Technical white paper

HP Device Manager

Security Mechanism

Table of contents

Executive summary 2

Database confidential 2

File repository confidential 2

HPDM logon confidential 2

Confidential data in log files 2

User management 3

Authentication management 3

Network communication 4

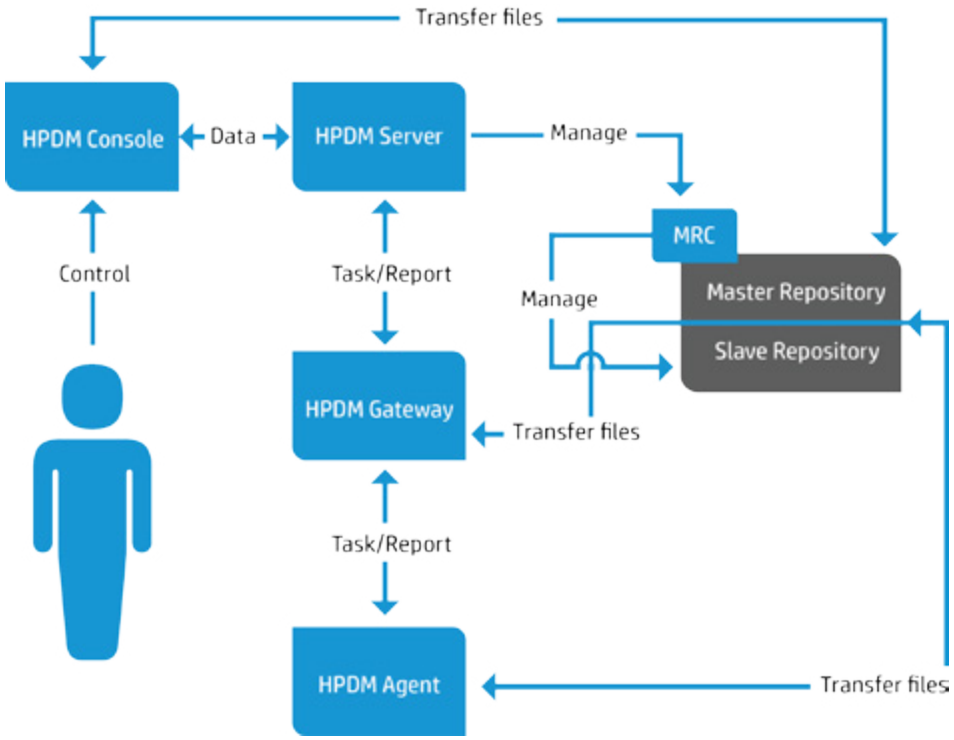
Secure file server 4

Task verification 4

Executive summary

HP Device Manager (HPDM) is a solution designed to help the IT administrators manage and control remote HP Thin Clients. The solution consists of the HPDM Console, HPDM Server, HPDM Gateway, HPDM Agent, Master Repository Controller, and file repositories. A standard setup is shown in Figure 1. The solution needs to store highly sensitive data, such as the passwords of the database and file repositories, and transfer it over the network. To protect the data, the solution introduces several security measures to authenticate devices and encrypt sensitive data locally. The solution also provides other measures to protect the client devices from misoperation.

Figure 1. HP Device Manager setup



Database confidential

In the solution, only the HPDM Server needs to access the database. The HPDM Server stores database account information on the local storage of the server and encrypts the password with a DES algorithm.

File repository confidential

HPDM stores file repository information in the database and encrypts the password with an AES algorithm.

HPDM logon confidential

When HPDM is installed, it will prompt you to set a password for the super administrator account. The HPDM Administrators' usernames and the MD5 hash values of their passwords will be saved in the database you select. When an HPDM Administrator tries to log on to the HPDM Console, the HPDM Server compares the input (username and MD5 hash value of the password) to the data in the database to determine whether to allow or deny access. HPDM saves only the MD5 hash value of the password, which is unlikely to reveal the original password to a hacker, because MD5 is an asymmetric cryptographic algorithm.

Confidential data in log files

Each part of HPDM supports different log levels. Set different log levels to trace errors or detail information. If you set the log level to the most detailed level, then the log messages might contain sensitive data, such as passwords in tasks. To protect this sensitive data, HPDM automatically hides it with an asterisk sequence. For example, an FTP password such as P@ssw0rd would be written in the log file as ********.

User management

HPDM supports the following user account and user group management tools to avoid any misoperation and make sure that the system is stable.

- One user is classified as the super administrator and others are classified as ordinary administrators.
- Each ordinary administrator can be put into or removed from a group. All administrators in the same group have the same privileges.
- Each ordinary administrator or group can be granted certain privileges, such as managing specific thin client devices or executing specific operations. The super administrator always has full control to the system.

Authentication management

HPDM provides an authentication capability that allows the HPDM Gateways and the HPDM Agents to recognize a secure management server. There are three features for providing authentication: Key Management, Master Repository Controller Access Control, and Gateway Access Control.

Key management

The authentication key enables the HPDM Agents to verify if the HPDM Server has the privilege to manage them. By default, the HPDM Agents and HPDM Server have the same original key. For security, you can use Key Management to create a new key, and then the HPDM Agents will update their keys automatically. After updating their keys, the HPDM Agents reject tasks sent by servers that do not have the correct key.

An HPDM Agent saves the keys in the files key0.key and key1.key. The file key0.key is the default key and the file key1.key is the current key. The key files are encrypted with DES in CBC mode. When the current key expires, the HPDM Agent uses the default key to overwrite the current key.

To update an HPDM Agent key:

1. In the HPDM Console, select **Key Management**. Add a new key.
2. The HPDM Server sends the new key to the HPDM Gateway because the HPDM Gateway keeps the key list in its memory.
3. When an HPDM Agent sends a startup report or tries to receive tasks, the HPDM Gateway will check the HPDM Agent key's MD5 hash value.
    A. If the agent key's MD5 cannot be recognized, the gateway will refuse the connection.
    B. If the agent key's MD5 belongs to an old key, the gateway will generate an update key task for the device. The new key will be encrypted with the old one via a DES algorithm before being sent to the agent.
    C. If the agent key's MD5 is the same as the new one, the gateway will not do any additional operations.
4. The HPDM Agent receives the update key task, decrypts the new key using the old key, and updates the old key to the new one.

Master Repository Controller access control

In the HPDM hierarchy, only the HPDM Server connects to the Master Repository Controller to manage the Master Repository and Child Repositories. When the HPDM Server connects to the Master Repository Controller successfully, both the HPDM Server and the MRC create an RSA key and an X.509 certificate. Then, they exchange the certificates, enroll them, and start a TLSv1.0 connection for security. After the Master Repository Controller enrolls a certificate from an HPDM Server, it rejects connections that either do not have a certificate or have a different certificate.

Gateway access control

The HPDM Server maintains the acknowledged status of a gateway, which is specified by the user from the HPDM Console. When a gateway is discovered by the HPDM Server, the gateway is set to unknown status. You can either acknowledge the gateway or ban it. The HPDM Server will neither establish a connection with a banned gateway nor receive any messages sent from it unless it is later acknowledged.

By default, any gateway with an unknown status is treated like it is safe. HP recommends banning any unexpected gateways that join the HPDM Server. Use the **Gateway Access Control** dialog to manually control access. Enable the option to treat any gateways with an unknown status as unsafe unless they are later acknowledged.

Network communication

The connections between the HPDM components (Console, Server, Gateway, Agent, and Master Repository Controller) are secure. The components communicate through TLSv1.0 connections created with OpenSSL (www.openssl.org). This prevents data from leaking during network communication.

The crypto algorithms in SSL/TLS use an RSA-created key pair of length 512 or 1024 and an X.509-created certificate. The symmetric cipher is AES (AES256-SHA).

Secure file server

To perform some tasks or operations, the HPDM Console, Gateway, and Agent need to access a repository, or file server, to download/upload files to perform some tasks or operations. To protect this data, HPDM 4.4.2 or higher supports two types of secure file servers: File Transfer Protocol over SSL (FTPS) and Secure File Transfer Protocol (SFTP). FTPS is an extension of the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cryptographic protocols. SFTP is a network protocol that provides file access, file transfer, and file management over any reliable data stream. It was designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH) 2.0 to provide secure file transfer capability.

Task verification

To protect thin clients, an HPDM Agent accepts only the tasks that pass task verification. Task verification is based on Key Authentication. The HPDM Gateway stores the whole key list, which is synchronized from the HPDM Server. The following procedure details how an HPDM Agent receives a task from the HPDM Gateway.

1. The HPDM Gateway connects to the HPDM Agent.
2. The HPDM Agent accepts the connection.
3. The HPDM Gateway sends an encryption request message and creates an SSL-Server instance with OpenSSL.
4. When the HPDM Agent gets the encryption request message, it creates an SSL-Client instance with OpenSSL and connects to the SSL Server.
5. The HPDM Gateway accepts the SSL connection and sends a task request message to the HPDM Agent.
6. The HPDM Agent sends a challenge message to the HPDM Gateway when it receives the task request message.
   A. A challenge message includes two parts:
      i. MD5 checksum of the HPDM Agent's current key.
      ii. 128-byte randomly generated string.
7. When the HPDM Gateway receives the challenge message, it searches the MD5 hash values of the keys from the key list. If it finds the key, it calculates the MD5 hash value of the key plus the random string and signs the result to the task for the HPDM Agent. Then, the HPDM Gateway sends the task to the HPDM Agent.
8. When the HPDM Agent receives the task, it verifies the signature first. The HPDM Agent uses its current key and the random string to calculate the MD5 hash value. If the MD5 hash value is not same as the task signature, it will reject the task. Otherwise, it accepts the task and adds the task to the execution queue.

For more information see the *HP Device Manager User Guide* for more details about User Management and Authentication Management.

Learn more at
hp.com/hpdm

Sign up for updates
hp.com/go/getupdated

4AA4-7878ENW, July 2013