HP Universal CMDB

Discovery and Integrations Content Guide - General Reference

Document Release Date: June 2014

Software Release Date: June 2014

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 1996 - 2014 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

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

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

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

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

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

UNIX® is a registered trademark of The Open Group.

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

Documentation Updates

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

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

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

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

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

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

Support

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

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts

- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

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

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

To find more information about access levels, go to:

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

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

Contents

Chapter 1: How to Define a New Port

Edit the **portNumberToPortName.xml** file to define a new port:

1. In the Adapter Management window (**Managers > Data Flow Management > Adapter Management**), search for the `portNumberToPortName.xml` file: click the **Find resource** button and enter **portNumberToPortName.xml** in the **Name** box. Click **Find Next**, then click **Close**.

   The file is selected in the Resources pane and the file contents are displayed in the View pane.

   For details about this file, see "portNumberToPortName.xml File" on page 27.

2. Add another row to the file and make changes to the parameters:

   ```
   <portInfo portProtocol="xxx" portNumber="xxx" portName="xxx" discover="0"
   cpVersion="xx"/>
   ```

Parameter	Description
portProtocol	The network protocol used for discovery (`udp` or `tcp`).
portNumber	The port number to be discovered. This attribute may be a number or a range. Ranges may be separated by commas or dashes or both. For example: "10, 21, 45", "10-21", or "10-21, 45, 110".
portName	The name that is to be displayed for this port.
discover	**1**. This port must be discovered. **0**: This port should not be discovered.

Parameter	Description

cpVersion	Use this parameter when you want to export the **portNumberToPortName.xml** file to another UCMDB system with the Package Manager. If the **portNumberToPortName.xml** file on the other system includes ports for this application but does not include the new port you want to add, the **cpVersion** attribute ensures that the new port information is copied to the file on the other system.
	The **cpVersion** value must be greater than the value that appears in the root of the **portNumberToPortName.xml** file.
	For example, if the root **cpVersion** value is **3**:
	`<portList parserClassName="com.hp.ucmdb.discovery.library.communication.downloader.cfgfiles.KnownPortsConfigFile" cpVersion="3">`
	the new port entry must include a **cpVersion** value of **4**:
	`<portInfo portProtocol="udp" portNumber="1" portName="A1" discover="0" cpVersion="4"/>`
	Note: If the root **cpVersion** value is missing, you can add any non-negative number to the new port entry.
	This parameter is also needed during Content Pack upgrade. For details, see "How to Use the cpVersion Attribute to Verify Content Update" on page 7.

Chapter 2: How to Use the cpVersion Attribute to Verify Content Update

The **cpVersion** attribute is included in the portNumberToPortName.xml file, and indicates in which Content Pack release a port has been discovered. For example, the following code defines that the LDAP port 389 has been discovered in Content Pack 11.00:

```
<portInfo portProtocol="tcp" portNumber="389" portName="ldap" discover="11"
cpVersion="11"/>
```

During a Content Pack upgrade, DFM uses this attribute to perform a smart merge between the existing portNumberToPortName.xml file (which may include user-defined ports) and the new file. Entries previously added by the user are not removed and entries previously deleted by the user are not added.

For details about the **portNumberToPortName.xml** file, see "portNumberToPortName.xml File" on page 27.

To verify that a Content Pack is successfully deployed:

1. Install the latest Service Pack release.

2. Start the UCMDB Server.

3. Verify that all services are running. For details, see the section about HP Universal CMDB Services in the *HP Universal CMDB Administration Guide*.

4. Install and deploy the latest Content Pack release. For details, refer to the Content Pack installation guide.

5. In the Adapter Management window, access the **portNumberToPortName.xml** file.

6. Verify that no user-defined ports have been deleted and that any ports deleted by the user have not been added.

Chapter 3: How to Delete Files Copied to Remote Machine

During discovery, the Data Flow Probe copies files to a remote Windows machine. For details, see "Files Copied to a Remote Machine" on page 10.

To configure DFM to delete files copied to the destination machine after discovery is finished:

1. Access the **globalSettings.xml** file: **Adapter Management > AutoDiscoveryContent > Configuration Files**.
2. Locate the **removeCopiedFiles** parameter.
   - **true**. The files are deleted.
   - **false**. The files are not deleted.
3. Save the file.

To control HPCmd behavior:

1. In the **globalSettings.xml** file, locate the **NtcmdAgentRetention** parameter.
2. Enter one of the following:
   - **0**. (The default) Unregister the service and delete the remote executable file. (**Unregister**: stop the service and remove it from the remote machine, so that it is no longer listed in the list of services.)
   - **1**. Unregister the service, but leave the executable file on the file system.
   - **2**. Leave the service running, and leave the executable file on the file system.

Chapter 4: How to Run HPCmd from Windows 2008 and Windows Server 2008 R2 Machines

Perform the following to ensure that HPCmd functions properly when the Probe is installed on a Windows 2008 or a Windows Server 2008 R2 machine:

1. Stop the Probe.

2. Open the standard Windows Registry Editor application by running the **regedit** executable.

3. In the Registry Editor navigate to the following registry key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

4. Under this key there should be a **REG_DWORD** parameter **SCMApiConnectionParam**

   a. If this is missing, add a new **REG_DWORD** parameter **SCMApiConnectionParam** and set its value to 0x80000000.

   b. If this value is already available in the registry, combine it with the 0x80000000 mask (using bitwise OR). For example, if there was a value 0x1 in there, you need to set this value to 0x80000001.

   > **Note:** To run HPCmd from a Windows 2008 machine **with UAC enabled**, also perform the following additional steps. **Do not perform these steps for a Windows Server 2008 R2 machine.**

5. Locate the **wrapper.exe** file, in the hp\UCMDB\DataFlowProbe\bin directory.

6. Right-click the **wrapper.exe** file, and select **Properties**.

7. In the **Compatibility** tab:

   a. Select **Compatibility mode**.

   b. Select **Run this program in compatibility for**: **Windows XP (Service Pack 2)**.

   c. Select **Run this program as administrator**.

8. Start the Probe.

> **Note:** HPCmd uses DCOM protocol for connecting to remote machines. The DCOM protocol requires that the following ports are open: **135**, **137**, **138,** and **139**. In addition it uses arbitrary ports between **1024** and **65535**, but there are ways to restrict the port range used by WMI/DCOM/RPC. For information about configuring DCOM to work with firewalls, see http://support.microsoft.com/kb/154596/en-us.

Chapter 5: Files Copied to a Remote Machine

During discovery, Data Flow Probe copies files to a remote Windows machine to enable discovery of the machine's components. The files are copied to the **%SystemRoot%\system32\drivers\etc\** folder on the remote machine.

Note:

- Data Flow Management runs **HPCmdSvc.exe** to connect to and retrieve the Shell on the remote machine.
- When the **wmic** command is launched on the remote Windows machine, by the **Host Connection by Shell** or **Host Resources by Shell** or **Host Applications by Shell** jobs, an empty **TempWmicBatchFile.bat** file is created.

The following files are copied:

File	Content Pack Version	Description
adsutil.vbs	All	The Visual Basic script used for discovery of Microsoft IIS applications. DFM copies this script to the remote machine to discover IIS. **Relevant DFM Job:** IIS Applications by NTCMD or UDA
diskinfo.exe	All	The executable that enables the retrieval of disk information when it is not available to be retrieved by **wmic**. DFM discovers default disk information with the **wmic** query. However, if the **wmic** query fails to execute, DFM copies the **diskinfo.exe** file to the remote machine. This failure can occur if, for example **wmic.exe** is not included in the PATH system variable or is completely absent on the remote machine, as is the case on Windows 2000. **Relevant DFM Job:** Host Resources by Shell

File	Content Pack Version	Description
Exchange_Server _2007_ Discovery.ps1	CP4	The PowerShell script for MS Exchange 2007 discovery. DFM uses a PowerShell scenario to discover Microsoft Exchange 2007 by NTCMD. This file, therefore, must be copied to the remote machine. **Relevant DFM Jobs:** • Microsoft Exchange Connection by NTCMD or UDA • Microsoft Exchange Topology by NTCMD or UDA
GetFileModification Date.vbs	CP5	The Visual Basic script for retrieving the file modification date (disregarding locale). The most common use case is when DFM must retrieve the last modification date of a configuration file of a discovered application. **Relevant DFM Jobs:** • Apache Tomcat by Shell • File Monitor by Shell • IIS Applications by NTCMD or UDA • JEE Weblogic by Shell • JEE WebSphere by Shell or JMX • JEE WebSphere by Shell • SAP System by Shell • Service Guard Cluster Topology by TTY • Siebel Application Server Configuration • Software Element CF by Shell • Veritas Cluster by Shell • Web Server by Shell

File	Content Pack Version	Description
getfilever.vbs	All	The Visual Basic script used to identify the version of the running software. The script retrieves the executable or DLL file version on Windows machines. This script is used by Shell-based application signatures plug-ins to retrieve the version of a particular software on the remote machine. **Relevant DFM Job:** Host Applications by Shell
junction.exe	CP5	This executable file, part of the Sysinternals Suite (http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx), enables the creation of a junction point. DFM uses this file if the **linkd.exe** and **mklink.exe** tools are absent on the remote machine. When DFM runs discovery on a Windows x64 machine, DFM needs to bypass the Windows redirect feature running on that machine. DFM does this by creating a link to the **%SystemRoot%\System32** folder with either the **linkd.exe** or **mklink.exe** tool. However, if these tools are missing on the remote machine, DFM transfers **junction.exe** to the remote machine. DFM is then able to launch the 64-bit version of the system executable files. (Without this 64-bit version, DFM would be locked into an isolated 32-bit world.) This junction point is automatically removed once discovery is complete. **Relevant DFM Jobs:** • Host Resources by Shell • Host Applications by Shell • Microsoft Exchange Connection by NTCMD or UDA • Microsoft Exchange Topology by NTCMD or UDA

File	Content Pack Version	Description
meminfo.exe	All	The executable that enables the retrieval of memory information. DFM discovers memory information with the **wmic** query. However, if the **wmic** query fails to execute, DFM copies the **meminfo.exe** file to the remote machine. This failure can occur if, for example, **wmic.exe** is not included in the PATH system variable or is completely absent on the remote machine, as is the case on Windows 2000. **Relevant DFM Job:** Host Applications by Shell
reg_mam.exe	All	The copy of the Microsoft reg.exe file that enables querying the registry. If DFM does not discover a native reg.exe file, this executable is copied to the remote Windows machine. This situation occurs with some previous Windows versions (for example, Windows 2000) where the tool is not included by default but can still function there correctly. **Relevant DFM Job:** Host Applications by Shell

Chapter 6: Content Pack Configuration Files

The Content Pack contains configuration files which enable you to configure commonly used parameters such as command timeouts, usage of some utilities, application signatures, and so on.

This section includes:

- "globalSettings.xml File" below
- "portNumberToPortName.xml File" on page 27

globalSettings.xml File

The following table describes the parameters in the **globalSettings.xml** configuration file (**Data Flow Management > Adapter Management > Resources > Packages > AutoDiscoveryContent > Configuration Files**):

Parameter	Description
AdditionalClasspath	Additional path that enables to run different patterns (i.e. database patterns); all paths should be relative to the **$PROBE_INSTALL/root/lib/collectors/ probeManager/discoveryResources/** folder and should be semicolon separated **Example:** **<property name="AdditionalClasspath"> db/oracle/.;db/mssqlserver/.</property>** means that following paths will be included in the classpath: • **$PROBE_INSTALL/root/lib/collectors/ probeManager/discoveryResources/ db/oracle/** • **$PROBE_INSTALL/root/lib/collectors/ probeManager/discoveryResources/ db/mssqlserver/**
allowGettingCredential SecuredAttribute	Indicates whether Jython scripts are allowed to get credentials secured data (true) or not (false). If this setting is set to false, then Jython scripts are not allowed to retrieve sensitive credentials data (like passwords that are stored on the server side). **Default:** true

Parameter	Description
clearCommandLineForProcesses	Clears the Command line for these processes. This option is used to ensure that no private or confidential data is stored in CMDB. **Default:** srvrmgr.exe, srvrmgr. **Syntax exceptions:** Process names are case insensitive and should be split by commas.
dbQueryTimeout	The timeout (in seconds) for all SQL queries. Indicates how long to wait for query results. The timeout applies only if the value is greater than zero (0). **Default:** 100 seconds **Note:** Some JDBC drivers cannot support this setting.
ddmagentCiphers	The algorithm used by the UD Agent to encrypt/decrypt the data transferred to/from client machines.
ddmagentProtocol	The protocol used by the Probe to communicate with UD Agent.
ddmagentEnableDownloadResume	Specifies whether the resumable download is enabled or not. **true.** The resumable download functionality is available. **false.** The resumable download functionality is not available.
ddmagentDefaultBlockLen	The default chunk size (in bytes) used to upload/download files to/from the UD Agent.
ddmagentResumableFileSuffix	The file extension used for parts of the resumable transfer file.
ddmagentDefaultResumeBlockLen	The default chunk size (in bytes) for resumable file transfer.
ddmagentEnableUploadResume	Specifies whether the resumable upload is enabled or not. **true.** The resumable upload functionality is available. **false.** The resumable upload functionality is not available.

Parameter	Description
defaultSapClients	When this parameter is defined, you do not need to specify the SAP Client Number parameter in the SAP ABAP protocol. Instead, you can create one or more comma-separated credentials for multiple SAP systems with different supported clients. **Example:** `<property name= "defaultSapClients"> 800,500,200,300 </property>` **Default:** 800
desktopOperating Systems serverOperating Systems	These two parameters are used to determine if the host's operating system is of type Desktop or Server. If the host's operating system name contains a value from one of these lists, its **host_isdesktop** is set accordingly. Otherwise the value of **host_isdesktop** attribute is left empty.
discovereAllListenPorts	Related to application signatures configuration.

Parameter	Description
discoveredStorageTypes	Describes storage types which have to be reported to UCMDB. Options are split by commas. Available options are: - FixedDisk - NetworkDisk - CompactDisk - RemovableDisk - FloppyDisk - VirtualMemory - FlashMemory - RamDisk - Ram - No Root Directory - Other - UNKNOWN
ignoreLocalized VirtualInterfaces PatternList	Lists patterns for localized Windows Virtual interface description that must not take part in the Host Key creation process. **Format:** Comma-separated list of strings, no additional white-spaces allowed.
ignoreVmwareInterfaces	Indicates whether to ignore the VMware MAC address. - **When there is a Physical MAC** (default). The VMware MAC address is used only if the pattern cannot find any physical MAC address. - **Always.** Always ignore VMware MAC address.

Parameter	Description

jdbcDrivers	This section enumerates driver classes used to connect to a dedicated Database server. Names of sub-keys must be the same as used in credentials (sqlprotocol_dbtype attribute of protocol).
	Change them if drivers other than OOTB JDBC drivers are used.
	Default values for OOTB-installation:
	`<property name="jdbcDrivers:>`
	`<oracle>`
	`oracle.jdbc.OracleDriver`
	`</oracle>`
	`<oracleSSL>`
	`oracle.jdbc.OracleDriver`
	`</oracleSSL>`
	`<MicrosoftSQLServer>`
	`net.sourceforge.`
	`jtds.jdbc.Driver`
	`</MicrosoftSQLServer>`
	`<MicrosoftSQLServer> net.sourceforge.jtds.`
	`jdbc.Driver`
	`</MicrosoftSQLServerNTLM>`
	`<MicrosoftSQLServerNTLMv2>`
	`net.sourceforge.jtds.jdbc.Driver`
	`</MicrosoftSQLServerNTLMv2>`
	`<Sybase>`
	`com.sybase.jdbc.SybDriver`
	`</Sybase>`
	`<db2>`
	`com.ibm.db2.jcc.DB2Driver`
	`</db2>`
	`<mysql>`
	`com.mysql.jdbc.Driver`
	`</mysql>`
	`</property>`

Parameter	Description

jdbcPreUrls	This section enumerates URL templates used to connect to dedicated the database server. Names of sub-keys must be the same as those used in credentials (sqlprotocol_dbtype attribute of protocol). Change them if drivers other than OOTB JDBC drivers are used. Values depend on used drivers and should be taken from driver documentation.
	Note: The ampersand symbol (&) must be escaped according to the XML standard (&amp;).
	Default values for OOTB-installation:
	`<property name="jdbcPreUrls">`
	`<oracle>jdbc:oracle:thin:@(DESCRIPTION=`
	`(ADDRESS=`
	`(PROTOCOL=tcp)`
	`(HOST=%%ipaddress%%)(PORT=%%protocol_port%%))`
	`(CONNECT_DATA=(%%connect_data%%=%%sqlprotocol_`
	`dbsid%%)))`
	`</oracle>`
	`<oracleSSL>jdbc:oracle:thin:@(DESCRIPTION=`
	`(ADDRESS=`
	`(PROTOCOL=tcps)`
	`(HOST=%%ipaddress%%)(PORT=%%protocol_port%%))`
	`(CONNECT_DATA=(%%connect_data%%=%%sqlprotocol_`
	`dbsid%%)))`
	`</oracleSSL>`
	`<MicrosoftSQLServer>`
	`jdbc:jtds:sqlserver://`
	`%%ipaddress%%:%%protocol_port%%;`
	`instanceName=%%sqlprotocol_dbname%%;`
	`loginTimeout=%%protocol_timeout%%;`
	`logging=false;ssl=request`
	`</MicrosoftSQLServer>`
	`<MicrosoftSQLServerNTLM>`
	`jdbc:jtds:`
	`sqlserver://%%ipaddress%%:`
	`%%protocol_port%%;instanceName=`
	`%%sqlprotocol_dbname%%;domain=`
	`%%sqlprotocol_windomain%%;`
	`loginTimeout=`
	`%%protocol_timeout%%;logging=false`
	`</MicrosoftSQLServerNTLM>`

Parameter	Description
jdbcPreUrls continued	<MicrosoftSQLServerNTLMv2>jdbc:jtds:sqlserve r://%% ipaddress%%:%%protocol_port%%;instanceName=%% sqlprotocol_dbname%%;domain=%% sqlprotocol_windomain%%;loginTimeout=%% protocol_ timeout%%;logging=false;ssl=request;useNTLMv2=t rue </MicrosoftSQLServerNTLMv2> <Sybase> jdbc:sybase:Tds: %%ipaddress%% :%%protocol_port%%?DatabaseName= %%sqlprotocol_dbname%% </Sybase> <db2> jdbc:db2://%%ipaddress%%: %%protocol_port%%/ %%sqlprotocol_dbname%% </db2> <mysql> jdbc:mysql://%%ipaddress%%: %%protocol_port%%/ %%sqlprotocol_dbname %%</mysql> <parameters> <parameter type="oracle" name="connect_data"> <value>SERVICE_NAME</value> <value>SID</value> </parameter> <fallbackExceptionList> <error type="oracle">.*ORA\-12514.*</error> </fallbackExceptionList> </parameters> </property> Each <parameter> element has a name attribute and one or more <value> tags. Each <parameter> can be used in the Oracle URL template by using the format "%%[parameter name]%%" (for example, %%connect_data%%). If a <parameter> has more than one <value> tag, then the parsing engine generates all permutations of the possible values in the template string, and the client tries to connect to the database server by each of these permutations. Since during connection errors can occur, the <fallbackExceptionList> element specifies which errors should be ignored if they occur. If the engine ignores such an error, then it tries to connect using another permutation of values in the template string. If an error occurs that is not specified by <fallbackExceptionList>, the engine does not try another permutation and the job fails with the error message that was caught.

Parameter	Description
loadExternalDTD	Used to configure file_mon_utils to prevent downloading DTD files while validating the XML. **Default:** false
maxExecutionRecords	Specifies maximal number of execution records that can be in the communication log. This parameter should be used when the discovery process discovers a lot of data. The parameter can be overridden on an adapter level. In this case, add the parameter to the adapter with desired record limit (see Probe documentation). **Default:** -1 means unlimited
maximumConnectionsPerSecond	Enables limiting the number of new connections per second created by the Probe to other machines. • **0.** Unlimited number of connections allowed. • **> 0.** The maximum number of connections. If this limit is reached, any job trying to create a new connection will wait for a period of time that is determined in the "timeToSleepWhenMaximumConnectionsLimitReached" parameter below. **Default:** 0 (unlimited)
maxStoreSentResults	Specifies maximal number of sent results that can be stored in the communication log. This parameter can be changed if there are too many results stored in the communication log. If this value is greater than 0, the log will store the corresponding number of results for deleted results AND updated results, meaning that the results set will contain double the value of **maxStoreSentResults.** **Default:** -1 means unlimited
multipleUpdateIgnore Types	Used by UCMDB. The Probe does not generate a **Multiple updates in bulk** warning for enumerated CI types.

Parameter	Description
NtcmdAgentRetention	NTCMD agent retention mode. Specifies how to handle a remote NTCMD service and its executable file when closing the connection. ● **0** (default)**.** Unregister the service and delete the remote executable file. ● **1.** Unregister the service but keep the executable file on the file system. ● **2.** Leave the service running, keep the executable file.
NtcmdSessionUse ProcessBuilder	This parameter is for **NtcmdSessionAgent** and should be always be **true**. This parameter tells how to create a new process. ● **true.** The new process will be created by ProcessBuilder (new API from Java 5.0) ● **false.** The new process will be created by Runtime.exec (old API, from Java 1.4.2). Set to false only in case of backward compatibility problems.
objectSendAmount Threshold	When the number of discovered objects exceeds this threshold, the objects are immediately sent to the server. Requires using the sendObject(s) API in jython scripts. **Default:** 2000 objects
objectSendTime Threshold	When more than the specified time (in seconds) has passed since the previous object report, the objects are immediately sent to the server. Requires using the 0sendObject(s) API in jython scripts. **Default**: 300 seconds
portExpirationTime	The expiration time (in seconds) of the TCP/UDP port entry in the Probe's database. **Default:** 60 seconds

Parameter	Description
powershellConnection IdleTimeout	Defines the maximum idle time (in milliseconds) for the powershellconnector.exe process. The timer resets its state after each command execution. **Default:** 3600000 milliseconds (1h)
processExpirationTime	The expiration time (in seconds) of the Process entry in the Probe database. **Default:** 60 seconds
remoteProcessTimeout	After being launched, the remote process should connect with the Probe within the defined time (in milliseconds), otherwise the following error is produced: **Failed to connect to remote process**. **Default:** 300000 milliseconds (5 minutes)
removeCopiedFiles	In some cases DFM copies scripts and third-party utilities on a client machine. The **removeCopiedFiles** parameter defines whether these files should (true) or should not (false) be deleted after discovery is finished.
ResultProcessIsLenient	When set to **true,** the discovery result processing is lenient (not recommended): • If a reported string attribute has too large a value, the string it is automatically truncated according to the CMDB Class Model definition • If the OSH attribute is invalid (type/nonexisting attribute/missing ID attribute) only the invalid OSH is dropped, rather than entire bulk (default)

Parameter	Description
setBiosUuidTo MicrosoftStandart	Indicates whether the BIOS UUID value for Windows operating systems should be reported in Microsoft style (some bytes order reversed) instead of the original BIOS value. Affects Host Connection jobs. • **false**. Converts to original BIOS stored value • **true**. Converts to Microsoft standard. **Note:** Setting this parameter to **true** may result in conflicts with the BIOS UUID value discovered by VMware jobs or some integrations.
shellGlobalBandwidthLimit	The maximum bandwidth (in kilobits per second) to upload and download files to and from the discovery node **Note:** If no value or 0 is assigned, all of the available bandwidth is used.
shellGlobal CommandTimeout	Global timeout (in milliseconds) for all Shell client commands. Indicates how long to wait for a command's result. **Default:** 15000 milliseconds
siebelCommandTimeout	The amount of time to wait for the Siebel command's result. **Default:** 3 minutes (180000 ms)
snmpGlobalRequestTimeout	This is the time, in milliseconds, after which a request using SNMP will timeout. **Default:** 3,000 milliseconds **Note:** This value is global for all SNMP requests. If you want to override the SNMP request timeout for a specific query (where you know the query takes more time than the default timeout), provide the timeout value as a second parameter to the executeQuery method on the SNMP client: **snmpClient.executeQuery(SNMP_QUERY_ STRING, QUERY_TIMEOUT_IN_ MILLISECONDS).**

Parameter	Description

snmpTestQueries	Defines the default SNMP test query for SNMP Agent. Can be overridden for specific devices.
	Default:
	`<property name="snmpTestQueries">`
	`<query> 1.3.6.1.2.1.1.1,1.3.6.1.2.1.1.2, string</query>`
	`</property>`

ssh-log-level	The SSH log level **Levels:** 1-7, where 7 is the most detailed defect level.
tcpExpirationTime	The expiration time (in hours) of TCP connection entry in probe database. **Default:** 24 hours
timeToSleepWhenMaximumConnectionsLimitReached	Determines how long (in milliseconds) a job needs to wait until a new connection can be created, assuming the maximum connections limit has been reached. (See "maximumConnectionsPerSecond" above.) **Default:** 1000 milliseconds (1 second) **Note:** If **maximumConnectionsPerSecond = 0** this property is ignored.
tnsnamesFilePaths	Paths to search the **tnsnames.ora** file (including **tnsnames.ora** itself, comma separated) **Example:** `<property name= "tnsnamesFilePaths"> c:\temp\tnsnames.ora </property>`
useIntermediateFileForWmic	Usage of an intermediate temporary file for data transfer by wmic command. **Default:** false

Parameter	Description
useJinteropOnLinux	This setting is used on non-Windows machines and ● **true** (default)**.** The Probe uses JInterop for WMI discovery. ● **false.** The Probe uses Windows remote Proxy.
useJinteropOnWindows	This property is used on Windows machines. ● **true.** The Probe uses JInterop for WMI discovery. ● **false** (default)**.** The Probe uses WMIdll native code.
useNtcmdModified Markers	● **true.** The Probe uses markers with counters in NTCMD agents' infrastructure. ● **false.** The Probe uses old NTCMD behavior - without markers with counters.
useSnmp4j	Affects jobs * by SNMP. Defines which SNMP library to use for SNMP queries. ● **true** (default). SNMP4J library are used. ● **false.** Inner implementations are used.
useWinexeOnLinux	This setting is used on non-Windows machines. ● **true.** The Probe uses local winexe executable for NTCMD Windows discovery. ● **false** (default)**.** The Probe uses Windows remote Proxy.

portNumberToPortName.xml File

The **portNumberToPortName.xml** file is used by DFM as a dictionary to create IpServiceEndpoint CIs by mapping port numbers to meaningful port names. When a port is discovered, the Probe extracts the port number, searches in the **portNumberToPortName.xml** file for the port name that corresponds to this port number, and creates the IpServiceEndpoint CI with that name. If the port name does not appear in this file, the Probe uses the port number as the port name.

You can specify different names for same port number for different IP ranges. In this case, the same port discovered for IPs contained in different ranges will have different port names.

Note: The **portNumber** attribute may be a number or a range. Ranges may be separated by commas or dashes or both. For example: "10, 21, 45", "10-21", or "10-21, 45, 110". You may use x as a wildcard in any position in a number. For example “5xx00” includes ports 50000, 50100, 50200, …51000, 51100, 51200, …59900.

For details on adding new ports to be discovered, see "How to Define a New Port" on page 5.

Chapter 7: Additional Protocol Information

This section includes:

Extended Shell Interface

UCMDB 10.00 extended the Shell Interface to remove limitations when uploading files to, and downloading files from, Windows machines. This increased functionality applies to the NTCMD and SSH protocols, and UD Agents.

- When uploading or downloading files to or from Windows machines, you can set the parameter **setBandwidthLimit**, to restrict network bandwidth consumption.

  You can set this parameter:

  - At the **job** level where the job supports this parameter

    > **Note:** The Install/Update UD Agent jobs support this parameter.

    i. Go to the job. For example, to **Universal Discovery > Discovery Modules/Jobs > Tools and Samples > UD Agent Management > Install UD Agent** .

    ii. Click the **Properties** tab.

    iii. Under **Parameters** select **Override** beside **Bandwidth Limit**. Enter the required value.

    The parameter sets a limit, in kilobits per second, on the amount of bandwidth consumed by the download or upload operation. The value must be a positive integer. The default is 0, meaning no limit.

  - At the **global** level in **globalSettings.xml**

    The property is **shellGlobalBandwidthLimit**. For shell objects that support file downloading and uploading, it sets a limit, in kilobits per second, on the amount of bandwidth consumed by the download or upload operation. The value must be a positive integer. The default is 0, meaning no limit. For example:

    ```
    <property name="shellGlobalBandwidthLimit">0</property>
    ```

    The speed can be overwritten at adapter level or at job level; for example, when installing or updating UD Agents.

How to Create an SSH Connection Based on Public/Private Keys Pair

To create a Secure Shell (SSH) connection based on a public/private keys pair, perform the following steps:

1. Open the Mindterm console (on the probe machine) and from the command line run following command:

   ```
   C:\hp\UCMDB\DataFlowProbe\bin\jre\bin\java.exe -jar C:\hp\UCMDB\DataFlowProb
   e\content\lib\Mindterm.jar
   ```

2. In the Mindterm console, go to **File > Create Keypair** and assign the following values:

   - **Key type/format:** choose DSA or RSA
   - **Key length:**
     - **If Key type/format = DSA:** choose 1024
     - **If Key type/format = RSA:** choose one of the following: 768, 1024, 1536, 2048, 4096, 8192, 16384 or 32768
   - **Identity file:** assign a name (the default name is **identity)**
   - **Password:** for no password, do not enter anything

   Caution: The **OpenSSH .pub format** option must be selected.

3. Click **Generate** and move your mouse to generate public/private keys.

4. Once the pair is generated, go to **C:\Users\<username>\AppData\Roaming\MindTerm**. This directory contains generated public/private keys pair. The public key has the **.pub** extension.

5. Copy the contents of **.pub** file to the remote Linux/Unix machine you want to connect to as follows:

   a. Connect to the Linux/Unix remote machine and locate the **~/.ssh/authorized_keys** file (if the file does not exist, create it).

   b. Open the file for editing as follows:

      ```
      vi ~/.ssh/authorized_keys
      ```

   c. Append the contents of the **.pub** file to the **authorized_keys** file.

d. Add <username>@<probe IP> to the end of the contents of the **.pub** file. For example, if the contents of the **.pub** file are:

```
ssh-dss AAAAB3N.....<snippet>.....r2LnQrqhncpJyL1s0id76j6wA==
```

and the probe's IP is 16.59.56.255 and the username to connect with is **root**, you would append the following to the contents of the **~/.ssh/authorized_keys** file:

```
ssh-dss AAAAB3N.....<snippet>.....r2LnQrqhncpJyL1s0id76j6wA== root@16.59.
56.255
```

e. Save the **~/.ssh/authorized_keys** file and close it.

6. Open the UCMDB and go to **Data Flow Management > Data Flow Probe Setup > Credentials > SSH Protocol**.

7. Add a new SSH protocol with the following parameters:

   - **Authentication Method:** publickey
   - **User Name:** root
   - **Key File Path:** C:\\Users\\<username>\\AppData\\Roaming\\MindTerm\\<identity file>, where <identity file> is the name you entered in step 2.
   - **Password:** if you provided a password during creation of the public/private keys pair, you must enter the same password here.

Chapter 8: Supported UNIX Shells

UCMDB supports use of the following UNIX shells:

- bash
- csh
- ksh
- tcsh

Chapter 9: Troubleshooting and Limitations

This section describes general troubleshooting and limitations related to performing discovery using Universal Discovery.

- **Problem**: Cannot Connect to Windows Vista/2008-R2 Machines with UAC Enabled

  Reason: Starting from Windows Vista, Microsoft has changed the security mechanism by introducing the UAC (User Account Control) technology. This change causes problems with HPCmd connecting to remote Windows Vista/2008-R2 machines when using the local administrator account.

  Solution: The following procedure enables HPCmd connection to remote Windows Vista/2008-R2 machines with UAC enabled.

  a. Verify the HPCmd connection

     i. Log on to the Probe machine.

     ii. Locate the **HPCmd.bat** file in hp\UCMDB\DataFlowProbe\tools directory.

     iii. Open **cmd.com** in the same directory.

     iv. At the command prompt, invoke following command:

     ```
     HPCmd.bat \\<problematic machine name or ip>
     /USER:<domain>\<username> /PWD:<password>
     ```

  b. If the HPCmd connection is not successful, check accessibility to the shared folder, admin$.

     Ensure that the Probe machine can access the shared folder, **admin$**, on the remote machine.

     i. Log on to the Probe machine.

     ii. Select **Start > Run**, and enter `\\<remote machine>\admin$ address`.

     iii. If there is no access to **admin$**:

        - Log on to the remote machine.

        - Select **Start > Run**, and enter `regedit`.

        - Locate the following registry subkey:

        ```
        HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
        LanmanServer\Parameters
        ```

- Right-click **Parameters**, and select the **Details** pane.
- If the **AutoShareServer** registry entry does not exist, in the **Edit** menu, select **New** > **DWORD (32-bit) Value.** Enter **AutoShareServer**, and click **OK**.
- Select **AutoShareServer**. In the **Edit** menu, select **Modify**, and in the **Value** box, type `1`.
- Exit the Registry Editor, and restart the computer.
- Select **Start > Run**, and enter `net start srvnet`.

iv. When access to **admin$** is successful, try to verify the HPCmd connection again as described in "Verify the HPCmd connection" on the previous page.

c. If the verification still fails, connect to Windows Vista/2008-R2 machines with UAC enabled.

i. On Windows Vista/2008-R2 machines, local administrators do not have full privileges when connected remotely.

Use one of the following options to overcome this problem:

- Connect using domain administrator credentials.
- Enable local administrators to have full privileges by modifying the registry on remote machine as follows:

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Policies\system
Value	LocalAccountTokenFilterPolicy should be set to 1. If this value is not available, create a new DWORD value and set it to 1.

ii. Restart the machine.

- **Problem:** The file transfer does not work when communicating with the remote Linux/UNIX/Mac OS X machines, as the result operations like Scanner-based Inventory Discovery or deployment of Universal Discovery agents fail.

  Solution:

  a. Make sure the SSH agent is configured to allow file transfer via the SCP/SFTP protocols.

  b. Make sure that the logon process for the user that is used for the SSH protocol does not have a banner that requires manual user input during the logon process.