

HP Discovery and Dependency Mapping Inventory

For the Windows® operating system

Software Version: 9.30

Store and Forward Server Guide

Manufacturing Part Number: None

Document Release Date: February 2011

Software Release Date: February 2011



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 1993-2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

Windows™ Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

UNIX® is a registered trademark of The Open Group.

Support

You can visit the HP Software Support web site at:

www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract. To find more information about support access levels, go to the following URL:

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

To register for an HP Passport ID, go to the following URL:

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

HP Discovery and Dependency Mapping Inventory

Store and Forward Server Guide

Software version: 9.30 / February 2011

This document provides an overview of the new Store and Forward server feature in Discovery and Dependency Mapping Inventory (DDM Inventory) version 9.30. It contains important information not included in the manuals or in the online help.

[Introduction](#)

[Installation](#)

[Uninstallation](#)

[How It Works](#)

[Configuration Options](#)

[Logging](#)

[Secure Communications via HTTPS](#)

[Bandwidth Throttling](#)

Introduction

The Store and Forward server is a standalone component of DDM Inventory that allows for more flexible inventory collection capabilities when running the scanners in the Manual Deployment mode. It is designed to facilitate the traversal of scan files through multiple firewalls until the scan files reach the DDM Inventory server that is going to process the collected inventory data.

Normally in the Manual Deployment mode, the Incoming directory of the XML Enricher is shared either via a network file share (Windows), HTTP (done out of the box) or FTP. The scanners are configured to save their off-site scan file to that UNC location or URL. In order for this to work, the managed device on which the scanners are running ought to be able to connect to the specified UNC path/URL directly. Unfortunately, in more complex deployment scenarios, this may not always be possible due to segmentation of the network or firewall restrictions. The chain of Store and Forward servers allows you to build an infrastructure that can move scan files through multiple firewalls until they finally reach the DDM Inventory server for processing.

The Store and Forward server works over one configurable TCP port and uses HTTP or HTTPS as the underlying network transport mechanism. It supports the forwarding of data to multiple locations, bandwidth throttling, and resumed file transfer between Store and Forward servers.

Installation

Windows (x86)

The Store and Forward server is packaged as an MSI file on Windows x86. The MSI is named **HP DDM Inventory Store and Forward Server (x86) 9.30.000.xxxx.msi**. You may install the Store and Forward server by double-clicking the MSI file and following the installation wizard. By default, the program is installed in the following location:

<ProgramFiles>\Hewlett-Packard\DDMI\9.30\Store and Forward

Table 1 – Windows installation

Subdirectory	Comment
bin	Contains Apache executable files and DLLs, as well as the Store and Forward server itself
conf	Contains the configuration files, including httpd.conf (the configuration file for Apache)
modules	Contains the Apache modules

The Windows service is registered with the following parameters:

Table 2 – Windows service parameters

Service attribute	Value
Apache Service Name	ovedApacheSF
Apache Display Name	HP DDMI Store and Forward Web Server
Apache Startup Type	Automatic
Store and Forward Service Name	ovedStoreAndForward
Store and Forward Display Name	HP DDMI Store and Forward Server
Store and Forward Startup Type	Automatic

The Store and Forward server uses a data directory to store various data, such as log files, and scan files that are in transit. By default, the directory is located in:

<ALLUSERSPROFILE>\Application Data\Hewlett-Packard\DDMI S&F

Under this directory, the Store and Forward server creates the following subdirectories:

Table 3 – Windows subdirectories

Subdirectory	Comment
Logs	Used for storing logs (Apache, Store and Forward server, etc.)

Incoming	Receives incoming files from scanners and/or other Store and Forward servers
InProgress	Contains the files that the server is currently working on
Status	Used to store status files recording the progress
Resume	Used to store files that are partially uploaded

Both the installation directory as well as the data directory can be configured in the installer screens to point to custom locations that are different from the defaults specified. The installer also allows the configuration of the following settings that affect the operation of the Store and Forward server:

- The TCP port that the server listens on
- The username and password to use for authentication
- The protocol to use:
 - HTTP: plain communications without encryption.
 - HTTPS: encrypted communications via SSL. Only one protocol can be selected at any one time.
 - The DNS host name of the Store and Forward server that will be recorded in the SSL certificate. This host name must then be used by other Store and Forward servers to send data to the current Store and Forward server. The host name is used in the URL instead of the IP.

Linux x86 (RHEL)

The Store and Forward server is packaged as a .tar.gz file on Linux x86. The file is named **hp-ddm-inventory-store-and-forward-linux-x86-9.30.000.xxxx.tar.gz**. The installation is performed as follows:

1. Create a local directory for the installation; for example, /usr/ddmi-saf.
2. Copy the .tar.gz file to the installation location.
3. Run the following command to decompress the archive:

```
tar -xzf hp-ddm-inventory-store-and-forward-linux-x86-9.30.000.xxxx.tar.gz
```

4. Run the following command as root (if not logged in as root already):

```
su root
```

5. Run the following command to set the current user to root (if not logged in as root already):

```
./configure
```



The installation directory must be the current directory when running the configure script.

The Store and Forward server automatically creates the startup/shutdown script **ddmisaf** in the standard system directory (/etc/init.d), and then registers this script to start the Store and Forward server on system boot. This script can also be used to start or stop the Store and Forward server manually. To do this, run the following commands as the root user:

- To start the Store and Forward server: **/etc/init.d/ddmisaf start**

- To restart the Store and Forward server: **/etc/init.d/ddmisaf restart**
- To stop the Store and Forward server: **/etc/init.d/ddmisaf stop**

Both the Apache web server and the Store and Forward server processes run under the daemon user account.

The directory structure under the ddmi-saf directory is as follows:

Table 4 – Linux installation

File name	Comment
bin	Contains Apache executable files and DLLs, as well as the Store and Forward server itself
conf	Contains the configuration files, including httpd.conf (the configuration file for Apache)
data	Data directory - used for storing files, logs, etc.
data/Logs	Used for storing logs (Apache, Store and Forward server, etc.)
data/Incoming	Receives incoming files from scanners and/or other Store and Forward servers
data/InProgress	Contains the file that the server is currently working on
data/Status	Used to store status files recording the progress
data/Resume	Used to store files that are partially uploaded
modules	Contains the Apache modules

The "configure" script allows the configuration of the following settings that affect the operation of the Store and Forward server:

- The TCP port that the server listens on
- The username and password to use for authentication
- The protocol to use:
 - HTTP: plain communications without encryption.
 - HTTPS: encrypted communications via SSL. Only one protocol can be selected at any one time.
 - The DNS host name of the Store and Forward server that will be recorded in the SSL certificate. This host name must then be used by other Store and Forward servers to send data to the current Store and Forward server.

Uninstallation

Windows (x86)

The Store and Forward server can be uninstalled manually by finding the entry "HP DDM Inventory Store and Forward Server (x86) 9.30.000.xxxx" in Add/Remove Programs (Windows Server 2003) or Programs and Features (Windows Server 2008) in Control Panel and clicking the **Remove** or **Uninstall** button.

Linux x86 (RHEL)

To uninstall the Store and Forward server on Linux x86, run the following commands:

1. `/sbin/chkconfig --del ddmisaf`
2. `rm -rf /etc/init.d/ddmisaf`

After running the previous commands, you may delete the installation files.



We recommend that you keep the certificates and configuration file (config.ini) in case the server is to be reinstalled.

How It Works

The DDM Inventory scanners should be configured to save their off-site scans to the following URL on the Store and Forward server:

```
http://<StoreAndForwardServer>:<port>/<channelname>
```

The Store and Forward server supports a concept of channels, where the data can be sent to using either HTTP or HTTPS. The channel appears as the top level directory on the Store and Forward server URL. By default, the server is configured with one channel called **ddmi**.

When such a scan file arrives into the Store and Forward server's channel, it gets queued for transfer. According to the channel's forwarding configuration, the file is then sent further to one or more other Store and Forward servers. Once the file is successfully sent to all destinations, it gets deleted. The final Store and Forward server in the chain needs to be installed on the computer running the DDM Inventory server and configured to forward files locally by moving them into the Incoming directory of the XML Enricher, where it will be processed.

The Store and Forward server supports resumed file transfers between Store and Forward servers. If the network connection is lost during data transfer, the partially uploaded file is kept on the upstream Store and Forward server (under <DataDir>\Resume\<ChannelName>) and at the next attempt the file transfer will be resumed from the place where the previous attempt stopped. This functionality is very useful when transferring large files over a slow or unreliable network.

Configuration Options

The configuration below is the printout of the config.ini file.

The Store and Forward server's behavior is configured using its configuration file, config.ini, located in the **conf** directory of the installation.

The following is a sample file that has two upstream Store and Forward servers configured, two channels, and three providers:

```
[Log]
filterLevel=default
rotateSizeMB=10
rotationFileCount=5

[BaseDirectories]
dataDir=C:\ProgramData\Hewlett-Packard\DDMI S&F\
incomingDir=C:\ProgramData\Hewlett-Packard\DDMI S&F\Incoming\

[Channels]
channel0=ddmi
channel1=hpca

[UpstreamProviders]
provider0=http://ddmi:ddm1passw0rd@ForwardS&Fserver1:5005/ddmi/
provider1=http://ddmi:ddm1passw0rd@ForwardS&Fserver2:5005/hpca/
provider2=http://ddmi:ddm1passw0rd@ForwardS&Fserver3>:5005/ddmi/

[ChannelMappings]
channel0=provider0,provider2
channel1=provider1

[StatusPage]
updateFrequencyMins=20
```

Table 5 – Config.ini keys

INI Key Name	Description
[Log] section	
filterLevel	Can be either default or debug . When debug is specified, more detailed logging is performed. This can be useful for troubleshooting.
rotateSizeMB	Specifies the size of each log file. The Store and Forward server can store the log information in several log files. Once the current log file size reaches its limit, it gets rolled into the next log file.
rotationFileCount	Specifies the number of log files to keep. When the current log file reaches its size limit, it gets rolled into the next log file. When the rotationFileCount is reached, the oldest log file is discarded.
[BaseDirectories] section	
dataDir	Specifies the location of the data directory. Normally, it is not necessary

	to modify this setting, as it gets configured automatically by the installer.
incomingDir	Specifies the location of the Incoming directory that receives incoming files. Normally, it is not necessary to modify this setting, as it gets configured automatically by the installer.
[Channels] section	
channelX	Specifies the name for each channel. Channel names are used to name the top level directory of the Store and Forward server. The corresponding physical directory is created under the Incoming directory of the Store and Forward server.
[UpstreamProviders] section	
providerX	<p>Specifies the URLs for upstream Store and Forward servers. The URL should include the HTTP username and password required to access the URL. When the HTTPS protocol is used, the host name of the Store and Forward server supplied in this URL must match the host name given during the installation of that Store and Forward server, as this host name is encoded in the HTTPS certificate.</p> <p>In addition to URLs for upstream Store and Forward servers, this key can also specify the full path to a local directory. In such cases, the received file is copied to that directory, or moved if the channel is mapped to only one upstream provider. This is the way the Store and Forward server, installed together with the DDM Inventory installation, should be configured. The only provider on it should be the incoming directory of the XML Enricher, as all files received by this Store and Forward server will be moved automatically to the Incoming directory of the XML Enricher.</p>
[ChannelMapping] section	
channelX	Specifies how the files arriving to this channel will be forwarded. One or more upstream Store and Forward servers from the [UpstreamProviders] section should be specified. Multiple servers are separated with commas.
[StatusPage] section	
updateFrequencyMins	Specifies how frequently (in minutes) the status page is updated. The default is 20. If the setting is set to 0 , the status page is not updated.

The sample INI file shown above has two channels – ddmi and hpca. The data sent to the ddmi channel is forwarded to the upstream Store and Forward servers ForwardS&Fserver1 and ForwardS&Fserver3, while data sent to the hpca channel is forwarded to the ForwardS&Fserver2 server.

The INI key names used in the [Channels], [UpstreamProviders], and [ChannelMapping] sections of the INI file do not have to follow the naming convention provided in this example. They can be any reasonable names (i.e. not containing any spaces or equal sign characters).

Whenever the providers and mappings specified in the configuration file are updated, the Store and Forward server recognizes that fact, and uses the new configuration for all new files. For the files that are currently in progress but not being sent yet, the Store and Forward server will validate their currently scheduled route as follows:

- If there are new providers configured, they will not take effect. They will only take effect for those files that the server will be receiving from that moment onwards.
- If there is a provider deleted, the Store and Forward server will not attempt to send the file to such a deleted provider.
- If the URL for the existing provider has changed, it will be used when the time comes to transfer the file.

In order for the changes to other settings to take effect, the Store and Forward server needs to be restarted. For example, from a command prompt, run the following commands:

- Windows:
`net stop ovedStoreAndForward`
`net start ovedStoreAndForward`
- Linux:
`/etc/init.d/ddmisaf restart`

Logging

As the Store and Forward server has no UI, any troubleshooting or status information is available in its log files, located in the <DataDir>\Logs directory. There are three log files available:

- webaccess.log: Apache Access log showing all URLs accessed on the web server.
- weblog.log: Collects other Apache log messages.
- storeNforward.log: Contains the log messages produced by the Store and Forward server itself.

Status Information

The Store and Forward server maintains a file showing various statistics and health information. It can be accessed via the following URL:

`http://<StoreAndForwardServer>:<port>/server_status.xml`

If HTTPS is used for communication, http needs to be replaced with https in the URL. When accessed via a browser, the status page shows a human readable web page with the statistics as follows:

Disk Usage	
Location	Usage
Status Directory	0 Bytes
Incoming Directory	0 Bytes
InProgress Directory	0 Bytes
Resume Directory	0 Bytes
Total Free Diskspace	47.39 GB

File Counts	
Location	File Count
Incoming Files	0
InProgress Files	0
Resume Files	0

Last updated: 12/22/10 08:23:30

The file can also be accessed by external programs or scripts to extract the latest status/health information. The file resembles the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="server_status.xsl"?>
<StoreAndForwardStatus version="1.0">
  <statusDirBytes>0</statusDirBytes>
  <incomingDirBytes>0</incomingDirBytes>
  <inProgressDirBytes>0</inProgressDirBytes>
  <resumeDirBytes>0</resumeDirBytes>
  <freeDiskSpaceBytes>50882215936</freeDiskSpaceBytes>
  <numIncomingFiles>0</numIncomingFiles>
  <numInProgressFiles>0</numInProgressFiles>
  <numResumeFiles>0</numResumeFiles>
  <modifiedTime>12/22/10 08:23:30</modifiedTime>
</StoreAndForwardStatus>
```

Secure Communications via HTTPS

When using HTTPS for secure communication, the following specifics apply:

- During the installation phase, the installer automatically generates the self-signed certificates/keys required for SSL communication with this server. The files `server.crt` and `server.key` are created in the `<DataDir>\Cert` directory of the Store and Forward server. If on subsequent installations the same data directory is selected, the initially generated certificates/keys are preserved.
- "http" needs to be changed to "https" in the provider URLs.
- The **forward_S&F_serverX** host name must match the host name used when installing that Store and Forward server (to match the name recorded in its SSL certificate).
- All certificates from the upstream Store and Forward servers must be manually copied to the downstream Store and Forward server and concatenated together in the file called `<DataDir>Cert\trustedcerts.crt`. Using the example of the configuration file above, the following needs to be done:
 - The `<DataDir>\Cert\server.crt` file from `forward_S&F_server1` needs to be copied to the current Store and Forward server as `server1.crt`.
 - The `<DataDir>\Cert\server.crt` file from `forward_S&F_server2` needs to be copied to the current Store and Forward server as `server2.crt`.
 - The `<DataDir>\Cert\server.crt` file from `forward_S&F_server3` needs to be copied to the current Store and Forward server as `server3.crt`.
 - The certificates can then be combined together as follows:

```
copy /b server1.crt + server2.crt + server3.crt trustedcerts.crt
```
 - The obtained `trustedcerts.crt` file should be copied to the `<DataDir>\Cert` directory. This ensures that the current Store and Forward server has all the certificates of the servers that it needs to send the data to available, so that it can successfully communicate with these Store and Forward servers via HTTPS.

Bandwidth Throttling

The Store and Forward server includes the ability to limit the bandwidth used by all uploads made to the server via a simple change to the Apache configuration file. To do this, perform the following steps:

1. Find the Apache configuration file in the following location:

```
<InstallDir>\httpd.conf
```

2. Locate and change the following line in the file:

```
saftwInputLimit 0
```

By default, this setting is set to **0** (meaning that no throttling is performed). If set to a non-zero value, it specifies the maximum bandwidth (in kilobytes per second) that will be consumed by the server for all uploads going to it.

3. Restart the Apache Web server so that the configuration change takes effect. For example, from a command prompt, run the following commands:

- Windows:
net stop ovedApacheSF
net start ovedApacheSF
- Linux:
<installdir>/bin/apachectl restart