EMC Control Center	Supported	-	-
Storage Essentials	Supported	-	-
HP Network Node Manager	Supported	-	Supported
HP Systems Insight Manager	Supported	-	-

Chapter 12: Localization

This section details localized versions of operating systems and applications that 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, Traditional Chinese

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Discovery and Integrations Content Guide - Supported Content (Universal CMDB Content Pack 19.00 (CP19))

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to cms-doc@hpe.com.

We appreciate your feedback!