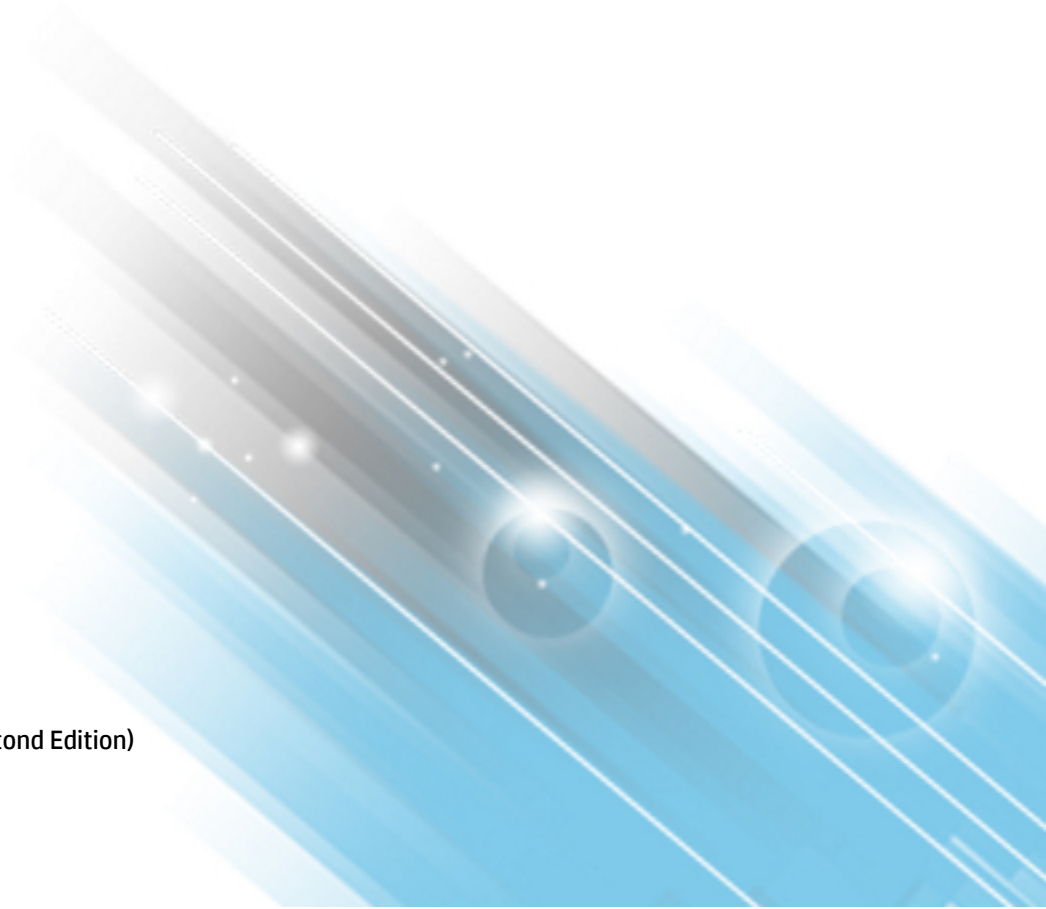
HP Universal CMDB & Configuration Manager

Software Version: 10.21 CUP1

Release Notes



Document Release Date: October 2015 (Second Edition)
Software Release Date: September 2015

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe™ 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 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 HP sales representative for details.

Document Changes

Version	Changes
10.21 CUP1 (2nd Edition, October 2015)	Corrected the directory for the **postgresql.conf** file in the workaround for QCCR1H101769.

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

HP Universal CMDB & Configuration Manager Release Notes 4
What's New in UCMDB 10.21 CUP1 4
Installation Notes 6
HP Universal CMDB and Configuration Manager 10.21 CUP1 Files/Components 6
System Requirements 6
Install 10.21 CUP1 on the HP Universal CMDB and Configuration Manager Servers 7
HP Universal CMDB 10.21 CUP1 Manual Data Flow Probe Installation 9
Uninstall HP Universal CMDB and CM 10.21 CUP1 9
Notes 11
Known Problems, Limitations, and Workarounds 12
Enhancements Requests 16
Fixed Defects for UCMDB 10.21 CUP1 17
Documentation Errata 21
Appendixes 22
CyberArk Integration 23
Overview 24
Deployment 24
How the CyberArk Integration Works 24
Supported Versions 25
Supported CyberArk Versions 25
Supported Probe Types 25
Supported Protocols 25
How to Configure CyberArk Integration 26
CyberArk Integration Configuration Workflow 27
How to Configure CyberArk Integration 28
How to Create and Configure CyberArk Account for the Integration 36
How to Add CyberArk Credential for Protocols from JMX 45
CyberArk Integration Troubleshooting and Limitations 47
Sample Script for IP Range Management API 49
Send Documentation Feedback 52

HP Universal CMDB & Configuration Manager Release Notes

Keep your system up to date with the most recent cumulative update package (CUP) for UCMDB 10.20. This package contains all of the UCMDB 10.20 hotfixes that have been released since the initial release of UCMDB 10.20.

What's New in UCMDB 10.21 CUP1

UCMDB 10.21 CUP1 contains the following new features and changes:

- Added the capability of integrating UCMDB/UD with CyberArk Enterprise Password Vault. The integration allows Universal Discovery administrators to configure credentials for supported Universal Discovery protocols, which enables administrators to manage the credentials in a secure and easy way.

  Instead of storing the passwords themselves in UCMDB/UD, this integration involves storing only references (in the CyberArk Enterprise Password Vault) to the passwords, and retrieving the passwords when they are needed from the vault using the stored references.

  For details, see "CyberArk Integration" on page 23.

- Added discovery indicators in the UCMDB Browser, which allow you to see a warning or an error flag on a discovered CI, if any of the discovery jobs have completed with warnings or errors.

  This feature requires UCMDB Browser 4.03. For details about the discovery indicators, see the *Release Notes*for UCMDB Browser version 4.03.

- The Data Flow Management Java API has a new **importIPRanges()** method in the **DDMConfigurationService** class. This method allows you to perform the following tasks by using a customized script to manage the IP ranges of specified Probes:

  - Overwrite the IP ranges of specified Probes. The **IPv4/6**, **Range**, and **Type** settings of an IP range are manageable through this method.

  - Assign certain probes in the same domain into a probe list, and then distribute the IP addresses in the specified ranges evenly to each probe in the group.

Note: Group is a temporary parameter used in this API method to group a set of probes assigned to the same domain, and to balance the IPs evenly among these probes.

You can perform this task on any computer that can access the UCMDB server. One or both of the following files are mandatory to set up the work environment on different computers:

- **ucmdb-api.jar**: On the UCMDB server or on a probe, you only need this file. This file is available for download from the UCMDB server through the following URL: http:// *<IP_or_FQDN>*:8080/ucmdb-api/download
- **api-client.jar**: On a computer other than the UCMDB server or a probe, you need this file in addition to the ucmdb-api.jar file. This file is available in the following directory on the UCMDB server: <UCMDB_server>\lib\

For more information about how to use the UCMDB API, refer to the following documentation:

- The **HP Universal CMDB API** chapter in the *HP Universal CMDB Developer Reference Guide*
- *API Reference*

For a sample script to perform the IP range management task, see "Sample Script for IP Range Management API " on page 49.

Note:

- This method does not support clusters.
- You can specify the excluded IP ranges in the script. The API will calculate the whole IP ranges and the excluded IP ranges, and only assign the resulting IP ranges to a probe.
- For both IPv4 and IPv6, you must specify an IP range with a starting IP address and an ending IP address in the format of x.x.x.x-x.x.x.x. If you want to specify a single IP address, the starting IP address and the endiassignng IP address are the same.
- An IP range should not overlap with another IP range in the script or with an IP range in another existing probe. Otherwise, the IP range will not be imported.
- When you add probe list in the Java API **importIPRanges()** method, make sure you only add the discovery probe list. Do not add integration probes (for example, Linux probes or integration services).

Linux Probes and integration services do not need IP ranges. If you add Linux probes or integration services, although the IPs in Linux probe or integration services do not display in the UI, they will be assigned to Linux Probes or integration services.

Installation Notes

HP Universal CMDB and Configuration Manager 10.21 CUP1 Files/Components

HP UCMDB 10.21 CUP1 is packaged in one .zip file.

The **UCMDB_00171.zip** (for Windows) includes the following files/components:

- **HPUCMDB_Server_10.21.CUP1.exe**. The installation of the version 10.21 CUP1 HP UCMDB Server and Data Flow Probe for Windows.
- **HPCM_10.21.CUP1.exe**. The installation of version 10.21 CUP1 HP UCMDB Configuration Manager for Windows.
- **ReleaseNotes.pdf** (this file)

The **UCMDB_00172.zip** (for Linux) includes the following files/components:

- **HPUCMDB_Server_10.21.CUP1.bin**. The installation of the version 10.21 CUP1 HP UCMDB Server and Data Flow Probe for the Linux platform.
- **HPCM_10.21.CUP1.bin.** The installation of version 10.21 CUP1 HP UCMDB Configuration Manager for the Linux platform.
- **ReleaseNotes.pdf** (this file)

System Requirements

For a list of system requirements, see the **HP UCMDB Support Matrix** PDF file. Check the most previous Release Notes for any additions or changes to the matrix.

Note: If you are using an Oracle version that is prior to 10.2.0.5, you must apply the Oracle patch that fixes Oracle defect # 5866410. For details, go to the Oracle website and find the information regarding this defect number.

Install 10.21 CUP1 on the HP Universal CMDB and Configuration Manager Servers

CUP Installation for both HP Universal CMDB and Configuration Manager is performed through an automated procedure using the installation wizard.

You can still install the Data Flow Probes separately by upgrading the Data Flow Probes using the UCMDB user interface. For details, see "Installation Notes" on the previous page.

Note:

- HP UCMDB 10.21 CUP1 can be installed only on top of an HP Universal CMDB version 10.21.
- HP UCMDB CM 10.21 CUP1 can be installed only on top of HP UCMDB CM 10.21.
- The UCMDB CUP version and the CM CUP version must be the same.

Pre-requisites - UCMDB Server and Data Flow Probes

1. Extract **UCMDB_00171.zip** (for Windows) or **UCMDB_00172.zip** (for Linux) to a temporary directory.
2. Stop the HP Universal CMDB 10.21 server and the HP Universal CMDB Integration Service (if running) before starting the 10.21 CUP1 installation.

   Note: If you have a High Availability configuration, the CUP must be installed on all the servers in the cluster, and prior to installation, you must stop all the servers in the cluster.

3. If you have received private patches for the Data Flow Probe, you must delete them before performing the upgrade. These steps for deleting a private patch must be followed whether you are upgrading the probes during the installation wizard, or if you upgrading the probes using the UCMDB user interface after installation is complete.

a. Stop the Data Flow Probe.

b. Delete all private patches that were installed on the system prior to this CUP by deleting the following directory:

\hp\UCMDB\DataFlowProbe\classes directory

c. Start up the version 10.21 Data Flow Probe.

CUP Installation

You must first install the UCMDB CUP, start up the server, and then perform the Configuration Manager (CM) CUP installation.

1. For UCMDB: Double-click the file **HPUCMDB_Server_10.21.CUP1.exe** (for Windows) or **sh HPUCMDB_Server_10.21.CUP1.bin** (for Linux) to open the HP Universal CMDB Server CUP Installation Wizard.

   For Configuration Manager: Double click the file **HPCM_10.21.CUP1.exe** (for Windows) or **sh HPCM_10.21.CUP1.bin** (for Linux) to open the HP Universal CMDB Configuration Manager CUP Installation Wizard.

2. While running the wizard:

   - In the Choose Install Folder screen, select the installation directory in which UCMDB/CM is already installed.
   - For UCMDB, in the Install Data Flow Probe CUP screen, select the following option:
     - **Automatically update Data Flow Probe with the new CUP version** to automatically update during this installation all the Data Flow Probes reporting to this UCMDB.
     - **Update the Data Flow Probe manually** to update the Data Flow Probes reporting to this UCMDB using the UCMDB user interface after completing the installation of this CUP on the UCMDB server. For details, see "Installation Notes" on page 6.
     - In the Required Actions screen, follow the instruction to ensure that the server is down.

3. Once the installation wizard for UCMDB is completed, start up the version 10.21 server per the instructions in the Deployment Guide for version 10.21. Go back to step 1 to install the CM CUP.

Once the CM CUP installation is completed, start up Configuration Manager version 10.21 per the instructions in the Deployment Guide for version 10.21.

HP Universal CMDB 10.21 CUP1 Manual Data Flow Probe Installation

Linux: Always required.

Windows: Applicable only when **Update the Data Flow Probes manually** is selected in the CUP installation wizard.

To install the Data Flow Probe CUP upgrade using the UCMDB user interface, follow these steps.

Note: All Data Flow Probes that are associated with the UCMDB are upgraded.

1. If you have received private patches for the Data Flow Probe, perform the steps in the section "Pre-requisites - UCMDB Server and Data Flow Probes" on page 7.
2. In UCMDB, go to **Data Flow Management > Data Flow Probe Setup**, and click **Deploy Probe Upgrade**.
3. In the Deploy Probe Upgrade dialog box, navigate to the **<SERVER_HOME>\content\probe_patch\probe-patch-10.21.CUP1-windows/linux.zip** and click **OK**.
4. **Linux only:**
   a. Stop the Data Flow Probe.
   b. Extract the upgrade package by running the following file:

      /opt/hp/UCMDB/DataFlowProbe/tools/upgrade/extractUpgradePackage.sh

   c. Restart the Data Flow Probe.

Uninstall HP Universal CMDB and CM 10.21 CUP1

When performing the uninstall procedure, this procedure must be performed for both the UCMDB Server and the Data Flow probes, as well as Configuration Manager.

1. Stop the HP Universal CMDB and Configuration Manager servers, and all running Data Flow Probes before uninstalling the version CUP.
2. For UCMDB:
   - Windows: Go to **<CMDB installation folder>\UninstallerCup** and double-click **Uninstall HP Universal CMDB Server CUP**. After the CUP is successfully uninstalled, go to **<CMDB installation folder>\runtime** and delete the **jsp** and **jetty-cache** folders.
   - Linux: Go to **<CMDB installation folder>/UninstallerCup** and run **Uninstall HP Universal CMDB Server CUP**. After the CUP is successfully uninstalled, go to **<CMDB installation folder>/runtime** and delete the **jsp** and **jetty-cache** folders.
3. For Configuration Manager:
   - Windows: Go to **Start** menu **> Programs > HP Universal CMDB Configuration Manager 10.21** and double click **Uninstall HP Universal CMDB Configuration Manager 10.21 CUP1.**
   - Linux: Go to **<CM installation folder>/_sp_installation/** and run **HPCM_10.21_CUP1-Uninstall**.
4. Uninstall all existing Probes as follows:
   a. **Start > All Programs > HP UCMDB > Uninstall Data Flow Probe**.
   b. Start the server.
   c. Undeploy the **probeUpdate** package.
5. Reinstall the Probes with the same configuration, that is, use the same Probe IDs, domain names, and server names as for the previous Probe installations. Remember that the Probe ID is case sensitive.

   Note: After performing an upgrade and installing the new Data Flow Probe, all the Discovery jobs that were active before the upgrade are automatically run.

Notes

- When upgrading the Data Flow Probe:
  - In a multi-customer environment, if the Data Flow Probe is not automatically upgraded to the latest CUP version, use the manual upgrade procedure to upgrade the Probe manually. For details on the manual upgrade procedure, see "How to Deploy a Data Flow Probe CUP Manually" in the *HP Universal CMDB Data Flow Management Guide*.
  - The automatic upgrade is not available for Data Flow Probes running on Linux. Use the manual upgrade procedure to upgrade the Probe manually.
  - The Data Flow Probe upgrade is only available for upgrades for minor-minor releases or upgrades between CUP releases. When performing an upgrade to a major or minor release, you must reinstall the Probe.
- If you encounter an error when installing the CUP under Linux on the **/tmp** directory because the **/tmp** directory is configured not to run executables, set the IATEMPDIR environment variable to a location with sufficient permissions and disk space. The IATEMPDIR variable is recognized by InstallAnywhere.

Known Problems, Limitations, and Workarounds

The following problems and limitations are known to exist in CMS 10.21 CUP1 (or later software, as indicated). The problems are categorized by the affected product area. If a problem has an assigned internal tracking number, that tracking number is provided (in parentheses) at the end of the problem descriptions.

Configuration Manager

PROBLEM: If Configuration Manager was running in FIPS mode before the installation of UCMDB 10.21 CUP1, the LW-SSO FIPS configuration is lost after installing the CUP.

Workaround: To revert to a working configuration, edit the **servers\server-0\webapps\cnc\WEB-INF\classes\cnclwssofmconf.xml** file relative to your CM installation folder and update the crypto tag with the following tag:

```
<crypto cryptoSource="jce"
cipherType="symmetricBlockCipher"
engineName="AES"
paddingModeName="CBC"
keySize="256"
pbeDigestAlgorithm="SHA1"
encodingMode="Base64Url"
jceProviderName="JsafeJCE"
jcePbeAlgorithmName="AES"
jcePbeMacAlgorithmName="AES"
macType="hmac"
macAlgorithmName="SHA1"
directKeyEncoded="true"
directKeyEncoding="Base64Url"
algorithmPaddingName="PKCS5Padding"
pbeCount="20"
macKeySize="256"
macPbeCount="20"
initString="12gHERamY1mD8LfeBp6FxwE8FU6BlabS"></crypto>
```

Universal CMDB - General

LIMITATION: The UCMDB Push Engine does not support the following TQL queries:

- TQL queries containing SubGraphs
- TQL queries containing Full Path Compound links

Workaround: None.

LIMITATION: The **Schedule Report** window and the **Job List** window may show different time for a scheduled report when the local machine is in a different time zone than the UCMDB server.

Workaround: None.

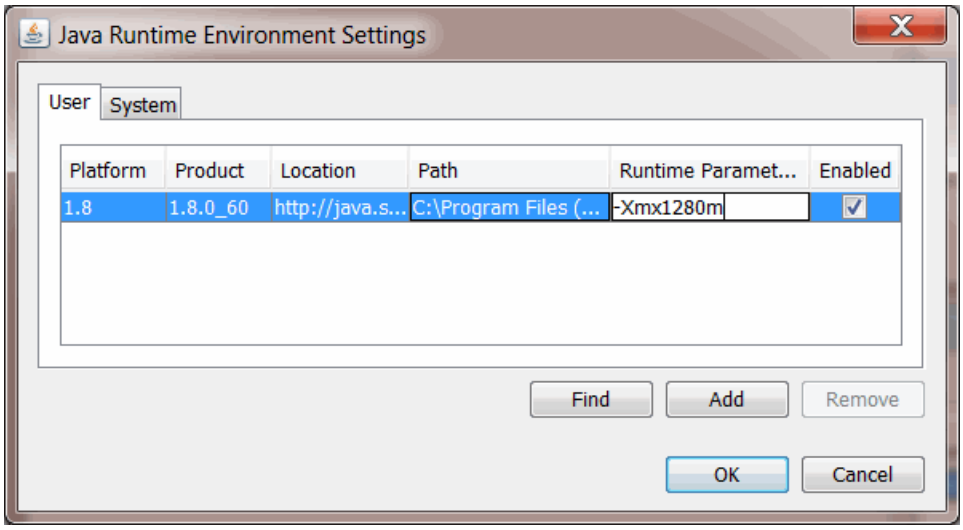
LIMITATION: Currently it is not possible to create two **Pattern Based Models** with the same name and different tenants in a multi-tenant UCMDB environment with the tenant aware setup. This is because the enrichments and the queries created behind the **Pattern Based Models** must have a unique name. (QCCR1H103293)

Workaround: None.

PROBLEM: Cannot deploy Probe Update on UCMDB 10.21 CUP1 Server, and then cannot close the Deploy Probe Update pop-up window when clicking **Close** or **Cancel**. (QCCR1H103164)

Workaround: To resolve the UI performance issue, increase Java memory.

1. From the **Start** menu, search **Java**.
2. Click **Configure Java**.
3. In the Java Control Panel, go to the **Java** tab, and click **View**.
4. In the Java Runtime Environment Settings dialog, double click the value field for the **Runtime Parameters** column, and type `-Xmx1280m` or a larger value.



5. Click **OK**.
6. Click **Apply** and then click **OK**.
7. Close all open Internet Browser windows and restart the UCMDB UI.

   The UCMDB UI works well now.

Universal CMDB - Topology

PROBLEM: The View result in **Browse Views** is not consistent with the result in the **Modeling Studio**, when creating a New Pattern View with the attribute condition **NOT Node Is Virtual Equal "True"**. (QCCR1H100696)

Workaround: To avoid this issue, create a New Pattern View and define the following attribute conditions in the **Query Node Properties** window: **Node Is Virtual Equal "False"** AND **Node Is Virtual Is null**.

Integrations

PROBLEM: After upgrading UCMDB to the latest CUP, an integration job using a Database connection may fail due to performance issues. (QCCR1H98428)

Workaround: To resolve this issue, close the communication logs for the integration job.

Universal Discovery - Inventory Discovery

PROBLEM: (PostgreSQL only) Some SQL statements are observed running more than 30 minutes, which causes Probe database to crash. The root cause is that the default value of the **statement_timeout** setting in the **postgresql.conf** file is **0**. (QCCR1H101769)

Workaround: To workaround the issue, locate and open the **hp\UCMDB\DataFlowProbe\pgsql\data\postgresql.conf** file in a text editor, and then modify the default value of the **statement_timeout** setting from **0** to **3600000**.

Enhancements Requests

The following table lists the enhancement requests that were implemented in the HP UCMDB 10.21 CUP1 release.

Global ID	Problem	Solution
QCCR1H83306	Invoking the **reindex** method in the High Availability environment does not trigger the re-indexing operation on all nodes in the cluster.	Implemented an enhancement by improving the **reindex** method in the**JMX** console **> UCMDB:service=Topology Search Services**. To perform reindex on all UCMDB nodes in the High Availability cluster, select **True.**
QCCR1H92883	This is a request to provide the capability of integrating UCMDB/UD with CyberArk along with its accompanying product, Password Vault, to provide a secure password management solution for the critical systems used to operate.	Implemented the enhancement to provide the capability of integrating UCMDB/UD with CyberArk. For details, see "CyberArk Integration" on page 23.
QCCR1H95577	Users request to remove the "**[ ]**" characters from the **Concatenated List** column in reports.	Implemented an enhancement so that the "**[ ]**" characters are no longer added automatically to the string representation of a Java ArrayList object. Now the **Concatenated List** column in reports does not contain the "**[ ]**" characters.
QCCR1H99728	In the High Availability (HA) environment, the reader server cannot be logged in to if the writer server is busy.	You can now log in to the reader server even if the writer is blocked.
QCCR1H100282	The user cannot create, update or delete the IP ranges of the connected Probes.	Implemented an enhancement by adding a new API method **importIPRanges()**. This method allows you to create, update, or delete the IP ranges of all the connected Probes. For details, see "What's New in UCMDB 10.21 CUP1" on page 4 section.
QCCR1H101710	Currently it is hard to reproduce complex reconciliation issues. It would help greatly if we can record the exact bulk and CMDB data that is being processed and reproduce the issue on any environment.	Implemented the enhancement by adding a new property **reconciliation.dump.bulks** to the **setSettingValue** JMX method in the **UCMDB:service=Settings Services** category. By setting the **reconciliation.dump.bulks** property to **true**, you can dump CMDB and bulk containers to files in the **<UCMDB_Server_**

Global ID	Problem	Solution
		Home>\runtime\log\bulkDumps directory.
QCCR1H102562	In the UCMDB Browser, the user cannot see if any of the discovery job have completed with warnings or errors, so that the problematic discovered CI cannot be identified.	Implemented the enhancement by adding new warning or error indicators in the UCMDB Browser. Now, a warning or an error flag will show on a discovered CI if any of the discovery jobs have completed with warnings or errors. **Note:** The discovery indicators will show up as long as you have the **View Discovery Status and Error** or the **Run Discovery and Integrations** permission. For details, see "What's New in UCMDB 10.21 CUP1" on page 4 section.
QCCR1H102290	This is a request to expose the count of CIs and create-read-delete operations for valid links to the UCMDB Browser.	Created new APIs which expose the count of CIs and create-read-delete operations for valid links to the UCMDB Browser.

Fixed Defects for UCMDB 10.21 CUP1

The following table lists the defects that were fixed in the HP UCMDB 10.21 CUP1 release.

Global ID	Problem	Solution
QCCR1H98436	The Perspective Based View does not show all the CIs and links that are displayed in TQL query.	Fixed the issue by implementing a code change. Now the Perspective Based View shows all the CIs and links as expected.
QCCR1H99183	Custom normalization rules do not have priority over the out-of-the-box rules.	Fixed the issue by implementing a code change so that custom normalization rules have priority over the out-of-the-box rules.
QCCR1H99244	When configuring HP SIM credential, the integration point has no reference to the credentials being used. The HP SIM Protocol entry has no reference to the HP SIM application server, only to the database.	Fixed the issue by applying a code change. Now the MSSQL_NTLMV2 type connection is available when configuring HP SIM credential. **Note:** This fix requires CP16 Update 1 (or later) to work.
QCCR1H100791	After UCMDB CUP5 is deployed, the out-of-the-box XML PushAdapter	Fixed the issue by applying a code change so that null value check will be performed

Global ID	Problem	Solution
	export crashes. Integration crashes with the NullPointerException error.	to avoid NullPointerException.
QCCR1H100917	After upgrading from UCMDB 10.11 to UCMDB 10.20, deleting a single relationship in the UCMDB UI takes too much time and the **reconciliation.audit** log shows that the operation took less than one minute.	Fixed the issue by implementing a code change. Now a single relationship is deleted quickly.
QCCR1H100919	The **Authorized** state of Customer ID 100001 appears with the failed status on the UCMDB server's status page. The **ping_url** is down, causing no probes to connect to the writer. This issue is reproducible when multiple states are present in UCMDB.	Fixed the issue by applying a code change. Now the UCMDB server is started without failure.
QCCR1H100963	The direct link for a parametrized Template Based View does not work in the UCMDB 10.20 if the user is not logged in.	Fixed the issue by implementing a code change. Now the direct link for a parametrized Template Based View works as expected.
QCCR1H101120	The following error message is returned by the **Oracle Database by SQL** job: "Failed to collect data from Oracle server".	Fixed the issue by applying a code change. Now the **Oracle Database by SQL** job works properly.
QCCR1H101223	The Data Flow Probe status appears disconnected (stopped) in the UCMDB UI for a long time. However, the Probe service is up, and the Probe is reporting data and connecting to UCMDB.	Now UCMDB sets the Data Flow Probe status correctly.
QCCR1H101252	The UCMDB servers experiences the performance issue. The UCMDB GUI becomes unresponsive from time to time.	Fixed the issue by increasing the default value for **jetty.maxThreads** to 300.
QCCR1H101413	After running the **Inventory Discovery by Scanner** job, the Probe failed to save the data into ID Mapping table, and many CIs are deleted incorrectly due to the auto deletion triggers.	Fixed the issue by implementing a code change so that the CIs are not deleted incorrectly anymore.

Global ID	Problem	Solution
QCCR1H101581	Universal Discovery 10.20 sets incorrect values in the **hwHostOS** field for HP-UX by including **hwOSHostHPUXType** into the value.	Fixed the issue by removing the inclusion of **hwOSHostHPUXType** in the **hwHostOS** field. **Note:** This fix requires CP15 Update 3 to work.
QCCR1H101772	Several discovery jobs fail with the "java.lang.IllegalStateException: Shutdown in progress" error.	Fixed the issue so that discovery jobs can successfully run.
QCCR1H102018	The **displayName** attribute is not updated if this setting is selected to be used for LDAP users.	The LDAP display name is now used and updated for users.
QCCR1H102362	The aging mechanism does not update the value of the **Is Candidate For Deletion** attribute to False.	Fixed the issue by implementing a code change. Now the aging mechanism works as expected.
QCCR1H102465	The Instance based adapter does not return the correct idToTypes map when it loads the referenced CIs and the push job fails with several errors.	Fixed the issue by implementing a code change. Now the Instanced based adapter works properly.
QCCR1H102592	Cannot move an Enrichment Rule from a sub-folder to the Root folder, using the **Move to Folder** function; instead of moving the selected rule, the whole sub-folder disappears.	Fixed the issue by implementing a code change. Now an Enrichment Rule can be moved to the Root folder.
QCCR1H102930	When the probe downloads ad hoc tasks to the AM Push Adapter, the jobs fail with the TimeoutException error.	Fixed the issue by implementing a code change. Now the probe can download ad hoc tasks to the AM Push Adapter successfully.
QCCR1H103086	The **Owner Tenant** attribute is overwritten when populating to a multi-tenant (MT) UCMDB and both integration servers are set as GlobalIDGenerator.	Fixed the issue by adding the following settings to the cmdb10xAdaper: • **shouldOmitTenantOwnerFromAuto Recon**. If not specified, it has **true** as default value. It will skip the tenant owner attribute from Auto Complete Reconciliation. • **population.autocomplete.reconciliatio n**. If not specified, it has **true** as default

Global ID	Problem	Solution

		value. This setting enables or disables Auto Complete Reconciliation.
		• **shouldOmitGlobalIDFromLayout**. If not specified, it has **false** as default value. It will not add the **global_id** attribute to the TQL query layout.
		You can add the new settings to the adapter XML file as needed in the following format. Otherwise, the default values will be used.
		`<adapter-setting name="shouldOmitGlobalIDFromLayout">true</adapter-setting>`
		`<adapter-setting name="shouldOmitTenantOwnerAutoRecon">true</adapter-setting>`
		Since **TenantOwner** is part of CIs identification, it should not be sent from the source UCMDB. To accomplish this, make sure you ensure the following:
		• The integration TQL query should not have the **TenantOwner**, **TenantsUses**, and **global_id** attributes in the TQL query layout.
		• The **shouldOmitTenantProperties** setting of the Cmdb10xAdapter must be set to **true**. It can be set from the adapter XML definition:
		`<adapter-setting name="shouldOmitTenantProperties">true</adapter-setting>`
		Note: This fix requires that you manually redeploy the UCMDB 10.x adapter package located in the **C:\hp\UCMDB\UCMDBServer\content\adapters** directory after installing UCMDB 10.21 CUP1.

Documentation Errata

The following items are listed incorrectly in the documentation.

HP Universal CMDB Hardening Guide

No information about the UCMDB-API client certificate key size

Location: *HP Universal CMDB Hardening Guide*, version 10.21, page 30 (QCCR1H102759)

Error: There is no information about the minimum key size for the UCMDB-API client certificate.

Correction: Add the following note under the *Enable Mutual Certificate Authentication for SDK* section:

Note: The UCMDB-API client certificate must have the minimum key size no less than 2048 bits.

Appendixes

This appendix includes:

CyberArk Integration 23
Sample Script for IP Range Management API 49

CyberArk Integration

This section includes:

Overview 24
Supported Versions 25
Supported Protocols 25
How to Configure CyberArk Integration 26
CyberArk Integration Troubleshooting and Limitations 47

Overview 24
Deployment 24
How the CyberArk Integration Works 24
Supported Versions 25
Supported CyberArk Versions 25
Supported Probe Types 25
Supported Protocols 25
How to Configure CyberArk Integration 26
CyberArk Integration Configuration Workflow 27
How to Configure CyberArk Integration 28
How to Create and Configure CyberArk Account for the Integration 36
How to Add CyberArk Credential for Protocols from JMX 45
CyberArk Integration Troubleshooting and Limitations 47

Overview

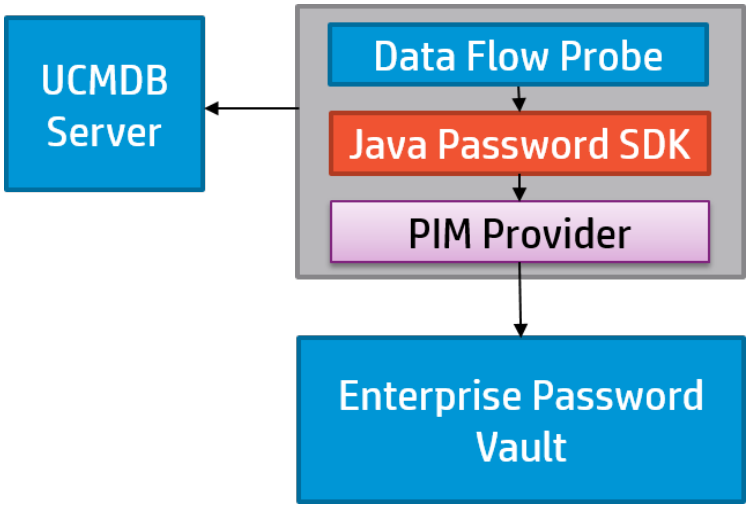
CyberArk is a product that implements an external password vault. CyberArk Enterprise Password Vault, part of the CyberArk Privileged Account Security Solution, enables organizations to secure, manage and track the use of privileged credentials whether on-premise or in the cloud, across operating systems, databases, applications, hypervisors, network devices and more.

The integration between UCMDB and CyberArk Enterprise Password Vault allows Universal Discovery administrators to configure credentials for supported Universal Discovery protocols, which enables administrators to manage the credentials in a secure and easy way.

Instead of storing the passwords themselves in UCMDB/UD, this integration involves storing only references (in the CyberArk Enterprise Password Vault) to the passwords, and retrieving the passwords when they are needed from the vault using the stored references.

Deployment

The following diagram illustrates the overall deployment.



How the CyberArk Integration Works

The CyberArk integration enables UCMDB/UD to retrieve usernames and passwords from the CyberArk Enterprise Password Vault as follows:

1. Administrators to create a Safe, Application, and Account on the CyberArk Server, including username, password, and unique reference ID.

2. Universal Discovery administrators to create a credential on UCMDB Server, using the same CyberArk Safe, Application, and Account values created in step 1 as reference ID in the following format: <Safe_Name>\<Folder_Path>\<Reference_ID>
3. The CyberArk integration synchronizes the CyberArk references to Data Flow Probes. No password information contained.
4. Universal Discovery administrators to run discovery jobs using the unique referenceID to retrieve username and password from CyberArk.

Supported Versions

Supported CyberArk Versions

This integration supports CyberArk Enterprise Password Vault version 8.6.0.

Supported Probe Types

This integration supports probes on the Windows platform only.

Platform	Probe Mode	Supported?
Windows	Union	Yes
	Separate	Yes
Probes on Linux		No
Integration Services		No

Supported Protocols

The following table describes protocols supported by CyberArk integration from UCMDB UI or supported from JMX console.

Protocols Supported from UCMDB UI (with CyberArk-related fields available)	Protocols Supported from JMX (no UI fields)
• AS400 • AWS • CA CMDB	• Asset Manager • CIM • HP Network Automation Java

Protocols Supported from UCMDB UI (with CyberArk-related fields available)	Protocols Supported from JMX (no UI fields)
• Generic DB • Generic • HP SIM • HTTP • NetApp • NTCMD • Powershell • Remedy • SNMP • SSH • Telnet • vCloud • WMI	• JBOSS • LDAP • NNM • SANscreen • SAP JMX • SAP • ServiceNow • Siebel Gateway • TIBCO • UCS • VMware VIM • WebLogic • WebSphere

- **Protocols Supported from UCMDB UI.** When CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled in the Protocol Parameters dialog box. The existing attributes **Username** and **Password** are grouped under the **Regular Credential** radio button, and two new attributes (**Type** and **Reference**) grouped under the **External Vault** radio button. For details about the protocol attributes, see the section about the supported protocols in the *HP UCMDB Universal Discovery Content Guide - Supported Content*.

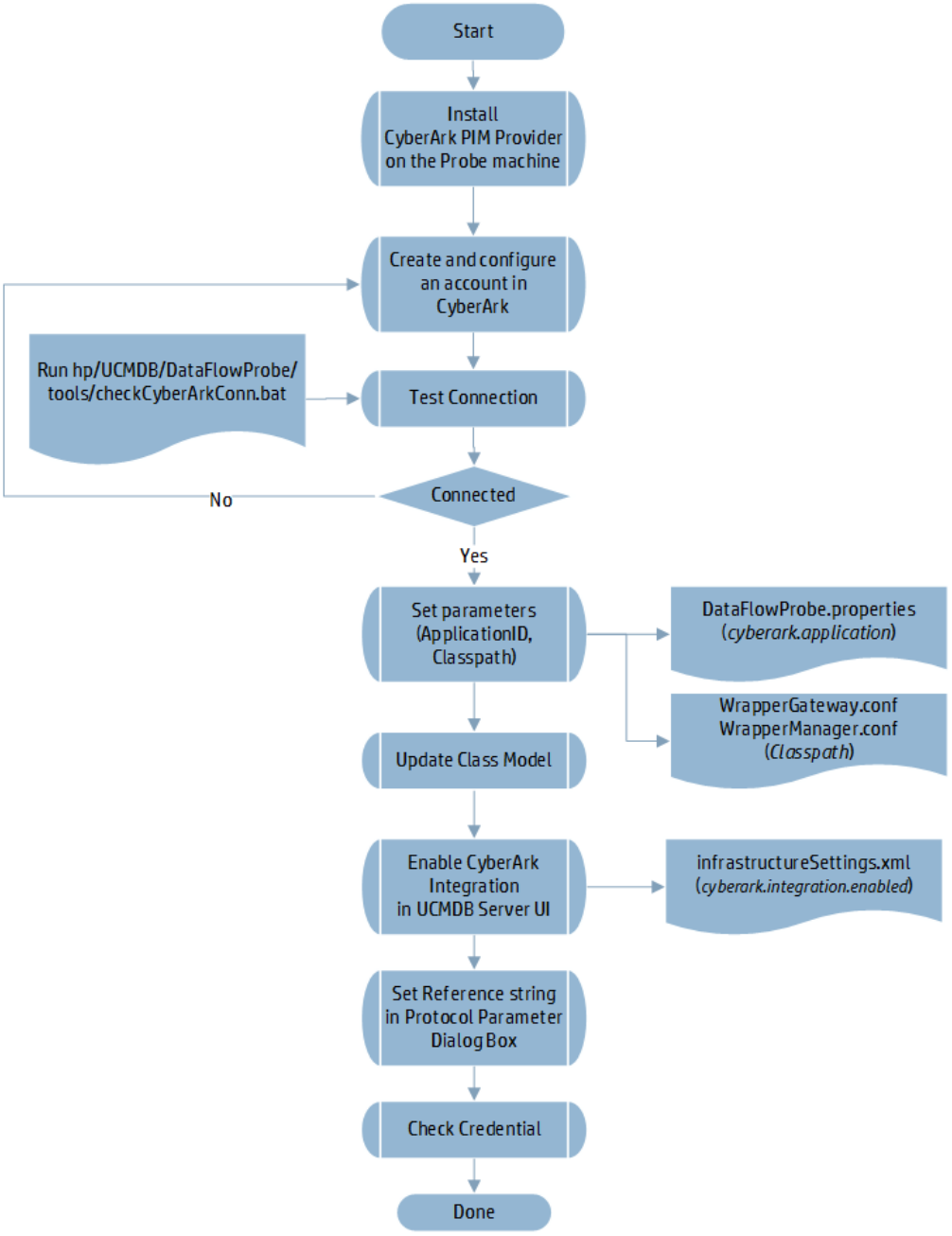
- **Protocols Supported from JMX.** There are no CyberArk related fields in the Protocol Parameter dialog box when the CyberArk integration is enabled, but you can run add CyberArk credential reference to these protocols with the help of JMX methods. For details, see "How to Add CyberArk Credential for Protocols from JMX" on page 45.

How to Configure CyberArk Integration

This section includes:

CyberArk Integration Configuration Workflow

The diagram below illustrates the overall workflow for configuring CyberArk integration.



How to Configure CyberArk Integration

This section contains detailed instructions about how to configure the CyberArk integration.

Note: Make sure that only administrators have the write permission to the **<DataFlowProbe_Home>** directory.

1. **Install CyberArk PIM Provider**

   Install CyberArk Privileged Identity Management (PIM) Provider (in AIM mode) on each of the supported Probe servers.

   Note: If the Probe is Manager, install the CyberArk PIM Provider on the Probe Manager.

   For a Probe in separate mode, install the CyberArk PIM Provider together with the Probe Manager.

   For detailed instructions, see CyberArk *Application Identity Manager Implementation Guide*.

2. **Configure CyberArk for the integration**

   Create a Safe, a CyberArk account, and an application ID in CyberArk, and configure CyberArk for the integration.

   For detailed instructions, see "How to Create and Configure CyberArk Account for the Integration" on page 36.

3. **Test connection**

   Go to the Probe server, run the **checkCyberArkConn.bat** tool using the following command:

   ```
   <DataFlowProbe_Home>\tools\checkCyberArkConn.bat "<SDK_Path>" <Safe_Name>
   <Folder_Path> <ApplicationID> <ReferenceID>
   ```

   where,

   `<SDK_Path>` is the path of the CyberArk Java Password SDK.

   `<Safe_Name>` is the name of the CyberArk Safe you created in step 2.

<Folder_Path> is the folder for CyberArk Safe. If not specified, it is **Root** by default.

<ApplicationID> is the CyberArk application ID you created in step 2.

<ReferenceID> is the name of the CyberArk account you specified or auto-generated in CyberArk. It can be found in the properties of the account you created in step 2.

For example,

```
C:\hp\UCMDB\DataFlowProbe\tools\checkCyberArkConn.bat "C:\Program Files
(x86)\CyberArk\ApplicationPasswordSdk\JavaPasswordSDK.jar" NancySafe Root
NancyApplication nancy-cyberark-testing-refid
```

4. **Set ApplicationID and Classpath parameters manually**

   Set the following parameters manually on the Probe server:

   - Set **ApplicationID** in the probe configuration file **DataFlowProbe.properties**.

     i. Open the probe configuration file **hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** using a text editor.

     ii. At the end of the file, add the following line:

     ```
     cyberark.application=<CyberArk Application ID>
     ```

     For example,

     ```
     cyberark.application=NancyApplication
     ```

   - Set **Classpath** in the wrapper configuration files.

i. Open the **WrapperGateway.conf** or **WrapperManager.conf** file in a text editor.

- If the current probe is in **union** mode, open the **WrapperGateway.conf** file;
- If the current probe is in **separate** mode (gateway and manager), open the **WrapperManager.conf** file on the manager.

ii. Locate the following line:

```
wrapper.java.classpath.7=%COMMON_CLASSPATH%
```

iii. Add the following line after it:

```
wrapper.java.classpath.8=<CyberArk_Install_
Dir>\ApplicationPasswordSdk\JavaPasswordSDK.jar
```

For example, set classpath in the **WrapperGateway.conf** file as follows:

```
wrapper.java.classpath.7=%COMMON_CLASSPATH%

wrapper.java.classpath.8=C:\Program Files (x86)
\CyberArk\ApplicationPasswordSdk\JavaPasswordSDK.jar
```

iv. Save the file.

v. Restart the probe.

5. **Update class model manually**

You need to update class model manually. To do so,

a. Modify the **Object Root** infrastructure setting.

i. Log in to UCDMB, go to **Administration > Infrastructure Setting Manager**.

ii. Locate the **Object Root** infrastructure setting.

iii. Modify the value of **Object Root** from **managed_object** to **root**.

iv. Click **Save**  .

v. Log out and re-log in to UCMDB.

b. Add two attributes in the **protocol** CI type to update class model.

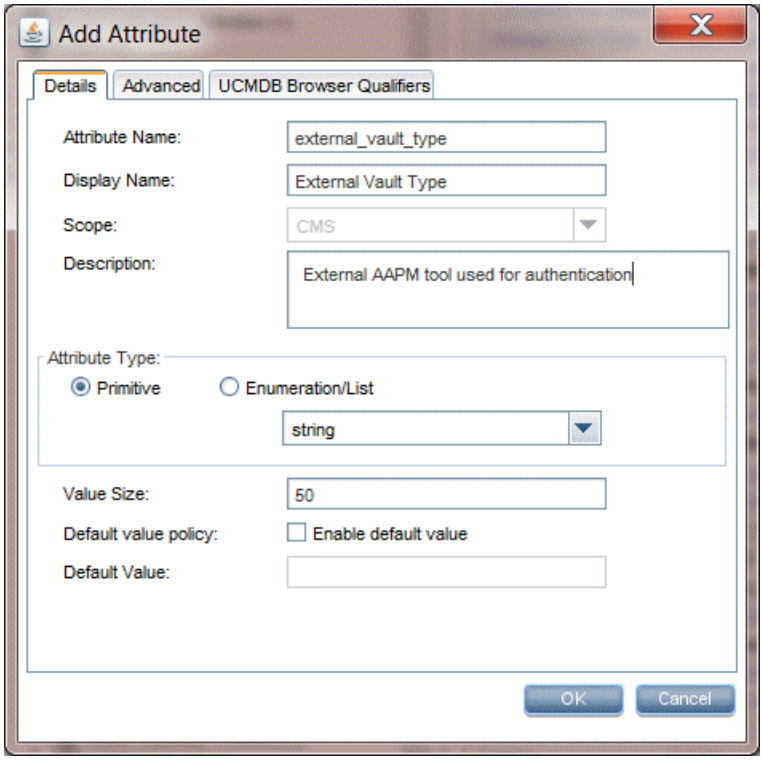
i. Locate the **protocol** CI type class. Go to **Modeling > CI Type Manager**, in the CI Types pane, expand **Root > Data > Object > Configuration > protocol**.

ii. On the **Attributes** tab, click **Add** to add two attributes as follows:

	Attribute 1	**Attribute 2**
Attribute Name	external_vault_type	external_password_static_key
Display Name	External Vault Type	External Password Static Key
Description	external AAPM tool used for authentication	reference ID/string used in AAPM
Attribute Type	string	string
Value Size	50	1024

For all other fields, keep default values.

For example,



iii. Click **OK**.

6. **(SSH and Telnet protocols only) Add SU parameters manually to update class model**

   a. Locate the **SSH** or **Telnet** CI type. Go to **Modeling > CI Type Manager**, in the CI Types pane, expand **Root > Data > Object > Configuration > protocol > SSH/Telnet**.

   b. On the **Attributes** tab, click **Add** to add two super user attributes to the SSH/Telnet protocol as follows:

	Attribute 1	**Attribute 2**
Attribute Name	su_external_vault_type	su_external_password_static_key
Display Name	External Vault Type for SU	External Password Static Key for SU
Description	External AAPM tool used for authentication for SU	Reference ID/string used in AAPM for SU
Attribute Type	string	string
Value Size	50	1024

   c. Click **OK**.

7. **Enable CyberArk integration on UCMDB server**

   You can enable CyberArk integration using either of the following:

   - Change the **Enable CyberArk integration** infrastructure setting value from **false** to **true**.

     i. In UCDMB, go to **Administration > Infrastructure Setting Manager**.

     ii. Locate the **Enable CyberArk integration** infrastructure setting and change its value from **false** to **true**.

     The default value for the setting is false.

     iii. Click **Save**.

     The setting is synchronized to all probes.

   - Enable CyberArk integration from JMX console.

i. On the UCMDB Server, go to **JMX console > UCMDB:service=Settings Services**.

ii. Locate and invoke the **setGlobalSettingValue** JMX method with the following parameters:

- **name**: cyberark.integration.enabled
- **value**: true

8. **Set CyberArk Reference String in the protocol credential UI for supported protocols**

To do so,

a. In UCMDB UI, go to **Data Flow Management > Data Flow Probe Setup**.

b. In the Domains and Probes tree, expand **DefaultDomain(Default) > Credentials**, select a supported protocol.

In this example, select **AS400 Protocol**.

c. In the AS400 Protocol pane, click  .

d. In the AS400 Protocol Parameters dialog, provide values as necessary.

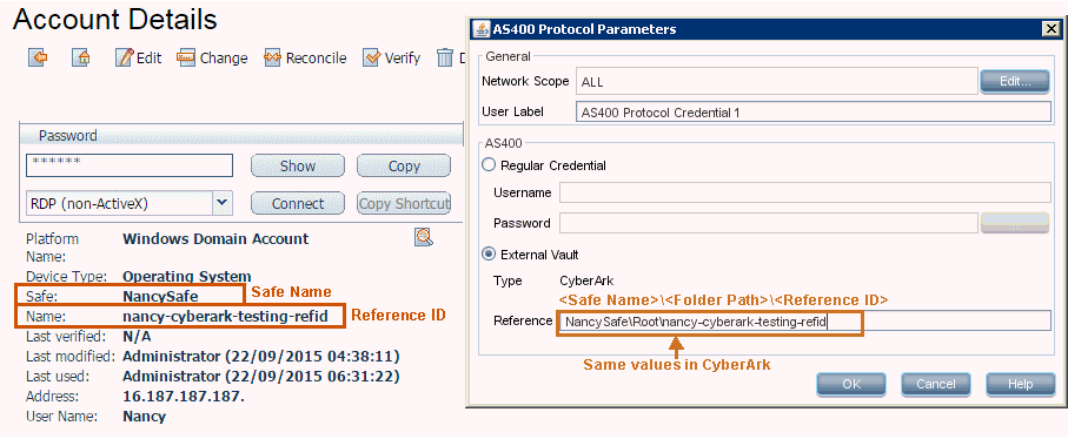
When CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled in the Protocol Parameters dialog. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and two new parameters (**Type** and **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 for the protocol in the *HP UCMDB Universal Discovery Content Guide - Supported Content*. • **Password.** See description for the protocol in the *HP UCMDB Universal Discovery Content Guide - Supported Content*.

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>\<ReferenceID>**. Where **<Safe_Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<ReferenceID>** is the name of the CyberArk account you specified or auto-generated in CyberArk. For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

In this case, select **External Vault** and set the **Reference** value as described in the table above.

The following screenshots illustrate the exact CyberArk values you should use in setting the reference string:



e. Click **OK**.

9. Check credential

To do so,

a. In UCMDB UI, go to **Data Flow Management > Data Flow Probe Setup**.

b. In the Domains and Probes tree, expand **DefaultDomain(Default) > Credentials**, select a

supported protocol.

In this example, select **AS400 Protocol**.

c. Right-click an AS400 protocol in the protocols list, and select **Check credential** from the context menu.

d. In the Check Credential dialog, provide the values as described below:

- **IP/Hostname**: Enter the IP address or hostname of the Probe server.
- **Timeout**: Keep the default value.
- **Data Flow Probe**: Select **DataFlowProbe**.

e. Click **OK**.

A "`Connection successful`" message is returned.

If CyberArk integration is not enabled, this action returns the following warning message: `CyberArk is disabled`.

How to Create and Configure CyberArk Account for the Integration

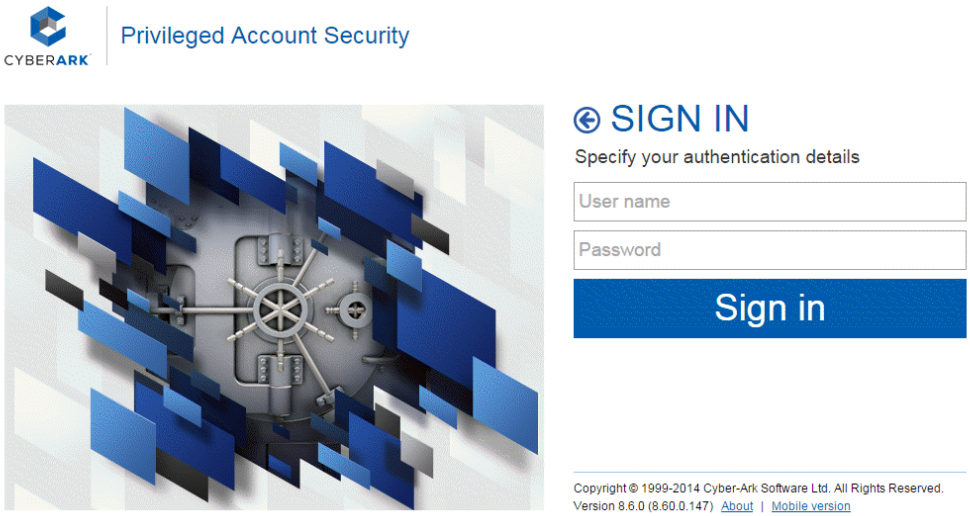
To successfully integrate UCMDB/UD with CyberArk, follow the instructions below strictly to create and configure a safe, an account, and an application ID in CyberArk for the integration.

1. **Sign in to CyberArk Password Vault**

   a. In your Web browser, enter **http://<IP address of CyberArk Password Vault Web Access machine>/PasswordVault**.

   b. Select **CyberArk** 

as the authentication method.



   c. Provide your user name and password, and click **Sign in**.

2. **Create and configure a Safe**

   To do so,

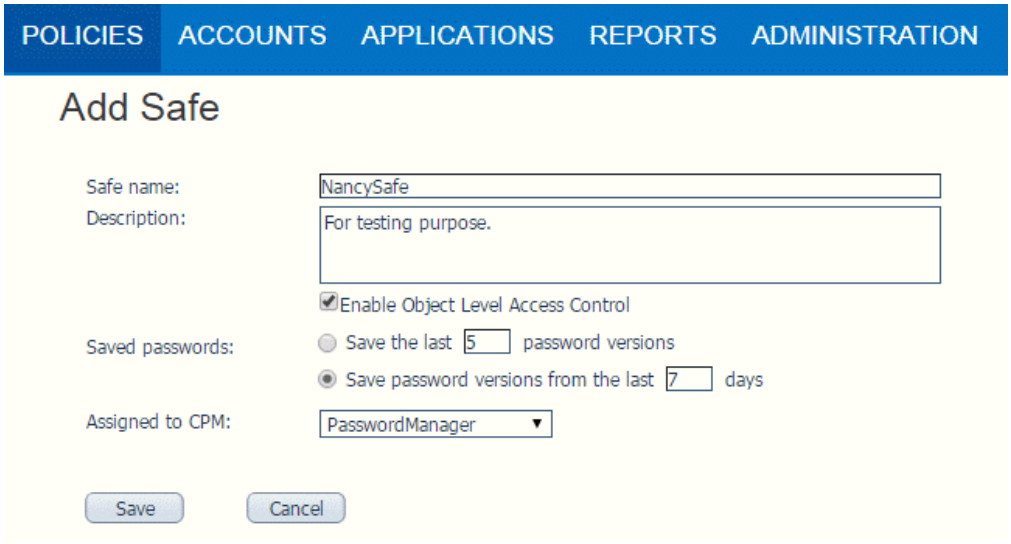
   a. Go to the **POLICIES** tab and create a safe.

      i. On the **POLICIES** tab, from the navigation pane select **Access Control (Safes)**, and then click **Add Safe** 

.

ii. On the Add Safe page, provide values as described below:

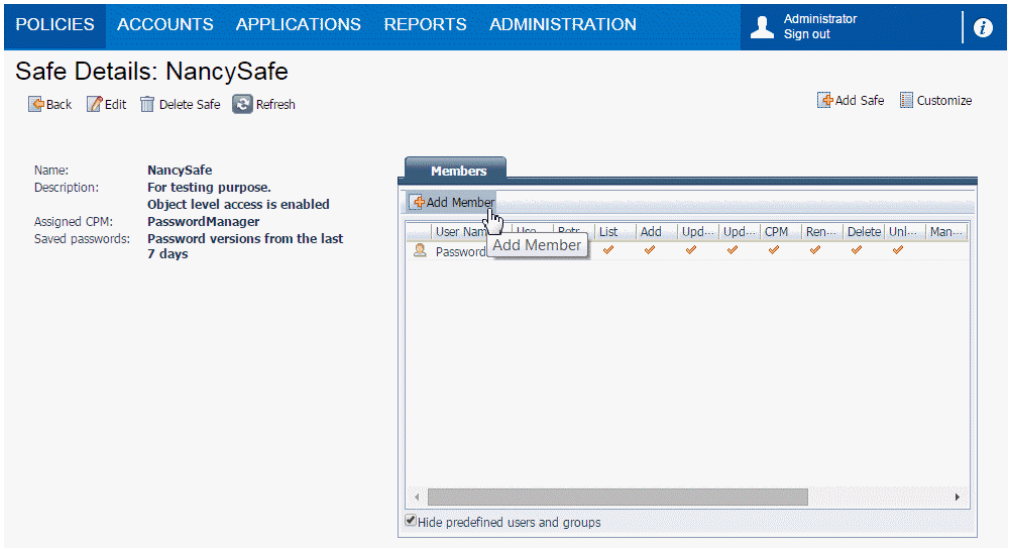
- **Safe name**: Provide a Safe name. For example, **NancySafe**.
- **Description**: Provide a description for the Safe name, and select the **Enable Object Level Access Control** check box.
- **Saved Passwords**: Keep the default **Save password versions from the last [7] days** option selected.
- **Assigned to CPM**: Keep the default **PasswordManager** option selected.



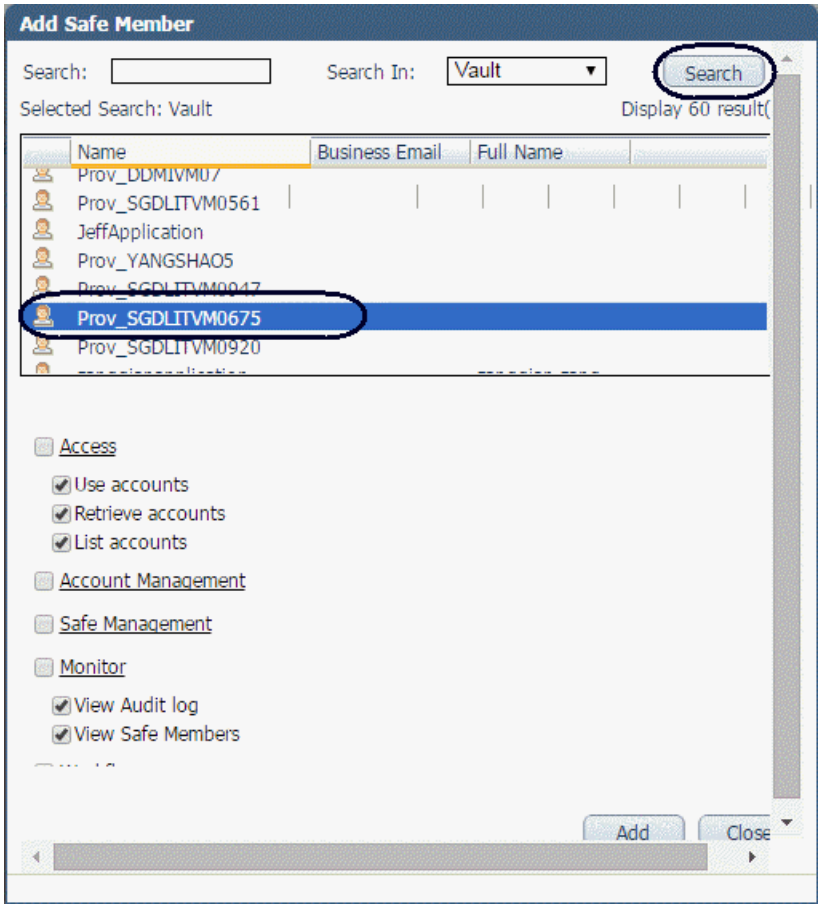
iii. Click **Save**

b. Add the new Safe to the Safe Members list.

i. On the Safe Details: <Safe Name> page, click **Add Member**.



ii. In the **Add Safe Member** dialog, click **Search**, and then from the returned list select a desired PIM provider machine.



iii. Click **Add**.

iv. Click **Close**.

The PIM provider machine you just added should now display in the Members list.

3. **Create and configure an account**

a. Go to the **ACCOUNTS** tab, click **Add Account** 

.

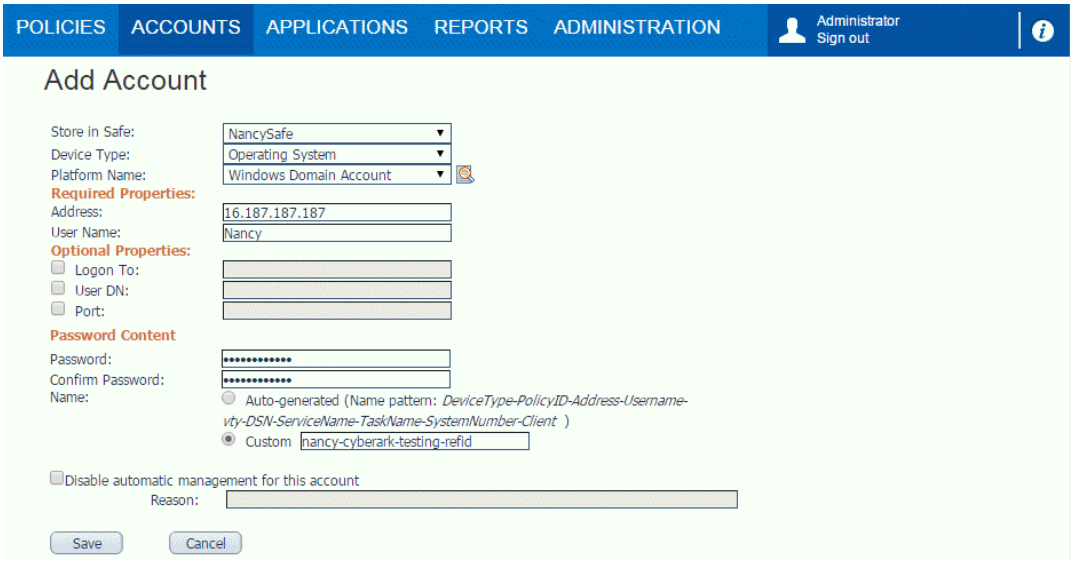
b. On the Add Account page, provide values as described below:

- **Store in Safe**: Select the Safe name you just created in step 2.
- **Device Type**: Select **Operating System** from the drop-down list.
- **Platform Name**: Select **Windows Domain Account**.

- **Address**: Enter the IP address of the CyberArk server.
- **User Name**: Specify your CyberArk account user name.
- **Password**: Enter the password for your CyberArk account.
- **Confirm Password**: Enter your password again.
- **Name**: Select an **Auto-generated** or **Custom** name for your Safe account.

  If you select **Custom**, provide a custom CyberArk account name. For example, **nancy-cyberark-testing-refid**.

For example,



c. Click **Save**.

4. **Create and configure an application ID**

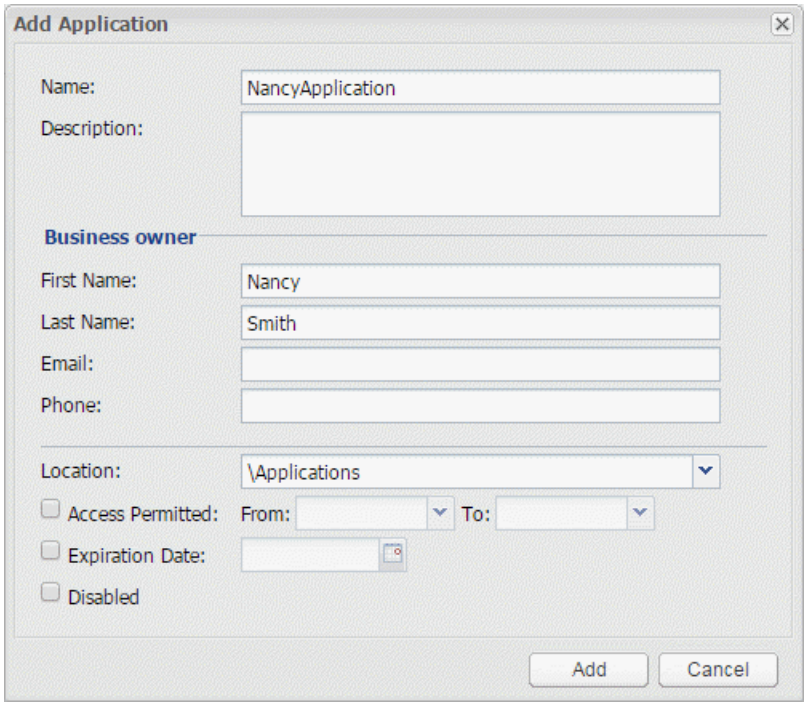
a. Go to the **APPLICATIONS** tab and create an application ID.

i. On the **APPLICATIONS** tab, click Add Application.

ii. In the Add Application dialog, provide values as described below:

- **Name**: Provide a name for your application ID. For example, **NancyApplication**.
- **Description**: Provide a description for your application ID.

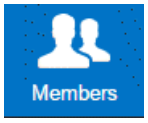
- **Location**: Select **\Applications**.
- Other fields: Provide values as necessary.



iii. Click **Add**.

b. Add the new application ID to the Safe members list.

i. Go to the **POLICIES** tab, from the navigation pane select **Access Control (Safes)**, and then select **NancySafe** from the Safe Name list.

ii. Click **Members** 

in the lower right corner of the page.

iii. On the **Safe Details: NancySafe** page, click **Add Member**.

iv. In the **Add Safe Member** dialog, locate the application you just added. In this example, select **NancyApplication**.

v. Click **Add**.

c. Add the full name of the PIM provider to the **Allowed Machines** list.

   i. Go to the **APPLICATIONS** tab, locate the new application ID. In this example, **NancyApplication**.

   ii. On the **Application Details: NancyApplication** page, go to the **Allowed Machines** tab.

   iii. Click **Add Machine** 

.

   iv. In the **Add allowed machine** dialog, enter IP, host name, or DNS.

   v. Click **Add**.

d. Add path authentication for the new application ID.

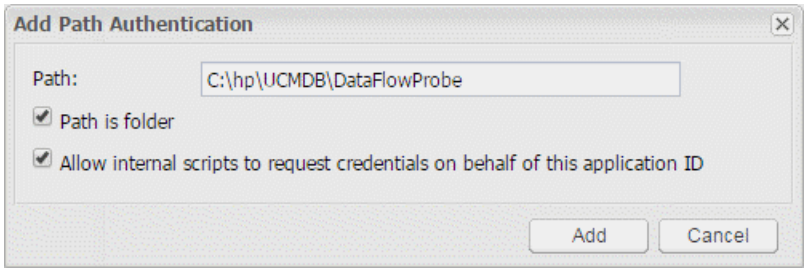
   i. Go to the **Authentication** tab, click **Add authentication details** 

, and then select **Path**.

   ii. In the **Add Path Authentication** dialog,

   - In the **Path** field, enter the path, for example, **C:\hp\UCMDB\DataFlowProbe**.
   - Make sure you select the check box for both of the following options:
     - **Path is folder**
     - **Allow internal scripts to request credential on behalf of this application ID.**

   For example,



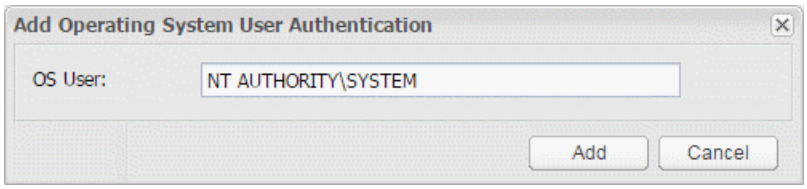
   iii. Click **Add**.

e. Add operating system user authentication for the new application ID.

i. On the **Authentication** tab, click **Add authentication details** 

, and then select **OS user**.

ii. In the **Add Operating System User Authentication** dialog, provide OS user information, for example, **NT AUTHORITY\SYSTEM**.



Note:

- If the Probe is running as a service, specify **NT AUTHORITY\SYSTEM** as OS user.
- If the Probe is running as console, specify **<hostname\username>** as OS User. For example, **HPSWVM0999\Administrator**.

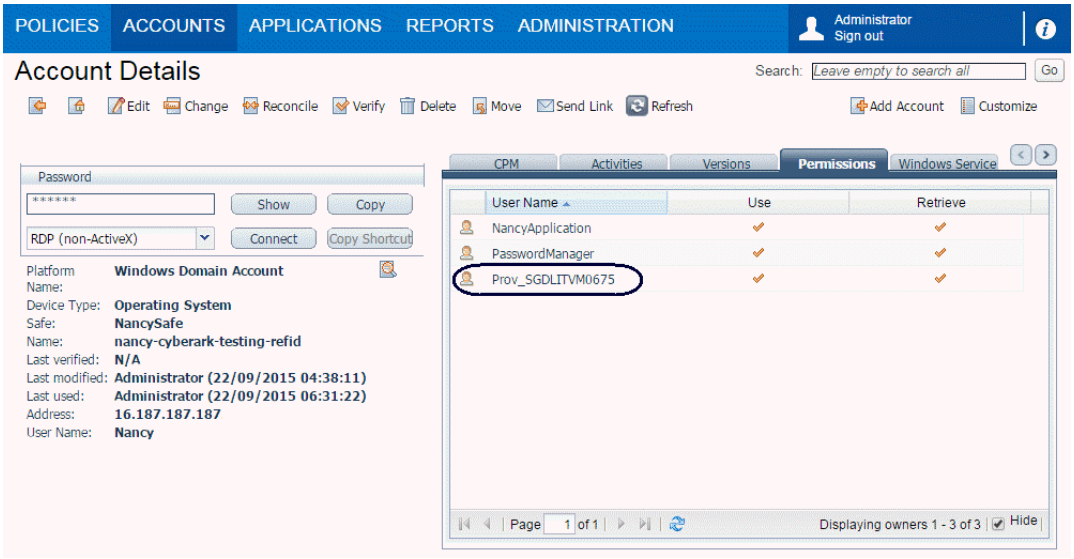
iii. Click **Add**.

5. ## Check account details

a. Go to the **ACCOUNTS** tab and locate the account you created and configured. In this example, **NancySafe**.

b. On the **Account Details: NancySafe** page, go to the **Permissions** tab.

The name of the PIM Provider that we installed on the Probe server should be displayed.


POLICIES
ACCOUNTS
APPLICATIONS
REPORTS
ADMINISTRATION
Administrator
Sign out
Account Details
Search:
Leave empty to search all
Go
Edit
Change
Reconcile
Verify
Delete
Move
Send Link
Refresh
Add Account
Customize
Password
Show
Copy
RDP (non-ActiveX)
Connect
Copy Shortcut
Platform Name: Windows Domain Account
Device Type: Operating System
Safe: NancySafe
Name: nancy-cyberark-testing-refid
Last verified: N/A
Last modified: Administrator (22/09/2015 04:38:11)
Last used: Administrator (22/09/2015 06:31:22)
Address: 16.187.187.187
User Name: Nancy
CPM
Activities
Versions
Permissions
Windows Service
User Name
Use
Retrieve
NancyApplication
PasswordManager
Prov_SGDLITVM0675
Page 1 of 1
Displaying owners 1 - 3 of 3
Hide

How to Add CyberArk Credential for Protocols from JMX

For the protocols that do not have the CyberArk related fields available after you enable CyberArk integration from the UCMDB Server, you can add CyberArk credential for these protocols with the help of JMX methods.

To do so,

1. **Export the existing credential**
   a. On the UCMDB Server, launch the Web browser and enter the following address: **http://localhost:8080/jmx-console**. You may have to log in with a user name and password.
   b. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
   c. Locate the **exportCredentialsAndRangesInformation** operation. Do the following:
      - Enter your customer ID (the default is 1).
      - Enter a name for the exported file.
      - Leave the password field empty.
      - Set **isEncrypted=False** since we want to edit the exported file and import it back later.
      - Set **includeProbeRange=True**
   d. Click **Invoke** to export.

      When the export process completes successfully, the file is saved to the following location: **C:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.

2. **Add CyberArk credential to the exported file**
   a. Navigate to the **C:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>** directory.
   b. Open the exported file using a text editor.
   c. At the end of the file, before the last `</object>` tag, manually add the following:

```
<attribute name="external_vault_type"
type="string">CyberArk</attribute><attribute name="external_password_
```

```
static_key" type="string">HPSupportSafe\Root\support-cyberrk-
refid</attribute></object>
```

d. Save the file.

3. **Import the updated credential file back to UCMDB**

a. Go to the JMX Console.

b. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.

c. Locate the **importCredentialsAndRangesInformation** operation. Do the following:

- Enter your customer ID (the default is 1).
- Enter a name for the exported file.
- Leave the password field empty.
- Set **isEncrypted=False** since we want to edit the exported file and import it back later.
- Set **includeProbeRange=True**.
- Set **notAllowOverlap=False**.

d. Click **Invoke** to import.

CyberArk Integration Troubleshooting and Limitations

- **Symptom:** Received an error message "`User <ApplicationID> is not defined`" when running the **checkCyberArkConn.bat** script to test connection.

  Possible Cause: The application ID is not added to the Safe in CyberArk.

  Solution: Add the applicaition ID to the Safe in CyberArk. For detailed instructions, see Create and configure an application ID.

- **Symptom:** From the UCMDB UI, failed to save the CyberArk credential to UCMDB Server.

  Possible Cause: Class model not updated.

  Solution: Update the class model. For detailed instructions, see Update class model manually.

- **Symptom:** Checking credential failed with an error message similar to the following:

  `Failed to get credential XYZ, please check the related error logs in probe side.`

  Scenarios:

  - Found the following error messages in the **WrapperProbeGw.log**:

    - `... Failed to get credential for id 52_1_CMS - Failed quering CyberArk Password, Application ID is empty.`
    - `...Failed to get credential for id 2_1_CMS - Failed quering attribute from CyberArk Password.`

    Possible Cause: Application ID or Classpath is not properly set.

    Solution: Set application ID and classpath properly. For detailed instructions, see Set ApplicationID and Classpath parameters manually.

  - Found the following error message in the **WrapperProbeGw.log**: `Query string not legal. Should be "safe\folder\name".`

    Possible Cause: The format of the Reference ID is not correct.

    Solution: Update the reference ID by strictly following the reference ID format:

    <Safe_Name>\<Folder Path>\<ReferenceID>

Where **<Safe_Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<ReferenceID>** is the name of the CyberArk account you specified or auto-generated in CyberArk.

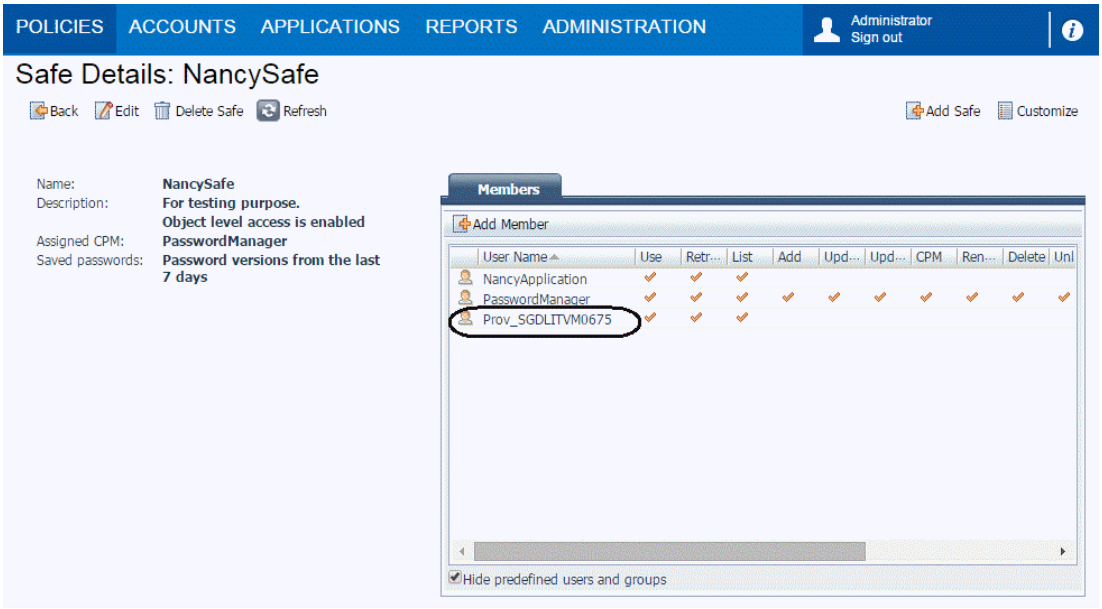
For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

- Found the following error message in the **WrapperProbeGw.log**:

  ```
  Password object matching query [object=ABC;Folder=Root;Safe=XYZ] was not found (Diagnotic Info: 9). Please check that there is a password object that answers your query in the vault and that both the provider and the application user have the appropriate permissions needed in order to use the password.
  ```

  Possible Cause: The CyberArk PIM Provider was not added as a member to the Safe.

  Solution: Add the CyberArk PIM Provider as a member to the Safe in CyberArk, as follows:



  For detailed instructions, see "How to Create and Configure CyberArk Account for the Integration" on page 36.

- Found the following error message in the **WrapperProbeGw.log**: `Error: CASVL012E User Name [ApplicationID] is invalid.`

  Possible Cause: This is related to the authentication. The OS user was not properly set when creating the Application ID in CyberArk.

Solution: If the Probe is running as a service, add **NT AUTHORITY\SYSTEM** as OS user.

If the Probe is running as console, add the **<hostname\username>** as OS User.

- **PROBLEM:** After enabling CyberArk integration, there are no CyberArk related fields in the Protocol Parameters dialog for some protocols. Is it possible to add CyberArk credential reference to those protocols?

  Solution: Yes. Apart from UDDI Registry and Universal Discovery protocols (which have no passwords at all), we can add CyberArk credential reference to these protocols with the help of JMX methods. For a list of protocols that are supported from JMX, see "Supported Protocols" on page 25. For detailed instructions, see "How to Add CyberArk Credential for Protocols from JMX" on page 45.

- **Limitation:** Probe will not be able to retrieve passwords from CyberArk if it is running on the local system account and that this account is not added as a member to the CyberArk Safe.

Sample Script for IP Range Management API

```
package com.hp.ucmdb.api.client.util;

import com.hp.ucmdb.api.UcmdbService;
import com.hp.ucmdb.api.UcmdbServiceFactory;
import com.hp.ucmdb.api.UcmdbServiceProvider;
import com.hp.ucmdb.api.client.types.IPRangeImpl;
import com.hp.ucmdb.api.client.types.IPRangeWithExcludingImpl;
import com.hp.ucmdb.api.discovery.types.IPRange;

import java.lang.reflect.Method;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.List;

/**
 * Created by dingmen on 8/12/2015.
 */
public class UpdateIpRangeTest {

    private static final String HOST_NAME = "16.187.189.134";
    private static final int HTTP_PORT = 8080;
    private static final String HTTPS = "https";
    private static final String HTTP = "http";
    private static UcmdbService ucmdbService;

    public static void main(String[] args) {
        testSenario1();
```

```
    }

    private static  void  testSenario1(){
        try {
            UcmdbServiceProvider provider = UcmdbServiceFactory.getServiceProvider
(HTTP, HOST_NAME, HTTP_PORT);
            ucmdbService = provider.connect(provider.createCredentials("admin",
"admin"), provider.createClientContext("Test"));
            HashMap<String, ArrayList<String>> probeLBGroup = new HashMap<String,
ArrayList<String>>();
            HashMap<String, ArrayList<IPRange>> IPRangeGroup = new HashMap<String,
ArrayList<IPRange>>();
            HashMap<String, ArrayList<String>> domainGroup = new HashMap<String,
ArrayList<String>>();

            //put domain name as key in domainGroup,  and its value is a list of
groups.  'DefaultDomain' is a existing name in UCMDB .
            domainGroup.put("DefaultDomain", new ArrayList<String>());
            domainGroup.get("DefaultDomain").add("PG1");

            //define 'PG1' as the first group name(The group name can be any other
values) in probeLBGroup ,
            //and its value is a list of probe name. 'Probe1' or 'Probe2' should be
existing name in UCMDB .
            probeLBGroup.put("PG1", new ArrayList<String>());
            probeLBGroup.get("PG1").add("Probe1");
            probeLBGroup.get("PG1").add("Probe2");

            //Below all ranges are defined in IPRangeGroup for 'PG1' , and they
will balanced distributed to probes in 'PG1'.
            IPRangeGroup.put("PG1", new ArrayList<IPRange>());
            //should specify ip type 'IPV4/IPV6' , and ip category
'DataCenter/Client' for each range.
            IPRangeGroup.get("PG1").add(new IPRangeWithExcludingImpl("1.1.1.1",
"1.1.1.9", IPRange.IPType.IPV4, IPRange.RangeCategory.CLIENT, new
ArrayList<IPRangeImpl>()));
            List<IPRangeImpl> excludedRange1=new ArrayList<IPRangeImpl>();
            IPRangeGroup.get("PG1").add(new IPRangeWithExcludingImpl("1.1.1.10",
"1.1.1.19", IPRange.IPType.IPV4,IPRange.RangeCategory.DATA_CENTER,
excludedRange1));
            excludedRange1.add(new IPRangeImpl
("1.1.1.10","1.1.1.19",IPRange.IPType.IPV4,IPRange.RangeCategory.DATA_CENTER));
            excludedRange1.add(new IPRangeImpl
("1.1.1.12","1.1.1.15",IPRange.IPType.IPV4,IPRange.RangeCategory.DATA_CENTER));
            IPRangeGroup.get("PG1").add(new IPRangeWithExcludingImpl
("fe80:0:0:0:41f8:4318:2000:80", "fe80:0:0:0:41f8:4318:2000:83",
IPRange.IPType.IPV6,IPRange.RangeCategory.CLIENT, new ArrayList<IPRangeImpl>()));

            //below is the second group 'PG2', and assign below 'GP2' range
```

```
(1.1.1.20~1.1.1.30)  to below 'PG2' probe(Probe3) .
            domainGroup.get("DefaultDomain").add("PG2");
            probeLBGroup.put("PG2", new ArrayList<String>());
            probeLBGroup.get("PG2").add("Probe3");
            IPRangeGroup.put("PG2", new ArrayList<IPRange>());
            IPRangeGroup.get("PG2").add(new IPRangeWithExcludingImpl("1.1.1.20",
"1.1.1.30", IPRange.IPType.IPV4,IPRange.RangeCategory.DATA_CENTER, new
ArrayList<IPRangeImpl>()));

            //the domain group with probe and range group in set to importIPRanges
API to update ip ranges.
            ucmdbService.getDDMConfigurationService().importIPRanges(probeLBGroup,
IPRangeGroup, domainGroup);
        } catch (Throwable e) {
            e.printStackTrace();
        }
    }

}
```

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 Release Notes (Universal CMDB & Configuration Manager 10.21 CUP1)

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@hp.com.

We appreciate your feedback!