Hewlett Packard Enterprise

HPE Structured Data Manager

Software Version: 7.52

SecureData Integration Guide

Document Release Date: December 2017

Software Release Date: December 2017

Legal notices

Warranty

The only warranties for Hewlett Packard Enterprise Development LP 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. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted rights legend

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

Copyright notice

Trademark notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent software updates, go to https://softwaresupport.hpe.com/patches.

To verify that you are using the most recent edition of a document, go to https://softwaresupport.hpe.com/manuals.

This site requires that you register for an HPE Passport and sign in. To register for an HPE Passport ID, go to https://hpp12.passport.hpe.com/hppcf/login.do.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support Online web site at https://softwaresupport.hpe.com.

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

HPE Software online 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 support customer, you can benefit by using the support web site to:

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

Most of the support areas require that you register as an HPE Passport user and sign in. Many also require a support contract.

To register for an HPE Passport ID, go to https://hpp12.passport.hpe.com/hppcf/login.do.

To find more information about access levels, go to https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

Contents

Introduction

HPE Structured Data Manager (SDM) provides automated information lifecycle management and structured data optimization by relocating inactive data from expensive tier 1 production systems and legacy databases while preserving data integrity and access.

HPE SecureData provides an end-to-end data-centric approach for enterprise data protection.

Now, with the increasing data volumes, more and more networked devices, individual data protection along with more and more government regulatory laws such as GDPR (General Data Protection Regulation) to protect personal data it becomes more important to figure out ways in which data can be preserved as well as protected.

As a company with both the above products in our portfolio we can offer a solution which helps our customers to comply with GDPR in an easy manner.

Purpose

Purpose of this document is to provide requirements for the developers implementing integration SecureData (private instance) with SDM.

Overview

SDM is a product which deals with large volume of data and in the context of securing the data following features are to be supported:

1. Identification/de-identification of bulk of data
    - This feature is available to SDM administrators only
    - Identification is required in case of undo business flow
2. Access to secured data (something like reporting) to the user based on the user's access rights – such as can view masked data (partial data – this is available in web services only, not for SimpleAPI), full access or no access to the data at all

In the given context following features of SecureData are important:

1. Authentication methods (credentials)
    - Shared secret
    - Username/password (LDAP Server is required)
    - Certificate (LDAP server is required if LDAP group based matching criteria is used for identity authorization rules)
2. Identity
    - Apart from the credentials, user identity plays an important role in generation of secure key
    - We can think of this as two factor authentication to gain access (or protect) different kind of data, can also be thought of as an answer to security question, after passing the authentication phase if they know the correct answer to given security question then only they are allowed to access/protect a particular kind of data
    - In SecureData an identity is set per format (the authorization is through pattern matching on identity but to get unique secure key for encryption/decryption of any given data the identity has to be the same), a point to be noted here that multiple formats can have same identity.

Visualization of Secured (De-identified) Data

In this section let us visualize the data access to various users based on the access rights on the system.

Let us assume that we have following users in the system:

User	Access Rights
Admin	Can see all the data
UserS	Can see SSN data
UserC	Can see Credit Card data
UserSC	Can see SSN and Credit Card data

Customer Data in Production Database[1]

CustID	Name	SSN	Credit Card Number
1	Customer1	489-36-8350	4929-3813-3266-4295
2	Customer2	514-14-8905	5370-4638-8881-3020
3	Customer3	690-05-5315	4916-4811-5814-8111
4	Customer4	421-37-1396	4916-4034-9269-8783
5	Customer5	458-02-6124	5299-1561-5689-1938

Customer Data in Archive Database

CustID	Name	SSN	Credit Card Number
1	Customer1	612-20-6832	5293-8502-0071-3058
2	Customer2	300-62-3266	5548-0246-6336-5664
3	Customer3	660-03-8360	4539-5385-7425-5825
4	Customer4	213-46-8915	4916-9766-5240-6147
5	Customer5	449-48-3135	4556-0072-1294-7415

Customer Data from Archive Database for the UserS

CustID	Name	SSN	Credit Card Number
1	Customer1	489-36-8350	5293-8502-0071-3058
2	Customer2	514-14-8905	5548-0246-6336-5664
3	Customer3	690-05-5315	4539-5385-7425-5825
4	Customer4	421-37-1396	4916-9766-5240-6147
5	Customer5	458-02-6124	4556-0072-1294-7415

Customer Data in Archive Database for the UserC

CustID	Name	SSN	Credit Card Number
1	Customer1	612-20-6832	4929-3813-3266-4295
2	Customer2	300-62-3266	5370-4638-8881-3020
3	Customer3	660-03-8360	4916-4811-5814-8111
4	Customer4	213-46-8915	4916-4034-9269-8783
5	Customer5	449-48-3135	5299-1561-5689-1938

Customer Data in Archive Database for the UserSC/Admin

CustID	Name	SSN	Credit Card Number
1	Customer1	489-36-8350	4929-3813-3266-4295
2	Customer2	514-14-8905	5370-4638-8881-3020
3	Customer3	690-05-5315	4916-4811-5814-8111
4	Customer4	421-37-1396	4916-4034-9269-8783

[1] Data in green is accessible and data in red is not.

5	Customer5	458-02-6124	5299-1561-5689-1938

Now, it is easy for us to understand that the key to encrypt the data plays important role. We need to have this key based on the data format. In the above example, if key used for SSN and Credit Card Number are different then we will be able to achieve data access to the users based on their rights. In case of SecureData the key is generated based on the identity provided by the user. With this in mind, let us have identities per format as below:

Format	Identity
Social Security Number	idSSN
Credit Card	idCC
Alpha Numeric	idAlphaNum

Now, let us create a table with identity and user access rights mapping:

Identity	Admin	UserS	UserC	UserSC
idSSN	Full	Full	-	Full
idCC	Full	-	Full	Full
idAlphaNum	Full	-	-	-

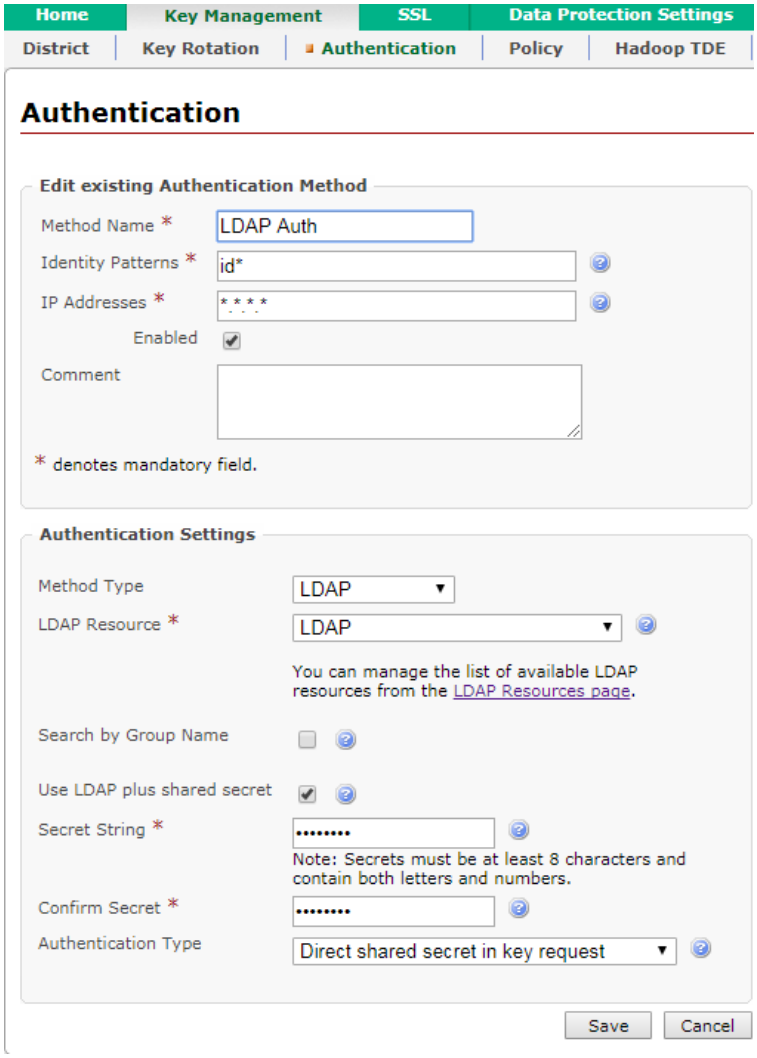
With this table, we understand that there should be some rules which are to be provided to restrict the identification (of the data) functionality based on the identity and user. This can be done using identity rules on SecureData side. We will be using this as an example in the following sessions.

Authentication Methods

SecureData uses shared secret, username/password and certificates as authentication mechanism. With SDM, we will be using only shared secret (in a limited manner) and username/password methods along with “LDAP + Shared Secret” mechanism.

Secure Data Settings

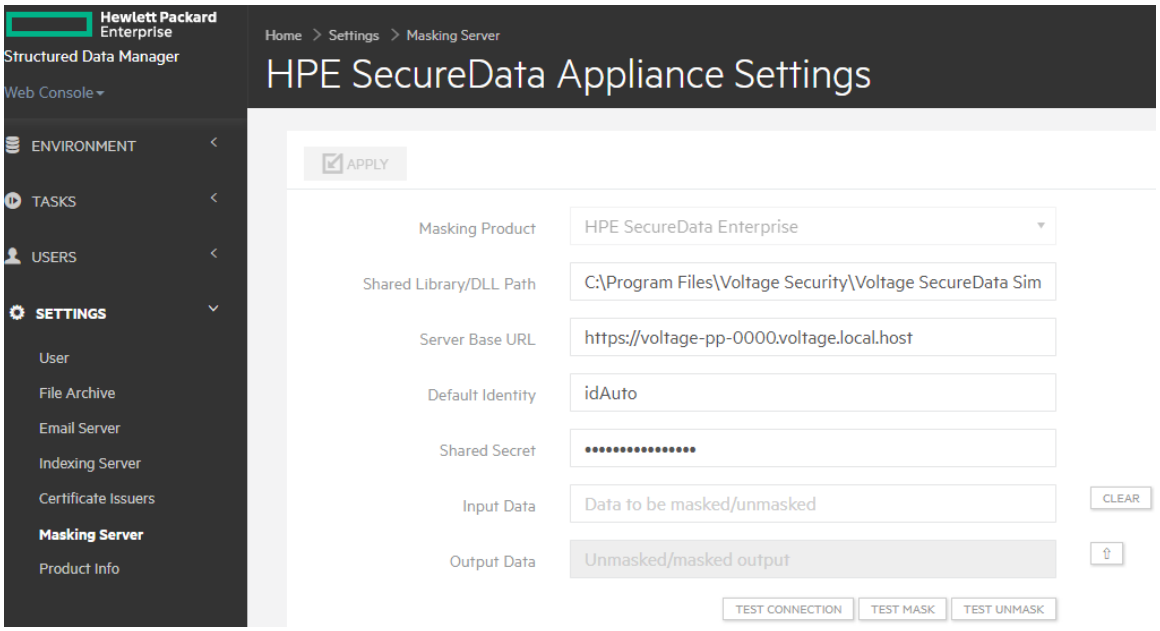
Create an authentication method as described on page 35 of SecureData Administrator Guide. Here is a screenshot for a quick reference:



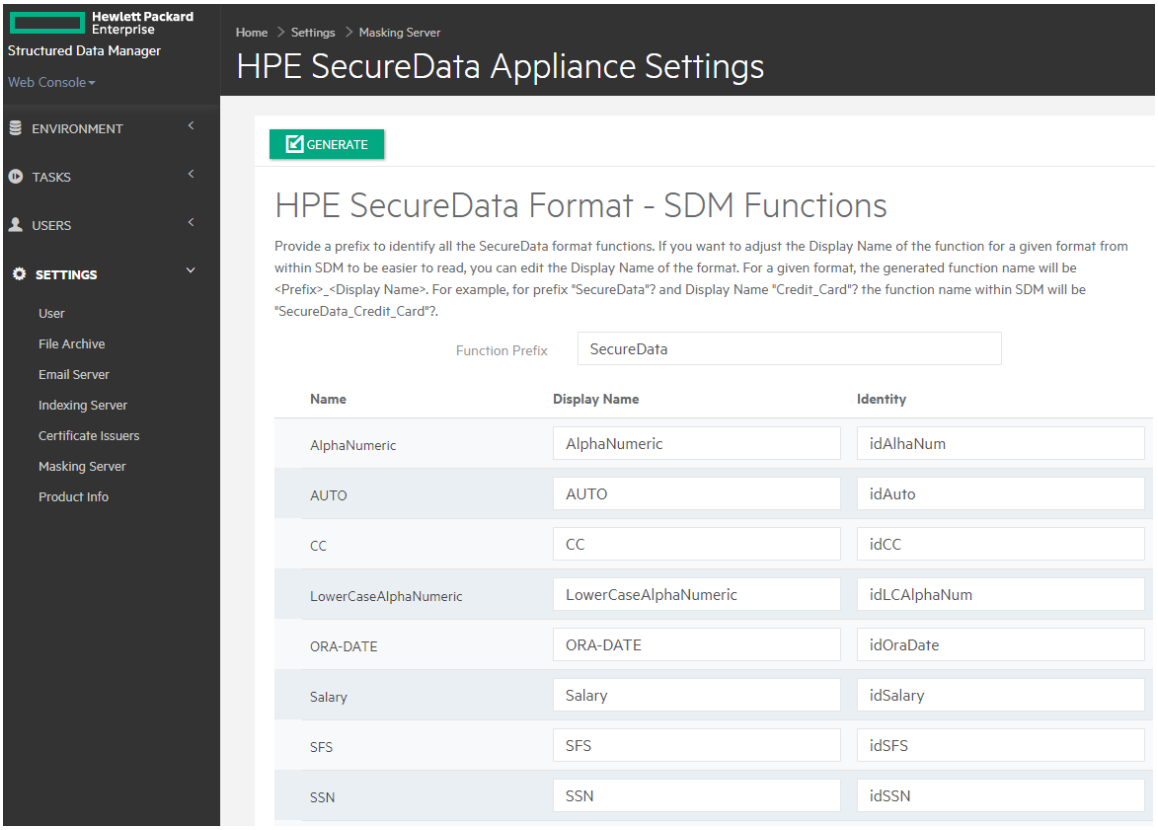
SDM Settings

The SDM side settings are to be done as below:

Default Identity



Format Specific Identity



Username/Password

This method requires LDAP instance. The identity rules on the SecureData side takes LDAP groups into account, so we need to make sure that we setup the LDAP group such that our access right requirements are satisfied.

LDAP Configuration

We need to make sure that we need to configure the groups such that they can be referred correctly in identity authorization rules of Secure Data. Also we need to make sure that identity groups are also formed for SDA to validate the identity for a given format. SDA needs the identity information for a group in “proxyAddresses” attribute and these identity groups can be made parent group of user groups. Following table specifies the details on users under a specific user group for the example data:

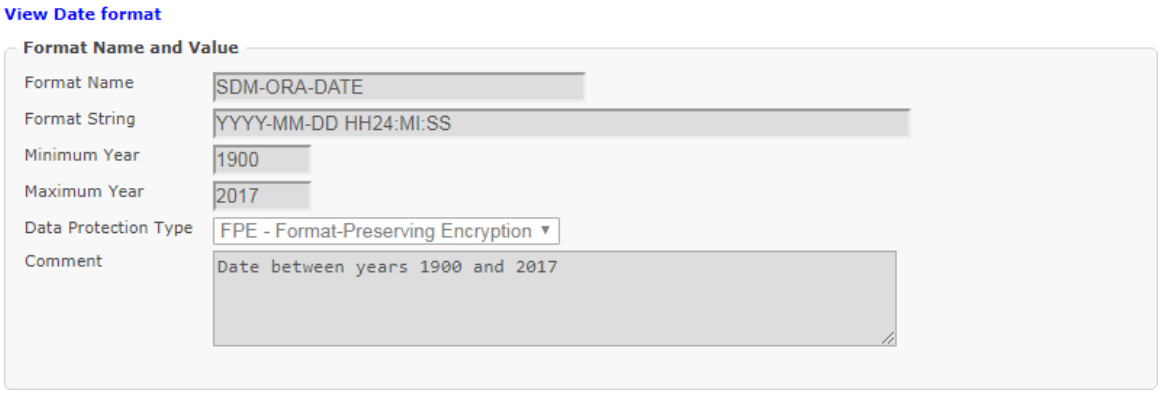
Group	Group Name	Users
Admin	G-Admin	Admin
Social Security Number	G-SSN	UserS, UserSC
Credit Card	G-CC	UserC, UserSC
OnlySDM	G-SDM	UserSDM

Following table specifies the identity groups with the user group as child groups:

Group	Group Name	User Groups	proxyAddresses
Social Security Number	G-idSSN	G-Admin, G-SSN	idSSN
Credit Card	G-idCC	G-Admin, G-CC	idCC

Date-Time Formats in SDM

In SDM the Date, DateTime or Timestamp database data types are treated in the same format as Timestamp type. The internal string representation of the Timestamp is of the format YYYY-MM-DD HH24:MI:SS.nnnnnnnnn (where n representation nanoseconds part). However, while using the same with SecureData for encryption/decryption the nanosecond part is ignored. SecureData appliance has ORA-DATE format which is different from SDM internal representation and it will not work for us. We need to create another Date type format in SDA to make sure that our Date-Time formats work correctly. You can create the same with the format string as YYYY-MM-DD HH24:MI:SS. This format has been shown in the screenshot below:



Note: Please note that anytime you add any new format to SDA, you need to make sure that you restart SDM Web Console.

Data Access Cartridge

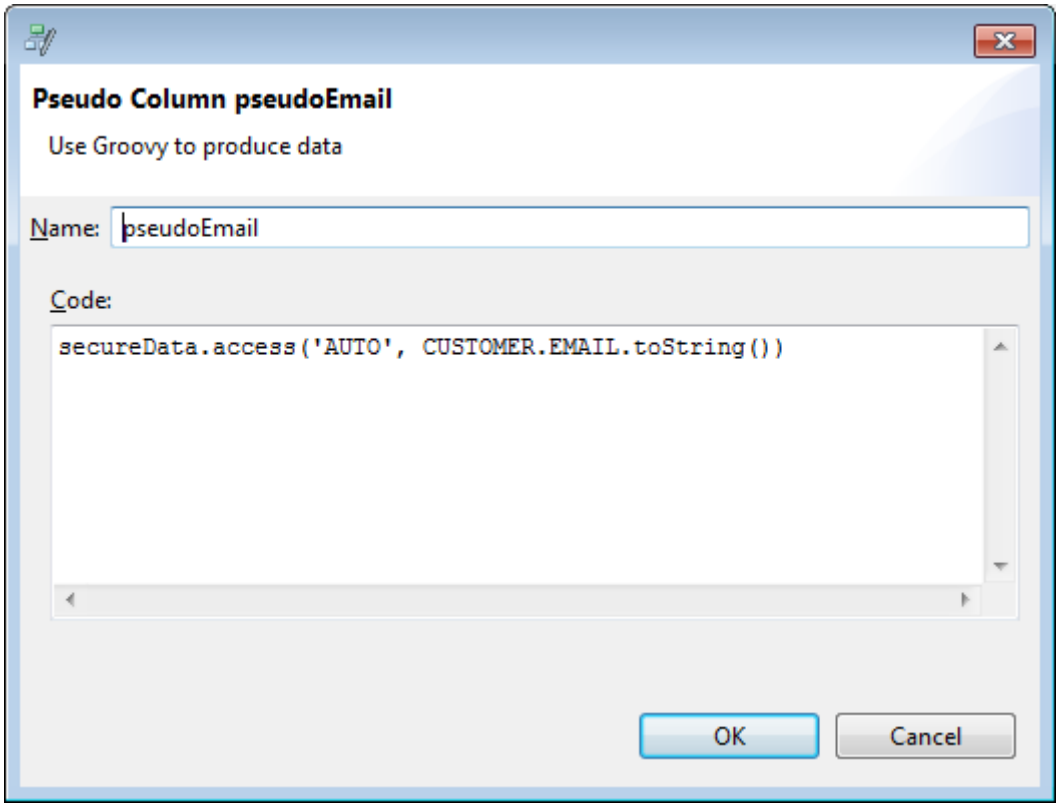
The de-identified data columns require pseudo column if the data is to be identified (decrypted). This identified data will be available to the user based on the privileges set in SDA. In the pseudo column one of the following groovy functions (of `secureData` object) is to be used to identify the data:

- String **access**(String format, String dataIn)
- Timestamp **access**(String format, Timestamp dataIn)
- BigDecimal **access**(String format, BigDecimal dataIn)

The format string is to be specified based on the format of the data stored in the column and appropriate conversion function is to be used for `dataIn`. For each of the function here are the example usages:

- `secureData.access('AUTO', CUSTOMER.EMAIL.toString())`
- `secureData.access('AUTO', CUSTOMER.DATEOFBIRTH.toTimestamp())`
- `secureData.access('AUTO', CUSTOMER.CUSTOMERID.toBigDecimal())`

An example screen shot is given below:



Similar identification of the de-identified (encrypted) data one can use protect method available in `secureData` object to encrypt (or de-identify) the data in DAC, following methods are available for the same:

- String **protect**(String format, String dataIn)
- Timestamp **protect**(String format, Timestamp dataIn)
- BigDecimal **protect**(String format, BigDecimal dataIn)

Appendix A

SSL Certificates

We need to make sure that we trust the SDA certificate. We need to add this certificate in our trust store. For Windows, please refer to HPE_SecureData_SimpleAPI_5.10_Install.pdf (Trusted Root Certificates section). Also, we need to make sure that Java trust store also has the SDA root certificate. A sample command is below:

"<SDM Install Directory>\jre\bin\keytool" -import -trustcacerts -alias VoltageInternal -file "<Path to Cerfiticate File>" -keystore "<SDM Install Directory>\jre\lib\security\cacerts"

Default password: changeit

For example:

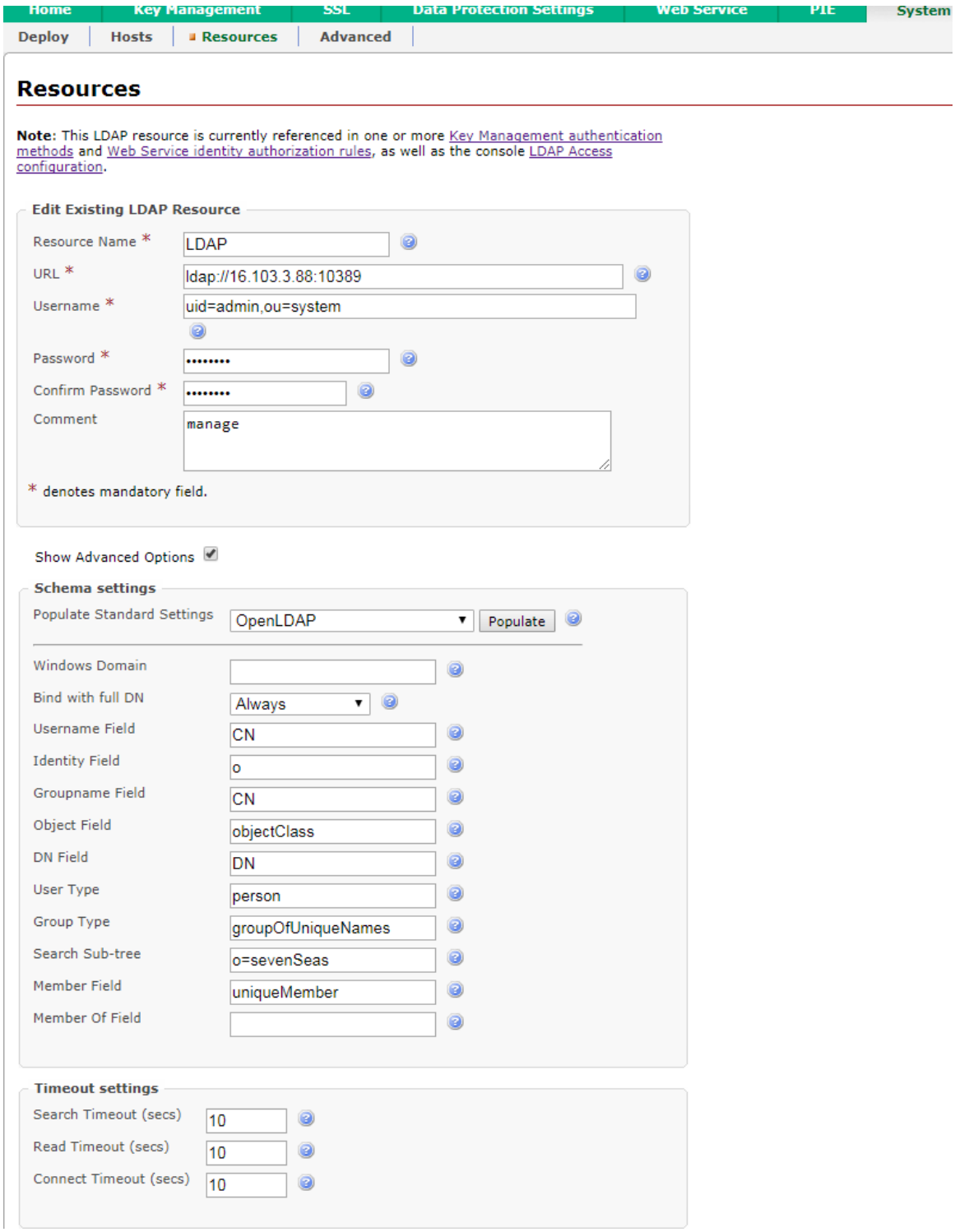
"C:\Program Files\HPESDM752\jre\bin\keytool" -import -trustcacerts -alias VoltageInternal -file "C:\Temp\Acne Root.cer" -keystore "C:\Program Files\HPESDM752**\jre\lib\security\cacerts**"

Please note that the keystore to be used is the cacerts file under jre/lib/security directory.

Note: If you are using Windows 7, it may so happen that the public SecureData instance (voltage-pp-0000.dataprotection.voltage.com) provided for testing purpose may give you an error (in the sdm.log file you will see an error VE_ERROR_CANNOT_VERIFY_CERT). This is due to one of the update is missing on your OS. Please refer to https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-default-secure-protocols-in for required Windows 7 update. If the update is done then you need to make sure that you apply “Easy fix” provided in the same article.

Appendix B

SDA Setup with OpenLDAP



Appendix C

SDA Setup with Active Directory