Technical white paper

# HPDM Embedded HTTPS Server Deployment Guide

## HP Device Manager 4.7

## Table of contents

Overview ... 2
Installation ... 2
Hardware environment ... 2
Network environment ... 2
Installing HPDM Embedded HTTPS Server ... 2
Configuration ... 5
User management ... 5
Port management ... 5
Root path ... 5
Certificate configuration ... 6
CA Certificate Trust List ... 6
Server certificate management ... 6
Importing a server certificate ... 7
Resetting a server certificate and key ... 7
Deploying the CA CTL to HPDM ... 7
Client certificate management ... 7
Configuring client authentication on the HPDM Embedded HTTPS Server side ... 7
Deploying a client certificate to HPDM components ... 9
Performance ... 9
Recommended performance data ... 9
Maximum number of connections ... 9
Capturing large files and images ... 9
Deploying large files and images ... 9
Managing the maximum number of connections ... 10
Hardware performance ... 11
Bandwidth throttling ... 12
Configuring the bandwidth throttling parameters ... 13
Adding an HPDM Embedded HTTPS Server as an HPDM Repository ... 13
For more information ... 14

# Overview

The purpose of this document is to assist customers with the installation and configuration of HPDM Embedded HTTPS Server, a component of the HP Device Manager (HPDM) solution. This document focuses on setting up an HTTPS repository. It also includes useful tips to fine-tune the performance of HPDM Embedded HTTPS Server, such as how to implement bandwidth throttling.

# Installation

## Hardware environment

The following table provides the supported operating systems and both the minimum and recommended hardware requirements of HPDM Embedded HTTPS Server.

| Operating system | Minimum hardware | Recommended hardware |
|---|---|---|
| • Windows® Server 2008 x64<br>• Windows Server 2008 R2 x64<br>• Windows Server 2012 x64<br>• Windows Server 2012 R2 x64 | • Intel® Core™ 2 or AMD Athlon 64 processor 2 GHz<br>• 2 GB RAM<br>• 2 GB free disk space<br>• 100 Mbps NIC | • Intel Core i5 quad-core processor 2.5 GHz or higher<br>• 4 GB RAM<br>• 20 GB free disk space<br>• 1000 Mbps NIC |

## Network environment

There are many network factors that might influence the deployment of HPDM Embedded HTTPS Server, such as the network bandwidth or whether related devices are deployed on a subnet.

HPDM Embedded HTTPS Server must be deployed on the same system with either with HPDM Master Repository or a HPDM Child Repository.

HP recommends deploying a HPDM Child Repository that has HTTPS support as close to its related devices as possible.

## Installing HPDM Embedded HTTPS Server

Before installing HPDM Embedded HTTPS Server, copy the installation files to the server.

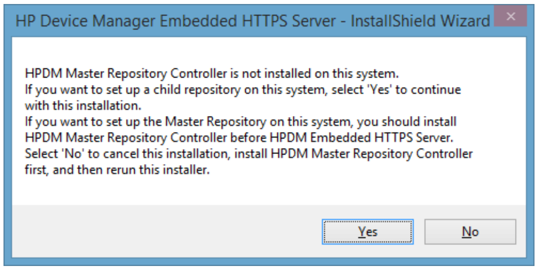
To run the installation file:

1. Right-click the HPDM Embedded HTTPS Server setup file and select **Run as administrator**.

   –or–

   From an Administrator command prompt, enter `HPDMEmbedHTTPSServer_x.x.3690.xxxxx.exe`.

2. If HPDM Master Repository Controller is not installed on this system, the following message appears.

   
   HP Device Manager Embedded HTTPS Server - InstallShield Wizard
   Yes
   No

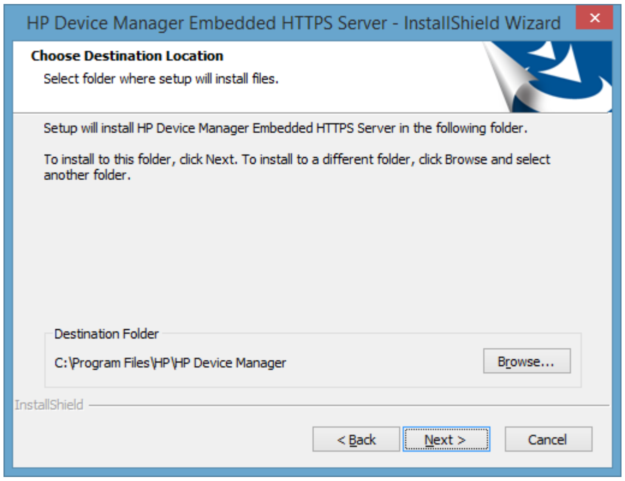
   HPDM Master Repository Controller is not installed on this system.
   If you want to set up a child repository on this system, select 'Yes' to continue with this installation.
   If you want to set up the Master Repository on this system, you should install HPDM Master Repository Controller before HPDM Embedded HTTPS Server.
   Select 'No' to cancel this installation, install HPDM Master Repository Controller first, and then rerun this installer.

   If you want to install a child repository on this system, select **Yes** and continue the installation.

   If you want to install HPDM Master Repository Controller on this system, select **No**, install HPDM Master Repository Controller, and then restart this procedure.

3. Select **Next**.
4. Accept the software license agreement, and then select **Next**.
5. If the operating system is supported, select **Yes**.

6. Specify the folder to install HPDM Embedded HTTPS Server to, and then select **Next**.



HP Device Manager Embedded HTTPS Server - InstallShield Wizard

**Choose Destination Location**

Select folder where setup will install files.

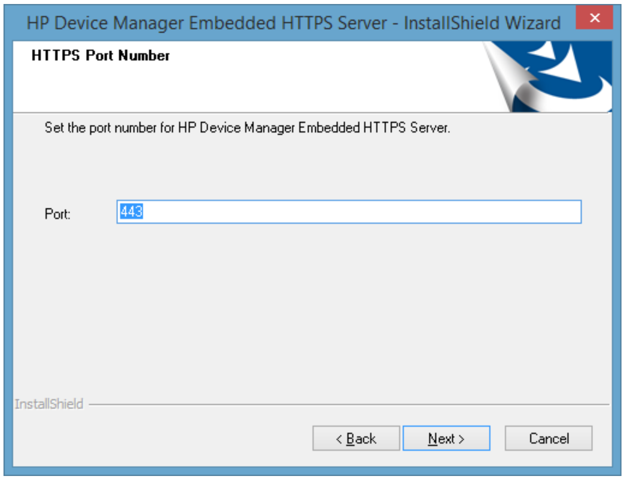
Setup will install HP Device Manager Embedded HTTPS Server in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\HP\HP Device Manager

7. On the HTTPS Port Number page, enter the HTTPS port, and then select **Next**. The default port is 443.



HP Device Manager Embedded HTTPS Server - InstallShield Wizard

**HTTPS Port Number**

Set the port number for HP Device Manager Embedded HTTPS Server.

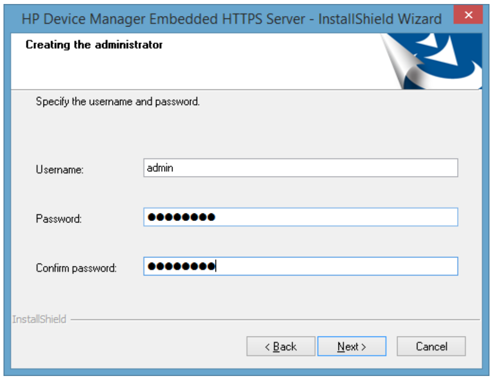
Port: 443

**Note**

An error message appears if the wizard detects that another program is using this port.

If you change the HTTPS port number, you also must update the port number for the HTTPS Repository in HPDM Console.

8. Enter a **Username** and **Password** for the administrator account for HPDM Embedded HTTPS Server, and then enter the same password in the **Confirm Password** box. Select **Next**.



HP Device Manager Embedded HTTPS Server - InstallShield Wizard

**Creating the administrator**

Specify the username and password.

Username: admin

Password: ●●●●●●●●

Confirm password: ●●●●●●●●

**Note**

The username must meet the following requirements:

– Cannot be blank

– Cannot be longer than 19 characters

– Case sensitive

– Can only contain letters (a–z, A–Z), numbers (0–9), hyphens (-), underscores (_), at symbol (@), and periods (.)

– Must contain at least one letter or number

– Cannot begin or end with a symbol (hyphen, underscore, at symbol, period)

– Cannot contain two or more consecutive symbols (hyphen, underscore, at symbol, period)

– Cannot contain more than two at symbols

**Note**
The password must be between 8 and 19 characters long and contain at least three of the following:

– Uppercase letters (A–Z)

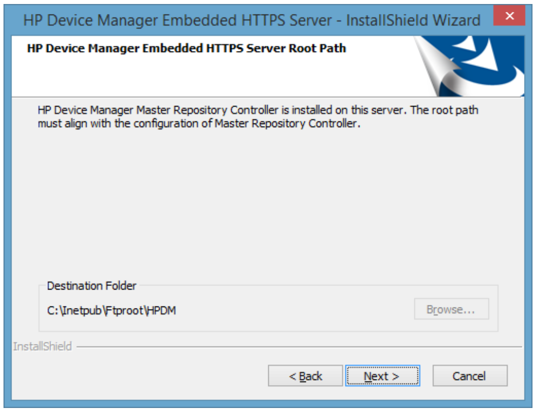
– Lowercase letters (a–z)

– Numbers (0–9)

– Symbols found on the keyboard (characters other than letters, numbers, or spaces)

9. Specify the root path of HPDM Embedded HTTPS Server, and then select **Next**.

   If HPDM Master Repository Controller is installed on the same server, the installation uses the root path of HPDM Master Repository by default.



HP Device Manager Embedded HTTPS Server - InstallShield Wizard

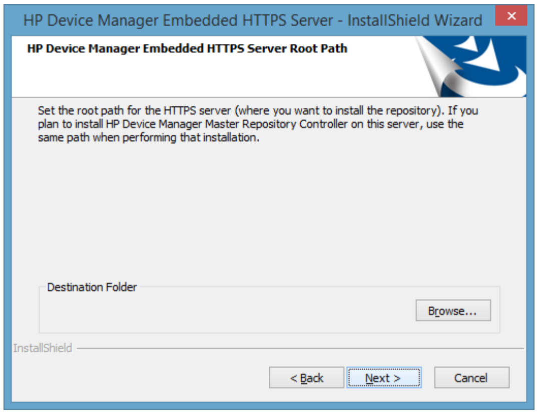
**HP Device Manager Embedded HTTPS Server Root Path**

HP Device Manager Master Repository Controller is installed on this server. The root path must align with the configuration of Master Repository Controller.

Destination Folder

C:\Inetpub\Ftproot\HPDM

   If HPDM Master Repository Controller is not installed on the same server, select **Browse**, and then navigate to the root path.



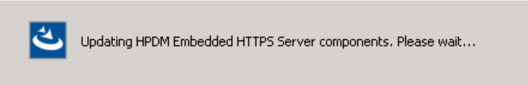
HP Device Manager Embedded HTTPS Server - InstallShield Wizard

**HP Device Manager Embedded HTTPS Server Root Path**

Set the root path for the HTTPS server (where you want to install the repository). If you plan to install HP Device Manager Master Repository Controller on this server, use the same path when performing that installation.

Destination Folder

10. Verify that all settings are correct, and then select **Next**.
11. The component updates. After the installation process is complete, select **Finish**.



Updating HPDM Embedded HTTPS Server components. Please wait...

The HPDM Embedded HTTPS Server installation log is saved in C:\HP Device Manager Embedded HTTPS Server-install.log.

# Configuration

## User management

During the installation process, you created an administrator user account for HPDM Embedded HTTPS Server; after the installation, this is the only active account and has full access permissions for the repository. The username and password of the administrator account were specified during installation.

In addition to installing HPDM Embedded HTTPS Repository, the procedure installs a User Management Tool that provides methods to update the username and password for the local administrator of HPDM Embedded HTTPS Server.

To update the username and password:

1. Select **Start**, select **All Programs**, select **HP**, select **HP Device Manager**, select **HP Device Manager Embedded HTTPS Server**, select **HPDM Embedded HTTPS Server Tools**, and then select **HPDM Embedded HTTPS Server User Management Tool**.
2. On the command console, enter the following command:

   ```
   HTTPSServerAccount -update <username>
   ```
3. When prompted, enter the new password.

**Note**
After changing the account password for HPDM Embedded HTTPS Repository using the User Management Tool, you also must update the username and password for HPDM Embedded HTTPS Repository in HPDM Console.

## Port management

You must specify the port number for the HTTPS service during HPDM Embedded HTTPS Server installation. By default, this number is 443. If the default port 443 or the port you entered is used by another program, you must select a different port.

After the installation is complete, you can use HPDM Embedded HTTPS Server Configuration Tool to change the port for the HTTPS service.

To change the port:

1. Select **Start**, select **All Programs**, select **HP**, select **HP Device Manager**, select **HP Device Manager Embedded HTTPS Server**, select **HPDM Embedded HTTPS Server Tools**, and then select **HPDM Embedded HTTPS Server Configuration Tool**.
2. On the command console, enter the following command:

   ```
   HTTPSServerConfig -port <portnumber>
   ```

**Note**
After changing the port configuration of HPDM Embedded HTTPS Repository, you also must update the port number for HPDM Embedded HTTPS Repository in HPDM Console.

## Root path

The root path points to the location where HPDM Embedded HTTPS Server is installed. During the HPDM Embedded HTTPS Server installation, set the root path for HPDM Embedded HTTPS Server as follows:

- If HPDM Master Repository Controller is installed on the same server, the root path of HPDM Embedded HTTPS Server must be the same location as HPDM Master Repository Controller.
- If HPDM Master Repository Controller is not installed on the same server, enter a root path for HPDM Embedded HTTPS Server.
- If you install HPDM Master Repository Controller after HPDM Embedded HTTPS Server on the same server, use the same root path to install HPDM Master Repository Controller after HPDM Embedded HTTPS Server.

After the installation is complete, you can use HPDM Embedded HTTPS Server Configuration Tool to change the root path for HTTPS Server.

To change the root path:

1. Select **Start**, select **All Programs**, select **HP**, select **HP Device Manager**, select **HP Device Manager Embedded HTTPS Server**, select **HPDM Embedded HTTPS Server Tools**, and then select **HPDM Embedded HTTPS Server Configuration Tool**.
2. On the command console, enter the following command:

   ```
   HTTPSServerConfig -rootpath rootpath
   ```

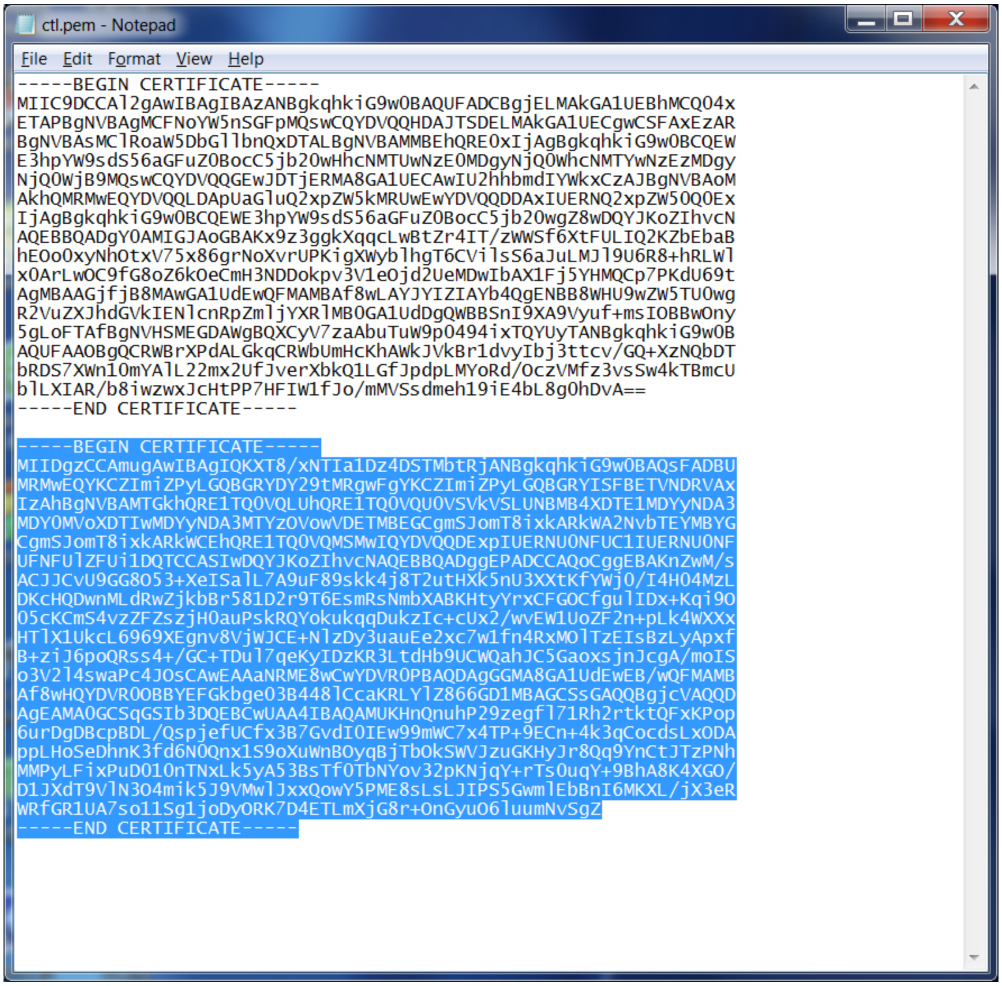
# Certificate configuration

HPDM Embedded HTTPS Server and all HPDM components support only Privacy Enhanced Mail (PEM) format certificates and keys. For other certificate formats, such as .pfx and .der, you can use the openssl tool to convert the certificate to PEM format.

To use the openssl tool, go to `<HPDM Embedded HTTPS Server install path>\HP Device Manager\Embedded HTTPS Server\Apache24\bin`.

## CA Certificate Trust List

In HPDM, the CA Certificate Trust List (CTL) is a file containing multiple certificates in PEM format. This file is used to verify peer certificates. The following is an example of a CTL file.



```
-----BEGIN CERTIFICATE-----
MIIC9DCCAl2gAwIBAgIBAzANBgkqhkiG9w0BAQUFADCBgjELMAkGA1UEBhMCQ04x
ETAPBgNVBAgMCFNoYW5nSGFpMQswCQYDVQQHDAJTSDELMAkGA1UECgwCSFAxEzAR
BgNVBAsMClRoaW5DbGllbnQxDTALBgNVBAMMBEhQRE0xIjAgBgkqhkiG9w0BCQEW
E3hpYW9sdS56aGFuZ0BocC5jb20wHhcNMTUwNzE0MDgyNjQ0WhcNMTYwNzEzMDgy
NjQ0WjB9MQswCQYDVQQGEwJDTjERMA8GA1UECAwIU2hhbmdIYWkxCzAJBgNVBAoM
AkhQMRMwEQYDVQQLDApUaGluQ2xpZW5kMRUwEwYDVQQDDAxIUERNQ2xpZW50Q0Ex
IjAgBgkqhkiG9w0BCQEWE3hpYW9sdS56aGFuZ0BocC5jb20wgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAKx9z3ggkXqqcLwBtZr4IT/zWWSf6XtFULIQ2KZbEbaB
hEOo0xyNhOtxV75x86grNoXvrUPKigXWyblhgT6CVilsS6aJuLMJl9U6R8+hRLWl
x0ArLwOC9fG8oZ6kOeCmH3NDDokpv3V1eOjd2UeMDwIbAX1Fj5YHMQCp7PKdU69t
AgMBAAGjfjB8MAwGA1UdEwQFMAMBAf8wLAYJYIZIAYb4QgENBB8WHU9wZW5TU0wg
R2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1UdDgQWBBSnI9XA9Vyuf+msIOBBwOny
5gLoFTAfBgNVHSMEGDAWgBQXCyV7zaAbuTuW9p0494ixTQYUyTANBgkqhkiG9w0B
AQUFAAOBgQCRWBrXPdALGkqCRWbUmHcKhAWkJVkBr1dvyIbj3ttcv/GQ+XzNQbDT
bRDS7XWn1OmYAlL22mx2UfJverXbkQ1LGfJpdpLMYoRd/OczVMfz3vsSw4kTBmcU
blLXIAR/b8iwzwxJcHtPP7HFIW1fJo/mMVSsdmeh19iE4bL8g0hDvA==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIDgzCCAmugAwIBAgIQKXT8/xNTIa1Dz4DSTMbtRjANBgkqhkiG9w0BAQsFADBU
MRMwEQYKCZImiZPyLGQBGRYDY29tMRgwFgYKCZImiZPyLGQBGRYISFBETVNDRVAx
IzAhBgNVBAMTGkhQRE1TQ0VQLUhQRE1TQ0VQU0VSVkVSLUNBMB4XDTE1MDYyNDA3
MDY0MVoXDTIwMDYyNDA3MTYzOVowVDETMBEGCgmSJomT8ixkARkWA2NvbTEYMBYG
CgmSJomT8ixkARkWCEhQRE1TQ0VQMSMwIQYDVQQDExpIUERNU0NFUC1IUERNU0NF
UFNFUlZFUi1DQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnZwM/s
ACJJCvU9GG8O53+XeISalL7A9uF89skk4j8T2utHXk5nU3XXtKfYWj0/I4H04MzL
DKcHQDwnMLdRwZjkbBr581D2r9T6EsmRsNmbXABKHtyYrxCFGOCfgulIDx+Kqi9O
O5cKCmS4vzZFZszjH0auPskRQYokukqqDukzIc+cUx2/wvEW1UoZF2n+pLk4WXXx
HTlX1UkcL6969XEgnv8VjWJCE+NlzDy3uauEe2xc7w1fn4RxMOlTzEIsBzLyApxf
B+ziJ6poQRss4+/GC+TDul7qeKyIDzKR3LtdHb9UCWQahJC5GaoxsjnJcgA/moIS
o3V2l4swaPc4JOsCAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMB
Af8wHQYDVR0OBBYEFGkbge03B448lCcaKRLYlZ866GD1MBAGCSsGAQQBgjcVAQQD
AgEAMA0GCSqGSIb3DQEBCwUAA4IBAQAMUKHnQnuhP29zegfl71Rh2rtktQFxKPop
6urDgDBcpBDL/QspjefUCfx3B7GvdI0IEw99mWC7x4TP+9ECn+4k3qCocdsLxODA
ppLHoSeDhnK3fd6N0Qnx1S9oXuWnBOyqBjTbOkSWVJzuGKHyJr8Qq9YnCtJTzPNh
MMPyLFixPuD01OnTNxLk5yA53BsTf0TbNYov32pKNjqY+rTs0uqY+9BhA8K4XGO/
D1JXdT9VlN3O4mik5J9VMwlJxxQowY5PME8sLsLJIPS5GwmlEbBnI6MKXL/jX3eR
WRfGR1UA7so11Sg1joDyORK7D4ETLmXjG8r+OnGyuO6luumNvSgZ
-----END CERTIFICATE-----
```

To verify a certificate, the CTL file must contains its CA certificates.

To create a CTL file:

1. If the certificate is a self-signed certificate, copy its PEM-format certificate content to the CTL file.
2. If the certificate is available in a CA chain, copy all CA certificates on the CA chain to the CTL file.
3. If you want to verify several certificates with one CTL file, repeat steps 1 and 2 to copy all CA certificates to one CTL file.

## Server certificate management

The default server certificate and key are deployed on the HDPM Embedded HTTPS Server side during installation.

All HTTPS Servers use the same certificate, by default. There are backups of the default certificate and key stored on HTTPS Server.

After the installation completes, HP recommends that you import your own certificate via HPDM Embedded HTTPS Server Configuration Tool.

### Importing a server certificate

1. Select **Start**, select **All Programs**, select **HP**, select **HP Device Manager**, select **HP Device Manager Embedded HTTPS Server**, select **HPDM Embedded HTTPS Server Tools**, and then select **HPDM Embedded HTTPS Server Configuration Tool**.
2. On the command console, enter the following command:

   ```
   HTTPSServerConfig -importcert <certificatefile> <keyfile>
   ```

**Note**

HPDM Embedded HTTPS Server does not support PEM files that use a password.

### Resetting a server certificate and key

1. Select **Start**, select **All Programs**, select **HP**, select **HP Device Manager**, select **HP Device Manager Embedded HTTPS Server**, select **HPDM Embedded HTTPS Server Tools**, and then select **HPDM Embedded HTTPS Server Configuration Tool**.
2. On the command console, enter the following command:

   ```
   HTTPSServerConfig –resetcert
   ```

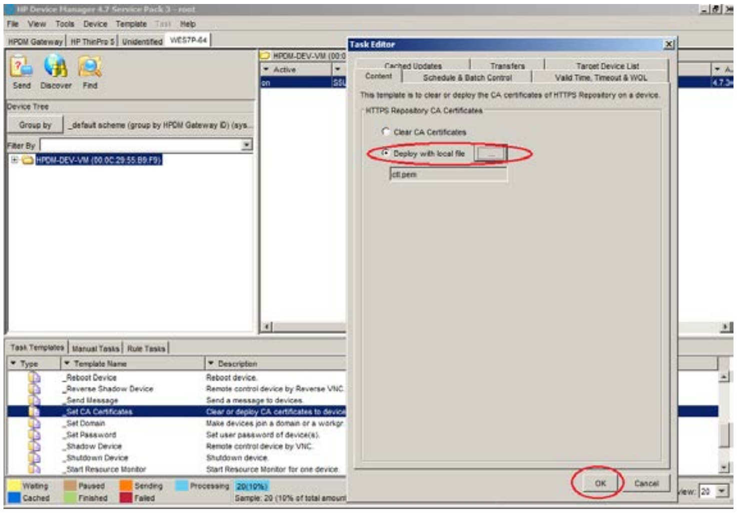
**Note**

If you import a new server certificate or revert to the default certificate, you must update the CA CTL for all client devices.

### Deploying the CA CTL to HPDM

To verify the server certificate when HPDM components connect to HPDM Embedded HTTPS Server, you must create a CTL file for your server certificate first, and then deploy this CTL file to HPDM components. Otherwise, HPDM does not authenticate the server certificate and accepts the connection automatically. In HPDM, the name of this CTL file is **ctl.pem** and cannot be changed.

1. For HPDM Console, HPDM Gateway, and HPDM Master Repository Controller, manually copy the **ctl.pem** file to `%HPDMInstallPath%\Certificates\repos_certs\https\`.
2. If the components are installed on separate machines, you need to copy it several to each system.
3. From HPDM Agent, send a "**Set CA Certificates**" template to each thin client. Select the **Deploy with local file** option, and then select the file **ctl.pem**.



| Type | Template Name | Description |
|---|---|---|
| | _Reboot Device | Reboot device. |
| | _Reverse Shadow Device | Remote control device by Reverse VNC. |
| | _Send Message | Send a message to devices. |
| | _Set CA Certificates | Clear or deploy CA certificates to device |
| | _Set Domain | Make devices join a domain or a workgr |
| | _Set Password | Set user password of device(s). |
| | _Shadow Device | Remote control device by VNC. |
| | _Shutdown Device | Shutdown device. |
| | _Start Resource Monitor | Start Resource Monitor for one device. |

This template is to clear or deploy the CA certificates of HTTPS Repository on a device.

HTTPS Repository CA Certificates

○ Clear CA Certificates

● Deploy with local file ...

ctl.pem

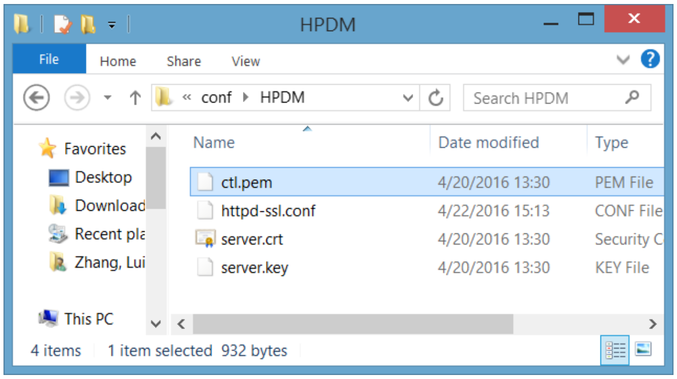
## Client certificate management

There is no client certificate or key on the client side, by default. That means the client connects the HPDM Embedded HTTPS Server directly.

### Configuring client authentication on the HPDM Embedded HTTPS Server side

If your deployment requires to the server to verify the client certificate, use the following procedure:

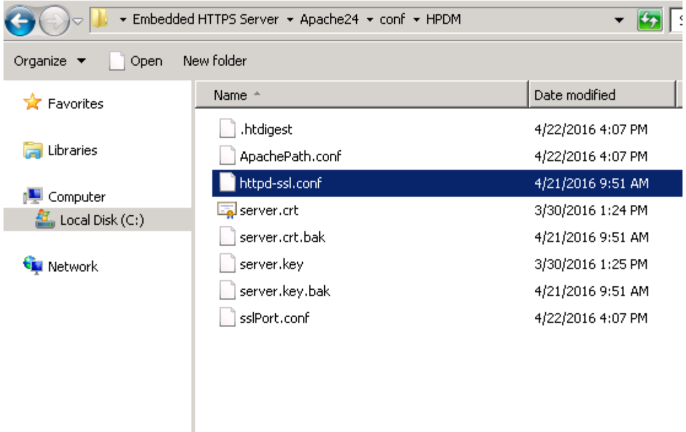
1. Create a CTL file for the client certificate and copy it to `<HPDM Embedded HTTPS Server install path>\HP Device Manager\Embedded HTTPS Server\Apache24\conf\HPDM`. The CTL file name must be named **ctl.pem**.



| Name | Date modified | Type |
|---|---|---|
| ctl.pem | 4/20/2016 13:30 | PEM File |
| httpd-ssl.conf | 4/22/2016 15:13 | CONF File |
| server.crt | 4/20/2016 13:30 | Security C |
| server.key | 4/20/2016 13:30 | KEY File |

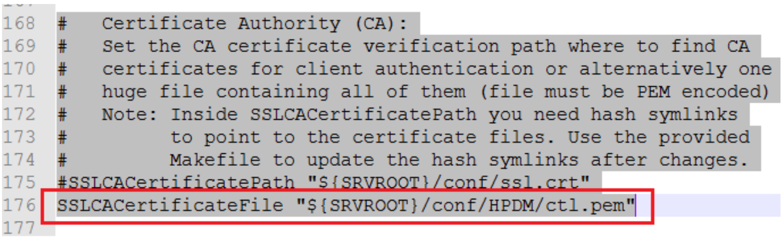
2. To configure the certificate authentication of HTTPS client, modify the SSL configuration on HPDM Embedded HTTPS Server.

   A. Locate the file `httpd-ssl.conf`. By default, this file is saved in the following location: `<HPDM Embedded HTTPS Server install path>\HP Device Manager\Embedded HTTPS Server\Apache24\conf\HPDM`

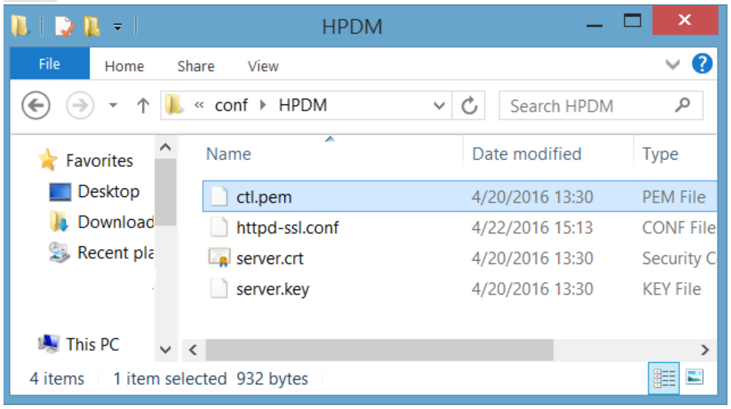


| Name | Date modified |
|---|---|
| .htdigest | 4/22/2016 4:07 PM |
| ApachePath.conf | 4/22/2016 4:07 PM |
| httpd-ssl.conf | 4/21/2016 9:51 AM |
| server.crt | 3/30/2016 1:24 PM |
| server.crt.bak | 4/21/2016 9:51 AM |
| server.key | 3/30/2016 1:25 PM |
| server.key.bak | 4/21/2016 9:51 AM |
| sslPort.conf | 4/22/2016 4:07 PM |

   B. Edit the configuration file. By default, the line **SSLCACertificateFile** is a comment. Make it not a comment, and then save the file.



```
#   Certificate Authority (CA):
#   Set the CA certificate verification path where to find CA
#   certificates for client authentication or alternatively one
#   huge file containing all of them (file must be PEM encoded)
#   Note: Inside SSLCACertificatePath you need hash symlinks
#         to point to the certificate files. Use the provided
#         Makefile to update the hash symlinks after changes.
#SSLCACertificatePath "${SRVROOT}/conf/ssl.crt"
SSLCACertificateFile "${SRVROOT}/conf/HPDM/ctl.pem"
```



| Name | Date modified | Type |
|---|---|---|
| ctl.pem | 4/20/2016 13:30 | PEM File |
| httpd-ssl.conf | 4/22/2016 15:13 | CONF File |
| server.crt | 4/20/2016 13:30 | Security C |
| server.key | 4/20/2016 13:30 | KEY File |

3. Restart the HPDM Embedded HTTPS Server service.

#### Deploying a client certificate to HPDM components

1. Verify that the client certificate name is client.pem and the private key name is client.key.

   **Note**
   Currently, HPDM supports only PEM format certificates and keys. For other certificate formats, such as .pfx and .der, you can use the openssl tool to transfer them to PEM format.

2. To deploy the files to HPDM Console, HPDM Gateway and HPDM Master Repository Controller:
   A. Copy client.pem and client.key to the folder `%HPDMInstallPath%\Certificates\repos_certs\https\`.
   B. To deploy the password for the client key, open a command prompt, change the current path to `%HPDMInstallPath%\Certificates\`, and then run the command `dmenc <password> -h` where `<password>` is the password of the private key.

      For example, if the password is HPDM, run the command `dmenc HPDM -h`.
3. To deploy the files to HPDM Agents running a Windows Embedded operating system:
   A. Copy client.pem and client.key to the folder `c:\windows\xpeagent\repos_certs\https\`.
   B. To deploy the password for the private key, send the following script task to the devices via HPDM:
      ```
      c:\windows\xpeagent\dmenc <password> -h
      ```
4. To deploy the files to HPDM Agents running HP ThinPro:
   A. Copy client.pem and client.key to the folder `/etc/hpdmagent/repos_certs/https/`.
   B. To deploy the password for the private key, send the following script task to the devices via HPDM:
      ```
      /usr/sbin/dmenc <password> -h
      ```

# Performance

There are many factors which impact performance, such as disk, CPU, RAM size, and so on. The suggested minimum hardware only ensures HPDM Embedded HTTPS Server can run on the machine, but the performance is very poor. HP recommends that you deploy HPDM Embedded HTTPS Server on a machine with the recommended hardware requirement or higher. This following sections describe the performance with the recommended hardware and how to tune the configuration or hardware to achieve maximum performance.

## Recommended performance data

The following performance data was obtained from a system running the recommended hardware configuration: 4 GB RAM, quad-core CPU, 1000 Mbps NIC, and 7200 RPM disk. The operating system used during testing was Windows Server 2008 R2 x64.

### Maximum number of connections

By default, the maximum number of connections is 64. This is an ideal value. The performance of HPDM Embedded HTTPS Repository degrades, if this number is raised too high for the supporting hardware configuration. For most configurations, HP recommends setting the number of concurrent connections to no more than 50.

### Capturing large files and images

Due to the I/O speed of the storage device (hard disk), performance can be compromised when capturing large files or images from multiple thin clients at the same time. The following are the recommended usage parameters when capturing large files or images.

- The total upload speed must not exceed 10 MBps.
- The recommended maximum concurrent connections is 5, and the upload bandwidth for each connection must not exceed 2 MBps.

  For example, if you want to capture images from 10 devices, you can send the capturing image task to 5 devices at first with the upload bandwidth set to 2 MBps. After those 5 tasks are finished, send the task to other 5 devices with the upload bandwidth set to 2 MBps.

For information regarding how to configure the bandwidth, see Bandwidth throttling.

### Deploying large files and images

The following are the recommended usage parameters for deploying large files and images.

If you are deploying the same file, folder, or image file to multiple devices, do the following:

- If the number of target devices does not exceed 50, deploy the same file, folder, or image file to all devices at the same time.
- If the number of target devices exceed 50, divide the target devices into batches, with the number of devices in each batch fewer than 50. Then, send the task to the devices batch by batch. Do not send the task to next batch until all tasks in the previous batch are finished.

If you are deploying different files, folders, or image files to different devices, do the following:

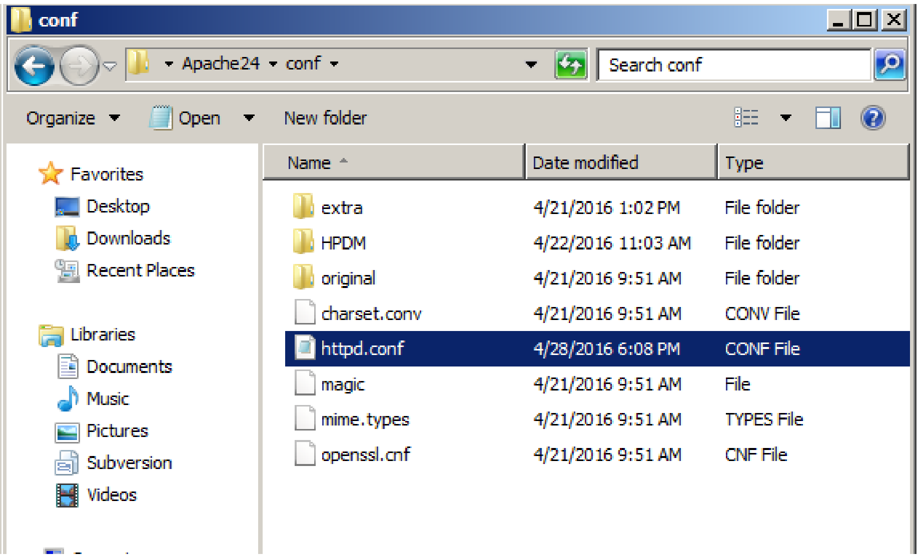
- Divide the target devices into different scenarios that would be used for targeting a single device. Execute each scenario one by one following the previous steps.

## Managing the maximum number of connections

By default, the maximum number of connections is 64. If you installed HPDM Embedded HTTPS Server on a more powerful machine, such as a workstation or server with greater disk I/O performance, you can modify this number to achieve the maximum performance of the hardware.

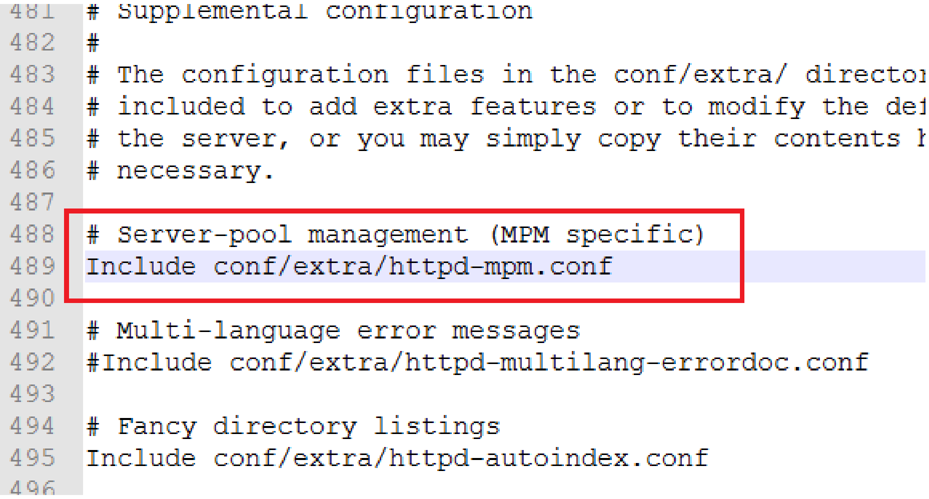
1. Locate the file `httpd.conf`. By default, it is saved in the following location:

   `<HPDM Embedded HTTPS Server install path>\HP Device Manager\Embedded HTTPS Server\Apache24\conf`



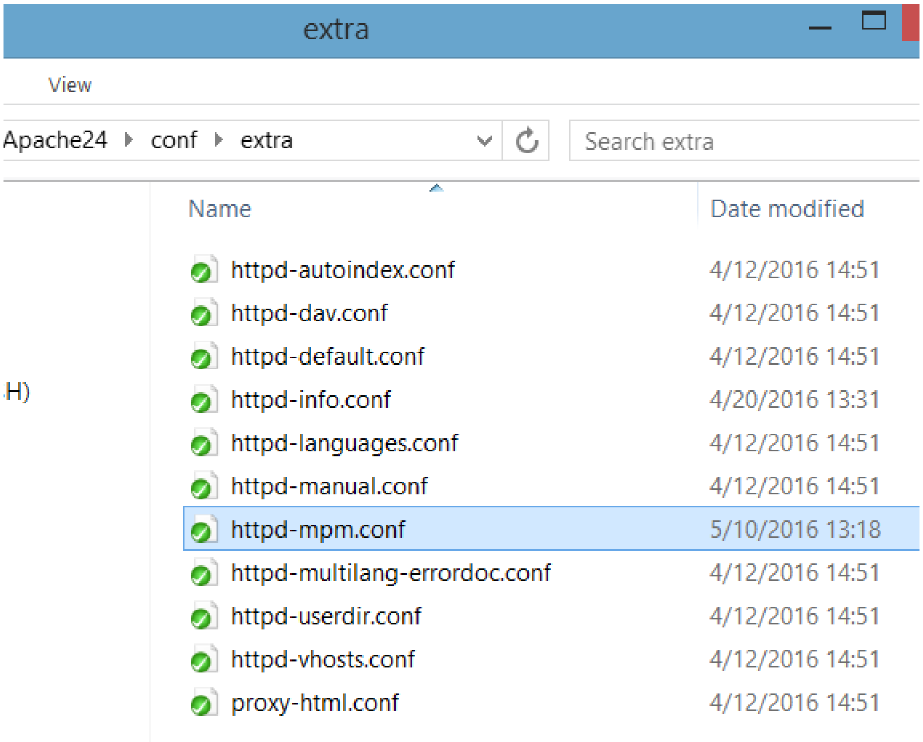
| Name | Date modified | Type |
|---|---|---|
| extra | 4/21/2016 1:02 PM | File folder |
| HPDM | 4/22/2016 11:03 AM | File folder |
| original | 4/21/2016 9:51 AM | File folder |
| charset.conv | 4/21/2016 9:51 AM | CONV File |
| httpd.conf | 4/28/2016 6:08 PM | CONF File |
| magic | 4/21/2016 9:51 AM | File |
| mime.types | 4/21/2016 9:51 AM | TYPES File |
| openssl.cnf | 4/21/2016 9:51 AM | CNF File |

2. Edit the configuration file.
   A. Go to line **489**, and locate the comment line `#Include conf/extra/httpd-mpm.conf`.
   B. Remove the # so that the line is `Include conf/extra/httpd-mpm.conf`.
   C. Save this file.



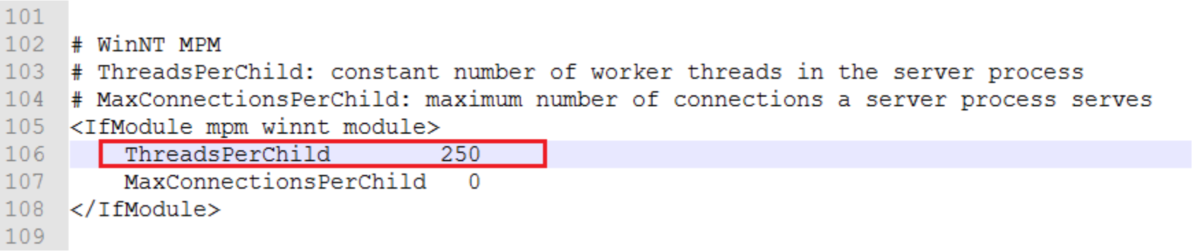
```
481  # Supplemental configuration
482  #
483  # The configuration files in the conf/extra/ directo
484  # included to add extra features or to modify the de
485  # the server, or you may simply copy their contents
486  # necessary.
487
488  # Server-pool management (MPM specific)
489  Include conf/extra/httpd-mpm.conf
490
491  # Multi-language error messages
492  #Include conf/extra/httpd-multilang-errordoc.conf
493
494  # Fancy directory listings
495  Include conf/extra/httpd-autoindex.conf
496
```

3. Locate the file `httpd-mpm.conf`. By default, it is saved in the following location:
   `<HPDM Embedded HTTPS Server install path>\HP Device Manager\Embedded HTTPS Server\Apache24\conf\extra`



| Name | Date modified |
|---|---|
| httpd-autoindex.conf | 4/12/2016 14:51 |
| httpd-dav.conf | 4/12/2016 14:51 |
| httpd-default.conf | 4/12/2016 14:51 |
| httpd-info.conf | 4/20/2016 13:31 |
| httpd-languages.conf | 4/12/2016 14:51 |
| httpd-manual.conf | 4/12/2016 14:51 |
| httpd-mpm.conf | 5/10/2016 13:18 |
| httpd-multilang-errordoc.conf | 4/12/2016 14:51 |
| httpd-userdir.conf | 4/12/2016 14:51 |
| httpd-vhosts.conf | 4/12/2016 14:51 |
| proxy-html.conf | 4/12/2016 14:51 |

4. Edit the configuration file.
   A. Find the section `WinNT MPM`, and then go to the `ThreadsPerChild` command. By default, the value of `ThreadsPerChild` is 150. The reasonable value scope is `100`–`500`. Enter a reasonable value for your hardware configuration
   B. Save the file.



```

# WinNT MPM
# ThreadsPerChild: constant number of worker threads in the server process
# MaxConnectionsPerChild: maximum number of connections a server process serves
<IfModule mpm_winnt_module>
    ThreadsPerChild         250
    MaxConnectionsPerChild    0
</IfModule>

```

5. Restart the HPDM Embedded HTTPS Server service.

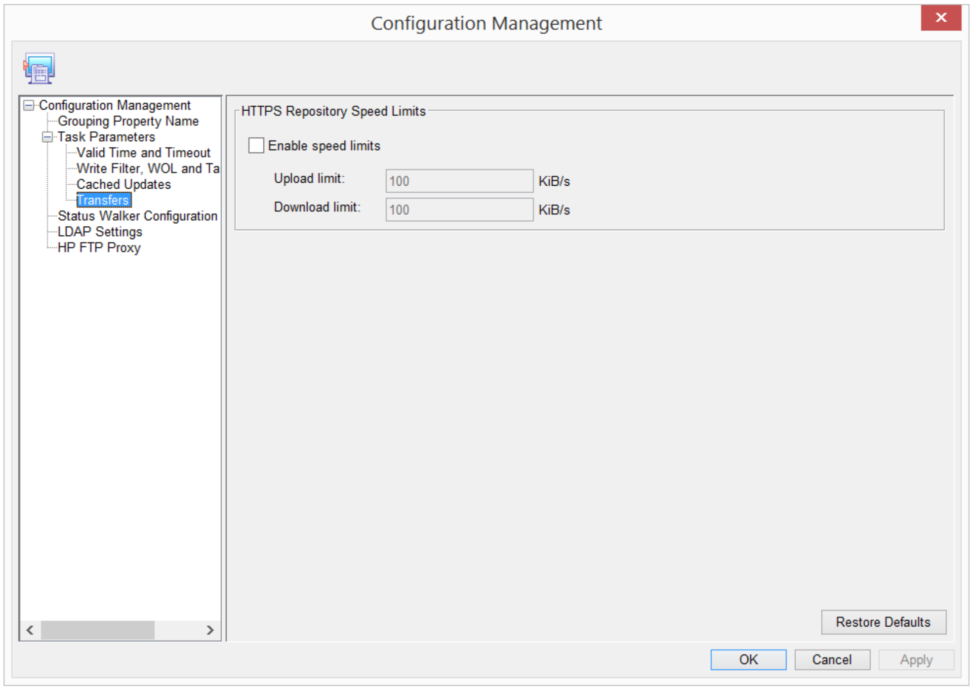
## Hardware performance

The performance of the disk I/O is the key factor that impacts performance of the HPDM Embedded HTTPS Server service. If the disk is a mechanical hard disk, the performance degrades when multiple clients are connected to the server and uploading and/or downloading large files simultaneously. In that scenario, the CPU usage generally shows high use and the file transfer speed decreases. To improve the performance, HP recommends using SDD or RAID disk storage.

# Bandwidth throttling

Administrators can configure bandwidth throttling for the HTTPS file transfer protocol. When logged in as the administrator, you can enable or disable the throttling feature, and you can set upload and/or download limits.

By default, the throttling function is disabled. After you enable the throttling function, the default value for the upload and download limits is 100 KiB/s each. You can set the upload and download limits to any value between 1 and 999999999 KiB/s.



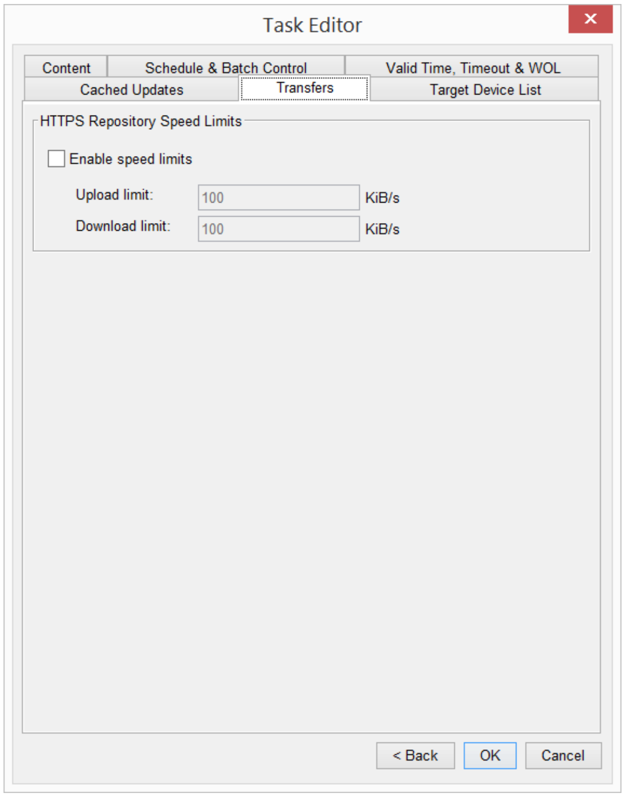
HTTPS Repository Speed Limits

☐ Enable speed limits

Upload limit: 100 KiB/s

Download limit: 100 KiB/s

Also, for every task within HPDM related to payload transferring, you can customize the bandwidth throttling parameters based on the global configuration.



HTTPS Repository Speed Limits

☐ Enable speed limits

Upload limit: 100 KiB/s

Download limit: 100 KiB/s

### Configuring the bandwidth throttling parameters

If you need to configure the bandwidth throttling parameters for all tasks, use the following procedure.

1. To open the Configuration Management dialog box, select **Tools**, and then select **Configuration**.
2. Select **Task Parameters**, and then select **Transfers.**
3. Configure the bandwidth throttling parameters for global settings.

To configure bandwidth throttling for a single task related to payload transferring:

1. Right-click the task, and then select **Send Task**.
2. On the Transfers tab in the Task Editor dialog box, configure the bandwidth throttling parameters for a single task.

## Adding an HPDM Embedded HTTPS Server as an HPDM Repository

See the *HPDM Repository Management* white paper.

## For more information

For more information about HP Device Manager, go to http://www.hp.com/go/hpdm.

**Sign up for updates**
**hp.com/go/getupdated**

The information contained herein is subject to change without notice. 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.

First Edition: May 2016

Document Part Number: 906412-001