



Management Presence Server Supporting Client-Initiated Remote Access

User Guide

Release 15.0.1.1, June 2021

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

The API and software may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document. Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an ordering number and are referenced in this document or other Intel literature may be obtained by calling 1-800-548-4725 or by visiting Intel's website at <http://www.intel.com>.

Copyright © 2008-2021 Intel Corporation. All rights reserved.

* Third party other names and brands may be claimed as the property of others.

Table of Contents

1	Introduction.....	4
2	MPS Overview.....	4
3	Authentication Considerations	5
4	Configuring the Intel AMT Platform for Remote Access	6
4.1	Loading Certificates	6
4.2	MPS Parameters	6
4.3	Enabling Remote Access	7
4.4	Preparing Console Applications to work with MPS	7
5	Installing the MPS	7
5.1	Preparation	8
5.2	Performing the Install.....	8
6	Configuring the MPS	8
6.1	MPS Configuration Parameters.....	9
6.2	Configuration Files.....	10
6.3	TLS Terminator Configuration	11
6.4	Proxy Server Configuration	11
7	MPS Notification and Authentication Interfaces.....	12
7.1	MpsNotification Command	12
7.1.1	EventNotificationRequest	12
7.1.2	EventNotificationType.....	13
7.2	Authentication Interface.....	13
7.2.1	Table Lookup Sample.....	14
7.2.2	SOAP Authentication Sample.....	14
8	Security Considerations	16
8.1	Outgoing Ports.....	16
8.2	Incoming Ports.....	17
8.3	Apache as the Inner Firewall	17
9	Management Considerations	17
10	MPS Troubleshooting	17
10.1	Issues and Solutions.....	17
10.2	Startup Considerations	19
10.3	Troubleshooting Using the MPS Logs	19

1 Introduction

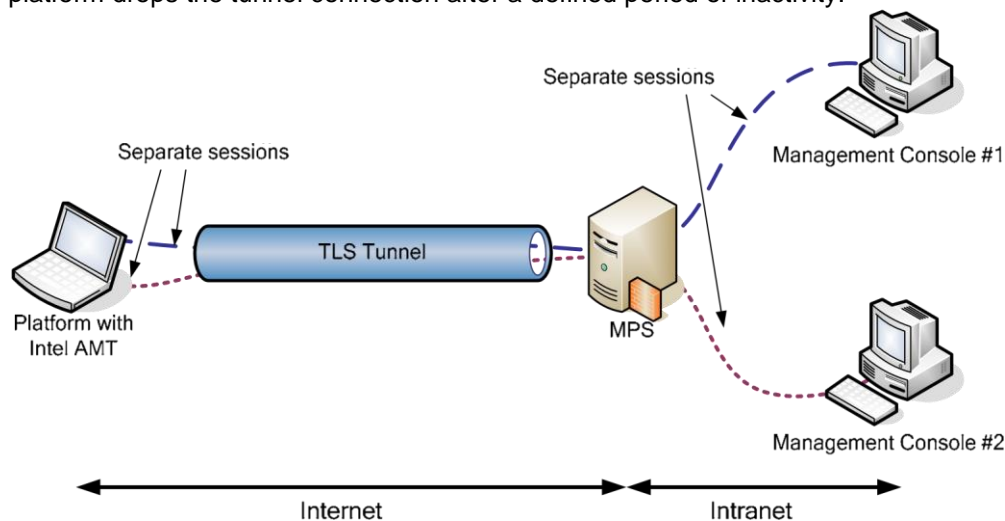
Intel® Active Management Technology (Intel® AMT) and platforms that support Intel® Remote PC Care Technology (Intel® RPCT) provide client initiated remote access (CIRA). In early releases, an Intel AMT platform needed to operate within an enterprise's network to be reachable by management consoles. Any enterprise separation between the Intel AMT device and the console, such as a firewall, would make the platform unreachable. By configuring the Intel AMT platform to be able to initiate a connection to an intermediate server running in the enterprise DMZ, the platform can be managed remotely when it is connected to the Internet anywhere in the world.

2 MPS Overview

The Management Presence Server (MPS) enables enterprise management consoles located behind the enterprise firewall to connect to Intel AMT platforms located outside the enterprise. The MPS mediates between the Intel AMT platform and Intel AMT management console, using a tunneling protocol to secure the communication with the Intel AMT platform.

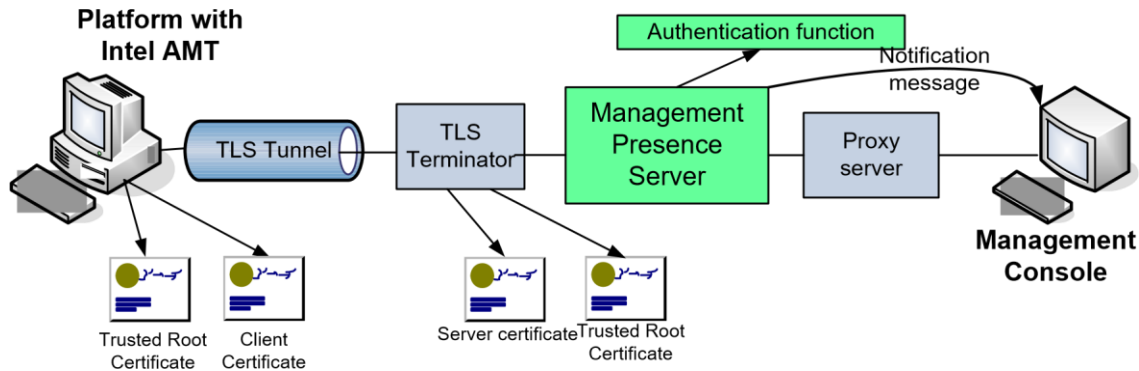
Management consoles see the MPS as a proxy server.

The Intel AMT platform connects to the MPS to establish a secure connection to the enterprise network. Once a TLS tunnel is established between the Intel AMT platform and the MPS, multiple management consoles can connect with the platform. The MPS uses the Intel AMT port forwarding protocol (APF) built into the Intel AMT platform to differentiate between different management console sessions. The MPS creates and tears down sessions and allocates/deallocates ports as management consoles initiate and complete actions. The Intel AMT platform drops the tunnel connection after a defined period of inactivity.



The MPS depends on third-party software to implement some of the required functionality.

- A **TLS Terminator** establishes the TLS tunnel with the Intel AMT platform and passes the traffic through to the MPS.
- A **Proxy server** handles proxy HTTP connections between management consoles and the MPS. The HTTP proxy forwards the connections to the MPS by proxy chaining to the MPS.



The MPS notifies registered management consoles that an Intel AMT platform has connected or disconnected by sending a message using the SOAP protocol.

The MPS can authenticate Intel AMT platform connections that are not configured for TLS mutual authentication by querying a user-supplied authentication function.

3 Authentication Considerations

Authentication can occur between different elements in a remote access configuration. This section summarizes the authentication possibilities.

1. Consoles can authenticate to Intel AMT devices just as they do when the devices are inside the enterprise. This is transparent to any authentication done on behalf of remote access.
 - a. Intel AMT can be configured for TLS and requires a certificate with an OID for a server certificate. The console needs a corresponding trusted root certificate. The Intel® Setup and Configuration Service (Intel® SCS) does this using the Microsoft* Certification Authority to create a certificate for each Intel AMT device.
 - b. If Intel AMT is configured for TLS mutual authentication, the console requires a certificate with a client OID, and the Intel AMT device needs the corresponding trusted root certificate.
 - c. Intel AMT can be configured not to use TLS at all for management console connections.
2. Independent of the Intel AMT–Console authentication, Intel AMT must have a trusted root certificate corresponding to the server certificate that the MPS has. (Actually, it is the TLS terminator that has the certificate. The TLS negotiation is with the TLS terminator; the TLS terminator forwards TCP packets to the MPS itself.)
3. The MPS authenticates to Intel AMT in one of two ways: TLS Mutual Authentication or username/password.
 - a. This is a configuration option that must be consistent on the Intel AMT platforms, in the TLS terminator configuration, and in the MPS configuration.
 - b. If the TLS mutual authentication option is configured, the Intel AMT device requires a client certificate. This can be the same certificate as in 1a above, with an additional OID for a client certificate, or it can be a different certificate. The TLS terminator needs to have the corresponding trusted root certificate.
 - c. If the username/password option is configured, the TLS terminator only negotiates server authentication; the MPS itself sends the username/password to an authentication function. The MPS receives the username/password as part of an APF authentication flow.

4. Consoles may need to authenticate to the HTTP/S proxy (e.g., the proxifier built into Apache) or to the MPS itself, which appears to the MCs as a SOCKSv5 proxy. This authentication to the MPS is either username/password or none, depending on how it is configured. Apache can be configured for additional authentication options, so this can be installation dependent. Consoles must be designed to either support additional authentication options or state their limitations explicitly.
5. The HTTP/S proxy, which converts messages to SOCKSv5, may need to authenticate to the MPS. The configuration options are either username/password or none.
6. The MPS authenticates SOCKSv5 username/password connections with a call to an authentication function that has the same interface as the Intel AMT username/password connection validation function.

4 Configuring the Intel AMT Platform for Remote Access

A setup and configuration application is required to prepare an Intel AMT platform for remote access. The setup and configuration activity must be performed when the setup and configuration application and the Intel AMT platform are on the same intranet.

The following documents, found in the Intel AMT Software Development Kit (SDK), describe the configuration commands. See the *Network Interface Guide* for the SOAP interface commands that perform the following functionality. See the *WS-Management Flows* document and the *WSManagement Class Reference* for WS-Management support to this process. The setup and configuration sample demonstrates configuring for remote access using the SOAP interface.

The setup and configuration application adds necessary certificates, adds MPS information and remote access policies, and then enables remote access:

4.1 Loading Certificates

The Intel AMT device requires a trusted root certificate at a minimum and a client certificate if TLS with mutual authentication will be used.

Trusted root certificate: Used to authenticate the server certificate sent by the TLS terminator when setting up the TLS tunnel.

Client Certificate: Sent by the Intel AMT device when mutual authentication is used. The TLS terminator must have a trusted root certificate corresponding to this certificate.

4.2 MPS Parameters

These parameters define how to connect to the MPS and specify the conditions that initiate a remote access connection.

MPS information: These parameters tell the Intel AMT device how to connect to an MPS. The parameters include:

- Address and port where the TLS terminator listens for Intel AMT connection requests.
 - The address is either an IP address or FQDN.
 - If an IP address is provided, a Common Name (CN) for the MPS must be provided.
 - Intel AMT uses either the CN provided with an IP address or the FQDN to validate the server certificate sent by the MPS.
- A pointer to a trusted root certificate used for TLS authentication of the MPS.

- Either a pointer to a client certificate used for TLS mutual authentication or a user name/password pair used by the MPS for authentication.

Remote access policies: A policy defines what can trigger a remote connection, which MPS is contacted, and how long the TLS tunnel is maintained. Policy parameters include:

- Trigger type — the trigger can be user-initiated, triggered by an alert, or triggered periodically.
 - o User initiated trigger — A user can initiate an MPS connection either from a host application or via an MEBX/BIOS request.
 - o Alert trigger — Whenever an event occurs that sends an alert to a network address
 - o Periodic trigger — The Intel AMT device connects to an MPS periodically. The policy includes a time interval that determines when a new connection should be attempted.
 - o Trigger type priorities — When multiple policies have been defined and a tunnel is already active with an MPS and another trigger occurs, then, if the new trigger is of higher priority and requires a connection to a different MPS, the current connection is dropped and the device connects to the other MPS. If the trigger is for a connection to the same MPS, the tunnel remains open for the longer of the two tunnel lifetime settings. A user-initiated trigger has the highest priority, while a periodic trigger has the lowest.
- Tunnel lifetime — specifies how long the TLS tunnel should stay open, in seconds, when there is not traffic. Any traffic on the tunnel restarts the lifetime countdown.
- MPS to connect to — When the trigger occurs, Intel AMT attempts to connect to the MPS designated in the policy. A policy can point to two MPS definitions. Intel AMT attempts to connect to the first MPS. If the attempt fails, it tries to connect to the second MPS. The sequence is repeated once more. Another trigger is required for an additional connection attempt.

4.3 Enabling Remote Access

The setup and configuration application must do two things to enable remote access.

- Enable environment detection, including with it a list of domain suffixes that define the locations that are “inside the enterprise”. When a trigger occurs, if the Intel AMT device detects that it is outside the enterprise, it connects to the MPS. Otherwise, alerts are sent directly to their destination and periodic and user-initiated triggers are ignored.
- If there is a policy with a user-initiated trigger, enable initiation either using an application running on the host or via the Intel® Management Engine BIOS extension (MEBX)/BIOS or both.

4.4 Preparing Console Applications to work with MPS

Console applications require proxy information to connect to Intel AMT platforms via the MPS. Intel AMT console applications that use HTTP/S require a proxy IP and port.

Redirection applications require SOCKSv5 server connection parameters for a proxy connection (hostname, port, username, and password).

Consoles can be configured with this information initially. The notification message also contains the necessary connection information, both for the MPS and for the Intel AMT platform.

5 Installing the MPS

For details of how to install the MPS, refer to the Readme file.

5.1 Preparation

Before starting the installation, the create a server certificate, trusted root certificate and certificate key with the following names:

- a. Certificate: cacert.cer
- b. Trusted root: remote_client.pem
- c. Key: remote_client_key.pem

5.2 Performing the Install

1. Install stunnel.

Note: For details on downloading and installing stunnel, see <http://www.stunnel.org/>.

The <stunnel installation directory>\config\stunnel.conf file already contains most of the configuration parameters suitable for MPS. The following parameters still need to be configured:

- CAfile = <path to trusted root certificate authority>. Use the CA created during ES (this can be found in CertGenerator\rootCA\cacert.cer).
- cert = <path to trusted server certificate>. Use the certificate created during ES (this can be found in CertGenerator\remote_client\remote_client.pem) .
- key = <path to certificate key>. Use the key created during ES (this can be found in CertGenerator\remote_client\remote_client.pem\private\remote_client_key.pem).
- accept = <port that AMT device uses to connect to MPS>
- connect = <ip: port that stunnel will use to send the received data to the MPS>.

This address is also configured in MPS.config (see section 3). (ip usually equals localhost)

More details about stunnel and its parameters can be found in: <http://www.stunnel.org/>

2. Update the configuration files as described in *Configuring the MPS*.
3. Install the Apache HTTP proxy from <https://httpd.apache.org/>. For configuration instructions, see Apache_MPS_Proxy_Manual.txt in the MPS zip file at \Docs\Apache User Guide.
4. Right-click **My Computer**, and select **Manage**.
5. Select the **Services and applications** branch in the left pane and open it, then open **Services**.
6. Stop the MPS, Stunnel and Apache services.
7. Apply the appropriate updates to the configuration files described below, and then restart all the services.

6 Configuring the MPS

Consoles running manageability applications can perform their functions by sending commands to a connected Intel AMT platform via the MPS. A console requires the following parameters to connect to a specific platform:

- Proxy address (the proxy server IP address and port)
- MPS username and password
- Intel AMT platform FQDN
- Intel AMT platform ACL username and password

Configuration files for the MPS, the console application, the TLS terminator and the proxy server need to be in synch to pass along the necessary parameters in each step of the communication path.

6.1 MPS Configuration Parameters

The following table lists the MPS configuration parameters. All the parameters listed are defined in the \Bin\Conf\mps.config file except the TraceLevels parameter, which is defined in \Bin\Conf\mps_dynamic.config.

Parameter	Description
Network Parameters	
AMTListenIP	IP address listening for Intel AMT connections. It is the IP address the TLS terminator uses to forward connections from the Intel AMT platform. When the TLS terminator runs on the same platform as the MPS, this will be the local host. (See the Stunnel connect configuration parameter.)
AMTListenPort	TCP port in connections from Intel AMT platforms to the MPS via a TLS terminator. This port number must match the port used by the TLS terminator to forward Intel AMT platform connections. (See the Stunnel connect configuration parameter).
SocksListenIP	This is the IP address of the network interface of the server where the MPS executes that faces the intranet.
SocksListenPort	Port used in SOCKSv5 connections from redirection applications or socksified traffic from proxy server.
HttpListenPort	Port used in HTTP/S proxy connections from management consoles. This is the port used in notification messages as the MPS HTTP port. Console applications address their HTTP traffic to Intel AMT platforms via this port. The proxy server listens on this port and forwards to the MCSocksListenPort.
Logger Parameters	
Heading	Text displayed as the first line of the log file
LogFilePath	Path to the directory where the log file will be created – relative to the local directory or an absolute path.
LogFileName	The name of the log file.
LogFileMaxSize	Maximum size of a log file, in Kbytes. When this size is reached, the MPS appends a digit to the file name and starts a new log file. For example, if LogFileName is MPS.log, the filename will be changed to MPS.log.1. The next full file will be MPS.log.2, and so on.
LogFileMaxFiles	The maximum number of log files created and maintained. When this number is reached, the next log file will overwrite the oldest log file.
TraceLevels	Level of messages to be logged. The options are “INFO”, “ERROR”, and “WARNING”, or any combination. Combine multiple selections by separating them with a “ ” character. For example, “INFO ERROR WARNING”. This parameter can be changed dynamically and is set in mps_dynamic.config .

Parameter	Description
AMT_Authenticate Parameters	
NeedAuthentication	true: The MPS will call the dll defined below to authenticate the User ID and password in connections from Intel AMT devices. false: The MPS will not perform authentication.
DllName	The dll used for authentication; required if NeedAuthentication is true. This parameter is the full path to the dll.
DllParameters	Command line parameters to pass to the dll. The sample dll that uses file authentication requires parameters to locate the file (e.g., "-file <path to file\filename>")
Socks_Authenticate Parameters	
NeedAuthentication	true: The MPS will call the dll defined below to authenticate the User ID and password in Socks connections from consoles. false: The MPS will not perform authentication.
DllName	The dll used for authentication; required if NeedAuthentication is true. This parameter is the full path to the dll.
DllParameters	Command line parameters to pass to the dll. The sample dll that uses file authentication requires parameters to locate the file (e.g., "-file <path to file\filename>") The SOAP authentication dll usage is described below .
Notification_Authentication Parameters	
NeedNotificationAuthentication	true: The MPS will send the username and password defined below to authenticate to management consoles when notifying them of new or closed Intel AMT tunnels. false: The MPS will not authenticate to consoles.
Username	Value used in a notification authentication response
Password	Value used in a notification authentication response
Filtering Parameters	
FilterUnauthorizedServers	Name of a file containing a list of subscribers receiving notifications of Intel AMT platform connections/disconnections. Defines processing of direct connections. true: the MPS will check AuthorizedServers.config to see if the target address of a direct connection or UDP message is listed there. If it is not, the message will be dropped. false: Direct connection or UDP messages will be forwarded unconditionally.

6.2 Configuration Files

The MPS requires the following configuration files, located in the MPS zip file at \Bin\Conf:

- **mps.config** All of the parameters in the above table are defined in this file, except for log tracelevels parameter. The MPS application reads this file on startup.
 - **Mps_dynamic.mps** defines parameters that can be changed dynamically. The tracelevels parameter is the only one in this category in this release.
 - **NotificationList.config** contains a list of subscribers receiving notifications of Intel AMT platform connections/disconnections.
The entries in the file are in the format (http/https)://(IP Address/FQDN):(Port)/(rest of url) (one per line). For example: <http://10.0.0.10:9971/EventNotificationClientService>
The MPS will support up to eight valid entries in this list. Entries beyond eight will be discarded.
 - **AuthorizedServersList.config** contains a list of servers that are authorized to receive alerts from Intel AMT platforms. If an Intel AMT device sends a PET alert to an address not in this list, the alert will be discarded. If a WS-Event connection is attempted to an address not in the list, the connection will be refused.
The entries in the file are in the format <IP Address/FQDN>:<port> (one per line).
- The installation includes samples of these files.

6.3 TLS Terminator Configuration

Configuration of the TLS terminator is a function of the product. The following parameters are based on the Stunnel product, which is installed with the MPS. Additional information about Stunnel can be found at <http://www.stunnel.org>. The Stunnel configuration file as downloaded is usable for Intel AMT purposes, with the following modifications:

- **Cafile** is set to a path to trusted root certificate used to validate the Intel AMT device's client certificate.
- **cert** must be set to a path to the server certificate used to authenticate to the Intel AMT platform. It must trace to the trusted root certificate installed in the Intel AMT platform by the setup and configuration application.
- **key** is a path to the private key associated with the certificate.
- **accept** is the port that the Intel AMT platform uses to connect to the MPS. Stunnel listens on this port and forwards connections to the MPS using the value in the **connect** parameter.
- **connect** is the IP address and port that Stunnel uses to send data received from the Intel AMT platforms to the MPS. The IP address will be 127.0.0.1 if Stunnel runs on the same platform as the MPS, or localhost:port#.

See the file stunnel.conf in the installation located at <root_directory>\Program Files\Intel\MPS.

6.4 Proxy Server Configuration

The Apache HTTP proxy server socksifies http connections and chains them to the MPS. The configuration file httpd.conf, located at <root_directory>\Program Files\Apache Software Foundation\Apache2.2\conf, requires settings to match the settings of the MPS and management consoles. The following parameters should be added to the file:

- Listen 8080 (or any other port) – This is the port where the proxy server listens for connections. This must be the same value as MCHttpListenPort in the mps.config file.
- Uncomment the LoadModule lines for the following modules: proxy_module modules/mod_proxy.so proxy_connect_module modules/mod_proxy_connect.so proxy_http_module modules/mod_proxy_http.so
- ProxySocks On – this turns on the SOCKS proxy function
- ProxySocksIp – This is the IP of the intranet-facing port on the platform where the Apache server executes.

- ProxySocksPort – This is the port that the MPS listens on. It must be the same as MCSocksListenPort in the mps.config file.

If Socks username/password authentication will be used, set the following:

- ProxySocksAuth **On**
- ProxySocksUsername – a username that can be authenticated using the Socks_Authenticate dll specified in the MPS configuration file.
- ProxySocksPassword – password of the user

Add the following lines to httpd.conf to allow the Apache server to handle HTTPS connections from management consoles:

- ProxySocksDnsMode Remote
- <Proxy *>
- Order deny,allow
- Deny from all
- # Add "Allow from" statements for all domains used by management consoles, for example Allow from managementservers.yourenterprise.com
- </Proxy>
- #add an AllowCONNECT statement for the special Intel AMT ports: AllowCONNECT 623 664 16992 16993 16994 16995

7 MPS Notification and Authentication Interfaces

The MPS had defined programmatic interfaces for notifying management consoles that an Intel AMT client has connected or for authenticating a username/password pair.

7.1 MpsNotification Command

The MPS notifies subscribers when Intel AMT clients connect to it or disconnect from it. The file named in the MCSubscribersList lists the subscribers that the MPS notifies. The following SOAP command is used to notify subscribers of a connection. Subscribers respond with a parameter indicating whether the connection should be maintained or dropped.

The WSDL defining this command is located in the MPS distribution at:

<root_dir>:\...\MpsNotification.wsdl

7.1.1 EventNotificationRequest

This command sends notification that a platform connected to the MPS.

Header

```
EventNotificationRequest (
  [in] EventNotificationType    MPSEvent
  [out] Boolean                 KeepConnection
);
```

Parameters

MPSEvent describes the event that occurred – that a platform connected or disconnected – and additional parameters.

KeepConnection if true, the MPS maintains the connection; if false, the MPS drops the connection.

7.1.2 EventNotificationType

Contains parameters that describe the client connection event that the MPS is reporting.

```
typedef struct _EventNotificationType
{
    ConnectionStateDefinition State;
    string DeviceFqdn;
    unsignedShort DevicePort[];
    string DeviceUuid;      string
MpsAddress;               unsignedShort
MpsHttpPort;              unsignedShort
MpsSocksPort;              boolean
WantReply; }
EventNotificationType;
```

Field	Description
<i>State</i>	Event associated with the notification: 0=CONNECTED; 1=DISCONNECTED
<i>DeviceFqdn</i>	FQDN of the Intel AMT platform
<i>DevicePort</i>	Up to two ports to be used for communicating with the Intel AMT platform
<i>DeviceUuid</i>	Platform UUID
<i>MpsAddress</i>	MPS IP address
<i>MpsHttpPort</i>	MPS port
<i>MpsSocksPort</i>	Port used for redirection connections
<i>WantReply</i>	True if the console is expected to reply to the notification

7.2 Authentication Interface

The MPS supports an interface for authenticating connections from Intel AMT platforms and for authenticating Socks connections from management consoles. The interface supports a username and password as input and returns a Boolean indication (true = authenticated).

Users can create their own authentication mechanism. This distribution includes two sample DLLs, one that performs authentication via a table lookup in a text file and one that sends a SOAP message requesting authentication from an external source. Note that the Intel AMT authentication DLL and the Socks authentication DLL must have different names.

Authentication DLLs should contain the following prototype:

```
extern "C" __declspec(dllexport)
bool Authenticate(string userName ,string userPassword ,
string paramStr ,string &errorString);
```

The first two parameters are the username and password to be authenticated.

paramStr is the string in DIIParameters in the MPS configuration file, used as a way to pass parameters to the DLL.

The DLL should return a string in **errorString** if there was an error during execution. The MPS will write this message to the log.

7.2.1 Table Lookup Sample

The MPS distribution includes two versions of the table lookup dll: AMTFileAuth.dll and SocksFileAuth.dll. The dlls are identical except for their names. They search a text file for an entry that matches the username and password. The text files are in the format <username>:<password>, one entry per line. See the files AMTAuthFile.txt and SocksAuthFile.txt for example of this format.

7.2.2 SOAP Authentication Sample

SOAPAuthentication.dll sends a SOAP request for authentication of a username/password pair to an external program. The request expects a Boolean authentication indication in the response to the request. The format of the request is based on the following WSDL:

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- Manageability Presence Server authentication interface version 1.0-->
<definitions
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"

  xmlns:mpa="http://schemas.intel.com/platform/client/MPSAuthentication/2006/01"

  targetNamespace="http://schemas.intel.com/platform/client/MPSAuthentication/2006/01">

  <types>

    <!-- MPSAuthentication namespace -->
    <xs:schema
      targetNamespace="http://schemas.intel.com/platform/client/MPSAuthentication/2006/01" elementFormDefault="qualified">
      <xs:element name="AuthenticateRequest">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="AuthenticateId"
              type="xs:string"/>
            <xs:element name="AuthenticatePassword"
              type="xs:string"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="AuthenticateResponse">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="AuthenticateResult"
              type="xs:boolean"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:schema>
  </types>
  <message name="AuthenticateIn">
    <part name="parameters" element="mpa:AuthenticateRequest"/>
  </message>
  <message name="AuthenticateOut">
    <part name="parameters" element="mpa:AuthenticateResponse"/>
  </message>

  <portType name="MPSAuthenticationSoapPortType">
    <operation name="Authenticate">
      <input message="mpa:AuthenticateIn"/>
      <output message="mpa:AuthenticateOut"/>
    </operation>
  </portType>

  <binding name="MPSAuthenticationSoapBinding"
    type="mpa:MPSAuthenticationSoapPortType">
    <soap:binding style="document"
      transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="Authenticate">

```

```

        <soap:operation
soapAction="http://schemas.intel.com/platform/client/MPSAuthentication/2006/01/
Authenticate"/>
        <input>
            <soap:body use="literal"/>
        </input>
        <output>
            <soap:body use="literal"/>
        </output>
    </operation>
</binding>

<!-- Service Types -->
<service name="MPSAuthenticationService">
    <port name="MPSAuthenticationSoapPortType"
binding="mpa:MPSAuthenticationSoapBinding">
        <soap:address
location="http://hostname:7792/MPSAuthenticationService"/>
    </port>
</service>
</definitions>

```

The sample displays the following usage:

```

Usage: -target <target> [-krb] [-user <username> -pass <password>]
[-cert <name>][-tls][-proxy <proxy> -proxyUserName <proxyUserName>
proxyPass <proxyPassword>]
Example: "-target http://hostname:7792/MPSAuthenticationService -user
admin -pass Admin!123"

```

8 Security Considerations

With Intel AMT platforms operating outside the enterprise firewall and the MPS operating inside the firewall, the firewall must be configured to allow traffic to flow between the Intel AMT platforms and the MPS. Further, the MPS may be in a DMZ, with another firewall between it and the Management Consoles.

Depending on installation policy, the external firewall must be configured to allow packets addressed to the incoming port and to the outgoing ports to cross the firewall.

8.1 Outgoing Ports

Intel AMT accepts the following ports:

Port	Use
16992	SOAP over TCP
16993	SOAP over TLS
16994	Redirection over TCP
16995	Redirection over TLS
623	DASH over TCP
664	DASH over TLS

8.2 Incoming Ports

Intel AMT platforms access the MPS using the port defined when the platform was configured (see [MPS Parameters](#).)

8.3 Apache as the Inner Firewall

The Apache server, used as a proxy server, filters incoming and outgoing packets in flows between Intel AMT platforms and Management Consoles. The consoles determine their own ports for each session they manage. The outgoing ports are the standard ones listed above. The Apache configuration contains an AllowCONNECT statement that lists the Intel AMT ports that Apache will accept. See [Proxy Server Configuration](#).

9 Management Considerations

An enterprise installation may require more than one instance of an MPS. Intel AMT platforms can be configured with four different MPS instances. A remote access policy can be associated with up to two MPS instances. Intel AMT will attempt to connect with the first instance, and then the second instance. The attempt to connect will be repeated once. At this point, a new trigger will be required before the next connection attempt.

It is required that no more than one instance of an MPS can run on a server.

10 MPS Troubleshooting

There are a number of issues that users may encounter when working with the MPS. The Windows log and the MPS log help in debugging the cause of any problems. The following section highlights some of the problems that may occur and their possible solution.

10.1 Issues and Solutions

Startup problems:

Most startup problems are due to configuration issues – port numbers, or IP addresses do not match; the necessary certificates are not available or are not in the proper directory, or there are other errors in the configuration files (see below).

First, start with the basic configuration files, changing the minimum number of parameters. Then add a more complex setup where necessary.

Check the system log for reasons why the MPS did not start. The log will indicate the file (or other issue) with the problem, but it probably not specify the exact problem.

Disk Space:

Check the free space on the drive where the MPS is installed. Lack of space might result in problems opening log files. Delete or archive older log files to free up space.

Problems Establishing a Connection between Intel AMT and the MPS:

If the connection does not open:

1. Check the values used to configure the Intel AMT device. Make sure the MPS IP address and port are the same values used to configure Stunnel.
2. Configure Stunnel to generate a log: Add output=stunnel.log to the stunnel config and restart the Stunnel service

3. Check that the connection shows up in the Stunnel log. If the connection shows, then check IP address and port in Stunnel.config and mps.config match.
4. Check MPS log. It may show an authentication problem or other issue related to the connection.

Also, Apache has by default both an error log and an access log. It may be necessary to check both.

Problems Establishing a Connection between a Management Console and an Intel AMT device:

The Management console receives a 502 error (HTTP Bad Gateway error): Check that the whole path to the Intel AMT device is running: Apache→MPS→Stunnel→Intel AMT platform.

404 Not Found error – Check the Apache configuration, especially ProxySocksAuth parameter. This parameter must be set to “On” when the MPS requires SOCKS authentication and “Off” when there is no SOCKS authentication.

Try changing Proxy *: Check that the Management Console domain is in the “allow from” list.

Temporarily remove Deny from all and add Allow from all.

Logging Problems:

The log file is empty: Check that the log file is not configured as “read-only”. Check that the TraceLevels parameter has been set (“INFO|ERROR|WARNING”) The current MPS log file cannot be deleted while the MPS is running.

MPS does not allow a connection to take place:

The MPS limits the number of connections that it can make to 1000. Any connection attempts beyond that will be refused.

MPS fails to forward Intel AMT PET alerts to Management Consoles:

1. Make sure the Intel AMT subscriber address is accessible to the MPS – This is the IP address used when configuring the alert in the Intel AMT platform. The MPS attempts to forward an alert to that address.
2. If the **Filtering** flag in the **mps.config** file is set to “true”, then the MPS checks that the **NotificationList.config** contains the target address of the alert. If it does not, then the alert will be dropped. Make sure that the alert target address is in this file.
3. Check that the corporate firewall does not block the destination ports used in alerts (UDP – 162 / TCP – per configuration).

Management Consoles do not Connecting/Disconnecting notifications from the MPS:

1. Include the FQDN or IP address of any consoles that should be notified in the **NotificationList.config** file.
2. Make sure that the corporate Firewall does not block the destination ports in the notification messages.
3. NotificationList accepts up to 8 entries – make sure that the list does not exceed this limit.
4. Does the server receiving the notification message server require authentication? Enable the **NeedNotificationAuthentication** flag in **mps.config** and provide the relevant credentials.

For Apache troubleshooting visit - <http://www.apache.org/>.

For stunnel troubleshooting visit - <http://www.stunnel.org/faq/troubleshooting.html>

10.2 Startup Considerations

As part of its startup process, the MPS checks various conditions that must be present. If they are not, startup will fail. Check that all configuration parameters are correct and consistent before retrying to restart the service.

The MPS can log the following messages in the Window event log during startup:

On a normal startup, the MPS will log "MPS has started its operation."

The following log messages indicate reasons why the MPS Service failed to start:

- Attempt to run two instances of the MPS process simultaneously - second attempt discarded.
- Failed loading AMT authentication dll.
- Failed loading Socks authentication dll.
- Error while reading dynamic configuration file.
- Error while reading static configuration file.

10.3 Troubleshooting Using the MPS Logs

The MPS can log its activities at increasing levels of detail, as defined by the TraceLevels parameter. These logs provide valuable information when the MPS seems not to be working correctly. It is recommended that the parameter be set to INFO|ERROR|WARNING to capture the most common occurrences.

The following sample log shows the results of doing the following:

- Opening a user-initiated connection from an Intel AMT platform
- Sending a SOAP command from a Management Console
- Closing the user-initiated connection

These are the messages that the MPS sends when configured for normal logging (INFO|ERROR|WARNING).

```
[Wed Jul  2 2008 12:21:34.203000] [LM_INFO] Intel(R) Management
Presence Server has started
[Wed Jul  2 2008 12:21:43.218000] [LM_INFO] Intel remote client
48534188-5245-4188-5348-455288415348 is now connected. [Wed Jul  2
2008 12:21:43.250000] [LM_INFO] Intel remote client
cant.rclient.intel.com started port forwarding to address
cant.rclient.intel.com:16992
[Wed Jul  2 2008 12:21:43.250000] [LM_INFO] Intel remote client
cant.rclient.intel.com started port forwarding to address
cant.rclient.intel.com:623
[Wed Jul  2 2008 12:21:43.250000] [LM_INFO] Intel remote client
cant.rclient.intel.com started port forwarding to address
cant.rclient.intel.com:16994
[Wed Jul  2 2008 12:21:50.718000] [LM_INFO] Channel between Intel
remote client cant.rclient.intel.com and management console
212.212.212.12 opened. Channel ID [0:12]
[Wed Jul  2 2008 12:21:51.156000] [LM_INFO] [212.212.212.12]
management console has shutdown
[Wed Jul  2 2008 12:21:51.312000] [LM_INFO] Channel between Intel
remote client cant.rclient.intel.com and management console
212.212.212.12 opened. Channel ID [0:13]
```

Management Presence Server Supporting Client-Initiated Remote Access

```
[Wed Jul 2 2008 12:22:07.046000] [LM_INFO]  
[cant.rclient.intel.com] Intel remote client has disconnected
```