Enabling Service Manager Clients to Use a Shared Certificate for Trusted Sign-On

(Document Release Date: January 2013)

Table of Contents

Applies to

The content of this document applies to the following releases of HP Service Manager (SM):

- Service Manager 9.30p4 or later
- Service Manager 9.31 or later

Note: This information may also be applicable to other future releases of Service Manager. In these cases, consult your version's Help Server.

Introduction

In a trusted sign-on scenario the Service Manager server grants access to clients only if the following conditions are met:

- The user's logon credentials match an existing operator record in Service Manager or a valid LDAP source that Service Manager recognizes
- A trusted authentication authority, such as the operating system, validates that the user's logon credentials are valid.
- The client (Service Manager Web Tier or Windows) must present a signed SSL certificate.

For a list of requirements for trusted sign-on, see the Service Manager help.

Beginning with Service Manager 9.30, Trusted Sign-On (TSO) requires the parameter `ssl_reqClientAuth:2` to be set. If you enable this parameter with the value `ssl_reqClientAuth:2` then in addition to presenting client certificates, the server validates each client certificate against a list of trusted clients as defined by the `ssl_trustedClientsJKS` parameter. Using this parameter with the value `ssl_reqClientAuth:2` is REQUIRED when using the Trusted Sign-On features of Service Manager (`trustedsignon:1`). You must then create unique client SSL certificates for each Service Manager client wanting to access Service Manager with Trusted Sign-On. For example, if you have 20 Service Manager Windows clients, you must create 20 unique client SSL certificates. If you have 4 Service Manager Web Tier servers, you must create 4 unique client SSL certificates.

Maintaining these unique client SSL certificates might incur unsustainable IT operation costs. As of version 9.30p4, Service Manager has introduced a server parameter named `acceptsharedcert`. When this parameter is enabled, only one client SSL certificate (the "shared certificate") needs to be created and maintained. This significantly minimizes the maintenance overhead costs and complexity associated with managing signed SSL client certificates.

***Note**: The shared certificate still needs to be copied and distributed to individual Service Manager Windows clients before Trusted Sign-On access can be successfully used.*

This document describes how to use this parameter, the security risks that may be incurred when using it, as well as recommended configurations before using it.

Enabling the Shared Certificate Mode for Trusted Sign-On

You can enable the Shared Certificate mode for TSO by specifying server parameter `acceptsharedcert :1`. In this mode, all clients can share one certificate when connecting to the SM server via TSO. This section describes how you should use this parameter.

Parameter
`acceptsharedcert`

Description
This parameter defines how the HP Service Manager server handles signed SSL certificates from incoming client requests in a Trusted Sign-On configuration and was introduced beginning with 9.30.274 Patch 4. When it is set to 0 (default), the SM server validates the signed SSL client certificates using standard best practices. The validation procedure is described in Help Server Topic: *Secure Sockets Layer (SSL) encryption and server certificates*.

Important: Using the default value of 0 is the recommended and most secure mode of operation.

When the parameter is enabled (`acceptsharedcert:1`), the Service Manager server allows Trusted Sign-On connections using a so-called "shared certificate." This shared certificate is validated by the Service Manager server using only the following two checks:

- Whether the certificate is issued by a trusted certificate authority.
- Whether the Common Name attribute of the certificate is in the SM Server's trusted clients keystore.

HP provides this parameter primarily for use in customer environments where the following are true:

- There is a requirement to allow access to Service Manager via Trusted Sign-On for a large number of Service Manager Windows clients.
- Creating and maintaining the required signed SSL client certificates adds too much maintenance overhead and complexity to IT operations.

Valid if set from

Server's OS command line prompt

Initialization file (sm.ini)

Requires restart of HP Server Manager server?

Yes

Default Value

0

Possible Values

0 (Disabled)

1 (Enabled)

Example Usage

Command line: `sm -httpPort:13080 -acceptsharedcert:1`

Initialization file: `acceptsharedcert:1`

Security Risks

By using `acceptsharedcert:1`, you will have minimized your maintenance overhead and complexity of your IT operations at the cost of reduced security in Service Manager. This is due to the two simple "shared certificate" validation checks performed by the Service Manager server (which were previously described) when running with `acceptsharedcert:1`. Running the Service Manager server with the recommended

default value for `acceptsharedcert` provides the most secure method for enabling Trusted Sign-On features because the Service Manager server performs additional validation checks against the client SSL certificate. It is also possible, though unlikely, that if a malicious user obtains the "shared certificate" they may be able to gain unauthorized access to Service Manager if they can then also defeat the NTLM-based implementation of Trusted Sign-On on the Service Manager Windows client.

Recommended Configurations

HP recommends customers run the Service Manager server in the default mode of "`acceptsharedcert:0`". Before attempting to modify the default behavior, consider the following alternative configurations:

- Do not use the Service Manager Windows client (use only the Service Manager Web Tier as it does not incur additional maintenance overhead or complexity).
- If the Service Manager Windows client must be used in your environment, consider limiting the distribution of this client to a limited and small number of users. This significantly minimizes the additional SSL certificate maintenance and overhead incurred in larger environments with hundreds of SM Windows clients.
- Use as many Service Manager Windows clients as needed (hundreds) but disable Trusted Sign-On for these users.

For more information

Please visit the HP Software support Web site at:

www.hp.com/go/hpsoftwaresupport

This Web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued customer, you can benefit by being able to:

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

Note: 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:

www.hp.com/go/hpsoftwaresupport/new_access_levels

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

www.hp.com/go/hpsoftwaresupport/passport-registration