Hewlett Packard
Enterprise

HPE Application Performance Management

Software Version: 9.30

Data Flow Probe Installation Guide

Document Release Date: July 2016
Software Release Date: July 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE 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 HPE 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.

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 is a registered trademark of Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

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.hpe.com/group/softwaresupport/search-result?keyword=.

This site requires an HPE Passport account. If you do not have one, click the **Create an account** button on the HPE Passport Sign in page.

PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Support

Visit the HPE Software Support website at: **https://softwaresupport.hpe.com**

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software 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 HPE 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 HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

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

HPE Software Integrations, Solutions and Best Practices

Access the Hewlett Packard Enterprise Software Support site (**https://softwaresupport.hpe.com/manuals**) to search for a wide variety of best practice documents and materials.

Contents

Chapter 1: Licensing Model for Run-time Service Model

This chapter includes:

Licensing Model Overview

HP Universal CMDB's licensing model is based on three complementary types of license, or licensing levels. The first one, known as the UCMDB Foundation License, is granted free of charge to eligible customers. The other two levels (the UCMDB Integration Only License and the DDM Advanced Edition License) are fee-based.

This section includes the following topics:

- "Licensing Levels" below
- "Units of Measure" on the next page

Licensing Levels

- **UCMDB Foundation License.** This license grants the rights to use UCMDB as the backbone component of select BTO products.
- **UCMDB Integration Only License.** This license grants the right to integrate third-party (non-HPE) products with UCMDB using various types of integrations.
- **DDM Advanced Edition License.** This license grants the rights to:
  - Integrate BTO and third-party (non-HPE) products with UCMDB, using any type of integration
  - Use all Discovery and Dependency Mapping (DDM) capabilities to populate UCMDB

The following table provides an overview of what is permitted with the various licenses:

License/Integration	Integrations with other BTO products	Integrations with third-party products	Custom Discovery-like integrations	All Discovery capabilities
UCMDB Foundation	Permitted	No	No	No
UCMDB Integration Only	Permitted	Permitted	No	No
DDM Advanced Edition	Permitted	Permitted	Permitted	Permitted

Units of Measure

- **OS Instance.** Each implementation of the bootable program that can be installed onto a physical system or a partition within the physical system. A physical system can contain multiple Operating System instances.
- **Managed Server.** A computer system or computer system partition where a bootable program is installed, but not including personal computers or computers primarily serving a single individual.

  Note: Printers and network devices are not counted as Managed Servers.

UCMDB Foundation License

This is a no charge entitlement license for the UCMDB product, which is automatically granted to any HPE customer who purchases Discovery and Dependency Mapping (DDMA), Service Manager (SM), or Asset Manager (AM).

License	Description
Standard BTO Integrations	With this license, you are entitled to integrate the following HPE BTO products with UCMDB: • Application Performance Management • Universal CMDB • Asset Manager • Service Manager • DDM Inventory • Storage Essentials • Systems Insight Manager • Operations Orchestration • Server Automation Data flows between these products are implemented by means of adapters provided out-of-the-box with HP Universal CMDB or bundled under the SACM solution. Most adapters can leverage the Data Flow Probe infrastructure of HP Universal CMDB - except those supporting a federation data flow or the push data flow from UCMDB to SM, due to a technical restriction. **Note:** The data flow from UCMDB to Asset Manager relies on a Connect-It connector, which is licensed free of charge to AM customers. The right granted by the UCMDB Foundation license to integrate BTO products with UCMDB does not remove the need for customers to properly license these products in the first place.
Other Integrations	With this license, you are also entitled to integrate BTO products with UCMDB using: • Standard integrations provided by HPE partners (additional charges may apply) • Custom data exchange integrations (that is, the Generic DB Adapter, the Generic Push Adapter and customer-developed Java adapters) • The HP Universal CMDB Web Service API and the HP Universal CMDB API (Java)
Number of CIs and Relationships	The UCMDB Foundation License does not restrict the number of CIs and relationships that can be stored in UCMDB or exchanged between UCMDB and other BTO products. The only limitation is physical capacity and performance.

License	Description
Number of UCMDB Instances	The UCMDB Foundation License does not restrict the number of UCMDB instances that can be deployed in a customer environment for the purpose of implementing development, test, production, HA and/or DR platforms. However, technical limitations may apply regarding how data can be managed and exchanged in a multi-instance installation. Servers that are discovered with DDM or sourced from a third-party product only need to be counted once under the DDM Advanced Edition license or the UCMDB Integration Only license, even if they appear in several UCMDB instances for the purpose of operational management.
Number of Data Flow Probe instances	The UCMDB Foundation License does not restrict the number of Data Flow Probe instances that can be deployed in a customer environment for the purpose of hosting discovery or integration adapters. However, technical limitations may apply regarding the maximum number of probes that can be used with UCMDB. Also, as mentioned above, some adapters cannot be hosted by a probe.
Particular Case of BSM	Customers who purchase HPE Application Performance Manager (APM) version 9.30 or later are automatically granted a no-charge license to use the embedded UCMDB component labeled as Run-time Service Model (RTSM) and to integrate BTO products with RTSM. As a result, APM customers do not have and do not need a UCMDB Foundation license. **Note:** APM was formerly known as HPE Business Availability Center version 8.0x (BAC) and RTSM as the Operational Database (ODB).

UCMDB Integration Only License

This license is based on the Managed Server unit of measure (for details, see "Units of Measure" on page 8). An appropriate quantity of that license must be acquired by customers who need to integrate third-party products with UCMDB.

License	Description
Licensing Rule	One License To Use (LTU) must be purchased for each Managed Server that is defined in a third-party product and whose definition then gets copied to UCMDB to be recorded in the form of CIs. The UCMDB Integration Only license requires an initial minimum purchase of 100 LTUs.

License	Description
Valid Types of Integrations	With this license, you can integrate third-party products with UCMDB using: • Standard integrations provided by HPE • Standard integrations provided by HPE partners (additional charges may apply) • Custom data exchange integrations (that is, the Generic DB Adapter, the Generic Push Adapter and customer-developed Java adapters) • The HP Universal CMDB Web Service API and the HP Universal CMDB API (Java) • But not Discovery-like integrations (that is, those created using Jython adapters) **Note:** HP Universal CMDB provides out-of-the-box adapters for third-party products such as Microsoft SCCM and BMC Atrium CMDB.

DDM Advanced Edition License

This license is based on the OS Instance unit of measure (for details, see "Units of Measure" on page 8). An appropriate quantity of that license must be acquired by customers who need access to all the Discovery and Dependency Mapping capabilities of DDM.

License	Description
Licensing Rule	One License To Use (LTU) must be purchased for each OS Instance that is discovered by DDM and gets recorded in UCMDB in the form of CIs. The DDM Advanced Edition license requires an initial minimum purchase of 100 LTUs. For example: A VMware ESX Server hosting one virtual machine requires two licenses to use (LTUs). Servers that are both discovered by DDM and sourced from a third-party product (to collect additional data) do not need to be counted under the UCMDB Integration Only license. The DDM Advanced Edition license covers that usage scenario.
Discovery and Dependency Mapping	With this license, you can use the Discovery Control Panel and other related functions to take advantage of all the discovery content available out of the box. In addition, you can create new Jython adapters to discover other resources.
Integrations	With this license, you can use the Integration Studio to create integration points with BTO and third-party products using Discovery-like integrations (custom Jython adapters).

License	Description
DDM Inventory No Charge Entitlement with DDM Advanced Edition	For each LTU purchased under the DDM Advanced Edition license for a given server, you are granted a free DDM Inventory license to collect inventory data on the same server.

Upgrade to the Integration Only or DDM Advanced Edition License

When you install Application Performance Management, you receive the Universal CMDB Foundation license. To obtain the file needed to upgrade to the Integration Only or DDM Advanced Edition license, contact HPE Software Support, then perform the following procedure:

To upgrade your license:

1. Obtain the appropriate file from HPE Software Support.
2. Replace the **ucmdb_license.xml** file in the **<Application Performance Management root directory>\odb\conf** folder on the Data Processing server machine.

   If Application Performance Management is installed in a distributed deployment, replace the file on the Gateway Server machine.
3. Use the JMX console to force a license change:
   a. Launch the Web browser and enter the server address, as follows: **http://<APM Server Host Name or IP>:21212/jmx-console**.
   b. When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator). The default user name and password are **admin**/**admin**.
   c. Under **UCMDB**, click **service=Server Services** to open the Operations page.
   d. Locate **getLicense** and enter the following information:

      In the Value box for the **customerID** parameter, enter 1.
   e. Click **Invoke**.

   Information about the license type, customer name, permitted packages, and whether any applications are blocked is displayed.

Chapter 2: Data Flow Probe Installation and Configuration

This chapter includes:

Before You Install the Data Flow Probe

Consider the following before installing the Data Flow Probe:

- To install the Probe, use the Probe installation file associated with the version of APM you are using. The Probe installation version should exactly match the RTSM version released with APM. Otherwise, the Probe will fail.

  For major/minor releases (for example, 9.00 or 9.20), this file is available on the DVD that comes with the APM media kit, or you can download it from the Software Updates page.

  For minor-minor patch releases (for example, 9.13 or 9.21), you download this file from the Software Patches page.

  Both files can be accessed from the HPE Software Support web site (https://softwaresupport.hpe.com).
- Review the Data Flow Probe system requirements in the version of the APM System Requirements and Support Matrixes Guide associated with the Probe you are installing.
- Review the APM Release Notes for any notes and limitations associated with the Probe.
- The Probe can be installed before or after you install the Application Performance Management Gateway server. However, during Probe installation, you must provide the name or IP of the APM Gateway Server, so it is preferable to install the APM Gateway Server before installing the Probe.
- Verify that you have enough hard disk space available before beginning installation. For details, see the section about Data Flow Probe requirements in the version of the APM System Requirements and Support Matrixes Guide associated with the Probe you are installing.
- It is recommended that you should install the Probe on a separate server from the APM servers, to

distribute the overall system load.

- **Data Flow Probe on Windows:**
  - Before installing the Probe on a Windows 2008 machine, a user must have full control permissions on the file system. In addition, after installing the Probe, verify that the user who will run the Probe has full administration permissions on the file system where the Probe is installed.
- **Data Flow Probe on Linux:**
  - This Probe on Linux is intended for integration use only, and cannot be used for discovery. That is, this Probe does not appear in the Data Flow Setup window.
  - Only integration with APM version 9.01 and later is supported on the Probe on Linux.
  - An instance of Microsoft MySQL database must not be running on the machine on which you are installing the Data Flow Probe. If an instance exists, you must disable it.
  - To install the Data Flow Probe on Linux, you must have root permissions to the Linux machine.

Installing the Data Flow Probe on Windows

The following procedure explains how to install the Data Flow Probe on a Windows platform.

Note: For important notes and considerations before you install the Data Flow Probe, see "Before You Install the Data Flow Probe" on the previous page.

To install the Data Flow Probe:

1. Download the Data Flow Probe for your APM version.
   a. Go to the HPE Software Support web site (https://softwaresupport.hpe.com) and sign in.
   b. Click **Search**.
   c. Select **Application Performance Management (BAC) > 9.2x**.
   d. Under Document Type, select **Patches**.
   e. Search for and select **APM - Data Flow Probe**.
2. Run the data flow probe installation file released with the version of APM you are installing (for example, for APM 9.30 run **HPBSM9.30_DataFlowProbe _10.22CUP2.exe**) and follow the instructions in the wizard.
3. The Introduction page opens. Click **Next**.
4. The License Agreement page opens. Accept the terms of the end-user license agreement and click **Next**.
5. The Setup Type page opens. Select **Full Data Flow Probe** installation. This installs the Data Flow Probe with all its components, including the Inventory Tools (Analysis Workbench, Viewer, SAI Editor,

and MSI Scanner) required for application teaching.

Note: The Inventory Tools option is used to install only the Inventory Tools. For details about application teaching, see the HP Universal CMDB Data Flow Management Guide.

Click **Next**.

6. The Select Installation Folder page opens. Accept the default installation folder, **C:\hp\UCMDB\DataFlowProbe**, or click **Choose** to select a different installation folder.

   Note: The installation folder that you select must be empty.

   To restore the default installation folder, after selecting a different folder, click **Restore Default Folder**.

7. The Data Flow Probe Configuration page opens, enabling you to configure the details of the application server to which the Data Flow Probe will report.

   a. Under Application to report to select **HP BSM** and in the Application Server address box, enter the name or the IP address of the HP Universal CMDB server with which the Probe is to connect.

      Note: In a High Availability environment, use the Writer virtual IP address of the load balancer.

   b. In the Data Flow Probe address box, enter the IP address or DNS name of the machine on which you are currently installing the Probe, or accept the default.

      Note: If the Data Flow Probe machine has more than one IP address, enter a specific IP address, and not the DNS name.

   c. Click Next.

   Note: If you do not enter the address of the application server, or if there is no TCP connection to the application server via default ports (8080,8443,80) (possibly because the application server has not fully started yet), a message is displayed. You can choose to continue to install the Probe without entering the address, or return to the previous page to add the address.

8. A second Data Flow Probe Configuration page opens, enabling you to configure an identifier for the Probe.

   a. In the Data Flow Probe Identifier box, enter a name for the Probe that is used to identify it in your environment.

      Note: The Probe identifier is case sensitive, must be unique for each Probe in your deployment, and it must not exceed 50 characters.

      When installing the Probe in separate mode, that is, the Probe Gateway and Probe Manager are installed on separate machines, you must give the same name to the Probe Gateway and all its

Probe Managers. This name appears in UCMDB as a single Probe node. Failure to give the same name may prevent jobs from running.

To use the default UCMDB IP address or machine name, as defined in the UCMDB Server installation, select Use Default CMDB Domain.

The Default UCMDB Domain is also configurable in UCMDB's Infrastructure Settings module. For details, see the HP Universal CMDB Administration Guide.

b. Click **Next**.

9. If you cleared the Use Default CMDB Domain box in the previous step, the Domain Configuration page opens.
   a. **Data Flow Probe domain type**. Select the type of domain on which the Probe is to run:
      - **Customer**. Select if you are installing one or more Probes in your deployment.

        Note: Always use this option for new installations.

      - **External**. Select this option for upgraded 6.x systems.

   b. **Data Flow Probe domain**. If you are not using the default domain defined in UCMDB enter the name of the domain here.

      Note: For external domains, this value must be identical to the Data Flow Probe Identifier defined in the previous step.

   c. Click **Next**.
10. The HP UCMDB Data Flow Probe Working Mode page opens. You can run the Probe Gateway and Probe Manager as one Java process or as separate processes.

    Note: The Probe can be configured in separate mode in IPv4 environments, and in IPv4/IPv6 environments, but not in pure IPv6 environments.

    - Click **No** to run the Probe Gateway and Probe Manager as one process.
    - Click **Yes** to run the Probe Gateway and Probe Manager as two processes on separate machines.

    Note: When running the Probe Gateway and Probe Manager as two processes ensure the following:

    - At least one Probe Gateway component must be installed. The Probe Gateway is connected to the UCMDB Server. It receives tasks from the Server and communicates with the collectors (Probe Managers).
    - Several Probe Managers can be installed. The Probe Managers run jobs and gather information from networks.

- The Probe Gateway should contain a list of attached Probe Managers.
- The Probe Managers must know to which Probe Gateway they are attached.

Click **Next**.

11. The HP UCMDB Data Flow Probe Memory Size page opens.
    a. Define the minimum and maximum memory, in megabytes, to be allocated to the Probe.

    Note: For information about changing the maximum heap size value at a later point in time, see the HP Universal CMDB Data Flow Management Guide.

    b. Click **Next**.
12. The PostgreSQL Account Configuration page opens. The PostgreSQL Data Flow Probe account is used by the Data Flow Probe to connect to the PostgreSQL database. This account is less privileged compared to the PostgreSQL root account. Its password is encrypted in the DataFlowProbe.properties configuration file.
    a. Enter the password for the PostgreSQL Data Flow Probe account and enter it a second time for confirmation.

    Note: Changing this password requires an update to the DataFlowProbe.properties file.

    b. Click **Next**.
13. A second PostgreSQL Account Configuration page opens where you configure the PostgreSQL root account. The PostgreSQL root account is the account used to administer the PostgreSQL database. When set, it may need to be provided while executing scripts under the Probe's installation.
    a. Enter the password for the PostgreSQL Data Flow Probe account, and enter it a second time for confirmation.

    Note: Changing the root account password does not affect operation of the Probe.

    b. Click **Next**.
14. The Account Configuration for Uploading Scan Files page opens. This is used for Manual Scanner Deployment mode. It enables uploading scan files directly to the XML Enricher's incoming directory on the Data Flow Probe using HTTP or HTTPS.
    a. Enter the user name and password for this account, and enter the password a second time for confirmation. The default user name is UploadScanFile.
    b. Click **Next**.
15. The Pre-Installation Summary page opens.

    Review the selections you have made and click **Install** to complete the installation of the Probe.
16. When the installation is complete, the Install Complete page opens.

> **Note:** Any errors occurring during installation are written to the following file:
>
> **C:\hp\UCMDB\DataFlowProbe\HP_UCMDB_Data_Flow_Probe_InstallLog.log**
>
> Any database-related errors occurring during installation are written to the following log:
>
> **C:\hp\UCMDB\DataFlowProbe\runtime\log\postgresql.log**

Click **Done**.

> **Note:** If you installed the Probe on a Windows 2008 machine:
>
> a. Locate the wrapper.exe file in the C:\hp\UCMDB\DataFlowProbe\bin folder.
> b. Right-click the wrapper.exe file and select Properties.
> c. In the Compatibility tab:
> i. Select Compatibility mode.
> ii. Select Run this program in compatibility for: Windows XP (Service Pack 2).
> iii. Select Run this program as administrator.

After installing the Probe, we recommend disabling virus scanning on the main directory that is used to store your PostgreSQL table data. The default directory is **C:\hp\UCMDB\DataFlowProbe\pgsql\data**.

17. Start the Probe: Select **Start > All Programs > HP UCMDB > Start Data Flow Probe**.

    To start the Probe from the console, at the command prompt execute the following script: **C:\hp\UCMDB\DataFlowProbe\bin\gateway.bat console**.

    > **Note:** In order for the Probe to connect to the application server, the application server must be fully started.
    >
    > The Probe is displayed in UCMDB in the Data Flow Management module, under **Data Flow Probe Setup > <Domain> > Probes**.

18. If you selected to run the Probe Gateway and Probe Manager as two processes on separate machines, you must configure the Probe Gateway and Probe Manager components.

Installing the Data Flow Probe on Linux

The following procedure explains how to install the Data Flow Probe on a Linux platform.

> **Note:** For important notes and considerations before you install the Data Flow Probe, see "Before You Install the Data Flow Probe" on page 13.

To install the Data Flow Probe:

1. Select **Admin > Platform > Setup and Maintenance > Downloads**.

   Note: The **Data Flow Probe** link in the Downloads page is displayed only if you have purchased a license for Data Flow Management and the administrator has added the Probe link to the Downloads page. For details, see the section about installing component setup files in the *HPE Application Performance Management Deployment Guide*.

2. To run the installation wizard, execute the following command:

   sh <path to the installer>/HPUCMDB_DataFlowProbe_10.20Linux.bin

   The following commands are executed:

   Preparing to install...

   Extracting the JRE from the installer archive...

   Unpacking the JRE...

   Extracting the installation resources from the installer

   archive...

   Configuring the installer for this system's environment...

   Launching installer...

3. When the initial process is complete, the splash screen opens. Choose the locale language and click **OK**.
4. The Introduction page opens. Click **Next**.
5. The License Agreement page opens. Accept the terms of the end-user license agreement and click **Next**.
6. The Select Installation Folder page opens. Accept the default installation folder, **opt/hp/UCMDB/DataFlowProbe**, or click **Choose** to browse to and select a different installation folder.

   Note:

   - You can change the location of the installation, but the folder must be located under **/opt/**.
   - If you selected a different folder and you want to restore the default installation folder, click **Restore Default Folder**.

   Click **Next**.

7. The Data Flow Probe Configuration page opens. The Data Flow Probe Configuration page enables you to configure the details of the application server to which the Data Flow Probe will report.

   Complete the following information:

   - **Application to report to.** Select the application server with which you are working:
     - **HP Universal CMDB**: In the **Application Server address** box, enter the name or the IP address of the HP Universal CMDB server to which the Probe is to be connected.

> **Note:** In a High Availability environment, use the Writer virtual IP address of the load balancer.

- In the **Data Flow Probe address** box, enter the IP address or DNS name of the machine on which you are currently installing the Probe, or accept the default.

  > **Note:** If the Data Flow Probe machine has more than one IP address, enter a specific IP address, and not the DNS name.

Click **Next**.

8. A second Data Flow Probe Configuration page opens, enabling you to configure an identifier for the Probe.
   - In the **Data Flow Probe Identifier** box, enter a name for the Probe that is used to identify it in your environment.

     > **Note:** The Probe identifier is case sensitive and must be unique for each Probe in your deployment, and it must not exceed 50 characters.

   - Select **Use Default CMDB Domain** to use the default UCMDB IP address or machine name, as defined in the UCMDB Server installation.

     The Default UCMDB Domain is also configurable in UCMDB's Infrastructure Settings module. For details, see the HP Universal CMDB Administration Guide.

   Click **Next**.
9. If you cleared the **Use Default CMDB Domain** box, the HP UCMDB Data Flow Probe Domain Configuration page opens. In the HP UCMDB Data Flow Probe Domain Configuration page:
   - **Data Flow Probe domain type.** Select the type of domain on which the Probe is to run:
     - **Customer.** Select if you are installing one or more Probes in your deployment.

       > **Note:** Always use this option for new installations.

     - **External.** Select if you are upgrading from version 6.x systems.
   - **Data Flow Probe domain.** If you are not using the default domain defined in UCMDB, enter the name the domain here.

     > **Note:** For external domains, this value must be identical to the Data Flow Probe Identifier defined in the previous step.

   Click **Next**.
10. The HP UCMDB Data Flow Probe Memory Size page opens. Define the minimum and maximum

memory to be allocated to the Probe.

Note: For information about changing the maximum heap size value at a later point in time, see the HP Universal CMDB Data Flow Management Guide.

Click **Next**.

11. The PostgreSQL Account Configuration page opens.

    The PostgreSQL Data Flow Probe account is used by the Data Flow Probe to connect to the PostgreSQL database. This account is less privileged compared to the PostgreSQL root account. Its password is encrypted in the **DataFlowProbe.properties** configuration file.

    a. Enter the password for the PostgreSQL Data Flow Probe account and enter it a second time for confirmation.

    Note: Changing this password requires an update to the **DataFlowProbe.properties** file.

    b. Click **Next**.

12. A second PostgreSQL Account Configuration page opens where you configure the PostgreSQL root account. The PostgreSQL root account is the account used to administer the PostgreSQL database. When set, it may need to be provided while executing scripts under the Probe's installation.

    a. Enter the password for the PostgreSQL Data Flow Probe account, and enter it a second time for confirmation.

    Note: Changing the root account password does not affect operation of the Probe.

    b. Click **Next**.

13. The Account Configuration for Uploading Scan Files page opens.

    a. Enter the user name and password for this account, and enter the password a second time for confirmation. The default user name is **UploadScanFile**.

    b. Click **Next**.

14. The Pre-Installation Summary dialog box opens. In the Pre-Installation Summary dialog box opens, review the selections you have made and click **Install** to complete the installation of the Probe.

15. When installation is complete, the Install Complete page opens.

    Note: Any errors occurring during installation are written to the following file:

    /opt/hp/UCMDB/DataFlowProbe/HP_UCMDB_Data_Flow_Probe_InstallLog.log.

    If you installed the Probe to another directory under **/opt/**, the log file is located there.

    Click **Done**.

    Note: After installing the Probe, we recommend disabling virus scanning on the main directory that

is used to store your PostgreSQL table data. The default directory is **/opt/hp/UCMDB/DataFlowProbe/pgsql/data**.

16. Activate the Probe.

    Note: The user running the Probe service must be a member of the Administrators group.

    In order for the Probe to connect to the application server, the application server must be fully started.

    Execute the following command:

    /opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh start

    To activate the Probe in a console, execute the following command:

    /opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh console

    Tip: A Probe installed on a Linux machine is displayed when creating a new integration point in the Data Flow Management Integration Studio. For details, see the section describing how to create integration points in the HP Universal CMDB Data Flow Management Guide.

    The Linux Probe does not appear in the list of Data Flow Probes in the Data Flow Probe Setup window.

Post-Installation Procedure

If you installed the Probe on a Windows 2008 machine:

1. Locate the **wrapper.exe** file in the **<Data Flow Probe Installation Path>\DataFlowProbe\bin** folder.
2. Right-click the **wrapper.exe** file and select **Properties**.
3. 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**.
4. Start the Probe: Select **Start > All Programs > HP UCMDB > Start Data Flow Probe**.

   Note: For details about launching the Probe in a Console, refer to the *RTSM Data Flow Management Guide*.

   The Probe is displayed in Application Performance Management: access **Admin > RTSM Administration > Data Flow Management > Data Flow Probe Setup**.

Note: We recommend disabling virus scanning on the main directory that is used to store your MySQL table data. The default directory is **<Data Flow Probe Installation Path>\DataFlowProbe\MySQL**.

Probe Version Detection

Note: This is relevant for Windows only.

The Probe reports its version when connecting to the server. The Probe version is displayed in Data Flow Management, in the **Details** pane of the Data Flow Probe Setup module. If the Probe version is not compatible with the server version (and there is no supported upgrade), an error is generated and the Probe is forced to shut down.

When you apply a new Cumulative Update Patch (CUP) to the UCMDB 10.22 server, the Probes do not shut down automatically, and are able to report new data to the server. However, this is not recommended. Therefore, when you apply a CUP to the server, you must also apply it to the Probes—either manually or automatically.

Running Probe Manager and Probe Gateway on Separate Machines

During installation, you can choose to separate the Probe Manager and Probe Gateway processes so that they run on separate machines. You must:

1. Install the Probe on both machines according to the procedure in "Installing the Data Flow Probe on Windows" on page 14. In the step that asks if you want to install the Probe Manager and Probe Gateway in separate mode, select **Yes**.
2. Perform the configuration in "Configuring the Probe Manager and Probe Gateway Components" on the next page.

Note:

- At least one Probe Gateway component must be installed. Gateway is connected to the UCMDB Server, receives tasks from the Server, and communicates with the collectors (Probe Manager).
- Several Probe Managers can be installed. Managers run jobs and gather information from networks.
- The Probe Gateway should contain a list of attached Managers.
- The Probe Managers must know to which Gateway they are attached.

Configuring the Probe Manager and Probe Gateway Components

This section explains how to set up the Data Flow Probe when the Probe Manager and Probe Gateway run as separate processes on two machines.

Note: The Probe Manager name in both the probeMgrList.xml and DiscoveryProbe.properties files must be identical. The name is case sensitive.

1. Set up the Probe Gateway machine.
   a. Open the following file:
   <Data Flow Probe Installation Path>\DataFlowProbe\conf\probeMgrList.xml
   b. Locate the line beginning `<probeMgr ip=` and add the Manager machine name or IP address, for example:
   ```
   <probeMgr ip="OLYMPICS08">
   ```
   c. Open the following file:
   <Data Flow Probe Installation Path>\DataFlowProbe\conf\DiscoveryProbe.properties
   d. Locate the lines beginning `appilog.collectors.local.ip =` and `appilog.collectors.probe.ip =` and enter the Gateway machine name or IP address, for example:
   ```
   appilog.collectors.local.ip = STARS01
   appilog.collectors.probe.ip = STARS01
   ```
2. Set up the Probe Manager machine.
   In **<Data Flow Probe Installation Path>\DataFlowProbe\conf\DiscoveryProbe.properties**:
   a. Locate the line beginning `appilog.collectors.local.ip =` and enter the Manager machine name or IP address, for example:
   ```
   appilog.collectors.local.ip = OLYMPICS08
   ```
   b. Locate the line beginning `appilog.collectors.probe.ip =` and enter the Gateway machine name in uppercase, for example:
   ```
   appilog.collectors.probe.ip = STARS01
   ```
3. Start the services.
   a. On the Probe Manager machine, start the Manager service:
   Start > All Programs > UCMDB > Start Data Flow Probe Manager
   b. On the Probe Gateway machine, start the Gateway service:
   Start > All Programs > HP UCMDB > Start Data Flow Probe Gateway

Data Flow Probe Installation - Troubleshooting and Limitations

Repairing Corrupted Databases

The Data Flow Probe MySQL database may become corrupt without the possibility of recovery, for example, because the machine was shut down but the MySQL service was not stopped.

To repair the corruption:

1. Stop the Probe.
2. Run the repair tool:
   - Windows: Run the **repair_mysql.bat** tool from the following folder:

     <Data Flow Probe Installation Path>\DataFlowProbe\tools.
   - Linux: Run the **repair_mysql.sh** tool from the following folder:

     /opt/hp/UCMDB/DataFlowProbe/tools
3. Start the Probe.

If this procedure does not fix the corruption, contact HPE Software Support.

Probe Downgrade or Rollback

Automatic downgrade or rollback of the probe version is not supported. To perform downgrade or to rollback a version upgrade, uninstall the probe and then install the required version.

Probe Restart

There are several situations where the Probe automatically restarts itself. For example, when deploying a new Content Pack or applying a CUP. In these cases, the Probe waits for 15 minutes to allow the running jobs to finish, and only then shuts down. Jobs that did not finish in that time (for example, long integrations) start running again when the Probe restarts.

Probe Terminated with OutOfMemoryError Error

If the Probe is terminated and the following error appears in probe-error.log file: **java.lang.OutOfMemoryError: PermGen space**, do the following:

1. Stop the probe.
2. Modify the PermSize parameters in the **WrapperGateway.conf** file:
   - **Windows:** Open **<Data Flow Probe Installation Path>\DataFlowProbe\bin\WrapperGateway.conf**
   - **Linux:** Open **/opt/hp/UCMDB/DataFlowProbe/bin/WrapperGateway.conf**

and add the following lines to line 65:

- `wrapper.java.additional.19=-XX:PermSize=128m`
- `wrapper.java.additional.20=-XX:MaxPermSize=256m`

3. Save the file.
4. Modify the PermSize parameters in the **WrapperGateway.conf** file:
   - **Windows:** Open **<Data Flow Probe Installation Path>\DataFlowProbe\bin\WrapperManager.conf**
   - **Linux:** Open **/opt/hp/UCMDB/DataFlowProbe/bin/WrapperManager.conf**

   and add the following lines to line 65:
   - `wrapper.java.additional.19=-XX:PermSize=128m`
   - `wrapper.java.additional.20=-XX:MaxPermSize=256m`
5. Save the file.
6. Start the Probe.

Chapter 3: Upgrading the Data Flow Probe

This task describes how to upgrade the Data Flow Probe.

Note: When you upgrade to the latest BSM 9.2x from BSM 9.12 or a later version or APM 9.30 or a later version on a Windows platform, any installed instances of Data Flow Probes are automatically upgraded to match the RTSM version released with the latest BSM 9.2x/APM 9.3x version you are installing. In that case, you do not need to manually upgrade the Probe. To detect which version of the Probe is currently installed, see the "Probe Version Detection" on page 23. If the automatic upgrade fails or you are upgrading on a Linux platform, you must upgrade the Probe manually.

To upgrade the Data Flow Probe manually:

1. **Stop the old Probe.**

   If the Probe is running, stop the Probe as follows:

   - **Windows:** Start **Programs** > **HP UCMDB** > **Stop Data Flow Probe**
   - **Linux:** Run the following command: `/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh stop`

2. **Uninstall the old Probe.**

   - **Windows:** Start **Programs** > **UCMDB** > **Uninstall Data Flow Probe**. When the Probe is uninstalled, delete the folder that contained the Probe: `<Data Flow Probe Installation Path>\DataFlowProbe`
   - **Linux:**
     i. Do one of the following:
        - In shell, execute: `sh /opt/hp/UCMDB/DataFlowProbe/UninstallerData/Uninstall_Discovery_Probe`
        - Double-click the **Uninstall_Discovery_Probe** file in `/opt/hp/UCMDB/DataFlowProbe/UninstallerData`

     ii. Delete the **/opt/hp/UCMDB/DataFlowProbe/** folder.

3. **Install the new Probe**

   Caution: To upgrade the Probe, use the Probe installation file associated with the version of APM you are using. The Probe installation version should exactly match the RTSM version released with APM. Otherwise, the Probe will fail.

For major/minor releases (for example, 9.00 or 9.20), this file is available on the DVD that comes with the APM media kit, or you can download it from the Software Updates page.

For minor-minor patch releases (for example, 9.13 or 9.21), you download this file from the Software Patches page.

Both files can be accessed from the HPE Software Support web site (http://www.hp.com/go/hpsoftwaresupport).

Install the new Probe with the same configuration as for the old Probe installation. That is, use the same Probe ID, domain name, and server name. Remember that the Probe ID is case sensitive.

- **Windows:** See "Installing the Data Flow Probe on Windows" on page 14.
- **Linux:** See "Installing the Data Flow Probe on Linux" on page 18.

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.
- A full data synchronization is automatically triggered.

Chapter 4: Data Flow Credentials Management

This chapter includes:

Data Flow Credentials Management Overview

To perform discovery or run integration, you must set up the credentials to access the remote system. Credentials are configured in the Data Flow Probe Setup window and saved in the RTSM Server. For details, see the section describing the Data Flow Probe setup in the RTSM Data Flow Management Guide.

Credentials storage is managed by the Confidential Manager (CM) component.

The Data Flow Probe can access the credentials using the CM client. The CM client resides on the Data Flow Probe and communicates with the CM server, which resides on the RTSM Server. Communication between the CM client and the CM server is encrypted, and authentication is required by the CM client when it connects to the CM server.

The CM client's authentication on the CM server is based on a LW-SSO component. Before connecting to the CM server, the CM client first sends an LW-SSO cookie. The CM server verifies the cookie and upon successful verification, communication with the CM client begins. For details about LW-SSO, see "Configure LW-SSO Settings" on page 34.

The communication between the CM client and the CM server is encrypted. For details about updating the encryption configuration, see "Configure CM Communication Encryption " on page 34.

Caution: The CM authentication uses the universal time defined on the computer (UTC). In order for the authentication to succeed, ensure that the universal time on the Data Flow probe and the UCMDB Server are the same. The server and probe may be located in different time zones, as UTC is independent of time zone or daylight savings time.

The CM client maintains a local cache of the credentials. The CM client is configured to download all credentials from the CM server and store them in a cache. The credentials changes are automatically synchronized from CM server on a continuous basis. The cache can be a file-system or in-memory cache, depending on the preconfigured settings. In addition, the cache is encrypted and cannot be accessed externally. For details about updating the cache settings, see "Configure the CM Client's Cache Mode on the Probe" on page 38. For details about updating the cache encryption, see "Configure the CM Client's Cache Encryption Settings on the Probe" on page 39.

For details on troubleshooting, see "Change Confidential Manager (CM) Client Log File Message Level" on page 41.

You can copy credentials information from one RTSM server to another. For details, see "Export and Import Credential and Range Information in Encrypted Format" on page 40.

Note: The **DomainScopeDocument** (DSD) that was used for credentials storage on the Probe (in UCMDB version 9.01 or earlier) no longer contains any credentials-sensitive information. The file now

contains a list of Probes and network range information. It also contains a list of credential entries for each domain, where each entry includes the credential ID and a network range (defined for this credential entry) only.

This section includes the following topics:

Basic Security Assumptions

You have secured the Gateway Server and Probe JMX console to enable access to APM system administrators only, preferably through localhost access only.

Data Flow Probe Running in Separate Mode

When the Probe Gateway and Manager run as separate processes, the Confidential Manager (CM) client component becomes part of the Manager process. Credentials information is cached and used by the Probe Manager only. To access the CM server on the RTSM system, the CM client request is handled by the Gateway process and from there is forwarded to the RTSM system.

This configuration is automatic when the Probe is configured in separate mode.

Keeping the Credentials Cache Updated

On its first successful connection to the CM server, the CM client downloads all relevant credentials (all credentials that are configured in the probe's domain). After the first successful communication, the CM client retains continuous synchronization with the CM server. Differential synchronization is performed at one-minute intervals, during which only differences between the CM server and the CM client are synchronized. If the credentials are changed on the RTSM server side (such as new credentials being added, or existing credentials being updated or deleted), the CM client receives immediate notification from the RTSM server and performs additional synchronization.

Synchronizing All Probes with Configuration Changes

For successful communication, the CM client must be updated with the CM server authentication configuration (LW-SSO init string) and encryption configuration (CM communication encryption). For example, when the init string is changed on the server, the probe must know the new init string in order to authenticate.

The RTSM server constantly monitors for changes in the CM communication encryption configuration and CM authentication configuration. This monitoring is done every 15 seconds; in case a change has occurred, the updated configuration is sent to the probes. The configuration is passed to the probes in encrypted form and stored on the probe side in secured storage. The encryption of configuration being sent is done using a symmetric encryption key. By default, the RTSM server and Data Flow Probe are installed with same default symmetric encryption key. For optimal security, it is highly recommended to change this key before adding credentials to the system. For details, see "Generate or Update the Encryption Key" on page 42.

Note: Due to the 15 second monitoring interval, it is possible that the CM client, on the Probe side, may not be updated with the latest configuration for a period of 15 seconds.

If you choose to disable the automatic synchronization of CM communication and authentication configuration between the RTSM server and the Data Flow Probe, each time you update the CM communication and authentication configuration on the RTSM server side, you should update all Probes with the new configuration as well. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the Server and Probes" on page 36.

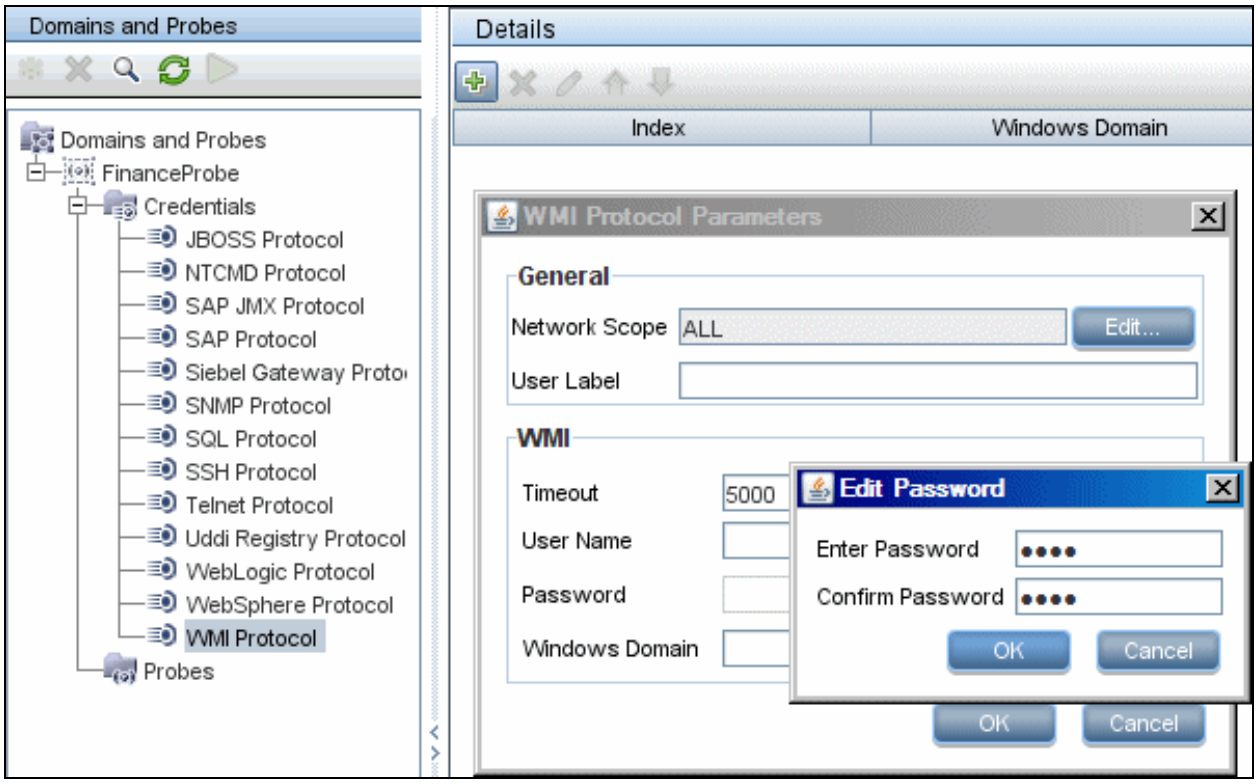
Secured Storage on the Probe

All sensitive information (such as the CM communication and authentication configuration and the encryption key) is stored on the Probe in secure storage in the **secured_storage.bin** file, located in **<Data Flow Probe Installation Path>\DataFlowProbe\conf\security**. This secured storage is encrypted using DPAPI, which relies on the Windows user password in the encryption process. DPAPI is a standard method used to protect confidential data—such as certificates and private keys—on Windows systems. The Probe should always run under the same Windows user, so that even if the password is changed, the Probe can still read the information stored in secure storage.

Viewing Credentials Information

Note: This section deals with viewing credential information when the data direction is from the RTSM to Application Performance Management.

Passwords are not sent from the RTSM database to the application. That is, Application Performance Management displays asterisks (*) in the password field, regardless of content:



Updating Credentials

Note: This section deals with updating credentials when the data direction is from Application Performance Management to the RTSM.

- The communication in this direction is not encrypted, therefore you should connect to the APM Gateway Server using https\SSL, or ensure connection through a trusted network.

  Although the communication is not encrypted, passwords are not being sent as clear text on the network. They are encrypted using a default key and, therefore, it is highly recommended to use SSL for effective confidentiality in transit.
- You can use special characters and non-English characters as passwords.

Configure CM Client Authentication and Encryption Settings

This task describes configuring the CM Client Authentication and Encryption Settings on the RTSM Server, and includes the following steps:

- "Configure LW-SSO Settings" below
- "Configure CM Communication Encryption " below

Configure LW-SSO Settings

This procedure describes how to change the LW-SSO init string on the RTSM server. This change is automatically sent to Probes (as an encrypted string), unless the RTSM server is configured to not automatically do this. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the Server and Probes" on page 36.

1. On the RTSM server, launch the Web browser and enter the following address: **http://localhost:8080/jmx-console**.
2. Click **UCMDB-UI:name=LW-SSO Configuration** to open the JMX MBEAN View page.
3. Locate the **setInitString** method.
4. Enter a new LW-SSO init string.
5. Click Invoke.

Configure CM Communication Encryption

This procedure describes how to change the CM communication encryption settings on the RTSM Server. These settings specify how the communication between the CM client and the CM server is encrypted. This change is automatically sent to Probes (as an encrypted string), unless the RTSM server is configured to not automatically do this. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the Server and Probes" on page 36.

1. On the RTSM server, launch the Web browser and enter the following address: **http://localhost:8080/jmx-console.**
2. Click **UCMDB:service=Security Services** to open the JMX MBEAN View page.
3. Click the **CMGetConfiguration** method.
4. Click **Invoke**.

   The XML of the current CM configuration is displayed.
5. Copy the contents of the displayed XML.

6. Navigate back to the **Security Services** JMX MBean View page.
7. Click the **CMSetConfiguration** method.
8. Paste the copied XML into the **Value** field.
9. Update the relevant transport-related settings.

   For details about the values that can be updated, see "CM Encryption Settings" on page 46.

   Example:

```
<transport>
        <encryptTransportMode>true</encryptTransportMode>
        <CMEncryptionDecryption>
                <encryptDecryptInitString>radiohead</encryptDecryptInitString>
                <cryptoSource>lw</cryptoSource>
                <lwJCEPBECompatibilityMode>true</lwJCEPBECompatibilityMode>
                <cipherType>symmetricBlockCipher</cipherType>
                <engineName>AES</engineName>
                <algorithmModeName>CBC</algorithmModeName>
                <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
                <keySize>256</keySize>
                <pbeCount>20</pbeCount>
                <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
                <encodingMode>Base64Url</encodingMode>
                <useMacWithCrypto>false</useMacWithCrypto>
                <macType>hmac</macType>
                <macKeySize>256</macKeySize>
                <macHashName>SHA256</macHashName>
        </CMEncryptionDecryption>
</transport>
```

10. Click **Invoke**.

Configure CM Client Authentication and Encryption Settings Manually on the Probe

This task includes the following steps:

Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the Server and Probes

By default, the UCMDB Server is configured to automatically send the CM/LW-SSO settings to all Probes. This information is sent as an encrypted string to the Probes, which decrypt the information upon retrieval. You can configure the UCMDB Server to not send the CM/LW-SSO configuration files automatically to all Probes. In this case, it is your responsibility to manually update all Probes with the new CM/LW-SSO settings.

To disable automatic synchronization of CM/LW-SSO settings:

1. In RTSM, click **Admin > RTSM Administration > Administration > Infrastructure Settings Manager > General Settings**.
2. Select **Enable automatic synchronization of CM/LW-SSO configuration and init string with probe.**
3. Click the **Value** field and change **True** to **False**.
4. Click the **Save** button.
5. Restart the RTSM server.

Configure CM Client Authentication and Encryption Settings on the Probe

This procedure is relevant if the RTSM Server has been configured to not send LW-SSO/CM configuration and settings automatically to Probes. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the Server and Probes" above.

1. On the Probe machine, launch the Web browser and enter the following address: **http://localhost:1977**.

   Note: If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows: **http://localhost:1978**.

2. Click **type=CMClient** to open the JMX MBEAN View page.

3. Locate the **setLWSSOInitString** method and provide the same init string that was provided for RTSM's LW-SSO configuration.
4. Click the **setLWSSOInitString** button.

Configure CM Communication Encryption on the Probe

This procedure is relevant if the RTSM Server has been configured to not send LW-SSO/CM configuration and settings automatically to Probes. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the Server and Probes" on the previous page.

1. On the Probe machine, launch the Web browser and enter the following address: **http://localhost:1977**.

   Note: If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows: **http://localhost:1978**.

2. Click **type=CMClient** to open the JMX MBEAN View page.
3. Update the following transport-related settings:

   Note: You must update the same settings that you updated on the RTSM server. To do this, some of the methods that you update on the Probe may require more than one parameter. To see the current probe configuration, click **displayTransportConfiguration** in the JMX MBEAN View page. For details, see "Configure CM Communication Encryption " on page 34. For details about the values that can be updated, see "CM Encryption Settings" on page 46.

   a. **setTransportInitString** changes the **encryptDecryptInitString** setting.
   b. **setTransportEncryptionAlgorithm** changes CM settings on the Probe according to the following map:
      - **Engine name** refers to the <engineName> entry
      - **Key size** refers to the <keySize> entry
      - **Algorithm padding name** refers to the <algorithmPaddingName> entry
      - **PBE count** refers to the <pbeCount> entry
      - **PBE digest algorithm** refers to the <pbeDigestAlgorithm> entry
   c. **setTransportEncryptionLibrary** changes CM settings on the Probe according to the following map:
      - **Encryption Library name** refers to the <cryptoSource> entry
      - **Support previous lightweight cryptography versions** refers to the <lwJCEPBECompatibilityMode> entry
   d. **setTransportMacDetails** change CM settings on the Probe according to the following map:

- **Use MAC with cryptography** refers to the <useMacWithCrypto> entry
- **MAC key size** refers to the <macKeySize> entry

4. Click the **reloadTransportConfiguration** button to make the changes effective on the Probe.

For details about the different settings and their possible values, see "CM Encryption Settings" on page 46.

Configure the Confidential Manager (CM) Client Cache

This task includes the following steps:

- "Configure the CM Client's Cache Mode on the Probe" below
- "Configure the CM Client's Cache Encryption Settings on the Probe" on the next page

Configure the CM Client's Cache Mode on the Probe

The CM client stores credentials information in the cache and updates it when the information changes on the Server. The cache can be stored on the file system or in memory:

- **When stored on the file system**, even if the Probe is restarted and cannot connect to the Server, the credentials information is still available.
- **When stored in memory**, if the Probe is restarted, the cache is cleared and all information is retrieved again from the Server. If the Server is not available, the Probe does not include any credentials, so no discovery or integration can run.

To change this setting:

1. Open the **DiscoveryProbe.properties** file in a text editor. This file is located in the **<Data Flow Probe Installation Path>\DataFlowProbe\conf** folder.
2. Locate the following attribute: **com.hp.ucmdb.discovery.common.security.storeCMData=true**
   - To store the information on the file system, leave the default (**true**).
   - To store the information in memory, enter **false**.
3. Save the **DiscoveryProbe.properties** file.
4. Restart the Probe.

Configure the CM Client's Cache Encryption Settings on the Probe

This procedure describes how to change the encryption settings of the CM client's file system cache file. Note that changing the encryption settings for the CM client's file system cache causes the file system cache file to be recreated. This recreation process requires restarting the Probe and full synchronization with the RTSM Server.

1. On the Probe machine, launch the Web browser and enter the following address: **http://localhost:1977**.

   Note: If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows: **http://localhost:1978**.

2. Click **type=CMClient** to open the JMX MBEAN View page.
3. Update the following cache-related settings:

   Note: Some of the methods that you update on the Probe may require more than one parameter. To see the current probe configuration, click **displayCacheConfiguration** in the JMX MBEAN View page.

   a. **setCacheInitString** changes the file system cache <encryptDecryptInitString> setting.
   b. **setCacheEncryptionAlgorithm** changes the file system cache settings according to the following map:
      - **Engine name** refers to the <engineName> entry
      - **Key size** refers to the <keySize> entry
      - **Algorithm padding name** refers to the <algorithmPaddingName> entry
      - **PBE count** refers to the <pbeCount> entry
      - **PBE digest algorithm** refers to the <pbeDigestAlgorithm> entry
   c. **setCacheEncryptionLibrary** changes the cache file system settings according to the following map:
      - **Encryption Library name** refers to the <cryptoSource> entry
      - **Support previous lightweight cryptography versions** refers to the <lwJCEPBECompatibilityMode> entry
   d. **setCacheMacDetails** changes the cache file system settings according to the following map:
      - **Use MAC with cryptography** refers to the <useMacWithCrypto> entry
      - **MAC key size** refers to the <macKeySize> entry
4. Click the **reloadCacheConfiguration** button to make the changes effective on the Probe. This causes

the Probe to restart.

Note: Make sure that no job is running on the Probe during this action.

For details about the different settings and their possible values, see "CM Encryption Settings" on page 46.

Export and Import Credential and Range Information in Encrypted Format

You can export and import credentials and network range information in encrypted format in order to copy the credentials information from one RTSM Server to another. For example, you might perform this operation during recovery following a system crash or during upgrade.

- **When exporting credentials information,** you must enter a password (of your choosing). The information is encrypted with this password.
- **When importing credentials information,** you must use the same password that was defined when the DSD file was exported.

Note: The exported credentials document also contains ranges information that is defined on the system from which the document was exported. During the import of the credentials document, ranges information is imported as well.

Caution: To import credentials information from a UCMDB version 8.02 domainScopeDocument, you must use the key.bin file located on the version 8.02 system.

To export credentials information from the RTSM Server:

1. On the RTSM 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.
2. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
3. Locate the **exportCredentialsAndRangesInformation** operation. Do the following:
   - Enter your customer ID (the default is 1).
   - Enter a name for the exported file.
   - Enter your password.
   - Set **isEncrypted=True** if you want the exported file to be encrypted with the provided password, or **isEncrypted=False** if you want the exported file to not be encrypted (in which case passwords and other sensitive information are not exported).
4. Click **Invoke** to export.

When the export process completes successfully, the file is saved to the following location: **<Data Flow Probe Installation Path>\UCMDBServer\conf\discovery\<customer_dir>**.

To import credentials information from the RTSM Server:

1. On the RTSM 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.
2. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
3. Locate one of the following operations:
   - Locate the **importCredentialsAndRangesInformation** operation if the file that you are importing was exported from a RTSM Server that is later than version 8.02.
   - Locate the **importCredentialsAndRangesWithKey** operation if the file that you are importing was exported from a RTSM version 8.02 Server.
4. Enter your customer ID (the default is 1).
5. Enter the name of the file to import. This file must be located in **<Data Flow Probe Installation Path>\UCMDBServer\conf\discovery\<customer_dir>**.
6. Enter the password. This must be the same password that was used when the file was exported.
7. If the file was exported from a RTSM version 8.02 system, enter the **key.bin** file name. This file must be located in **<Data Flow Probe Installation Path>\UCMDBServer\conf\discovery\<customer_dir>**, together with the file to be imported.
8. Click **Invoke** to import the credentials.

Change Confidential Manager (CM) Client Log File Message Level

The Probe provides two log files that contain information regarding CM-related communication between the CM server and the CM client. The files are:

- "CM Client Log File" below
- "LW-SSO Log File" on the next page

CM Client Log File

The **security.cm.log** file is located in the **<Data Flow Probe Installation Path>\DataFlowProbe\runtime\log** folder.

The log contains information messages exchanged between the CM server and the CM client. By default, the log level of these messages is set to INFO.

To change the log level of the messages to DEBUG level:

1. On the Data Flow Probe Manager server, navigate to **<Data Flow Probe Installation Path>\DataFlowProbe\conf\log**.
2. Open the **security.properties** file in a text editor.
3. Change the line:

   `loglevel.cm=INFO`

   to:

   `loglevel.cm=DEBUG`
4. Save the file.

LW-SSO Log File

The **security.lwsso.log** file is located in the **<Data Flow Probe Installation Path>\DataFlowProbe\runtime\log** folder.

The log contains information messages related to LW-SSO. By default, the log level of these messages is set to INFO.

To change the log level of the messages to DEBUG level:

1. On the Data Flow Probe Manager server, navigate to **<Data Flow Probe Installation Path>\DataFlowProbe\conf\log**.
2. Open the security.properties file in a text editor.
3. Change the line:

   `loglevel.lwsso=INFO`

   to:

   `loglevel.lwsso=DEBUG`
4. Save the file.

Generate or Update the Encryption Key

You can generate or update an encryption key to be used for encryption or decryption of CM communication and authentication configurations exchanged between the RTSM Server and the Data Flow Probe. In each case (generate or update), the RTSM Server creates a new encryption key based on parameters that you supply (for example, key length, extra PBE cycles, JCE provider) and distributes it to the Probes.

The result of running the **generateEncryptionKey** method is a new generated encryption key. This key is stored only in secured storage and its name and details are not known. If you reinstall an existing Data Flow Probe, or connect a new Probe to the RTSM Server, this new generated key is not recognized by the new Probe. In these cases, it is preferable to use the **changeEncryptionKey** method to change encryption keys. This way, when you reinstall a Probe or install a new Probe, you can import the existing key (whose name and location you know) by running the **importEncryptionKey** method on the Probe JMX console.

Note:

- The difference between the methods used to create a key (**generateEncryptionKey**) and update a key (**changeEncryptionKey**) is that **generateEncryptionKey** creates a new, random encryption key, while **changeEncryptionKey** imports an encryption key whose name you provide.
- Only one encryption key can exist on a system, no matter how many Probes are installed.

This task includes the following steps:

- "Generate a New Encryption Key" below
- "Update an Encryption Key on a RTSM Server" on the next page
- "Update an Encryption Key on a Probe" on page 45
- "Manually Change the Encryption Key when the Probe Manager and Probe Gateway are Installed on Separate Machines" on page 46
- "Define Several JCE Providers" on page 46

Generate a New Encryption Key

You can generate a new key to be used by the RTSM Server and Data Flow Probe for encryption or decryption. The RTSM Server replaces the old key with the new generated key, and distributes this key among the Probes.

To generate a new encryption key through the JMX console:

1. On the RTSM 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.
2. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
3. Locate the generateEncryptionKey operation.
   a. In the **customerId** parameter box, enter 1 (the default).
   b. For **keySize**, specify the length of the encryption key. Valid values are 128, 192, or 256.
   c. For **usePBE**, specify **True** or **False**:
      - **True:** use additional PBE hash cycles.
      - **False:** do not use additional PBE hash cycles.

d. For **jceVendor**, you can choose to use a non-default JCE provider. If the box is empty, the default provider is used.

e. For **autoUpdateProbe**, specify **True** or **False**:
   - **True:** the server distributes the new key to the Probes automatically.
   - **False:** the new key should be placed on the Probes manually.

f. For **exportEncryptionKey**, specify **True** or **False**.
   - **True:** In addition to creating the new password and storing it in secured storage, the Server exports the new password to the file system (**<Data Flow Probe Installation Path>\UCMDBServer\conf\discovery\key.bin**). This option enables you to update Probes manually with the new password.
   - **False:** The new password is not exported to the file system. To update Probes manually, set **autoUpdateProbe** to False and **exportEncryptionKey** to True.

> **Note:** Make sure that the Probe is up and connected to the server. If the Probe goes down, the key cannot reach the Probe. If you change the key before the Probe goes down, once the Probe is up again, the key is sent again to the Probe. However, if you have changed the key more than once before the Probe goes down, you must change the key manually through the JMX console. (Select **False** for **exportEncryptionKey**).

4. Click **Invoke** to generate the encryption key.

Update an Encryption Key on a RTSM Server

You use the **changeEncryptionKey** method to import your own encryption key to the RTSM server and distribute it among all Probes.

To update an encryption key through the JMX Console:

1. On the RTSM 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.
2. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
3. Locate the **changeEncryptionKey** operation.
   a. In the **customerId** parameter box, enter **1** (the default).
   b. For **newKeyFileName**, enter the name of the new key.
   c. For **keySizeInBits**, specify the length of the encryption key. Valid values are 128, 192, or 256.
   d. For **usePBE**, specify **True** or **False**:
      - **True:** use additional PBE hash cycles.
      - **False:** do not use additional PBE hash cycles.

e. For **jceVendor**, you can choose to use a non-default JCE provider. If the box is empty, the default provider is used.

f. For **autoUpdateProbe**, specify **True** or **False**:

- **True:** the server distributes the new key to the Probes automatically.
- **False:** the new key should be distributed manually using the Probe JMX console.

> **Note:** Make sure that the Probe is up and connected to the server. If the Probe goes down, the key cannot reach the Probe. If you change the key before the Probe goes down, once the Probe is up again, the key is sent again to the Probe. However, if you have changed the key more than once before the Probe goes down, you must change the key manually through the JMX console. (Select **False** for **autoUpdateProbe**).

4. Click **Invoke** to generate and update the encryption key.

Update an Encryption Key on a Probe

If you choose not to distribute an encryption key from the RTSM Server to all Probes automatically (because of security concerns), you should download the new encryption key to all Probes and run the **importEncryptionKey** method on the Probe:

1. Place the encryption key file in **<Data Flow Probe Installation Path>\DataFlowProbe\conf\security**.
2. On the Probe machine, launch the Web browser and enter the following address: **http://localhost:1977**.

   You may have to log in with a user name and password.

   > **Note:** If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows: **http://localhost:1978**.

3. On the Probe domain, click **type=SecurityManagerService**.
4. Locate the **importEncryptionKey** method.
5. Enter the name of the encryption key file that resides in **<Data Flow Probe Installation Path>\DataFlowProbe\conf\security**. This file contains the key to be imported.
6. Click the **importEncryptionKey** button.
7. Perform a restart of the probe.

Manually Change the Encryption Key when the Probe Manager and Probe Gateway are Installed on Separate Machines

1. On the Probe Manager machine, start the Probe Manager service (**Start > Programs > HP UCMDB > Probe Manager**).
2. Import the key from the server, using the Probe Manager JMX. For details, see "Generate a New Encryption Key" on page 43.
3. After the encryption key is imported successfully, restart the Probe Manager and Probe Gateway services.

Define Several JCE Providers

When you generate an encryption key through the JMX Console, you can define several JCE providers, using the **changeEncryptionKey** and **generateEncryptionKey** methods.

To change the default JCE provider:

1. Register the JCE provider jar files in **$JRE_HOME/lib/ext**.
2. Copy the jar files to the $JRE_HOME folder:
   - For the RTSM Server: $JRE_HOME resides at: **<Data Flow Probe Installation Path>\UCMDBServer\bin\jre**
   - For the Data Flow Probe: $JRE_HOME resides at: **<Data Flow Probe Installation Path>\DataFlowProbe\bin\jre**
3. Add the provider class at the end of the provider list in the **$JRE_HOME\lib\security\java.security** file.
4. Update the **local_policy.jar** and **US_export_policy.jar** files to include unlimited JCE policies. You can download these jar files from the Sun Web site.
5. Restart the RTSM Server and the Data Flow Probe.
6. Locate the JCE vendor field for the **changeEncryptionKey** or **generateEncryptionKey** method, and add the name of the JCE provider.

CM Encryption Settings

This table lists the encryption settings that can be changed using various JMX methods. These encryption settings are relevant for encryption of communications between the CM client and the CM server, as well as for encryption of the CM client's cache.

CM Setting Name	Probe CM Setting Name	Setting Description	Possible Values	Default Value
cryptoSource	Encryption Library name	This setting defines which encryption library to use.	lw, jce, windowsDPAPI, lwJCECompatible	lw
lwJCEPBE Compatibility Mode	Support previous lightweight cryptography versions	This setting defines whether to support previous lightweight cryptography or not.	true, false	true
engineName	Engine name	Encryption mechanism name	AES, DES, 3DES, Blowfish	AES
keySize	Key size	encryption key length in bits	For AES - 128, 192 or 256; For DES - 64; For 3DES - 192; For Blowfish - any number between 32 and 448	256
algorithm Padding Name	Algorithm padding name	Padding standards	PKCS7Padding, PKCS5Padding	PKCS7Padding
pbeCount	PBE count	The number of times to run the hash to create the key from password (init string)	Any positive number	20
pbeDigest Algorithm	PBE digest algorithm	Hashing type	SHA1, SHA256, MD5	SHA1
useMacWith Crypto	Use MAC with cryptography	Indication if to use MAC with the cryptography	true, false	false
macKeySize	MAC key size	Depends on MAC algorithm	256	256

Troubleshooting and Limitations

- If you change the default domain name on the UCMDB server, you must first verify that the Data Flow Probe is not running. After the default domain name is applied, you must execute the **DataFlowProbe\tools\clearProbeData.bat** script on the Data Flow Probe side.

  Note: Execution of the **clearProbeData.bat** script will cause a discovery cycle on the Probe side after the Probe is restarted.

- When trying to run an integration, you receive the following error message:

  `Failed to log in to host <hostname> with customer name <default client>, user [null], password [null], state [null], application name <CMDB Adapter>”.`

  This message appears because the credentials from the Confidential Manager on the server are not synchronized to the Probe.

  To prevent this problem:

  a. Stop the Probe.

  b. Run the **DataFlowProbe\tools\clearProbeData.bat** script on the Probe side.

  c. Restart the Probe.

  Note: Execution of the **clearProbeData.bat** script will cause a discovery cycle on the Probe side after the Probe is restarted.

Chapter 5: Data Flow Probe Hardening

This chapter includes:

Set the MySQL Database Encrypted Password

This section explains how to encrypt the password for the MySQL database user.

1. **Create the Encrypted Form of a Password (AES, 192-bit key)**
   a. Access the Data Flow Probe JMX console. Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

      You may have to log in with a user name and password.

      > **Note:** If you have not created a user, use the default user name admin and the password admin to log in.

   b. Locate the **Type=MainProbe** service and click the link to open the Operations page.
   c. Locate the **getEncryptedDBPassword** operation.
   d. In the **DB Password** field, enter the password to be encrypted.
   e. Invoke the operation by clicking the **getEncryptedDBPassword** button.

The result of the invocation is an encrypted password string, for example:

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
```

2. **Stop the Data Flow Probe**
   Start > All Programs > HP UCMDB > Stop Data Flow Probe
3. **Run the set_dbuser_password.cmd Script**
   This script is located in the following folder: **<Data Flow Probe Installation Path>\DataFlowProbe\tools\dbscripts\set_dbuser_password.cmd**
   Run the **set_dbuser_password.cmd** script with the new password as an argument, for example, **set_dbuser_password <my_password>**.
   The password must be entered in its unencrypted form (as plain text).
4. **Update the Password in the Data Flow Probe Configuration Files**
   a. The password must reside encrypted in the configuration files. To retrieve the password's encrypted form, use the **getEncryptedDBPassword** JMX method, as explained in step 1.
   b. Add the encrypted password to the following properties in the **<Data Flow Probe Installation Path>\DataFlowProbe\conf\DiscoveryProbe.properties** file.
      - **appilog.agent.probe.jdbc.pwd**
        For example:

        ```
        appilog.agent.probe.jdbc.user = mamprobe
        appilog.agent.probe.jdbc.pwd =
        66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
        ```

      - **appilog.agent.local.jdbc.pwd**
5. **Start the Data Flow Probe**
   Start > All Programs > HP UCMDB > Start Data Flow Probe

Using the clearProbeData.bat Script

The **clearProbeData.bat** script recreates the database user with a password that is provided as an argument to the script.

After you set a password, each time you execute the **clearProbeData.bat** script, it retrieves the database password as an argument.

After running the script:

- Review the following file for errors:
  <Data Flow Probe Installation Path>\DataFlowProbe\runtime\log\probe_setup.log
- Delete the following file, as it contains the database password: **<Data Flow Probe Installation Path>\DataFlowProbe\runtime\log\probe_setup.log**

Set the JMX Console Encrypted Password

This section explains how to encrypt the password for the JMX user. The encrypted password is stored in the DiscoveryProbe.properties file. Users must log in to access the JMX console.

1. **Create the Encrypted Form of a Password (AES, 192-bit key)**
   a. Access the Data Flow Probe JMX console. Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

      You may have to log in with a user name and password.

      Note: If you have not created a user, use the default user name admin and the password admin to log in.

   b. Locate the **Type=MainProbe** service and click the link to open the Operations page.
   c. Locate the **getEncryptedKeyPassword** operation.
   d. In the **Key Password** field, enter the password to be encrypted.
   e. Invoke the operation by clicking the **getEncryptedKeyPassword** button.

      The result of the invocation is an encrypted password string, for example:

      ```
      85,-9,-61,11,105,-93,-81,118
      ```
2. **Stop the Data Flow Probe**
   Start > All Programs > HP UCMDB > Stop Data Flow Probe
3. **Add the Encrypted Password**

   Add the encrypted password to the following property in the **<Data Flow Probe Installation Path>\DataFlowProbe\conf\DiscoveryProbe.properties** file.

   appilog.agent.Probe.JMX.BasicAuth.Pwd

   For example:

   ```
   appilog.agent.Probe.JMX.BasicAuth.User=admin
   appilog.agent.Probe.JMX.BasicAuth.Pwd=-85,-9,-61,11,105,-93,-81,118
   ```

   Note: To disable authentication, leaves these fields empty. If you do so, users can open the main page of the Probe's JMX console without entering authentication.
4. **Start the Data Flow Probe**
   Start > All Programs > HP UCMDB > Start Data Flow Probe

   Test the result in a Web browser.

Restrict the Data Flow Probe's Access to the MySQL Server

This section explains how to permit access to the Data Flow Probe's MySQL database from the local machine only.

To restrict MySQL access:

Run the following script in a command prompt window or by double-clicking it: **<Data Flow Probe Installation Path>\DataFlowProbe\tools\dbscripts\remove_remote_user_access.cmd.**

Any user (other than the root user) trying to connect from a remote computer will now be denied access.

Note: Users who have root credentials to the MySQL database will still be able to access the database from the remote machine.

Enable Authentication on the Data Flow Probe with Basic HTTP Authentication

Important: The basic authentication method of enabling authentication on the Data Flow Probe is the least preferred method. It is recommended to use mutual authentication security, as it is a much more effective method of security (it combines data encryption and certificate authentication). For details, see "Connect the Data Flow Probe to APM Using Client Certificates" on page 54.

If SSL is not enabled, credentials are transmitted to UCMDB as plain-text.

To set basic authentication:

1. Locate the following file: **<Data Flow Probe Installation Path>\DataFlowProbe\conf\DiscoveryProbe.properties**.
2. Remove the comment markers (#) from the following properties, and enter the relevant credentials:

```
appilog.agent.Probe.BasicAuth.Realm=
appilog.agent.Probe.BasicAuth.User=
appilog.agent.Probe.BasicAuth.Pwd=
```

The credentials should match those defined on the APM server.

Connect the Data Flow Probe to APM Using SSL

When a session is started between the Data Flow Probe and the Gateway Server, the Gateway Server sends the Probe a server-side certificate that was issued by a Certification Authority (CA) recognized by the Gateway Server. The Data Flow Probe engine should be configured to trust the certificate or the CA that issued it, and to communicate via SSL.

1. Establish trust with the CA which issued the APM virtual server certificate.
   a. Obtain the root certificate of the issuing authority and save it to a file, for example, **C:\ca.cer**.
   b. Import this certificate into the Data Flow Probe JVM: **<Data Flow Probe Installation Path>\DataFlowProbe\bin\jre\bin** with the following values:

      ```
      <Data Flow Probe Installation Path>\DataFlowProbe\bin\jre\bin\keytool -import -trustcacerts -alias <your alias> -keystore ..\lib\security\cacerts -file C:\ca.cer
      ```

   c. Enter the password (default: **changeit**) and click **Yes** to confirm.
2. Set the connection parameters in the Data Flow Probe.
   a. Open the file **<Data Flow Probe Installation Path>\DataFlowProbe\conf\DiscoveryProbe.properties**.
   b. Configure the URL of the APM server:

      ```
      serverName = <APM virtual server fully qualified domain name>
      ```

      Note: The SSL connection may fail if an IP address is used instead of domain name.

   c. Configure the port number to use for HTTPS:

      ```
      # Ports used for HTTP/s traffic
      #serverPort = 80
      serverPortHttps = 443
      ```

   d. Set the schema to be used by the Agent to HTTPS:

      ```
      # Can be either HTTP or HTTPS
      appilog.agent.probe.protocol = HTTPS
      ```

3. Restart the Data Flow Probe.

Connect the Data Flow Probe to APM Using Client Certificates

If the APM front-end requires SSL and a client certificate, you need to configure the Data Flow Probe to provide a certificate as described below.

Prerequisite: The Data Flow Probe must be configured with SSL, as described in "Connect the Data Flow Probe to APM Using SSL" on the previous page.

1. Obtain the client certificate issued to the name of the Data Flow Probe server. The certificate can be in either PFX or JKS format. If you want to create your own keystore manually, see "SSL Certificates" in the APM Hardening Guide.

   If the client certificate is in PFX format, you must convert it to JKS format. For example:

   ```
   <Data Flow Probe Installation Path>\DataFlowProbe\bin\jre\bin>keytool.exe -
   importkeystore -srckeystore <Data Flow Probe Installation
   Path>\DataFlowProbe\conf\security\certificate.pfx -destkeystore <Data Flow Probe
   Installation Path>\DataFlowProbe\conf\security\keystore.jks -srcstoretype PKCS12.
   ```

   Note: The keystore password must be the same as the private key password.The keystore password should already be configured in the **ssl.properties** file as **logomania** (the default password). If the keystore password is not **logomania**, you must re-encrypt the password and change it in the **ssl.properties** file. To re-encrypt the password, see step 4 below.

2. Import the Certificate Authority certificate into the Data Flow Probe Java truststore by running the following command:

   ```
   <Data Flow Probe Installation Path>\DataFlowProbe\bin\jre\bin>keytool.exe -import -
   trustcacerts -alias <your alias> -file <path to certificate location>\ca.cer\ca.cer -
   keystore <Data Flow Probe Installation
   Path>\DataFlowProbe\conf\security\MAMTrustStoreExp.jks
   ```

   Enter the keystore password (default: **logomania**). To change the password, see "Update the keystore and truststore passwords" below.

3. Change the **ssl.properties** file, located in the **<Data Flow Probe Installation Path>\DataFlowProbe\conf\security** folder. Update the keystore file name to point to the client keystore file you created previously:

   ```
   # Path to Keystore file

   javax.net.ssl.keyStore=keystore.jks
   ```

4. (Optional) Update the keystore and truststore passwords:

a. You encrypt the password through the Probe's JMX console: Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

   You may have to log in with a user name (default: **sysadmin**) and password (default: **sysadmin**).

b. Locate the **Type=MainProbe** service and click the link to open the JMX MBEAN View page.

c. Locate the **getEncryptedKeyPassword** operation.

d. Enter your keystore or truststore password in the **Key Password** field and click **getEncryptedKeyPassword**.

e. Open the **ssl.properties** file in the following folder: **<Data Flow Probe Installation Path>\DataFlowProbe\root\lib\security**.

f. Copy and paste the encrypted password (numbers separated by commas, for example, 1,2,3,4,5) into the relevant keystore or truststore line of the **ssl.properties** file.

g. Save the file.

5. Update the **<Data Flow Probe Installation Path>\DataFlowProbe\conf\DiscoveryProbe.properties** file:
   a. Change the **appilog.agent.probe.protocol** parameter to **HTTPS**.
   b. Make sure the **serverPortHttps** value is **443**.
6. Restart the Data Flow Probe.

Connect the Data Flow Probe to APM Using Reverse Proxy

Perform the following procedure to connect the Data Flow Probe to APM through the reverse proxy.

1. Edit the **discoveryProbe.properties** file (located in **<Data Flow Probe Installation Path>\DataFlowProbe\conf**).
2. Set the **serverName** property to the reverse proxy server's IP or DNS name.
3. Set the **serverPort** and **serverPortHttps** properties to the reverse proxy server's ports.
4. Save the file.

The following proxy server configuration is required if Data Flow Probes only are connected via a reverse proxy to APM.

Note: In the URLs in this table, you can use either https or http.

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/mam/*	https://[APM server]/mam /* or

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/mam_images/*	https://[APM server]/mam_images/*
/mam-collectors/*	https://[APM server]/mam-collectors/*
/cm/*	https://[APM server]/cm/* https://[APM server]/cm/*
/axis2/*	https://[APM server]/axis2/* **Note:** Required if SOAP adaptor is used with embedded RTSM for replication into secure APM via reverse proxy.

Control the Location of the domainScopeDocument File

The Probe's file system holds (by default) both the encryption key and the **domainScopeDocument** file. Each time the Probe is started, the Probe retrieves the **domainScopeDocument** file from the server and stores it on its file system. To prevent unauthorized users from obtaining these credentials, you can configure the Probe so that the **domainScopeDocument** file is held in the Probe's memory and is not stored on the Probe file system.

To control the location of the domainScopeDocument file:

1. Open **<Data Flow Probe Installation Path>\DataFlowProbe\conf\DiscoveryProbe.properties** and change:

   ```
   appilog.collectors.storeDomainScopeDocument=true
   ```

   to:

   ```
   appilog.collectors.storeDomainScopeDocument=false
   ```

   The Probe Gateway and Probe Manager serverData folders no longer contain the **domainScopeDocument** file.

   For details on using the **domainScopeDocument** file to harden DFM, see "Data Flow Credentials Management" on page 29.

2. Restart the Probe.

Create a Keystore for the Data Flow Probe

1. On the Probe machine, run the following command:

   ```
   <Data Flow Probe Installation Path>\DataFlowProbe\bin\jre\bin\keytool -genkey -alias
   probekey -keyalg
   RSA -keystore <Data Flow Probe Installation
   Path>\DataFlowProbe\conf\security\client.keystore
   ```

2. Enter a password for the new keystore.
3. Enter your information when asked.
4. When asked **Is CN=… C=… Correct?** enter **yes**, and press **Enter**.
5. Press **Enter** again to accept the keystore password as the key password.
6. Verify that **client.keystore** is created in the following directory: **<Data Flow Probe Installation Path>\DataFlowProbe\conf\security**.

Encrypt the Probe Keystore and Truststore Passwords

The Probe keystore and truststore passwords are stored encrypted in **<Data Flow Probe Installation Path>\DataFlowProbe\conf\security\ssl.properties**. This procedure explains how to encrypt the password.

1. Start Data Flow Probe (or verify that it is already running).
2. Access the Data Flow Probe JMX console: Launch a Web browser and enter the following address: http://<Data Flow Probe machine name or IP address>:1977. If you are running the Data Flow Probe locally, enter http://localhost:1977.

   Note: You may have to log in with a user name and password. If you have not created a user, use the default user name admin and the password admin to log in.

3. Locate the **Type=MainProbe** service and click the link to open the Operations page.
4. Locate the **getEncryptedKeyPassword** operation.
5. Enter your keystore or truststore password in the **Key Password** field and invoke the operation by clicking **getEncryptedKeyPassword**.
6. The result of the invocation is an encrypted password string, for example:

   ```
   66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
   ```

7. Copy and paste the encrypted password into the line relevant to either the keystore or the truststore in the following file: **<Data Flow Probe Installation Path>\DataFlowProbe\conf\security\ssl.properties.**

Server and Data Flow Probe Default Keystore and Truststore

This section includes the following topics:

RTSM Server

The files are located in the following directory: **<Data Flow Probe Installation Path>\UCMDBServer\conf\security.**

Entity	File Name/Term	Password/Term	Alias
Server keystore	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
Server truststore	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	clientcert (default trusted entry)
Client keystore	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Data Flow Probe

The files are located in the following directory: **<Data Flow Probe Installation Path>\DataFlowProbe\conf\security.**

Entity	File Name/Term	Password/Term	Alias
Probe keystore	MAMKeyStoreExp.jks (pKeyStoreFile)	logomania (pKeyStorePass)	mam
Data Flow Probe uses the **cKeyStoreFile** keystore as the default keystore during the mutual authentication procedure. This is a client keystore that is part of the UCMDB installation.			
Probe truststore	MAMTrustStoreExp.jks (pTrustStoreFile)	logomania (pTrustStorePass)	mam (default trusted entry)
The **cKeyStorePass** password is the default password of **cKeyStoreFile**.			

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 Data Flow Probe Installation Guide (Application Performance Management 9.30)

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 SW-Doc@hpe.com.

We appreciate your feedback!