



Administration Guide | INTERNAL – Authorized for SAP Customers and Partners
yyyy-mm-dd

General

Content

1	General	6
1.1	Introduction - Manage Data Retention App.	6
	Manage Data Retention Periods.	6
	Export Data.	6
	Delete Expired Data.	7
	Change Log.	7
1.2	Manage Users - Introduction.	8
	View Users.	8
	View Apps and User Access.	8
	Add User.	9
	Copy User.	9
	Edit User.	9
	Delete User.	10
	Approve User Request.	10
	Export or Delete Personal Data.	10
1.3	Manage Connections - Introduction.	10
	View Connections.	11
	Disconnect a Business Partner.	11
	Activate Connection to a SAP Customer.	11
	Reconnect to a SAP Customer.	12
	Subscription Metrics.	12
1.4	Manage Certificates - Introduction.	12
1.5	Certificate based Authentication.	13
	SAP Certificates.	14
1.6	Trusted Certificate Authorities.	14
1.7	Manage Certificates App.	21
	View your company Certificates.	21
	Download your company certificates.	22
	Replace Expiring Certificate.	22
	Delete Unused Certificate.	23
	Download SAP Certificates.	23
	Notification of Expiring Certificates.	23
1.8	Important Disclaimers and Legal Information	24
2	Regulatory Reportings	26
2.1	EU Hub - Reporting App.	26
2.2	Home Page.	27

	Personalize Homepage.	27
2.3	Requesting Reports.	27
	Finding Your EMVO Organization ID.	27
	Requesting a Report.	28
	Available Reports.	28
2.4	Downloading Reports.	29
	Downloading a Report.	29
2.5	Managing Alerts.	29
	Configuring Alert Management.	30
	Setting up Authentication.	30
	Viewing and Processing Alerts.	32
	Authenticating Alerts.	32
3	Supply Chain Partner Collaboration.	35
3.1	Creating Trade Items - Introduction.	35
4	U.S. Drug Supply Chain Security.	37
4.1	Exception Management	37
	Purpose and scope.	37
	About Exception Management.	37
	Manage Exceptions Web App.	38
	Integration with SAP ATTP.	38
4.2	Transaction Information Exchange.	39
	Introduction.	39
	About.	40
	View Transaction Information with Onboarding.	40
	View Transaction Information without Onboarding.	42
	Introduction -Transaction Information (TI) Exchange Service Description	45
	About.	46
	Transaction Information (TI) Exchange.	47
	Onboarding Partners.	48
	Transaction Information Web App.	49
	Sending TI Messages to Partner without GLN	50
	Sending HDA 856 ASN to Partners.	50
	Message Format.	51
4.3	Trace Management	51
	Introduction	51
	User Access and Roles.	52
	Trace Management Web App.	52
	Optional Approval Process.	56
	Setting Up Trace Management.	56
	Integrating ATTP for Trace Response.	56

4.4	Verification Router Service	57
	Introduction.	57
	Managing the Lookup Directory	58
	About this document.	87
	Lookup Directory.	90
	Sending Product Information to SAP Verification Repository.	92
	Verification.	94
	Managing Alerts.	121
	Verification Repository Explorer.	124
	Manage Verification Settings.	125
4.5	About US Drug Supply Chain Security.	126
	Trace Request Management.	126
	Web Apps.	127
	Verification.	129
	Introduction.	132
5	Manage Users - Introduction.	133
5.1	View Users.	133
5.2	View Apps and User Access.	133
5.3	Add User.	134
5.4	Copy User.	134
5.5	Edit User.	135
5.6	Delete User.	135
5.7	Approve User Request.	135
5.8	Export or Delete Personal Data.	135
6	Web Apps Introduction.	136
6.1	Permitted Apps.	136
6.2	Technical Pre-requisites.	136
6.3	Test Area.	137
6.4	Home Page.	137
	Personalize Homepage.	137
6.5	Filter Data Displayed.	137
6.6	View Change Logs.	137
7	Manage Users - Introduction.	139
7.1	View Users.	139
7.2	View Apps and User Access.	139
7.3	Add User.	140
7.4	Copy User.	140
7.5	Edit User.	141
7.6	Delete User.	141

7.7	Approve User Request.	141
7.8	Export or Delete Personal Data.	141
8	Manage Messages - Introduction.	142
9	Manage Company Data - Prerequisites.	143
9.1	Add Company Data.	143
9.2	Edit Company Data.	144
9.3	Delete Company Data.	144
9.4	Global Company Prefix.	145
9.5	View Change Log.	145
10	Manage Company Data - Partners.	146
11	Manage Certificates - Introduction.	147
12	Certificate based Authentication.	148
12.1	SAP Certificates.	149
13	Trusted Certificate Authorities.	150
14	Manage Certificates App.	158
14.1	View your company Certificates.	158
14.2	Download your company certificates.	159
14.3	Replace Expiring Certificate.	159
14.4	Delete Unused Certificate.	160
14.5	Download SAP Certificates.	160
14.6	Notification of Expiring Certificates.	161
15	Important Disclaimers and Legal Information	162

1 General

1.1 Introduction - Manage Data Retention App

The Manage Data Retention app allows you to define the data retention period for different scenarios based on region specific regulations. You can also export and delete expired data.

1.1.1 Manage Data Retention Periods

Context

Data retention settings define how long message and transaction data is stored in the system. Retention periods can be configured to meet organizational policies and regional regulatory requirements.

Procedure

1. Log on to SAP Traceability Hub Connectivity, navigate to Manage Data Retention.
2. Select [Data Retention Period settings](#).
3. Click [Add](#).
4. Select a scenario.
5. Enter the retention period.
6. Save.

1.1.2 Export Data

Context

Before deleting expired records, users can export and download retained data for archival, compliance, or audit purposes. The exported files are packaged in ZIP format for easy storage and retrieval.

Procedure

1. Log on to SAP Traceability Hub Connectivity, navigate to Manage Data Retention.
2. Click [Data Retention](#).
3. Ensure the retention period is defined for the scenario.
4. Select the scenario.
5. Click [View Expired](#).
6. Click [Continue](#).

Expired data is added to zip files.

Zip files are available in the Expired Data File column.

The Last Retrieved On column is updated with the date when data is retrieved.

7. Click the link in the Expired Data File column.
Zip files are displayed.
8. Select all or individual files.
9. Click [Download](#).

1.1.3 Delete Expired Data

Context

Delete Expired Data permanently removes records that have exceeded the configured retention period. This helps organizations manage storage efficiently while maintaining compliance with data retention policies

Procedure

1. Select a scenario.
2. Click [Delete Expired](#).
3. Confirm deletion.

When data is deleted, Last Deleted On is updated and Status shows Deletion Completed.

The Zip files containing Expired data remain available for two months.

1.1.4 Change Log

The Change Log provides a complete audit trail of user activities within the application, including retention-period changes, data exports, and deletion actions. This improves transparency and supports compliance requirements.

The Change Log records all actions, including data retention period settings, export or deletion of data.

1.2 Manage Users - Introduction

As an Administrator, you can:

- Add, edit, and delete users and administrators
- Give users access to apps, and define the rights and actions each user can perform in each app
- Reset password of users

1.2.1 View Users

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.

The Manage Users screen displays user details, including the following:

- Display Name
 - Email address
 - User Type: Administrator or User
 - Last Login
 - Changed on & Created on details
 - Status: Active or inactive
2. To search the list, enter text in the search field, and press [Enter](#).
 3. To clear the search field, select [X](#).
 4. To sort the list based on Display Name or Changed Date, click the [Sort](#) icon .
 5. To view details of a user, click the user name in the list.

The User Details screen displays the details along with the list of applications that the user has access to.

1.2.2 View Apps and User Access

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Click [Applications](#) from the Left Navigation Menu .
A list of apps displays, and active users display.
3. To view users of an app, select the app.

1.2.3 Add User

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Click [Add](#).
3. Select User Type whether Administrator or User .
An Administrator has access to the Manage Users app.
4. Select the applications as required.
5. Click [Add](#).
The user receives an activation email.

1.2.4 Copy User

Context

To add a new user, you can copy one user and edit the app details as required. The user type and permitted apps are copied.

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Select a user you wish to copy.
The User Details screen displays.
3. Click [Copy](#).
The New User screen displays. The User Type and permitted apps are copied to a new user.
4. Enter First Name, Last Name, Email of new user . You can change User Type, and add or remove app access.
5. Click [Save](#).
The new user is created with input details.

1.2.5 Edit User

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the Manage Users tile.
2. Select a user.

The User Details screen displays.

3. Click [Edit](#). You can change the First Name, Last Name, Status, User Type and add or remove app access.
4. Click [Save](#). For changes to take effect, the user must log out and log in again.

1.2.6 Delete User

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Select a user.
The User Details screen displays.
3. Click [Delete](#).
A Confirmation dialog box displays.
4. Click [OK](#) to confirm deletion.

1.2.7 Approve User Request

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Click [User Request](#) from the Left Navigation Menu.
New User Request for Approval or Rejection will be available.
3. Choose the User Type, to Approve (or) reject the request with a comment.

1.2.8 Export or Delete Personal Data

To export or delete personal data, contact SAP Support. See also, [Security Policy and Procedures](#).

1.3 Manage Connections - Introduction

You must be authorized to use the Manage Connections app. If you do not have access to the app, contact your company Web App Administrator.

The Manage Connections app allows you to:

- View the list of business partners connected to your organization through the SAP Traceability Hub Connectivity

- Disconnect a business partner
- Activate connections to other SAP Customers

1.3.1 View Connections

SAP customers can view connections to their business partners on the Customer View tab, and their connections to other SAP customers on the Business Partner View tab, which shows:

- Connections by status including Open, Connected and Disconnected
- Accepted connection requests in the Connected section
- Disconnected connections in the Disconnected section

1.3.2 Disconnect a Business Partner

Procedure

1. On the SAP Traceability Hub Connectivity Homepage, navigate to [General > Manage Connections](#).
2. Click [Customer View](#).
3. Select [Connected](#) status in the drop-down. The Connected Business Partners list is displayed.
4. For the required connection, click [Disconnect](#). The status of the connection changes to Disconnected.

1.3.3 Activate Connection to a SAP Customer

Procedure

1. On the SAP Traceability Hub Connectivity Homepage, navigate to [General > Manage Connections](#).
2. Click [Business Partner View](#).
3. Select the [Open](#) status from the drop-down.
4. Select [Activate Connection](#).
The status of the connection changes to Connected and displays in the Connected section.

📘 Note

Automatic reminders are sent every two days for a maximum of five times to the Business Partner to activate the connection.

1.3.4 Reconnect to a SAP Customer

Procedure

1. On the SAP Traceability Hub Connectivity Homepage, navigate to [General > Manage Connections](#).
2. Click [Business Partner View](#).
3. Select [Disconnected](#) status in the drop-down. The associated list is displayed.
4. Click [Reconnect](#).

1.3.5 Subscription Metrics

Context

You can view metrics of scenarios and sub-scenarios.

Procedure

1. On the SAP Traceability Hub Connectivity Homepage, navigate to [General > Manage Connections](#).
2. Click [Subscription Metrics](#). The Count column shows metrics for scenarios and sub-scenarios.
3. You can also download details of partners who use the View Transaction App if required.

1.4 Manage Certificates - Introduction

This document describes the security certificate process for connecting to the SAP Information Collaboration Hub for Life Sciences including a list of approved Certificate Authorities.

This document also describes the features and use of the Manage Certificates app which allows you to upload and download certificates and monitor upcoming certificate replacement dates.

Target Audience

This document is for all stakeholders including:

- Security Officers
- Integration engineers
- Implementation engineers and partners

Related Information

- [SAP Traceability Hub Connectivity help pages](#).

1.5 Certificate based Authentication

Context

In the interest of securing your data, the SAP Traceability Hub Connectivity uses certificate-based authentication. To comply with security best practices, all certificates must be signed by one of the SAP Trusted Certificate Authorities, in .cer or .crt format. Self-signed certificates are not accepted.

Note

Transport Layer Security version must be TLS 1.2.

Note

SAP Traceability Hub Connectivity security certificates are available in the Security section of the [Help page](#).

Procedure

1. To begin, you need to generate a keypair on your system. At this point, the keypair is self-signed, that is, you trust your own certificate!
2. You now raise a Certificate Signing Request. This is a block of text, which contains a thread of: private key some public key materials
3. Next you choose a Certificate Authority if you don't already have one.
4. Then you log onto the Certificate Authority's secure website to upload your Certificate Signing Request.
5. Enter information such as: proof of domain ownership, names, email addresses, physical addresses.
6. The Certificate Authority then investigates to ensure the request is from an authentic source. The investigation may include emails, phone calls, correspondence.
7. After the Certificate Authority confirms the authenticity of the request, the Certificate Authority provides a signed certificate response.
8. You import this into your keystore.
9. At this point, your self-signed key is promoted to a signed keypair, which you can share with SAP and all business partners who will be happy that you are using a trusted certificate.

For more information see

https://sapvideo.cfapps.eu10-004.hana.ondemand.com/?entry_id=1_5yu1np2e

1.5.1 SAP Certificates

SAP Traceability Connectivity certificates are available in the Security section of the [Help page](#).

1.6 Trusted Certificate Authorities

This list may contain links to foreign (i.e. non SAP group of companies) sites. SAP is not responsible for the privacy practices or the content of other websites outside the SAP Group of companies. Therefore, we recommend that you carefully read the privacy statements of such foreign sites. Please refer to the SAP Privacy Statement here: <https://www.sap.com/about/legal/privacy.html> 

See also [2801396 - SAP Global Trust List - SAP for Me](#) 

Certificate Authority	DN	Serial Number	Expiration Date MM-DD-YYYY
Baltimore CyberTrust Root	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	02 00 00 b9	05-13-2025
Entrust Root Certification Authority	CN = Entrust Root Certification Authority OU = (c) 2006 Entrust, Inc. OU = www.entrust.net/ CPS  is incorporated by reference O = Entrust, Inc. C = US	45 6b 50 54	11-27-2026
Entrust Root Certification Authority - G2	CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms  O = Entrust, Inc. C = US	4a 53 8c 28	12-07-2030

Entrust.net Certification Authority (2048)	CN=Entrust Root Certification Authority, OU=(c) 2006 Entrust\, Inc., OU= www.entrust.net/CPS is incorporated by reference,O=Entrust\, Inc., C=US	38 63 de f8	07-24-2029
Go Daddy Root Certificate Authority - G2	CN = Go Daddy Root Certificate Authority - G2 O = GoDaddy.com , Inc. L = Scottsdale S = Arizona C = US	00	01-01-2038
DigiCert Global Root CA	CN = DigiCert Global Root CA OU = www.digicert.com O = DigiCert Inc C = US	08 3b e0 56 90 42 46 b1 a1 75 6a c9 59 91 c7 4a	11-10-2031
DigiCert High Assurance EV Root CA	CN=DigiCert High Assurance EV Root CA, OU= www.digicert.com , O=DigiCert Inc, C=US	2A C5 C26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	11-10-2031
COMODO RSA Certification Authority	CN = COMODO RSA Certification Authority O = COMODO CA Limited L = Salford S = Greater Manchester C = GB	4c aa f9 ca db 63 6f e0 1f f7 4e d8 5b 03 86 9d	01-19-2038

USERTrust RSA Certification Authority	CN = USERTrust RSA Certification Authority O = The USERTRUST Network L = Jersey City S = New Jersey C = US	01 fd 6d 30 fc a3 ca 51 a8 1b bc 64 0e 35 03 2d	01-19-2038
QuoVadis Root CA 2 G3	CN = QuoVadis Root CA 2 G3 O = QuoVadis Limited C = BM	44 57 34 24 5b 81 89 9b 35 f2 ce b8 2b 3b 5b a7 26 f0 75 28	01-12-2042
SAP Global Root CA	CN = SAP Global Root CA O = SAP AG L = Walldorf C = DE	5d 03 d9 3d 31 61 5d 8f 48 8b 39 70 c7 8f 1b 99	04-26-2032
Roche G3 Root CA	CN=Roche G3 Root CA, O=F. Hoffmann-La Roche Ltd	1B 10 29 15 BC 10 2B B8 4C E3 16 59 C2 02 CB 93	06-15-2038
GlobalSign Root CA	CN = GlobalSign Root CA OU = Root CA O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 15 4b 5a c3 94	01-28-2028
DigiCert Global Root G2	CN = DigiCert Global Root G2 OU = www.digicert.com 📌 O = DigiCert Inc C = US	03 3a f1 e6 a7 11 a9 a0 bb 28 64 b1 1d 09 fa e5	01-15-2038
SAP Cloud Root CA	CN=SAP Cloud Root CA, O=SAP SE,L=Walldorf, C=DE	18 77 0F BE 65 06 6B BF 4C EA 93 38 D9 B1 85 62	02-13-2039

DigiCert Assured ID Root CA	CN = DigiCert Assured ID Root CA OU = www.digicert.com 🌐 O = DigiCert Inc C = US	0ce7e0e517d846fe8fe560fc1bf03039	11-10-2031
Amazon Root CA 1	CN=Amazon Root CA 1 O=Amazon C=US	06 6c 9f cf 99 bf 8c 0a 39 e2 f0 78 8a 43 e6 96 36 5b ca	01-17-2038
Atos TrustedRoot 2011	CN = Atos TrustedRoot 2011 O = Atos C = DE	5c 33 cb 62 2c 5f b3 32	01-01-2031
Certum CA	CN=Certum CA O=Unizeto Sp. z o.o. C=PL	01 00 20	06-11-2027
COMODO Certification Authority	CN=COMODO Certification Authority O=COMODO CA Limited L=Salford SP=Greater Manchester C=GB	20 a4 c4 7f dd df e1 c7 53 63 07 13 88 77 60 12	01-01-2031
COMODO ECC Certification Authority	CN = COMODO ECC Certification Authority O = COMODO CA Limited L = Salford S = Greater Manchester C = GB	1f 47 af aa 62 00 70 50 54 4c 01 9e 9b 63 99 2a	01-19-2038
GlobalSign Root CA - R3	CN=GlobalSign O=GlobalSign OU=GlobalSign Root CA - R3	04 00 00 00 00 01 21 58 53 08 a2	03-18-2029
Go Daddy Class 2 Certification Authority	OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US	00	06-29-2034

GTS Root R1	C = US O = Google Trust Services LLC CN = GTS Root R1	02 03 e5 93 6f 31 b0 13 49 88 6b a2 17	06-22-2036
GTS Root R2	C = US O = Google Trust Services LLC CN = GTS Root R2	02 03 e5 ae c5 8d 04 25 1a ab 11 25 aa	06-22-2036
GTS Root R3	C = US O = Google Trust Services LLC CN = GTS Root R3	02 03 e5 b8 82 eb 20 f8 25 27 6d 3d 66	06-22-2036
GTS Root R4	C = US O = Google Trust Services LLC CN = GTS Root R4	02 03 e5 c0 68 ef 63 1a 9c 72 90 50 52	06-22-2036
ISRG Root X1	CN=ISRG Root X1 O=Internet Security Re- search Group C=US	00 82 10 cf b0 d2 40 e3 59 44 63 e0 bb 63 82 8b 00	06-04-2035
QuoVadis Root CA 2	CN=QuoVadis Root CA 2 O=QuoVadis Limited C=BM	05 09	11-24-2031
Starfield Class 2 Certification Authority	OU=Starfield Class 2 Certifi- cation Authority O=Starfield Technologies, Inc. C=US	00	06-29-2034

Starfield Services Root Certificate Authority - G2	CN=Starfield Services Root Certificate Authority - G2 O=Starfield Technologies, Inc. L=Scottsdale S=Arizona C=US	00	01-01-2038
SwissSign Gold CA - G2	CN=SwissSign Gold CA - G2 O=SwissSign AG C=CH	00 bb 40 1c 43 f5 5e 4f b0	10-25-2036
SwissSign Platinum CA - G2	CN=SwissSign Platinum CA - G2 O=SwissSign AG C=CH	4e b2 00 67 0c 03 5d 4f	10-25-2036
SwissSign Silver CA - G2	CN=SwissSign Silver CA - G2 O=SwissSign AG C=CH	4f 1b d4 2f 54 bb 2f 4b	10-25-2036
T-TeleSec GlobalRoot Class 2	CN=T-TeleSec GlobalRoot Class 2 OU=T-Systems Trust Center O=T-Systems Enterprise Services GmbH C= DE	01	10-02-2033
Autoridade Certificadora Raiz Brasileira v10	CN=Autoridade Certificadora Raiz Brasileira v10 OU=Instituto Nacional de Tecnologia da Informacao – ITI O=ICP-Brasil C=BR	d2 d5 8b 44 bf 81 93 42	07-01-2032

Autoridade Certificadora Raiz Brasileira v11	CN=Autoridade Certificadora Raiz Brasileira v11 OU=Instituto Nacional de Tecnologia da Informacao – ITI O=ICP-Brasil C=BR	24 2b 60 d4 cd 43 69 7f	07-01-2032
Autoridade Certificadora Raiz Brasileira v2	CN=Autoridade Certificadora Raiz Brasileira v2 OU=Instituto Nacional de Tecnologia da Informacao – ITI O=ICP-Brasil C=BR	01	06-22-2023
Autoridade Certificadora Raiz Brasileira v5	CN=Autoridade Certificadora Raiz Brasileira v5 OU=Instituto Nacional de Tecnologia da Informacao – ITI O=ICP-Brasil C=BR	01	03-03-2029
AAA Certificate Services	CN=AAA Certificate Services O=Comodo CA Limited L=Salford ST=Greater Manchester C=GB	01	01-01-2029
GeoTrust Primary Certifica- tion Authority - G2	CN=GeoTrust Primary Certif- ication Authority - G2 OU=(c) 2007 GeoTrust Inc. - For authorized use only O=GeoTrust Inc. C=US	3c b2 f4 48 0a 00 e2 fe eb 24 3b 5e 60 3e c3 6b	01-19-2038

SAP Internet of Things CA	CN=SAP Internet of Things CA	00	07-18-2040
	O=SAP IoT Trust Community II		
	C=DE		

1.7 Manage Certificates App

The Manage Certificates app allows you to:

- Upload and activate a certificate to replace an expiring certificate
- View the number of days before a certificate expires
- View and download your TLS and MLS certificates
- Delete unused certificates
- View changes made by different users
- Download SAP certificates

You must be authorized to use the Manage Certificates app. If you do not have access to the app, contact your company Web App Administrator.

The app sends email notifications when a certificate is due to expire.

1.7.1 View your company Certificates

Context

This feature enables users to access and review company certificates, helping ensure secure and uninterrupted communication with SAP systems.

Procedure

1. Log on to the Traceability Hub Connectivity portal and navigate to General > Manage Certificates tile.
2. The Manage Certificates screen displays your TLS and MLS certificate details, including: Certificate Status: Active, Inactive or Expired Environment: Dev, QA, Staging Number of days before certificate expires with expiry Date <https://me.sap.com/notes/>  The Environment refers to your backend system's environment connected to SAP.
3. To search the list, enter text in the search field, and press Enter.
4. To clear the search field, select X.

5. To Sort the list based on Certificate Name, Status, Alias Name, Expiry Date or Last Modified, select Sort.
6. To view details of a certificate, select the certificate. The Certificate Details screen displays.

1.7.2 Download your company certificates

Context

The process starts at the Homepage. It allows users to securely download their organization's TLS and MLS certificates for backup, validation, or configuration purposes, ensuring continued secure communication with SAP systems.

Procedure

1. Log on to the Traceability Hub Connectivity portal and navigate to General > Manage Certificates.
2. Click the Download Certificate icon for the certificate you want to download.

1.7.3 Replace Expiring Certificate

Context

The process starts at the Homepage. It enables users to upload and activate a new certificate before the existing one expires, ensuring uninterrupted secure communication and compliance with SAP's certificate requirements

Procedure

1. Log on to the Traceability Hub Connectivity portal and navigate to General > Manage Certificates.
2. Upload your Client certificate in .cer or .crt format. This is used for authentication when you send messages to SAP. Self-signed certificates are not accepted. The certificate must be from an SAP Certificate Authority. <https://me.sap.com/notes/>  The Web App allows you to upload a maximum of five certificates, with only one active.
3. To activate the certificate, select the certificate and click Activate. The status of the certificate changes to Active and In Use for sending messages to SAP.

1.7.4 Delete Unused Certificate

Context

The process starts at the Homepage. It allows users to remove inactive or obsolete certificates that are no longer required, helping maintain an organized and secure certificate repository.

Procedure

1. Log on to the Traceability Hub Connectivity portal and navigate to General > Manage Certificates.
2. Select a certificate. The certificate details screen displays.
3. Select an unused certificate.
4. Click Delete. Note: You cannot delete a certificate that is in use.

1.7.5 Download SAP Certificates

Context

The process starts at the Homepage. It allows users to download SAP certificates required for establishing secure and trusted connectivity with SAP systems.

Procedure

1. Log on to the Traceability Hub Connectivity portal and navigate to General > Manage Certificates.
2. Select Download SAP Certificates. This downloads SAP's TLS and MLS certificates for sending to SAP and receiving from SAP in a Zip file.
3. Import these certificates into your backend system.

1.7.6 Notification of Expiring Certificates

Context

Customers receive email alerts for TLS and MLS certificates due to expire within 30 days. An email is sent to all administrators and users of the Manage Certificates app.

The email is sent 30 days, 15 days, 7 days, 6 days, 5 days, 4 days, 3 days, 2 days and 1 day before expiry of a certificate.

Procedure

To add and remove administrators, use the Manage Users app.

Caution: Customers are responsible for monitoring, managing and updating valid certificates. Failure to do so can result in disruption of message exchange.

1.8 Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines/strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: <http://help.sap.com/disclaimer>)

2026 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.

2 Regulatory Reportings

2.1 EU Hub - Reporting App

Purpose and Scope

This document describes the Web App Reporting service provided by the SAP Traceability Hub Connectivity for Regulatory Reporting to the European Medicines Verification Organization (EMVO)

Target Audience

This document is for customers and partners of the SAP Traceability Hub Connectivity who use the EMVO Regulatory Reporting Web App Reporting function.

Functions Available

The EU-Hub Reporting App meets the business requirements for the requesting and downloading of reports from the EU-Hub.

The EU-Hub Reporting App allows you to:

- Request all products in CSV or PDF format
- Download reports once the request has been submitted
- Review alerts from the EU-Hub

Technical Prerequisites

The following are required to use the Web App.

- High speed Internet connection > 1 Mbps
- Chrome browser which includes the following enabled:
 - Downloads - for downloading serial numbers in a file
 - base64 decoder
 - Certificate-based authentication
 - SAP trusted certificates - certificates are probably trusted already
 - Pop ups - for selecting items, and uploading commissioned serial numbers
 - Browser redirect
- Hostname provided by SAP allowed on your firewall
- Network configured to allow resolution of URLs provided by SAP using public DNS
- Email addresses must be on a corporate domain, and you must manage the validity of email addresses
- Your internal network and firewall is configured to allow outbound SSL calls from your network to the Internet using port 443

Note

If you are unsure about some of these technical details, contact your IT team.

Assumptions

This user guide assumes you are familiar with the pharmaceutical industry and EU-Hub terminology.

2.2 Home Page

The Homepage is the main access for all Apps.

Tiles are displayed for each App you use. The number of tiles present depends on your permissions. If you do not see a tile that you need, contact SAP.

To begin, you can:

- Log in to start using your Apps.
- View your user profile in Settings.
- Search for information by selecting the magnifying glass icon.
- Use the Help available, by selecting the Help icon.

2.2.1 Personalize Homepage

You can personalize the Homepage by selecting the [Edit Homepage](#) option in the EU-Hub user profile. You can create new Launchpad groups and move tiles around between groups.

2.3 Requesting Reports

To request a report, you need the four-digit Organization ID that the EMVO assigned to you.

2.3.1 Finding Your EMVO Organization ID

To find your EMVO Organization ID:

- Go to your EMVO onboarding portal.
- View IQE or PRD connection details.
- Download the IQE or PRD certificate.

The certificate name includes:

- A letter, D or M
- Four digits
- A dot
- One digit

Your Organization ID is the four-digit number:

M. **XXXX**.1

In the example

M. **1234**.1

1234 is the Organization ID.

2.3.2 Requesting a Report

Procedure

1. Logon to the SAP Traceability Hub Connectivity portal.
2. Navigate to the [Regulatory Reporting > EU Regulatory Reporting](#) section in the left pane.
3. Select [Request Report](#) tile.
4. Select [Request all Products](#), and CSV or PDF file type.
5. Select [New Request](#) at the bottom of the screen.
6. Enter your four-digit Organization ID given to you by the EMVO.
7. Select [Start Request](#) at the bottom of the screen.
8. To view requested reports, go to the [Report Download App](#).

2.3.3 Available Reports

The following reports are available:

- Batch Recall Report
- Pack Disclosure Report
- Product Master Report (Single)
- Product Master Report (All)
- Packs by Batch Report
- Withdrawn Product Report

The content of each report is defined by the EMVO in the SDK for OBPS v16.0 Appendix B: Reports Reference

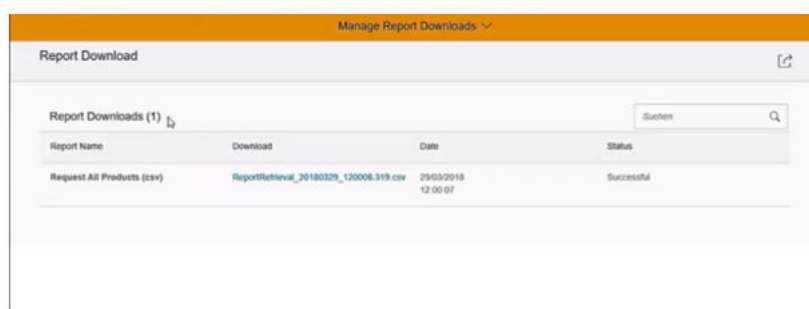
2.4 Downloading Reports

This page allows you to view and download your requested reports.

2.4.1 Downloading a Report

Procedure

1. Logon to the SAP Traceability Hub Connectivity portal.
2. Navigate to Regulatory Reporting > EU Reporting.
3. Select the Report Download tile.
Downloaded reports are visible.
4. To view the status of a report, select the report. Successful reports are highlighted in blue.
5. Select the highlighted text of the report to download.



The screenshot shows a web interface titled 'Manage Report Downloads'. Below the title is a 'Report Download' section with a search bar. A table lists the downloaded reports. The first entry is highlighted in blue.

Report Name	Download	Date	Status
Request All Products (csv)	ReportRetrieval_20180529_130008.319.csv	29/05/2018 12:00:07	Successful

2.5 Managing Alerts

Overview

The Alert monitor allows you to manage alerts from the EU-Hub.

You can:

- View alerts
- Delete alerts
- Download a list of alerts
- Group alerts
- Set processing status
- Select issue and resolution
- View history for specific alerts
- Find related alerts

- Post comments
- Authenticate alerts against an SAP ATTP system

2.5.1 Configuring Alert Management

Using the Configure Alerts Tile, you can define issues and resolutions.

To view details of an alert, you can enable automatic authentication of alerts by connecting to an SAP ATTP system.

2.5.1.1 Defining Issues and Resolutions

Using the Configure Alerts Tile, you can define issues for alerts in the Issues List.

You can also define a list of resolutions.

Default values are as follows:

Issue

- Wrong Format SNR
- Wrong Format Batch
- Expiry date wrong
- Data not in ATTP
- Data not uploaded

Resolution

- Ignored
- Data uploaded
- Expiry date changed
- Master data changed
- Potential Counterfeit

2.5.2 Setting up Authentication

To use Authentication, you need to configure setup in SAP Traceability Hub Connectivity and SAP ATTP.

2.5.2.1 Setting up Authentication in SAP Traceability Hub Connectivity

Context

You need to set up authentication only once, and automatic authentication is then available for all the users of the Configure Alerts App in your organization.

Procedure

1. On the Configure Alerts screen, enter authentication URL of SAP ATTP system.
2. Save.
3. To test the connection, choose Test.
4. If test is successful, select Authenticate Incoming Alerts.
The Manage Alerts screen now includes the magic wand icon.
5. If the test is not successful, check the SAP ATTP service.
6. To change the URL, select Edit. After editing, test the connection.

2.5.2.2 Setting up Authentication in SAP ATTP

Context

To obtain the URL of the oData service of your SAP ATTP System used for authentication:

Procedure

1. Run [Transaction SICF](#).
2. Search for Service Path `/sap/opu/odata/sttp/att_cockpit_210_srv`.
3. If the service is available and not greyed out, it is already active.
4. For the full URL of the service, choose Test Service in the context menu.
A popup shows the full URL.
5. Optionally, to test the service, in the pop-up, choose [Allow](#).

If the service is operational, an XML file including oData service metadata shows in your default browser.

If the service is not yet operational, to activate the oData Service for Alert authentication, perform the following steps once for each system.

Check whether the service is already active and available in your system:

6. Use Transaction SICF.
7. Search for Service Path /sap/opu/odata/sttp/att_cockpit_210_srv
8. If the service is not yet active, activate it using the context menu. If the Service is not in this list, perform the following:
9. Use Transaction /IWFND/MAINT_SERVICE
10. Add Service.
11. Search for Service in the Namespace "/STTP*"

System Alias: LOCAL

Technical Service Name: /STTP

If the service is not configured in your system, the service shows in the list, and you can activate it.

2.5.3 Viewing and Processing Alerts

Procedure

1. To view and process alerts, select the [Manage Alerts](#) tile in EU Regulatory Reporting section under [Regulatory Reporting](#) section in left pane on the homepage.
The Alerts screen displays.
2. To view an alert, select the alert.
Details of the alert display, including the text of the message.
3. When you have investigated the alert, and no further action is necessary, you can set the processing status to solved. Select an alert and choose [Change Status](#).
4. To delete an alert, select the alert, and select [Delete](#) in the bottom right of the screen.
5. To download the list of alerts to a CSV file, select [Download](#) in the top right of the screen.
6. To group alerts based on specific parameters, select [View group settings](#).
7. Select issue and resolution from the drop-down fields.
8. When you select an alert, the Alert Details screen displays more information about the alert

Tabs show the following:

- Details: all information received by EU-Hub
- Comments: you add a comment
- History: change log of the alert.
- Related alert: All alerts that have the same GTIN, batch, and serial number.
- For related alerts, the status, issue and resolution decision are displayed

2.5.4 Authenticating Alerts

The app allows you to view alert details that are stored in a connected SAP ATTP system.

For example, alert details can include wrong serial or batch number.

You can configure the app so that all alerts are authenticated automatically which adds the details of each alert to the Alert Monitoring screen. You can also manually authenticate one or several alerts.

Automatic Authentication

After Release 2008, all alerts are automatically authenticated.

Manual Authentication

To authenticate one alert, select the alert and choose the Wand icon.

2.5.4.1 Authentication Results

The Additional Information column shows authentication results. The following table outlines each status.

Authentication Status	Description
Grey	Authentication is in process. When the result is available, the status changes.
Green	All parameters (GTIN, batch, exp date, serial number) validated successfully
Orange	Not all item identifiers validated successfully
Red	Technical error

2.5.4.2 Filtering Authentication Results

You can filter on alert authentication status.

The following table shows filter options available.

Filter	Alerts Displayed
All	No filter applied; all alerts displayed
Success	Only alerts with status green displayed
Functional error	Only alerts with status orange displayed
Technical error	Only alerts with status red displayed

2.5.4.3 Authentication Status

The following table shows authentication status and relevant information.

Category	GTIN	Serial Number	Batch	Exp	Status	Error Description	Wand color
SUCCESS	Match	Match	Match	Match	SUCCESS	All parameters validated	Green
Functional Error	Match	Match	Match	No match	Alert Expiry Date mismatch	SGTIN validated. Validation for Alert Expiry date x and y failed.	Orange
Functional Error	Match	Match	No match	- (does not matter)	Batch mismatch	SGTIN validated. Validation for Alert Batch x and y failed.	Orange
Functional Error	Match	No match	- (does not matter)	- (does not matter)	sGTIN mismatch	Validation for GTIN x and Serial Number x failed.	Orange
Functional Error	No match	No match	- (does not matter)	- (does not matter)	sGTIN mismatch	Validation for GTIN x and Serial Number x failed.	Orange
Technical error	-	-	-	-	Technical Error	A technical error occurred.	Red

3 Supply Chain Partner Collaboration

3.1 Creating Trade Items - Introduction

You must create a trade item before you can request a serial number for a product from your trading partner.

Context

Process - The process starts at the Homepage.

Procedure

1. Go to the *Supply Chain Partner Collaboration* section in left pane.
2. Select the *Trade Items* tile.
The Trade Items Screen displays.
3. Select *New Trade Item* at the bottom right of screen.
4. Select a Customer.
5. Enter a Product description for the new trade item.
6. To make the trade item active, select *Active*. You can only make requests on an active trade item.
7. Select *Add Identifier* to add an identifier.

Note

A GTIN Identifier is required even if the GTIN Identifier is inactive. You can have multiple identifiers but one of the identifiers must be specified as the Default Identifier.

8. Select an Identifier Type. The list available depends on the selected customer.
9. Enter an identifier number.
10. Select whether the identifier is active or inactive. Only details of active identifiers are included in serial number and shipping serial code requests.

You can delete an Identifier during creation, but when you save, you can no longer delete. However, you can always make an identifier inactive.

11. To use the encoded format, select Encoded. If you select encoded, you receive serial numbers separated by Application Identifiers.

Note

To receive sGTINs and crypto codes, Encoded is mandatory.

12. Select [Create](#) to complete the trade item creation and [Create](#) again in the confirmation popup.
13. Ensure that the items has been correctly added by viewing the trade item details.

4 U.S. Drug Supply Chain Security

4.1 Exception Management

4.1.1 Purpose and scope

This document describes the service offered to manage exceptions within an organization and between trading partner such as a Market Authorization Holder (MAH) Supplier, U.S. Wholesale Distributor or U.S. Dispenser in accordance with the U.S. Drug Supply Chain Security Act (DSCSA) on the SAP Traceability Hub Connectivity.

Target and Audience

This document is for MAHs who manufacture and supply, U.S. Pharmaceutical Wholesale Distributors, and U.S. Dispensers who trade prescription drugs that fall under U.S. DSCSA, including:

- Supply chain managers
- Integration experts
- Implementation teams
- Quality and Compliance teams

Glossary

Abbreviation	Definition
API	Application Programming Interface
DSCSA	U. S. Drug Supply Chain Security Act
EPCIS	EPCIS Electronic Product Code Information Services - GS1 Standard, refer to http://www.gs1.org/epcis . This specification is based on EPCIS 1.2.
ICH	SAP Traceability Hub, formerly SAP Information Collaboration Hub for Life Sciences
SAP ATTP	SAP Advance Track and Trace for Pharmaceuticals

4.1.2 About Exception Management

The SAP Traceability Hub connects pharmaceutical organizations, supply chain partners and regulatory entities on a secure network that is owned and managed by SAP. The Hub supports the transfer and

transformation of data between members of the pharmaceutical supply chain connected to the Hub. Connected partners can exchange serialization messages across a secure and reliable network.

The Hub provides services to support pharmaceutical organization to comply with requirements of U.S. DSCSA including:

- Exchange of transaction information (TI) to support Interoperable Exchange
- Verification Router Service (VRS) to support Interoperable Verification
- Integration service for Wallet provider in lieu to support electronic validation of Authorized Trading Partner
- Trace Management to support Interoperable Tracing
- Exception Management to process exceptions through exchange of transaction information (TI) between trading partners.

For an overview of the U.S. Drug Supply Chain Security service, see the [U.S. Drug Supply Chain Security Help page](#).

The Exception Management service enables SAP customers to handle exceptions by integrating SAP ATTP and SAP Traceability Hub data logs to analyze and resolve exceptions. An API is also available on the [SAP Business Accelerator Hub](#).

4.1.3 Manage Exceptions Web App

The service includes the Manage Exceptions web app.

The app allows you to:

- Create and manage exceptions
- Analysis of Exception with transaction information (TI), by gathering Transaction Information from SAP ATTP and Message logs from SAP Traceability Hub
- Add Attachment
- Add Notes
- Collaborate with external partners by transferring an exception
- A change log records all actions
- Store relevant information for a minimum of six years as required by U.S. Drug Supply Chain Security Act
- Download to PDF

4.1.4 Integration with SAP ATTP

The service integrates with SAP Advance Track and Trace for Pharmaceuticals to gather transaction information (TI).

Note

This integration is available only with SAP ATTP 3.0 FP 2 or above.

Manage Exception API

SAP offers an API to create, update and read exceptions which integrates with the Manage Exceptions web app. For details, see the Manage Exception section on the [SAP Business Accelerator Hub](#).

4.2 Transaction Information Exchange

4.2.1 Introduction

SAP Traceability Hub provides services to support pharmaceutical organizations to comply with the requirements of U.S. DSCSA including exchange of transaction information (TI) for Interoperable Exchange.

For an overview of the U.S. Drug Supply Chain Security service, see the U.S. Drug Supply Chain Security - Service Overview on the [U.S. Drug Supply Chain Security Help page](#).

Assumptions

This guide assumes you are familiar with the pharmaceutical industry and serialization terminology.

Data Protection and Privacy

To have user data removed, contact your SAP team.

Target Audience

This document is for organizations that trade prescription drugs which fall under U.S. DSCSA:

- MAH organizations that manufacture
- U.S. Pharmaceutical Wholesale Distributors
- U.S. Dispensers

This document is typically for the following roles in an organization:

- Supply chain managers
- Integration experts
- Implementation teams
- Quality and Compliance teams

Glossary

Abbreviation	Definition
DSCSA	U. S. Drug Supply Chain Security Act
ICH	SAP Traceability Hub, formerly SAP Information Collaboration Hub for Life Sciences
MAH	Marketing Authorization Holder

4.2.2 About

Participants on the SAP Traceability Hub can exchange messages relative to serialization, regulatory reporting and transaction information for U.S. Drug Supply Chain Security.

SAP offers various options to send, receive or view messages, depending on whether an invited organization is onboarded.

Viewing TI Messages – Onboarded Organizations

To send or receive messages, an organization must be onboarded.

In the context of Transaction Information, SAP customers can invite a partner organization to onboard and view Transaction Information messages relative to transactions with that organization. To onboard to the SAP Traceability Hub, an invited organization must have a GLN.

Onboarded organizations have access to the Transaction Information Web app.

Viewing TI Messages – Non-Onboarded Organizations

For organizations that do not have a GLN, SAP offers the View Transaction web app which does not require onboarding. SAP customers must perform some setup steps.

4.2.3 View Transaction Information with Onboarding

The Transaction Information web app allows you to view and download messages. The app is available to trading partner organizations who are onboarded to SAP Traceability Hub which requires that they own or are assigned a GLN.

You must be authorized to use the Transaction Information app. If you do not have access, contact your organization's Web App Administrator.

The Transaction Information web app is also available to SAP Customers to view information sent to trading partners who choose to use the app.

4.2.3.1 View Messages

Context

The process starts at the Homepage.

Procedure

1. Select Transaction Information Tile.
A list of messages displays.
2. You can filter messages, for example, based on date ranges, sender GLN and receiver GLN.
3. You can search for a message based on Delivery Number, Purchase Order, product information such as NDC, GTIN, serial number, expiry date, and batch or lot.

4.2.3.2 Download Messages as PDF

Context

The process starts at the Homepage.

Procedure

1. Select Transaction Information Tile.
2. Select message.
3. Select Download item level or lot level as PDF.
The downloaded file contains a summary of Transaction Information sent by the supplier.

4.2.3.3 Download Message as XML

Context

The process starts at the Homepage.

Procedure

1. Select Transaction Information Tile.
2. Select message.
3. Select Download item level or lot level as XML.
The downloaded XML file contains a summary of Transaction Information sent by the supplier.

4.2.3.4 Download list of Messages

Context

The list content depends on filters you apply. The process starts at the Homepage.

Procedure

1. Select Transaction Information Tile.
2. Select Export in the top right corner of screen.
The list of messages exports to an MS Excel file on your device.

4.2.3.5 Message Status

If a message contains erroneous EPCIS data when sent to a trading partner, you can make the message inactive.

The trading partner can view an inactive message but cannot download the message.

You can set the status of a message to Inactive or Active.

4.2.4 View Transaction Information without Onboarding

The View Transaction web app allows trading partners who do not own a GLN to view and download messages. Users accessing Transaction Information for their organization are not required to onboard to SAP Traceability Hub Connectivity.

4.2.4.1 Set Up Process for SAP Customer

To set up this service:

- Configure SAP GLN
- Enter customization parameters
- Define your URL

4.2.4.1.1 Configure SAP GLN

Your trading partner uses the View Transaction app to view Transaction Information messages.

The View Transaction app only shows messages sent to the SAP GLN, which is for partners without GLN.

Note

If a trading partner with GLN has been onboarded to SAP Traceability Hub, messages sent to that trading partner are not visible in the View Transaction app.

4.2.4.1.2 SAP ATTP

To send a Transaction Information message to a trading partner without GLN, in your ATTP system, configure GLN 4063973010014 for Destination Owning Party (Sold to) and 4063973010021 for Destination Location (Ship-to) .

The SAP team creates a connection between your GLN and the SAP GLN. You can then send messages to the SAP GLN.

Only messages sent to the SAP GLN are visible in the View Transaction app.

To get address details from a delivery document, use [SAP Note 3333175](#)  – Get Address Data from Outbound Delivery in ECC / S4 HANA.

4.2.4.1.3 Define Suffix for Customer URL

Each SAP customer has one URL for Staging-Test, and one URL for Production.

The URL leads to a page that is unique for your organization, and trading partners can only access data for your organization.

The format of the URL is: https://sta.ich4ls.cloud.sap#/staLogin/{customer_value} 

You define **only** the *customer_value* portion of the URL which is added to the end of <https://sta.ich4ls.cloud.sap#/staLogin>.

Example

You can choose to add *your* company name:

<https://sta.ich4ls.cloud.sap#/staLogin/Pharmalnc> 

where *Pharmalnc* is your company name.

Staging-Test URL

https://test.sta.ich4ls.cloud.sap#/staLogin/Your_Company 

Production URL

https://sta.ich4ls.cloud.sap#/staLogin/Your_Company 

Replace *Your_Company* with, for example, your company name.

Use the Manage Customizations app to enter a number of parameters, described in the following section.

4.2.4.1.4 Manage Customization Parameters

Use the Manage Customizations app to configure necessary parameters. See the Manage Customizations app guide on the [Help page](#).

The service allows you to add your company logo, links to your company specific Data privacy and protection that will be used in the View Transaction app.

The following table outlines the parameters available.

Parameters marked with an asterisk * are mandatory for the View Transaction app to operate successfully.

Scenario	Parameter	Parameter Option	Parameter Description	Examples - not for productive use
Transaction Information Exchange	Suffix for URL Path for View Transaction*	(blank)	Specific page for your organization	Staging-Test: https://test.sta.ich4ls.cloud.sap/index.html#/staLogin Production: https://sta.ich4ls.cloud.sap#/staLogin/Your_CompanyName In the Manage Customizations app, you enter only the company name. For example, your company name: https://sta.ich4ls.cloud.sap#/staLogin/Pharmalnc
Transaction Information Exchange	Logo URL for View Transaction	(blank)	URL of your Logo displayed in the View Transaction app	https://www.your-company.com/your-logo-svg.svg
General	Data privacy protection for View Transaction*	URL	URL of data privacy protection	https://www.your-company.com/about/trust-center

4.2.4.2 Trading Partner View Transaction App

This section describes the View Transaction app which your trading partners use to view Transaction Information you send to your URL. To configure your URL, see relevant section.

4.2.4.2.1 App Access

To access the View transaction app, a trading partner provides:

- Trading Partner's Company name
- Email

The trading partner then:

- Creates a One-Time Password
- Completes a captcha test

4.2.4.2.2 Access Log

The company name and email entered by a trading partner is logged.

SAP Customers have access to the Transaction Information app which shows an Access Log for the View Transaction app. This allows you to see which of your partner organizations accessed the View Transaction app. and downloaded the PDF.

4.2.4.2.3 View Transaction Using Delivery Details

A trading partner enters the Delivery number, Lot or Batch Number, and ZIP code from the Packing slip to view transaction information.

To view another transaction, the trading partner must perform the access steps again.

4.2.4.2.4 Download Transaction Information to PDF

A trading partner can download Transaction Information to PDF.

The PDF can be downloaded only once in each session.

A message set as inactive by supplier of the Transaction Information cannot be downloaded.

4.2.5 Introduction -Transaction Information (TI) Exchange Service Description

Purpose and Scope

This document describes the service offered to exchange messages (TI/TS) between Market Authorization Holders (MAH, aka, Suppliers), U.S. Wholesale Distributors and U.S. Dispenser in accordance with the U.S. Drug Supply Chain Security Act (DSCSA) on the SAP Traceability Hub.

Target Audience

This document is for MAHs that manufacture, U.S. Pharmaceutical Wholesale Distributors and U.S. Dispensers that trade prescription drugs that fall under DSCSA, specifically:

- Supply chain managers

- Integration experts
- Implementation teams
- Compliance teams

References

- [EPCIS](#) ➡
- [GS1 US DSCSA Implementation Suite](#) ➡
- [TI Message Specification on Help Page](#)

Glossary

Abbreviation	Definition
ASN	Advance Shipping Notice
DSCSA	U. S. Drug Supply Chain Security Act
EPC	Electronic Product Code, often used to summarize different formats of unique identifiers
EPCIS	Electronic Product Code Information Services - GS1 Standard, refer to http://www.gs1.org/epcis ➡. This specification is based on EPCIS 1.2.
GCP	Global Company Prefix (GS1 Standard)
GLN	Global Location Number (GS1 Standard)
GS1	Global Standardization Body ➡
GTIN	Global Trade Identification Number (GS1 Standard)
HDA	Healthcare Distribution Alliance
ICH	SAP Traceability Hub, formerly SAP Information Collaboration Hub for Life Sciences
MAH	Marketing Authorization Holder
NDC	National Drug Code
SGTIN	Serialized GTIN, special case of EPC
TI/TS	Transaction Information (TI) and Transaction Statement (TS)
TPI	Third Party Integrator
WHO	Wholesale Distributors

4.2.6 About

The SAP Traceability Hub is an on-demand service that connects pharmaceutical organizations and their supply chain partners on a secure network that is owned and managed by SAP.

SAP Traceability Hub supports the transfer and transformation of data between members of the pharmaceutical supply chain. Connected partners can exchange serialization messages across a secure and reliable network.

SAP offers various integration capabilities such as content-based routing and mapping, as well as a number of connectivity options such as web services, SFTP servers, or a Web App.

Connectivity options for a participant are made available through a guided self-onboarding process using a web app, or discussed with the SAP team during the onboarding process.

4.2.7 Transaction Information (TI) Exchange

Supply Chain Notification Messages (TI/TS Messages) are exchanged for each shipment according to U.S. DSCSA and require full serialization aggregation.

Messages must comply to HDA 856 ASN.

4.2.7.1 Transaction information (TI) Exchange - Manufacturer

The service allows MAHs to send product pack data to their wholesale distribution customers and dispensers.

MAHs who are customers of SAP invite their trading partners to participate and receive Transaction Information through the SAP Traceability Hub.

The SAP Onboarding team can perform onboarding steps. A self-onboarding Web App is also available.

Connection can be B2B or through a Web App.

4.2.7.2 Transaction information (TI) Exchange – U.S Wholesalers

The service allows wholesale distribution customers to receive product pack data from MAHs and send product pack data to their partners including secondary U.S. Wholesalers or Dispensers.

U.S. Wholesalers who are customers of SAP can invite their suppliers and dispensers to participate.

The SAP Onboarding team can perform onboarding steps. A self-onboarding Web App is also available.

Connection can be B2B or through a Web App.

4.2.7.3 Transaction information (TI) Exchange – U.S. Dispensers

The service allows U.S. Dispenser to receive product pack data from MAHs and U.S. Wholesalers.

U.S. Dispensers who are customers of SAP can invite their suppliers and wholesale distributors to participate.

The SAP Onboarding team can perform onboarding steps. A self-onboarding Web App is also available.

Connection can be B2B or through a Web App.

4.2.8 Onboarding Partners

SAP Customers are onboarded by the SAP Onboarding team.

Partners onboard as follows:

- An SAP customer sends an email invitation to a partner through the Manage Onboarding app
- Partners send an SAP customer a request to onboard through a customer-specific URL
 - For more information see the Onboarding Your Partners Guide on the [Help](#) page.

4.2.8.1 Inviting Your Partners to Onboard

SAP Customers can invite business partners to use self-onboarding web apps.

Use the Manage Onboarding app to enter the following information to send an invitation to a business partner:

- Name of the business partner
- Email of business partner contact
- GLN
- Optional information, such as DEA, state license number

Invited business partners have the following options to onboard:

- B2B
- Through a pre-qualified Third Party solution provider
- Web App

4.2.8.2 Partner Requests to Onboard

To request to onboard, your trading partners use the Onboarding Request app which is accessible through a URL you share.

4.2.8.3 Onboarding Options

The following options are available for onboarding.

4.2.8.3.1 B2B

Partners who select B2B receive messages to their repository endpoint which is configured during onboarding. The receiver GLN in the EPCIS message is used as the identifier and routed to the business partner endpoint.

SOAP, HTTP and AS2 are supported.

4.2.8.3.2 Third Party Integrator

Invited partners can use a Third Party solution provider to connect to the SAP Traceability Hub. SAP provides a pre-qualified list of solution providers, which SAP can add to, on request.

4.2.8.3.3 Web App

Invited partners have access to a Transaction Information Web App. The app provides access to all TI/TS messages received based on the GLN configured by the inviting SAP customer during onboarding.

4.2.9 Transaction Information Web App

SAP offers the Transaction Information Web App to SAP customers and their invited business partners who cannot establish a B2B connection or connect through a Third Party Integrator.

The Web App allows you to review Transaction Information and Transaction Statement (TI/TS) messages in compliance with the U.S. Drug Supply Chain Security Act (DSCSA).

4.2.9.1 Transaction Information Web App Features

SAP Customers or business partners can view data related to a GLN or GLNs that are assigned during onboarding.

Manufacturers or U.S. Wholesalers acting as senders can view data related to sender GLN.

Invited business partners acting as receivers can view data related to receiver GLN.

The app allows you to:

- View a list of TI/TS messages exchanged including Delivery Number, Delivery Date, Sender GLN, Receiver GLN, Message ID, Message Date, Purchase order and Downloaded
- Filter or search based on Delivery Number, Delivery Date, Sender GLN, Receiver GLN, Message ID, Message Date, Purchase order, Downloaded and product identifier
- Download a list of messages to MS Excel
- Download a TI/TS message as received by SAP in XML format
- Download a TI/TS message in PDF format, with item level or lot level information
- View audit logs that include login email, and timestamp for actions such as download to PDF or download to XML

4.2.10 Sending TI Messages to Partner without GLN

SAP customers can provide TI/TS messages to trading partners who do not have a Global Location Number (GLN). The View Transaction app allows a trading partner to view a TI/TS message without onboarding to SAP Traceability Hub.

Features include:

- A trading partner is authenticated by entering Company Name, Email and One Time Password.
- Transactions can be searched through a combination of Delivery Number, Lot Number and Zip Code (Ship-to or Sold-to).
- Transaction Information can be downloaded to PDF.
- The supplier of Transaction Information can view information sent, and a log of Transaction Information downloaded by a trading partner.

You must perform configuration steps. See the [TI Configuration Guide](#).

You use the Manage Customizations app to configure necessary parameters. See the [Help](#) page.

4.2.11 Sending HDA 856 ASN to Partners

SAP customers can send Lot level information according to HDA EDI Guidelines for 856 Advance Ship Notice to meet lot level requirements of U.S. DSCSA. A partner can receive information through B2B, TPI or web app.

4.2.11.1 Partner Receiving through B2B or TPI

SAP Traceability Hub uses an identifier such as Drug Enforcement Administration (DEA), Health Industry Number (HIN), D-U-N-S Number, Dun & Bradstreet, D-U-N-S+4, D-U-N-S Number with Four Character Suffix or GLN to identify partners in the EDI.

To enable this, contact SAP support.

4.2.11.2 Partner Receiving through Web App

SAP Customers can send Lot level information according to HDA 856 EDI guidelines to the View Transaction.

Use GLN 4063973010014 for Buyer and 4063973010021 for Ship-to Location.

4.2.12 Message Format

Message must follow the GS1 EPCIS 1.2 standard and the GS1 U.S. Healthcare Implementation Guideline (EPCIS 1.2 USHC). Messages include Transaction Information (TI) and Transaction Statement (TS) in compliance with U.S. DSCSA.

Trading partners for supply chain notification must follow the [GS1 US Implementation Guideline: Applying GS1 Standards for DSCSA and Traceability Release 1.2](#),  (GS1 USHC).

SAP Traceability Hub message specification following GS1 USHC guidelines is described in the U.S. Transaction Information (TI) Message Specification on the U.S. Drug Supply Chain Security [Help Page](#).

For lot-level requirements, the service supports [HDA EDI Guidelines for 856 Advance Ship Notice](#) .

4.2.12.1 Sample Message

Sample message files are available on the U.S. Drug Supply Chain Security [Help Page](#).

4.3 Trace Management

4.3.1 Introduction

The U.S. Tracing service provides trace management web apps to manage Trace Requests as an Initiator and Trace Responses as a Responder.

Trace requests are received from regulators, agencies, or other trading partners in the event of investigation.

For an overview of the U.S. Drug Supply Chain Security service, see the U.S. Drug Supply Chain Security - Service Overview on the [U.S. Drug Supply Chain Security Help page](#).

Assumptions

This guide assumes you are familiar with the pharmaceutical industry and serialization terminology.

Data Protection and Privacy

To have user data removed, contact your SAP team.

Target Audience

This document is for MAHs that manufacture, U.S. Pharmaceutical Wholesale Distributors and U.S. Dispensers that trade prescription drugs that fall under U.S. DSCSA, including:

- Supply chain managers

- Integration experts
- Implementation teams
- Quality and Compliance teams

Glossary

Abbreviation	Definition
DSCSA	U. S. Drug Supply Chain Security Act
ICH	SAP Traceability Hub, formerly SAP Information Collaboration Hub for Life Sciences
SAP ATTP	SAP Advance Track and Trace for Pharmaceuticals

4.3.2 User Access and Roles

The service allows your organization to assign users to various roles, each with different authorizations and app access:

- Trace Manager - Create and manage Trace Requests and Trace Responses using the Trace Management app
- Trace Approver (optional) - Approve or Reject Trace Request and Response using the Trace Management app
- Trace Administrator - Perform all actions of a Trace Manager and Trace Approver using the Trace Management app and the Trace Management Settings app

The App administrator of your organization provides app access and authorizations to users, using the Manage Users app. If you do not have access to an app, contact your App administrator.

4.3.3 Trace Management Web App

The Trace Management app allows you to manage trace requests including creating requests, responding to requests, and optionally approving a request response.

Overview of Trace Requests

The overview screen shows a list of trace requests.

You can search and filter for a trace based on certain criteria.

4.3.3.1 Overview of Trace Requests

The overview screen shows a list of trace requests.

You can search and filter for a trace based on certain criteria.

4.3.3.2 Create Trace Request

Create Trace Request

The app allows you to create a Trace Request by entering text or choosing from the various options, as follows:

Description

Free text to describe a trace request

Type

- As a Responder
 - To respond to a trace request received from Trace Initiators such as regulators and agencies
- As a Requester
 - To create a trace request as a Trace Initiator, for example, in case of audit

Trace Details

- Request ID
 - Identify the trace request, UUID
 - Auto Generated in case of trace created as a Requester
- External Reference ID
 - Reference to other internal systems in your organization for example, your Quality Management System
- Response Type
 - Based on response required:
 - All Known Owners, Last Known Owner, Transaction Information
- Reason
 - Audit, Illegitimate, Recall, Suspect

Product Identifier

- GTIN
- Lot Number
- Expiration Date
 - Format YYDDMM
- Serial Number
 - Serial Number of the product
- GS1 Element
 - Auto populated as GS1 element string

Contact Details - Mandatory

- Your Company Details
 - Code – GLN of your company
 - Company – Name of your company
 - Email – Contact email of your company contact person or department
 - Address – Address of your company

All above information is mandatory.

- External Contact – requestor or responder
 - Code – GLN of the external contact
 - Company – Company name
 - Email
 - Address

4.3.3.3 Copy Trace Request

To create a trace request, you can copy a trace request which you can then edit.

4.3.3.4 Trace Details

The Trace Details screen displays trace request information response information described in the following section.

4.3.3.4.1 Transaction Information

The Transaction Information required by U.S. DSCSA to respond to a trace request can be gathered by directly connecting to SAP ATTP or through manual upload.

4.3.3.4.1.1 Retrieve from SAP ATTP

The service offers the ability to integrate with SAP ATTP to retrieve Transaction information.

4.3.3.4.1.2 Manual Upload

You can upload relevant transaction information (TI) in an EPCIS XML file. The Transaction information you upload is validated for mandatory information required by the GS1 EPCIS 1.2 USHC implementation guideline.

4.3.3.4.2 Download

You can download an XML file that contains only information about the serial number for which the trace is created and download a PDF that contains trace details.

The PDF includes all relevant Trace Request details and product information.

4.3.3.5 Task List

The service provides the ability for a Trace Manager to complete a list of tasks to respond to a trace request. The tasks can be defined to match your business processes.

Your Trace Administrator defines a task list using the Trace Management Settings app.

4.3.3.6 Attachments

You can upload attachments to support trace requests and responses.

Attachments include description, uploaded date, and uploader username.

The following file types are supported:

.jpeg, .jpg, .png, .pdf, .xml, .xlsx, .xls, .doc, .docx, .csv, .txt, .ppt

4.3.3.7 Notes

You can enter notes for a trace request.

Notes are timestamped and logged to a username.

4.3.3.8 Change Log for Auditing

All actions performed for a given trace request are logged and visible in a Change Log.

4.3.3.9 Trace Request and Response Status

The service provides the ability to track statuses for Trace Management. These include:

- New
- In-progress
- Complete
- Canceled

If you use the optional Approval process, other statuses are available.

4.3.4 Optional Approval Process

You can enable an approval process for trace request and response.

The option allows a Trace Manager to assign a Trace Request and Trace Response to a Trace Approver for approval or rejection.

The Trace Administrator enables or disables the approval process using the Trace Management Settings app.

Approval Status

In addition to the standard statuses described in section 3.9, the following approval statuses are available when you enable the Approval process.

Optional Approval Status

- Request Sent for Approval
- Request Rejected
- Request Approved
- Response Sent for Approval
- Response Approved
- Response Rejected

4.3.5 Setting Up Trace Management

This section describes options and tasks for the nominated Trace Administrator in your organization.

The Trace Management Settings app allows you to:

- Enable an optional approval process
- Set up a list of tasks to respond to a trace request

Enable Optional Approval Process

You can enable or disable an approval process to respond to a trace request.

By default, this option is disabled.

Manage Task List

You can create and edit a list of tasks for a Trace Manager to respond to a request.

4.3.6 Integrating ATTP for Trace Response

The service integrates with SAP Advance Track and Trace for Pharmaceuticals to retrieve transaction information (TI) relevant to the product identifier of a trace request when your organization acts as a responder.

Note

This is available with SAP ATTP 3.0 FP 2 or above.

For companies acting as buyer and seller, such as a U.S. Wholesaler, the service responds with two files corresponding to inbound and outbound.

4.3.6.1 Connect ATTP to Trace Management Service

Use the Manage Customizations app to configure the following:

- Cloud Connector Location ID
- Receiver endpoint of ATTP system for Trace Management - Run transaction SOAMANAGER in ATTP
- Username and Password for Basic Authentication

In case of questions, contact Onboarding support.

Related Information

- Trace Management in the SAP ATTP Configuration Guide on the [Help page](#)
- Manage Customizations app guide on the [Help page](#)

4.4 Verification Router Service

4.4.1 Introduction

This document describes the service provided by the SAP Traceability Hub, option for U.S. The service enables pharmaceutical manufacturers providing products for the U.S. market, U.S. wholesale distributors and U.S. dispensers to comply with the regulations of the U.S. Drug Supply Chain Security Act, especially requirements for verification.

The service complies with the GS1 U.S. Implementation Guideline R1.3 that applies to the GS1 Lightweight Messaging Standard for DSCSA Verification of Product Identifiers. In this document, this is referred to as the GS1 LWMS R1.3.

Target Audience

This document is for:

- Supply Chain Managers
- Integration Engineers
- Implementation teams
- Compliance teams

Assumptions and Prerequisites

To use the verification service of the SAP Traceability Hub, participants must be onboarded to the SAP Traceability Hub. For further information, see the onboarding documentation on the SAP Traceability Hub Help Page.

Related Links

- Service Overview on the [U.S. Drug Supply Chain Security Help page](#)
- [SAP Traceability Hub Help Page](#)
- [SAP Advanced Track and Trace for Pharmaceuticals Help Page](#)
- [GS1 Healthcare US Implementation Guideline](#) ➡
Applying the GS1 Lightweight Messaging Standard for DSCSA Verification of Returned Product Identifiers
(Available on the relevant GS1 web page: [GS1 US DSCSA Implementation Suite](#) ➡)

4.4.2 Managing the Lookup Directory

The Lookup Directory (LD) contains the Connectivity Information (CI) of the MAH responder's repository to respond to verification requests. CI is stored by product ID (GTIN) and date range. The LD is an integral part of any Verification Routing Service (VRS) because it determines the destination for a verification request issued by a requester wholesaler or dispenser. The content in the LD is exchanged with other LDs in the ecosystem. Therefore, every LD contains all CI maintained in the ecosystem.

SAP provides an LD as part of the service that responders use to maintain their CI. SAP LD supports maintenance of single GTINs, transfer of GTINs between MAHs, and a view of the entire set of GTINs in the LD.

The SAP LD also supports:

- Bulk upload of GTINs and their descriptions into the LD from a CSV file
- Integration with SAP Advanced Track and Trace for Pharmaceuticals to create new GTINs automatically
- Checking if a GTIN is in the LD

4.4.2.1 Primary and Secondary GCPs

GCP/Labeler Codes can be primary or secondary.

- **Primary** - Owned by SAP Customers and to which a customer can associate a GTIN
- **Secondary** - Used in a co-marketing scenario or for GTIN transfer

In such cases the embedded Labeler Code in the GTIN can be different to the assigned Labeler Code identifying the owner of the GTIN .

4.4.2.2 Setting Up the LD

SAP sets up the LD for each SAP customer. Set up depends on role.

MAH Responder

SAP sets up:

- MAH's verification endpoint that points to the verification repository or a customer's EPCIS repository

- An MAH's GCPs that must comply to the U.S. GTIN nomenclature and includes the company's Labeler Code with a 03 prefix. The SAP team verifies that the customer has ownership of GCPs and related Labeler Codes (primary GCPs) or can provide documented evidence that the customer is not the owner but is eligible to respond to verification requests for GTINs with the GCP (secondary GCP).
- Default responder GLN used in verification responses where the responder GLN cannot be determined in the verification repository, for example, because the PI cannot be found. This GLN is used as the default responder GLN for all verifications performed against a customer's EPCIS repository.

MAHs create and update their GTINs in the LD to:

- Define CI
- Review LD content
- Transfer GTINs

Requester Wholesaler and Dispenser

Wholesalers and dispensers have access to the LD to view content but cannot define GTINs and related verification endpoints.

4.4.2.3 Maintaining Your LD Content

Responders must define the Connectivity Information (CI) to enable verification.

4.4.2.3.1 Creating Connectivity Information

Responders enter CI in the LD using the Manage Products web app. The CI includes:

- **Product ID (GTIN):** The GTIN in the LD must match the GCPs configured in the LD. U.S. GTINs include the 03 prefix and the National Drug Code (NDC).
- **Product Description:** The product description supports any character and has a maximum length of 5000 characters. Product description provides context to the user but is not used in the verification process and is not exchanged with other LDs.
- **Verification Endpoint:** The SAP team configures the verification endpoint. SAP customers have one endpoint that points to the SAP verification repository or a customer's EPCIS repository. This endpoint is associated to all GTINs.
- **Start and End Date:** Start and End Dates define the validity period for the CI. The dates refer to the expiration date in the PI of the verification request and define the correct CI in case of product transfer. See section 2.3.2.
- **Labeler Code:** The labeler code identifies the record owner. You can use the labeler code derived from the GTIN or pick a labeler code from the drop-down list. You can only select a labeler code that matches a primary GCP.

SAP offers different methods for responders to maintain data in the LD.

Manage CI Information in Manage Products Web App

The Manage Products app allows you to enter connectivity information. You can enter a GTIN and GTIN description, select an endpoint, and define start and end dates.

Bulk Upload

The app allows you to write a list of GTINs to the LD. SAP provides a template. You can upload a file that contains the GTIN and related description, as well as start and end dates. After uploading the file, you can check and update data.

Integration with SAP Advanced Track and Trace for Pharmaceuticals

SAP provides the option to integrate SAP Advanced Track and Trace for Pharmaceuticals with the SAP LD to automatically create CI for new GTINs that have been created in ATTP. Contact SAP for details.

4.4.2.3.2 Transfer GTIN Ownership

An MAH can transfer ownership of a product (GTIN) to another MAH, so the new owner can use the existing GTIN during the transfer period. As the old and the new owner may use different repositories for verification, the Connectivity Information for the GTIN may change because of the transfer. The VRS must enable verification depending on expiry date of the PI, because product from the old owner and the new owner are in the market at the same time.

Start and End Dates

To accommodate this process, start and end dates for a CI are stored in the Lookup Directory. Start and End Date reflect the expiration date in the PI that is provided in the verification request. Lookup for a verification request is performed against the CI based on the GTIN and expiration date.

Example

A transfer for a product with two years shelf life is negotiated and signed to become effective by year end 2019. Therefore, the old owner produces and ships product until December 31, 2019. Product shipped on that day will expire on Dec 31, 2021. The new owner will start producing the product from January 1, 2020.

The product from the old owner will be in the market until the end of its shelf life, which is Dec 31, 2021. Product from the new owner is in the market starting from January 2020.

A wholesaler is executing verification on June 1, 2020. On that date, both products from the old and new owner are on the market. The wholesaler however cannot distinguish whether the product pack has been produced by the old or new owner.

To determine where verification has to be performed, the lookup must take expiration date into account, which is part of the verification request. If the PI originates from the old owner, the expiration date must be before Dec 31, 2021, in which case the verification is routed to the old endpoint. A product pack from the new owner must have an expiration date in January 2022 or later. A verification will therefore be routed to the new endpoint.

Performing Transfer

A GTIN must be transferred manually. In any case, the current (old) owner must act first, by setting the end date. After the change is synced to the new owners LD, the new owner can maintain the GTIN in the LD with a corresponding start date, which must be after the end date of the old owner.

Caution

To prevent validity periods from overlapping, the old and new owners must agree the transfer date, and enter start and end dates accurately. Otherwise, synchronization between the LDs will fail.

4.4.2.3.3 Co-marketed Products

Pharmaceutical companies may co-market a product in certain markets.

In such cases, a product is associated to company A by its labeler code and corresponding GCP. However, company B has market authorization, performs serialization, and responds to verification requests.

Steps are required in SAP Lookup Directory to ensure that VRs for that product are directed to company B's repository for verification.

Company A is an SAP Customer, Company B is not

No action is required. Company A must NOT maintain the GTIN for the co-marketed product in the SAP Lookup Directory.

Company B is an SAP Customer, Company A is Not

Company B must ask the SAP team to add the GCP to the SAP Lookup Directory. Subsequently Company B must add the GTIN to SAP Lookup Directory. SAP asks for proof that Company B can use the GCP and verifies that company A has ownership of the GCP and related labeler code.

Company A must NOT add the GTIN to their LD.

Company A and Company B are SAP customers

Company B must ask the SAP team to add the GCP to the SAP Lookup Directory. Subsequently Company B must add the GTIN to SAP Lookup Directory. SAP asks for proof that Company B can use the GCP and verifies that company A has ownership of the GCP and related labeler code.

If company A owns other GTINs using the same GCP that company A is managing, company A also needs to ask SAP to maintain the same GCP. Company A must NOT add the co-marketed GTIN to SAP LD, but may maintain any other GTIN in SAP LD.

4.4.2.3.4 Synchronize LD Content with Other Service Providers

To enable routing of verification requests, all Lookup Directories in the ecosystem must be synchronized, that is, store the same Connectivity Information. The SAP Lookup Directory ensures consistent synchronization with other service providers through the following processes:

- SAP LD push: upon creating, changing, or deleting CI in SAP LD the corresponding information is pushed to all connected LDs in the VRS ecosystem immediately. It can take several minutes until changes are reflected in third-party LDs.
- Third-party LD push: All lookup directories are expected to perform an immediate push if CI is created or changed. However, SAP cannot guarantee that all third-party LDs perform the push.

- SAP LD pull: SAP pulls all changes made since the last successful pull from all connected LDs every twelve hours. This ensures synchronization even in cases where the third-party LD fails to push a CI creation or change.
- Third-party LD pull: SAP LD provides an endpoint to all third-party LDs to perform a pull from SAP LD. This allows third-party LDs to update CI in case a push from SAP LD fails. However, SAP cannot guarantee that all third-party LDs perform the pull and frequency of LD pull can vary by third-party.

The Manage Products web app provides a sync status that reflects whether a CI was successfully synchronized with all connected LDs.

4.4.2.4 View Industry-wide LD Content

As all LDs in the ecosystem are synchronized, each LD stores the same Connectivity Information. You can review the entire LD content in the View Lookup Directory Web App.

The app provides all CI for all GTINs managed in the ecosystem. Beside the basic CI data (see 2.3.1), the app provides:

- Labeler code owner derived from the labeler code through a query of the FDA NDC database
- VRS Solution provider where the CI is stored, and the VRS ID
- Timestamp of last change

The app allows you to download the entire LD content, depending on search criteria and the columns you choose to display.

4.4.2.5 Check for GTIN in Lookup Directory

A service is provided to check if a GTIN is maintained in the Lookup Directory. This is useful for wholesalers and dispensers who rely on their suppliers (MAHs) to maintain supplier GTINs correctly in the Lookup Directory. Customers must be onboarded for this B2B-service and must enable the respective backend to perform the check. Contact SAP for further details.

4.4.2.6 Writing Product Pack Data to the Verification Repository

Note

This section is not relevant for MAHs who offer verification against their own EPCIS repository.

MAHs send product pack data to a verification repository by sending an EPCIS message. The message format is similar to that of the U.S. Supply Chain Notification with no aggregation required. See section 7.

A message can contain multiple batches. An MAH can send data to the verification repository through a B2B connection or by using an SAP Web App. The service supports:

- EPCIS 1.2 USHC
- EPCIS 1.1

The verification repository stores the four data elements, GTIN, Lot, Expiration Date, Serial Number, as well as the event timestamp and disposition showing the status of the product pack.

The data is then available for verification requests.

4.4.2.6.1 Message Validation

Only MAHs can send product pack data into the verification repository and update the status of product packs, and only for their own product packs. To enforce this, messages are only accepted containing GTINs that match a pre-defined set of Global Company Prefixes (GCPs) and sent from a pre-defined sender GLN.

To add company prefixes or sender GLNs, contact SAP.

4.4.2.6.2 Batch and Expiry Date Extension

Requirement

An event that changes the status of an object, such as decommissioning or shipping, must contain the complete PI, including Batch Number and Expiry Date.

Typically, these events, such as OBJECT event OBSERVE or DELETE, only include the GTIN and Serial Number. Therefore, changes are required in a backend such as SAP ATTP, to ensure the message includes all required information.

If the events are sent in the same message as the commissioning event, the lot and expiration date can be derived from the commissioning event.

If one EPC is found that cannot be assigned an expiration date or lot number from the context of the message, the entire message is rejected.

4.4.2.6.3 Event Types

Data from an EPCIS message is extracted and written to the verification repository according to the following rules.

- A key representing the PI is created for every product identifier (PI) referenced in an object event.
- If the key already exists, the key is updated, and the new event added to the list of events.
- All object events require mandatory extensions in the EPCIS message for “batch number” and “expiration date”.
- Aggregation and de-aggregation events (AGGREGATION event ADD or DELETE) are ignored. No inference is executed.
- Events are only recognized if they effect an SGTIN directly. No inference is executed on any event. Therefore, an aggregation event packing EPCs on a pallet and a subsequent shipping event for the pallet

do not change the disposition of the EPCs unless the inference is executed in the backend, for example in ATP, and the shipping event, for example OBJECT event OBSERVE, disposition INTRANSIT, for all EPCs is sent to the verification repository.

- OBJECT Events with an empty EPC List, such as for reporting quantities for an LGTIN, are ignored.

A new key is created, or an existing key is updated for:

- Commissioning events (OBJECT event ADD, disposition ACTIVE)
- Decommissioning events (OBJECT event DELETE, disposition INACTIVE)
- Observation Events (OBJECT event OBSERVE, disposition can be any)

4.4.2.6.4 Pack Status Dispositions

The status of a pack can be set using dispositions. SAP does not limit the status (disposition) that can be sent to and stored in the verification repository. Therefore, all dispositions, standard and custom, are permitted and written to the verification repository.

The industry agreed on a common set of values to include additional information in the verification response, such as "recalled" or "suspect", that are also in the GS1 LWMS R1.3. Responders can configure what additional information to include in the response based on disposition. For details of response configuration based on disposition, see relevant topic.

4.4.2.6.5 Batch Expiry

The service supports expiry dates from 2015 to 2055 inclusive. This applies to all messages.

If a message has an expiry date before 2015 or after 2055, the message is rejected, and an error returned.

4.4.2.6.6 Sender GLN and Responder GLN

An MAH sends product identifier (PI).data in an EPCIS message to the verification repository.

When sending data to the verification repository, an MAH provides a Sender GLN in the EPCIS Document Header which is stored with the product identifier (PI). The sender GLN can be any GLN that the MAH chooses and can be different for each message.

This supports the requirement to include specific Responder GLNs in a verification Response. The Sender GLN is stored with the hash of the PI and is used as the responder GLN in response to verification requests.

The service checks that the sender of PI data to the verification repository is the owner of the PI data. This check is based on the company prefixes provided to SAP by customers. To add company prefixes, contact SAP.

4.4.2.6.7 Event Timestamp

The timestamp of the event is stored with every entry made in the verification repository. This is required to determine the latest status of the PI during the verification.

4.4.2.6.8 Message ID

The message ID is logged in the Write Log Web App.

Caution

The message ID must be unique across all messages sent.

4.4.2.6.9 Message Timestamp

The message timestamp is logged in the Write Log Web App but is not stored in the verification repository and is therefore not used in the verification process. The message timestamp is derived from the message header and may deviate from the time the message was loaded, for example, in the Web App.

4.4.2.6.10 Real Time Commissioning Mapping

SAP has implemented Real Time Commissioning (RTC) mapping for all messages sent to the verification repository.

RTC mapping was developed to transform messages that reflect a homogeneous batch but contain thousands of events with one EPC each. The events differ by the event timestamp reflecting the exact time when the pack was commissioned on the packaging line. This is beneficial in cases such as temporary packaging line contamination as effected packs can be clearly identified. In downstream processes, however, these messages create problems due to message size and event volume.

In the context of writing to the verification repository, RTC mapping improves write speed and readability in the write log where otherwise each event would create an entry.

The RTC mapping consolidates object events in one message that have the same event action, disposition, and extension into one event. Several events with the same event action and disposition, but without an extension are also consolidated. All EPCs are included in the new event. The event time stamp is either the first event timestamp (actions ADD and OBSERVE) or the last timestamp (action DELETE).

4.4.2.6.11 Write Log Web App

To confirm that data was written to the verification repository, an MAH can use the Write Log Web App. For each message, the Web App shows information such as:

- Message ID
- Message Timestamp
- Event Timestamp
- GTIN
- Batch
- Expiry date
- Disposition
- Number of units received and written
- Sender GLN – this will be the responder GLN in a verification request response

The message timestamp in the Write Log Web App shows the timestamp in the message header. When you manually upload messages through the Web App, this timestamp may differ from the time the message was uploaded.

Writing to Repository Time Lag

Writing PI data to the repository takes a certain amount of time.

- When you send a message to SAP Traceability Hub, the message shows in the Manage Messages app with status Processing. The message is not visible in the Write Log app at this point.
- When SAP Traceability Hub starts processing the message, which may be minutes or hours later depending on message traffic, the message shows in the Write Log app and shows 0% complete.
- When the message is fully processed, that is all PI data is written to the verification repository, the status in the Manage Messages app changes to Completed, and the status in the Write Log app shows 100% complete.

For more information, see the Web App Guide on the [SAP Traceability Hub U.S. Drug Supply Chain Security Help Page](#).

4.4.2.6.12 Retrieve Item Count from Verification Repository

You can determine the number of Product Identifiers (PI) written to the verification repository for a particular product batch directly from the verification repository. This is possible B2B from any backend system, such as SAP ATTP, and allows you to reconcile PI data written to the verification repository with the quantities stored in SAP ATTP.

Integration into customer backend systems and reconciliation details are not part of the SAP Traceability Hub service, therefore must be implemented by customers in relevant backend applications. The service only provides the number of PI written for a combination of GTIN, batch and expiry date.

Contact SAP for further details.

4.4.2.6.13 Retrieve Data from Write Log

You can view detailed information about data written to the verification repository from the write log. This is possible B2B from any backend system, such as SAP ATTP, and allows you to reconcile PI data written to the verification repository with the quantities stored in SAP ATTP.

Integration into customer backend systems and reconciliation details are not part of the SAP Traceability Hub service, therefore must be implemented by customers in relevant backend applications.

The service provides the ability to retrieve data from the write log. Customers can query the write log by one or more of the following:

- Message ID
- GTIN
- Lot
- Disposition
- Message Date

As response, the service provides a JSON payload containing one or several sets of data including Message ID, Sender GLN, GTIN, Lot, Expiry Date, Disposition, Captured Number of EPCs and Message Date.

Contact SAP for further details.

4.4.2.7 Verification Requests

Requesters send a verification request that is processed by the responder. The response is sent back to the requester. All verification requests contain the following data according to the GS1 LWMS R1.3:

Message Field	Description	Content
PI information	GTIN, lot number, expiration date, serial number	
linkType	Allows to request a specific type of information or service	Permitted value: verificationService
reqGLN	Requestor GLN, the GLN of the requesting company	Example: 0321012345676
corrUUID	Correlation UUID, universally unique identifier, uniquely generated by the requestor for identification of the verification request	Example: 21EC2020-3AEA-4069-A2DD-08002B30309D
context	Objective or purpose of the verification request	Permitted values according to GS1 LWMS R1.3: dscsaStatusCheck dscsaExceptionVerification dscsaSuspectIllegitimate dscsaSaleableReturn

<code>email or telephone</code>	Contact information, email or telephone, of contact point responsible for verification request	Examples Email: <code>anyone@anynet.com</code> Telephone: <code>011234567890</code>
<code>ctrlPossessAtt</code>	Requestor is making an attestation that they have possession or control of the product if a value of true is supplied.	Permitted values: <code>true</code> or <code>false</code>

To create verification requests, SAP provides a B2B option as well as Web App and mobile access. In all cases, the verification request and response follow the GS1 LWMS R1.3.

The app uses SAP Fiori and is available on any device. On a mobile device, the app allows a user to scan the 2D Matrix Barcode, decode the barcode and send a verification request to SAP. On devices that do not have a camera, a user can enter the GS1 element string or the four data elements separately.

How a verification request is processed depends on the requester role, such as wholesaler, manufacturer, logistics service provider or dispenser. For example, a request sent by a wholesaler is routed through the entire VRS ecosystem to the responder, while manufacturers can only verify their own GTINs against the verification repository with no routing performed. The following sections describe the different use cases.

4.4.2.7.1 Wholesaler or Dispenser acting as Requester

The service is the same for dispensers and wholesalers. When an SAP customer sends a verification request (VR), the request is sent to the Lookup Directory, where connectivity information is determined based on the GTIN and expiration date in the request. The request is then routed based on connectivity information to one of the following:

- If the MAH acting as responder is an SAP customer, the VR is routed either to the SAP verification repository or the customer repository. If the MAH acting as responder is using a third-party VRS and lookup directory service, the VR is sent to the third-party VRS system.

Verifications initiated by wholesalers or dispensers outside the SAP service, that is, using a third-party solution provider, are received in the service and routed to the SAP verification repository or the customer's EPCIS repository.

Note

This section does not cover SAP Advanced Track and Trace for Pharmaceuticals and SAP WM or EWM capabilities. See SAP [Help](#).

For wholesalers or dispensers who use SAP Traceability Hub, a user can scan an item in the warehouse. A verification request is created in WMS that is sent to the wholesaler's or dispenser's track and trace system, for example SAP Advanced Track and Trace for Pharmaceuticals.

If the unit cannot be verified by the wholesaler's or dispenser's track and trace system, the request is sent to the SAP Traceability Hub, and the verification request is routed as described above. SAP Traceability Hub sends the response to the wholesaler's or dispenser's track and trace system which in turn routes the response to the scanning device.

For wholesaler and dispenser users, a web app supports routing and verification of any product identifier. The app can act as a fallback for B2B verification.

Context Value	Wholesalers	Dispensers
dscsaStatusCheck	Yes	Yes
dscsaExceptionVerification	Yes	Yes
dscsaSuspectIllegitimate	Yes	Yes
dscsaSaleableReturn	Yes	No

4.4.2.7.2 MAH acting as Requester

📘 Note

Verification capabilities for MAHs are similar to the capabilities for wholesalers and dispensers. This section describes exceptions and additional capabilities.

The service supports B2B verification for MAHs. In addition, the service supports on-behalf scenarios using B2B verification. See relevant sections.

For MAH users, the Web App supports verification of PIs of an SAP customer's products stored in the SAP verification repository or the MAH's repository, such as SAP Advanced Track and Trace for Pharmaceuticals. VRs sent by an MAH user using context = SAPdscsaSelfTest do not use the Lookup Directory for verification routing but only to determine GTIN ownership. Therefore, while VRs are not routed to third-party solution providers through the Lookup Directory, customers must enter the GTIN in the Lookup Directory for the GTIN owner check.

4.4.2.7.3 Verification on-behalf of MAHs

MAHs may require verification of their own product packs by affiliated organizations or other service providers such as Third-Party Logistics Service Providers (3PLs). These organizations can verify products from SAP manufacturing customers (MAHs) on their behalf. An MAH can provide access to 3PLs to verify that MAH's products.

Verification is performed against the verification repository without routing. The service performs a GTIN owner check based on GTIN and expiry date to ensure only that MAH's products are verified. SAP can switch off the GTIN owner check for certain customers for B2B verification only if the calling system performs a product owner check or there are other means to ensure that no PI can be verified that includes a GTIN that is not owned by the MAH. For example, the system performing the verification is running in a warehouse that stores MAH products only.

The MAH can select any value for the context field within the verification request.

B2B onboarding of a third-party service provider is required. The SAP onboarding team facilitates onboarding.

This is only available for customers who use the SAP verification repository for verification.

4.4.2.7.4 Verification through MAH Website or Portal

An SAP manufacturing customer (MAH) can use the verification service to verify products through that MAH's own Web site or portal. This capability supports verification by secondary wholesalers.

An MAH must set up the Web site or portal, manage access and checks required to ensure authorized trading partner status of users. An MAH can connect its own Web site or portal with the verification service.

Verification is performed against the verification repository without routing. The service performs a GTIN owner check based on GTIN and expiry date to ensure only that MAH's products are verified. The MAH can select any value for the context field within the verification request.

This is only available for customers who use the SAP verification repository for verification.

4.4.2.7.5 Verifying Authorized Trading Partner Status

According to the DSCSA, verification requests initiated from authorized trading partners (ATP) must be responded to. To identify an ATP, the data in the body of the verification request is insufficient. GLNs are public and can be used by any entity. Therefore, a GLN does not suffice to validate the ATP status of a requester.

The service supports the use of verifiable credentials to prove ATP status. The service adds a verifiable presentation to a verification request so a responder can verify the ATP status of the requester.

The requester can also check the credentials provided in the verification response. See relevant section 6.6.

4.4.2.7.6 Verification Request Validation

Verification Requests (VR) are validated for syntactical correctness. VRs are declined by the system, that is return an error, if they do not comply to the LMVS 1.3. In addition, verification requests may be declined for reasons defined by the responder's VRS. If the responder's VRS is SAP, verification requests are declined if:

- UUID is not unique
- Requester GLN is not on the allowlist of the responder or is on the blocklist of the responder, see relevant section 5.4.3
- The parameter to attest control or possession is false, and the responder chose to decline a response, see section 5.4.1
- GTIN cannot be found in the LD

4.4.2.7.7 Verification Context

According to the GS1 LWMS R1.3, verification requests that are routed to other VRS providers to verify a PI for must include one of the context values defined in the implementation guideline, which are `dscsaStatusCheck`, `dscsaExceptionVerification`, `dscsaSuspectIllegitimate` and `dscsaSaleableReturn`.

For other purposes in which verification is managed entirely within the SAP service, other values can be used, as outlined above:

- When MAHs verify their own product identifiers through the web app to ensure the correct response is sent, context = SAPdscsaSelfTest is used.
- When MAHs allow verification on their behalf through 3PLs or other service providers or offer verification through their own Web site or portal, MAHs can choose the context.

4.4.2.7.8 Mandatory Contact Information

A verification request must contain contact information.

You enter contact information in the Manage Verifications app. You must provide email or telephone or both.

4.4.2.7.9 Summary

SAP Customer Role	Connection Type	Capability	Context value in VR	Checks
Wholesaler, Dispenser	B2B	Full routing	according to GS1 LWMS R1.3, see 4.1	Requester GLN
Wholesaler, Dispenser	SAP Web App	Full routing	according to GS1 LWMS R1.3, see 4.1	Requester GLN
MAH	B2B	Full Routing	according to GS1 LWMS R1.3, see section 4.1	Requester GLN
MAH	SAP Web App	No routing	SAPdscsaSelfTest	MAH GTIN Ownership
3PL on behalf of MAH	B2B	No routing	Any	Requester GLN, MAH GTIN Ownership
Any entity through MAH Customer Web site	B2B	No routing	Any	Requester GLN MAH GTIN Ownership

Related Information

For more information, see the Web App Guide on the [SAP Traceability Hub U.S. Drug Supply Chain Security Help Page](#).

4.4.2.8 Verification Response

When a verification request reaches the repository, the service checks if the PI is present, then determines the response based on disposition and expiry date, and the customer-specific response configuration.

4.4.2.8.1 Verification Response Message Details

The verification response as defined by GS1 LWMS R1.3 contains the following data:

VR Response Field	Description	Example
Responder GLN	GLN of the responder see section 5.6	Example: 0321012345676
corrUUID	Correlation UUID, identification of the verification request	Example: 21EC2020-3AEA-4069-A2DD-08002B30309D
verified	true or false	true or false
verificationFailureReason	Only if verified=false: Information detailing why a PI was not verified. See section 5.5.	No_reason_provided
additionalInfo	Information providing additional information can be included in true and false verifications	Not provided or suspect or recalled
verificationTimestamp	Timestamp when verification was performed	
email or telephone	Contact data, either Email or telephone, of contact point responsible for verification response	Examples for email: anyone@anynet.com For telephone: 011234567890

4.4.2.8.2 Verification Response Standard

GS1 LWMS R1.3 restricts responses to a number of scenarios. The standard explicitly does not permit any combinations of "verified", "verificationfailureReason" and "additionalInfo" beyond the defined scenarios. For example, a response containing "verified=true" and "additionalInfo=Suspect" is non-compliant.

The verification response configuration app (see section 5.4) uses the GS1 Scenario IDs for the response content for "verified", "verificationfailureReason" and "additionalInfo".

GS1 LWMS R1.3 Response Scenarios

GS1 Scenario	PI found?	Information to indicate product is UNFIT for distribution	Verified	VerificationFailureReason	AdditionalInfo
A1	YES	NO	True		
A2	YES	NO	True		ExpirationExtended

B1.1	YES	YES	True		Recalled
B1.2	YES	YES	True		Expired
B2.1	YES	YES	False	Manufacturer_policy	Recalled
B2.2	YES	YES	False	Manufacturer_policy	Expired
C1.1	YES	YES	False	Not_for_re-distribution	Suspect
C1.2	YES	YES	False	Not_for_re-distribution	Illegitimate
C2	YES	YES	False	Manufacturer_policy	
D	NO	NO	False	No_reason_provided	
E	NO	NO	False	Various, for example No_match_GTIN_Serial	

Related Information

For details of response scenarios, see the verification Responses section of:

[GS1 Healthcare US Implementation Guideline](#) 

Applying the GS1 Lightweight Messaging Standard for DSCSA Verification of Returned Product Identifiers

Available on the relevant GS1 web page:

[GS1 US DSCSA Implementation Suite](#) 

4.4.2.8.3 Verification Response Options

Responses can originate from the SAP verification repository or a customer's own repository. Depending on the response configuration, the final response is determined by the PI disposition and expiry date.

Verification against the SAP Verification Repository

A verification response is determined based on:

- The owner of the PI is determined from the Lookup Directory based on the GTIN and expiry date.
- From the GTIN, batch, expiry date and serial number, the service checks whether the hash exists in the verification repository and determines the verification response. See section 7.1.
- If the PI hash is not found, a response with "verified = false" and "verificationFailureReason = No_Reason_Provided" is sent according to GS1 scenario D.

Note

Verification Failure Reason

HDA requirement RES-020 states “The Responder shall have the option to indicate which of the four PI data elements were found/not found and include in the “Not Verified” response.”

SAP does not provide additional information with a negative response. Therefore, the service always responds using scenario D when the PI is not found

- If the PI hash is found, by default, a positive response ("verified = true") is returned. In addition, disposition and responder GLN are determined based on the last event in the verification repository for the verified PI.
- The response configuration determines the final response based on business rules for disposition, expiry date and requester GLN. See section 5.4.

Verification against Other Repositories

The service supports verification against other repositories, such as SAP Advanced Track and Trace for Pharmaceuticals or site server systems. As a minimum requirement the repository must offer a web service that provides a Serial Global Trade Item Number (SGTIN - serial number + GTIN), and returns the related batch, expiry date, and disposition.

Based on each customer's preference, during onboarding, the SAP team configures:

- Fixed responder GLN
- Whether to respond with scenario D ("verificationFailureReason = No_reason_provided"), or scenario E

The response is determined as follows:

- If the SGTIN is not found in the repository, the service returns a "verified=false" according to scenario D or E.
- If the SGTIN is found in the repository, the returned batch and expiry date are compared with the batch and expiry date in the request:

sgtin	Batch	Expiry date	verified	verificationFailureReason - Scenario E only
Found	Match	Match	true	Not provided
Found	Match	No match	False	No_match_GTIN_Serial_Expiry
Found	No match	Match	False	No_match_GTIN_Serial_Lot
Found	No match	No match	False	No_match_GTIN_Serial_Lot_Expiry
Not found			False	No_match_GTIN_Serial

📌 Note

The option to choose between Scenario D and Scenario E, and therefore provide a verification failure reason, is only available for customers who chose to respond to verification requests with their own repository. The customer who owns the repository can choose whether or not to provide the failure reason. This requires setup by the SAP Team.

4.4.2.8.4 Configuring Verification Responses

GS1 LWMS R1.3 requires response configuration. Responders can define responses based on product pack status (disposition) and expiry date, and can decline a response based on the value of `ctrlPossessAtt` or the requester GLN.

SAP provides the Configure Verification Responses Web App to responders to configure responses. By default, if the PI is found and the responder has not configured a response, the response is sent with "`verified = true`" and "`additionalInformation`" not provided, that is, Scenario A1.

By configuring responses, a responder can respond with scenarios A2, B1, B2, C1.1, C1.2 or C2 based on disposition or expiry date.

4.4.2.8.4.1 Contact Information

It is a requirement to provide contact information in a verification response. You enter contact information in the Manage Verification Settings web app. Enter email or telephone or both.

Note

Verification responses fail if you do not enter contact information.

4.4.2.8.4.2 Control Attestation

A responder can choose whether to respond to a verification request that lacks the attestation of possession or control, that is a request with `ctrlPossessAtt=false`. If the responder chooses not to respond to the request, the requester receives a 403 HTTP error.

Configuration changes are recorded in the Change Log.

4.4.2.8.4.3 Block or Allow Requester GLNs

A Responder can choose to block **or** allow certain requesters based on GLN.

You must choose to block **OR** allow.

Blocklist

You can reject requests from certain requesters. The Configure Verification Responses app allows you to add GLNs to a Blocklist.

A verification request that includes a requester GLN on the Blocklist is rejected. The requester receives a 403 HTTP error. All other GLNs not on the Blocklist are permitted to make a request.

Allowlist

You can allow verifications from certain requesters. The Configure Verification Responses app allows you to add GLNs to an Allowlist. A verification request from a requester GLN that is **not** on the Allowlist is rejected.

⚠ Caution

Only GLNs on the Allowlist can make a request.

Change Log

Changes to the Blocklist or Allowlist are recorded in the Change Log.

4.4.2.8.4.4 Disposition Rules

A verification response depends on the status of the product pack in the disposition. The disposition can include information in the response that the product pack was, for example, recalled or destroyed to avoid resale.

When verification is performed against the verification repository, the service returns the disposition associated with the latest event written to the verification repository.

If verification is performed against a customer ATTP repository, the service returns the disposition as an ID. This ID, such as 001, is translated to the relevant disposition, such as active. To ensure correct matching, the SAP Team maintains custom dispositions. If a disposition ID is not found, a 500 HTTP error is returned.

Users can define the response scenario for each disposition in the Configure Verification Responses web app. The five valid response scenarios (B1, B2, C1.1, C1.2 and C2) that depend on the PI disposition are predefined and users can choose one option for each disposition. Dispositions configured during response configuration can be any, standard, or custom.

Changes to response configuration are recorded in the Change Log.

The following table shows examples for response configuration.

Disposition	Scenario
Recalled	B1
Inactive	C1.1
XX_illegitimate	C1.2
Destroyed	C2
Custom_disposition_XY	B1

📘 Note

Changes can take up to ten seconds to become effective.

4.4.2.8.4.5 Expiry Rules

Users can define the response scenario for expired PI in the Configure Verification Responses web app. The two valid response scenarios (B1 and B2) are predefined, and users can choose one option. In addition, a "default" option is available in case the user decides not to check for expired PI.

Changes to the response configuration are recorded in the Change Log.

Note

When a dedicated response is determined based on disposition, the check for expired PI is skipped. Therefore, for a product pack that is recalled, suspect or illegitimate and expired, the service only uses the recalled (or suspect, illegitimate) information in the response.

AdditionalInfo=suspect, recalled or illegitimate therefore supersedes additionalInfo=expired.

Configuration for Extended Expiration

The service supports the definition of extended expiry dates for certain lots, and the ability to respond to verification requests accordingly. A user can define the GTIN lot combination and the extended expiry date.

When determining the response for a verification request with an expired PI, the service checks the list of lots. If the lot is on the list, the service takes the extended expiry date into account.

- If the extended expiry date is in the past, that is the PI is expired even through the expiry was extended, a response is sent according to scenario B1 or B2 depending on the expiry rule configuration.
- If the extended expiry date is today or in the future, a response is sent according to scenario A2, that is with `verified=true` and `additionalInfo=ExpirationExtended`.

Changes to extended expiration configuration are recorded in the Change Log.

4.4.2.8.5 Determining verificationFailureReason

The verificationFailureReason provides information about why a PI was not verified.

PI not found

According to GS1 LWMS R1.3, responders can choose between scenario D or Scenario E, that is, chose to provide verificationFailureReason in case the PI was not found.

However, when verification is performed against the verification repository, and the PI is not found in the verification repository, the service always responds using Scenario D, that is, "No reason provided".

For verification against a customer repository, during onboarding to SAP Traceability Hub, a customer can decide whether to respond with Scenario D or provide detailed verificationFailureReason through Scenario E.

PI found

In all cases where the PI is found, but the responder chose to respond with `verified=false`, the verificationFailureReason is provided as defined in the GS1 LWMS R1.3 for scenarios B2, C1.1, C1.2 or C2.

4.4.2.8.6 Determining Responder GLN

The responder GLN in the verification response indicates the owner of the GTIN who responded to the verification request, the responder.

Verification against SAP Verification Repository

Manufacturers can define the responder GLN for a dedicated PI through the EPCIS messages written to the SAP verification repository. In addition, a default responder GLN is defined in the Lookup Directory for every MAH.

During verification, the responder GLN is derived depending on the verification result:

- If the PI is found in the verification repository, the responder GLN stored in the SAP verification repository for the PI is used.
- If the PI is not found in the verification repository, the default responder GLN from the Lookup Directory (LD) is used.
- If the GTIN is not maintained in the LD, verifications from Wholesalers fail with a HTTP 404. For verifications initiated by MAHs, the GTIN owner check fails, and an error message returned.

Verification Method:		Verification through Lookup Directory (Wholesalers and Dispensers)	Verification without routing (MAHs, 3PL on-behalf scenario, MAH Web App)
Scenario			
GTIN in Lookup Directory	PI in verification repository	GLN from verification repository	GLN from verification repository
	PI not in verification repository	Default GLN	Default GLN
	Verification against customer repository	Default GLN	Default GLN
GTIN NOT in Lookup Directory	PI in verification repository	B2B: HTTP 404 Error	B2B: HTTP 404 Error
		Portal Web App: Error - GTIN not found in LD	Portal Web App: Error - GTIN not found in LD
	PI not in verification repository	B2B: HTTP 404 Error	B2B: HTTP 404 Error
		Portal Web App: Error - GTIN not found in LD	Portal Web App: Error - GTIN not found in LD
	Verification against customer repository	B2B: HTTP 404 Error	B2B: HTTP 404 Error
		Portal Web App: Error - GTIN not found in LD	Portal Web App: Error - GTIN not found in LD

Verification against Other Repositories

Manufacturers define the static responder GLN when onboarding to SAP Traceability Hub.

When Wholesalers or Dispensers perform a verification, this responder GLN is derived from the configuration at the responder. If the GTIN is not in the LD, verifications from Wholesalers or Dispensers fail with HTTP 404.

Verifications initiated by MAHs or MAH affiliates, that is, verifications without routing, are not supported when verifying against another repository.

4.4.2.8.7 Date Handling

A verification request is created from the PI decoded from the 2D matrix barcode printed on the package or from data entered manually. The expiration date in the barcode is in the format YYMMDD.

Some pharmaceutical products have an expiration date that only contains the year and month, indicating expiration on the last day of the month. This is typically reflected in the human readable part of the artwork, such as "June 2020". Such an expiration date may be encoded in the barcode including the last day of the month, 200630, or DD=00 resulting in 200600. EPCIS data exchange requires a full date and a non-zero day. Therefore, the date in EPCIS will always show as 20-06-30.

As this can create a mismatch between the expiration date transmitted and expiration date scanned, the industry agreed to omit the day and consider a match in year and month as sufficient.

For more information, see Healthcare Distribution Alliance (HDA) Business Requirement Document (BRD), Requirement ENB-150.

Verification against SAP Verification Repository

During verification against the verification repository, the day in the expiry date is NOT taken into account. The day portion of the expiry date is ignored, and verification is only performed using YYMM.

Verification against Customer Repository

For verification against other repositories, for all requests with DD=00, the last day of the month is determined.

4.4.2.8.8 Verification Response Credentialing

According to the DSCSA, verification requests initiated from authorized trading partners (ATP) must be responded to. To identify an authorized trading partner, the data transmitted in the verification request or response body are insufficient. Requester and responder GLNs are public and can be used by any entity and therefore don't suffice to validate authorized trading partner status of a requester or responder.

The service therefore supports the use of verifiable credentials to prove ATP status. A responder can check credentials provided with a verification request. In turn, the responder can add verifiable credentials to the verification response that the requester can verify to prove the ATP status of the responder. See section 6.6.

4.4.2.9 Verification Management

This section describes the way the data are stored in the SAP verification repository.

4.4.2.9.1 Request and Response Logs

Every verification request and response is stored in a verification log. This is required for an MAH to know a verification request occurred, and is a prerequisite for investigation of a suspect product. It also provides requesters with a history of all verifications.

Verification request and response information is available to the MAH who owns the verified product and the wholesaler or dispenser who created the request, including:

- Request time stamp
- PI (GTIN, lot, expiration date, serial number)
- Verified (true or false)
- Additional information (blank, suspect, recalled, expired)
- Verification Failure Reason
- Requester GLN (Wholesaler, Dispenser) and responder GLN (MAH)
- Company name of requester or responder based on GLN - see section 6.2
- Context
- linkType
- Verification request UUID
- Response duration - see section 6.3
- Status (Success/Error)
- Response Code and Response Code Description - see section 6.2
- Alert status - see section 6.5
- Credentials - see section 6.6

Related Information

The Verification Log is accessible through a Web App or an API. For more information, see the Web App Guide on the [SAP Traceability Hub U.S. Drug Supply Chain Security Help Page](#).

To connect to the API and pull verification log data, contact SAP.

4.4.2.9.2 GLN Company Matching

In verification requests and responses, parties are identified by their respective GLN. The service provides a match between GLN and company name.

The company name is displayed for requesters and responders in:

- Verification web app on the response screen
- Verification log app overview and detail screens
- Manage Alerts app
- Alert emails

Company Names are maintained centrally for each GLN by SAP based on the GS1 GEPIR service. Unknown GLNs are displayed as "unknown".

The company name is determined asynchronously, that is, not as part of the actual verification, by calling the GS1 GEPIR service at regular intervals. This may result in cases where a GLN is initially unknown and shows a valid company name later.

4.4.2.9.3 Response Duration

When a verification is successful, a HTTP 200 code is provided along with the response content described in section 5. If the verification is not successful, the verification response does not provide the usual data, only an error code and an error description.

The verification log includes verification requests that fail, that is, HTTP response codes other than 200, such as 400, 401, 403, 404, 408, 500, 502.

4.4.2.9.4 Verification Response HTTP error codes

When a verification is successful, a HTTP 200 code is provided along with the response content described in section 5. If the verification is not successful, the verification response does not provide the usual data, only an error code and an error description.

The verification log includes verification requests that fail, that is, HTTP response codes other than 200, such as 400, 401, 403, 404, 408, 500, 502.

4.4.2.9.5 Verification Alerts

To allow requesters (wholesaler, dispensers) and responders (manufacturers, MAHs) to manage false verification or issues in the verification process, the service provides alert management capabilities. Based on configurable rules, alerts are created and sent by email and/or stored in the Manage Alerts app for further action.

4.4.2.9.5.1 Alert Configuration

Users can define when alerts are created. Users can define:

- Several rules
- For each rule, to display the alert in the Manage Alerts app instead of, or in addition to sending an alert email
- One or more email recipients for each rule
- Conditions for each rule based on request and response content

The system collects alerts every five minutes and sends a notification for each alert to the email address or distribution list you defined. For VRs that trigger an alert, the column in the verification log shows TRUE.

An alert email includes the following:

Field	Example
Rule Name	Rule for recalled product
Verification Timestamp	2020-07-21T08:24:10+00:00
Requester GLN	0363391100002
Requester Company	Unknown
Requester Email	test@sap.com
Requester Telephone	999999999999
Possession or Control Attribute	true
Verified	true
Verification Failure Reason	
Additional Information	Recalled
Responder Email	sap_ich_vrs@sap.com
Responder Telephone	000000000000
Correlation ID	3c2ef4d9-314a-4ba2-b2f4-000d4ba49932
GTIN (01)	00363391100118
Serial Number (21)	4251991030
Batch or Lot Number (10)	BATCH_01_JAN_02
Expiry (17)	200717 [yyMMdd]
HTTP Response Code	200
HTTP Response Code Description	VR processed successfully

The email shows which system created the alert:

- SAP -STAGING U.S. Verification Alert
- SAP -PRODUCTION U.S. Verification Alert

Note

Though alerts are collected every five minutes, the email may be sent later. In some cases, it can take up to thirty minutes for the email to be sent.

In addition to defining rules, users can define issue and resolution categories to categorize alerts using the Manage Alerts app. Both issue and resolution categories can be changed and deleted as long as the category has not yet been assigned to an alert in the Manage Alerts app.

4.4.2.9.5.2 Manage Alerts App

The Manage Alerts app lists alerts generated by the service based on alert rules that you configure. The app allows you to manage alerts by assigning an issue and/or resolution, add a free text comment and define the status of an alert. The app displays the same information that is sent in the alert email. You can group alerts,

for example for a given batch, to set issue, resolution, and status for all alerts in the group. The app provides a change log.

4.4.2.9.5.3 Credentialing for Authorized Trading Partner

Although manufacturers, wholesalers, and dispensers currently establish the authorized trading partner status of direct trading partners, that is, partners they purchase from or sell to directly, there are a number of DSCSA required interactions between companies where a direct trading partner relationship has not been established, such as product information (PI) verification. In such an indirect interaction, trading partners are required by the DSCSA to respond to an authorized trading partner.

The service provides the option to exchange digital proof for identity and authorized trading partner status in a verification request or response. The receiver of a request or response can cryptographically verify credentials.

4.4.2.9.5.3.1 Technical Background

The service provides integration to a wallet that holds credentials. SAP onboards and connects a customer's wallet to the service. Through integration to the wallet, customers can:

- Retrieve a presentation of a verifiable credential (VC) for SAP customer's decentralized identifier (DID) and attach to outbound verification requests and responses
- Check the presentation of a verifiable credential (VC) for incoming verification requests and responses for authorized trading partner status, including revocation

The wallet holds SAP customer credentials and logs all credentialing activities.

The service integrates to the wallet according to the Open Credentialing Initiative (OCI) Conformance Criteria - [VRS Integration Conformance Criteria \(open-credentialing-initiative.github.io\)](https://open-credentialing-initiative.github.io) 📄

Adding Credentials

The service supports presentation of a verifiable credential to verification requests and responses. The service requests from the wallet a verifiable credential (VC) by providing the SAP customer's:

- Decentralized identifier (DID)
- Credential type Authorized Trading Partner
- Correlation UUID

The wallet provides the requested credential type, including the correlation UUID, signs with the DID of the SAP customer and provides it to the SAP service in the form of a JSON Web Token (JWT).

The SAP service adds the JWT to verification requests and response messages.

When a credential presentation is requested, the wallet executes a credential check. Therefore, only valid credentials are sent in a request or response.

Verifying Credentials

The SAP service checks the verifiable credential for incoming verification requests and responses to ensure that only messages from authorized trading partners are accepted.

For this check, the SAP service sends the received JSON Web Token (JWT) and the correlation UUID to the wallet of the SAP customer. The wallet verifies the credentials by checking signatures, expiration date, and revocation list, and then provides a response with the result of the verification to the SAP service.

4.4.2.9.5.3.2 Configure Verifiable Credentials for GLN

You can choose to use verifiable credentials for each GLN. Credentials are always verified when credentials are included in a request or a response, and the GLN matches the SAP customer's responder GLN or requester GLN.

In the ATP Credentials section of the Manage Verification Settings app, you can:

- Not enter credentials for a GLN:
Credentials are not added when sending a verification request or response
- Enter credentials for a GLN:
- Credentials are always added when sending a verification request with this GLN.
- If the verification request has credentials, then credentials are added in the verification response for this responder GLN.
- You can choose to accept a request without credentials, or require credentials in a request.

4.4.2.9.5.3.3 Verification Log

Whether or not credentials are exchanged by business partners is recorded in the verification log.

Depending on whether credentials are exchanged, for each verification request, the log shows:

- None – When both requester and responder have not sent credentials
- Response only – When responder has sent credentials
- Request only – When requester has sent credentials
- Request and response – When both requester and responder have sent credentials

4.4.2.9.5.3.4 Error Handling

If credentials are invalid, a 403 error is generated.

- If a responder cannot validate requester credentials a 403 error is returned.
- If a requester cannot validate responder credentials, the response is discarded, and a 403 error logged.
The error is not communicated to the responder.

4.4.2.9.5.3.5 Boundary Conditions

To be able to provide credentials, customers must sign up with a credential issuer that can provide credentials to prove ATP. This may require a separate subscription. The credentials must be stored in the customer

wallet connected to the SAP service. To enable credentialing, customers connect to a wallet provider of their choice. SAP establishes the connection between the SAP service and the customer wallet. SAP certifies wallet providers for use with the SAP service. The following service providers are certified:

- [Spherity \(CARO - Credentialing of ATP for Regulatory Observance\)](#) 
- [LedgerDomain](#) 

4.4.2.10 Verification Repository Implementation

This section describes the way the data are stored in the SAP verification repository.

4.4.2.10.1 PI Key Creation

Data in the SAP verification repository is stored using a composite key. To keep compatibility with the former blockchain structure, the composite key is created from the Lot hash (see section 7.2) and the PI hash (see section 7.3).

4.4.2.10.2 Product Lot Hash

The lot hash is created as follows:

- Remove DD from Expiry Date YYMMDD to create short Expiry Date YYMM
- Concatenate to a string: [GTIN][Lot Number][Short Expiry Date]
- Hash with md5 algorithm and store as Hex encoded string

4.4.2.10.3 Product Identifier (PI) Hash

The PI hash is created as follows:

- Remove DD from Expiry date YYMMDD to create Short Expiry Date YYMM
- Concatenate to a string: [GTIN][Serial Number][Lot Number][Short Expiry Date]
- Hash with sha256 algorithm, and store in the verification repository as Hex encoded string

4.4.2.10.4 Event Data

For a verification repository key which represents a Product Identifier (PI), the related events are stored in JSON format. This includes the event action ("a"), event time ("t"), event disposition ("d") and sender GLN ("s"):

```
{"a":1, "t":"2018-02-23T11:30:44Z", "d":"active", "s":"7612790000752"}
```

The event time is used to determine the last event during the verification.

4.4.2.11 Web Apps

The SAP Launchpad provides access to a number of SAP web apps, each represented as a tile. The Manage Users app allows the designated app administrator in your organization to assign one or more apps to each user in your organization. For more information on the apps, see the [Verification Web App Guide](#).

Manage Products

Web App that allows MAHs to define GTINs, related descriptions, start and end date in the Lookup Directory, see section 2.

View Lookup Directory

Web App that allows to review the LD content, including the connectivity information synced from all other LDs, see section 2.

Write Log

Web App that allows MAHs to confirm that messages are successfully written to the SAP verification repository, see section 3.11

Configure Verification Responses

Web App that allows MAHs to configure verification responses, see section 5.4.

Verify Product Pack

Web app to perform verifications, see section 4.4

Verification Log

The tile shows the number of verifications that returned a false response in the past week and provides access to the verifications log app, see section 6.1

Configure Alert Creation Rules

Web App that allows you to configure conditions and recipients for alert creation. See 6.5.

Manage Alerts

Web App that allows you to manage received alerts. See 6.5.

Manage Verification Settings

Web App to configure:

- Alert issue and alert resolution types for use in Manage Alerts app, see section 6.5,
- Contact information, email and telephone for verification requests (section 4) and responses (section 5.1)

4.4.2.12 Data Retention

4.4.2.12.1 Retention of Write Log Data

Write Log data belongs to an MAH. SAP plans to delete write log data after a customer-defined retention time. The process is planned to be fully automated:

- Customer defines a retention time
- Retention time may or may not depend on expiry date, for example, retention time = expiry + 36 months
- SAP runs a report monthly to flag entries to be deleted
- Run a report monthly deleting flagged entries

4.4.2.12.2 Retention of Verification Log Data

Verification log data is used by requester and responder but stored by SAP only once. SAP plans to delete verification log data after the longer retention time set by either requester or responder. The process is planned to be fully automated:

- Both partners communicate a retention time to SAP or define a retention time in the solution.
- Retention time may or may not depend on expiry date, for example, retention time = expiry + 36 months. SAP runs a report monthly to flag entries to be deleted.
- SAP runs a report monthly deleting entries that are flagged for deletion from both request and responder.

Verifications that belong to requester or responder organization will be flagged for deletion and no longer display in the log. The data is physically deleted when the other owner also deletes the data.

4.4.3 About this document

Purpose and Scope

This document describes how to use the Web App that is part of the U.S. Supply Chain service of the SAP Traceability Hub.

The service enables pharmaceutical manufacturers providing products for the U.S. market, and U.S. wholesale distributors and U.S. dispensers to comply with the regulations of the U.S. Drug Supply Chain Security Act (DSCSA, especially requirements for verification).

This document describes web apps provided to manage the verification process, according to the GS1 U.S. Implementation Guideline R1.3 that applies to the GS1 Lightweight Messaging Standard for U.S. DSCSA Verification of Product Identifiers (GS1 LWMS R1.3). See the Service Description on the U.S. Supply Chain Help page.

Target Audience

This document is intended for use by service users and administrators.

Assumptions

This guide assumes you are familiar with the pharmaceutical industry and serialization terminology, and with the Saleable Returns service of the SAP Traceability Hub. For more information, see [Getting Started on the SAP U.S Supply Chain Verification Help page](#).

Glossary

Term	Explanation
CI	Connectivity Information of a responder's repository fulfilling verification requests. CI is stored in the Lookup Directory (GTIN).
Dispenser	Entities that dispense pharmaceutical products to patients, such as hospitals, clinics and pharmacies
Disposition	The disposition describes the status of a product pack per the GS1 EPCIS standard. A valid product pack typically carries the disposition "active". Decommissioned items typically carry the disposition "inactive", referring to a destroyed item.
EPCIS	Electronic Product Code Information Services (EPCIS) is a GS1 standard that enables trading partners to share information about the physical movement and status of products as they travel through the supply chain – from business to business to consumers.
EPC	Electronic Product Code; uniquely identifies a product pack through a GTIN and serial number.
Expired	Refers to a product pack with a past expiration date. Usually, expired pharmaceutical products cannot be sold or used.
GS1 LWMS R1.3	GS1 U.S. Implementation Guideline R1.3 that applies to the GS1 Lightweight Messaging Standard for U.S. DSCSA Identifiers.
ICH	SAP Traceability Hub, formerly SAP Information Collaboration Hub for Life Sciences
LD	Lookup Directory contains the GTINs and the related connectivity information of the responder's repository used as the destination of a verification request.
MAH	Marketing Authorization Holder is also known as the manufacturer or supplier and is similar to an OEM. A MAH is a firm or non-profit organization that has been granted a marketing authorization, also known as a license. The MAH allows the holder to market a specific medicinal product in a specific market, for example, the EU or the U.S. Once marketed and in use by patients, the MAH continues to be responsible for monitoring safety (pharmacovigilance).
PI	The Product Identifier (PI) uniquely identifies a product pack. PIs are created from a GTIN, Serial Number, Lot number and expiration date.
Requester	Entity initiating a verification request, typically a wholesaler or dispenser. However, MAHs can also act as requesters for their own PI.
Responder	The entity responding to a verification request, typically an MAH
VRS	Verification Routing Service. Solutions that support routing of verification requests are referred to as VRS. They allow users to verify products that are not stored in the SAP verification repository but stored elsewhere using other technologies or solution providers through verification routing.
Wholesale Distributor	Entities that distribute pharmaceutical products in the U.S. market to hospitals, pharmacies and other points-of-care.

4.4.3.1 Getting Started

Prerequisites

To use the verification service of the SAP Traceability Hub, your organization must be onboarded to the SAP Traceability Hub. For further information, contact your SAP representative.

The following are required to use the Web App.

- High speed Internet connection > 1 Mbps
- Chrome browser which includes the following enabled:
 - Downloads - for downloading serial numbers in a file
 - base64 decoder
 - Certificate-based authentication
 - SAP trusted certificates - certificates are probably trusted already
 - Pop ups - for selecting items, and uploading commissioned serial numbers
 - Browser redirect
 - Hostname provided by SAP allowed on your firewall
 - Network configured to allow resolution of URLs provided by SAP using public DNS
 - Email addresses must be on a corporate domain, and you must manage the validity of email addresses

Your internal network and firewall are configured to allow outbound SSL calls from your network to the Internet using port 443.

Note

If you are unsure about some of these technical details, contact your IT team.

Getting Started

You access the Web App through a browser. SAP recommends Google Chrome.

The SAP Traceability Hub team supply a login and password,

If you do not have a login, contact your SAP representative.

4.4.3.1.1 Home Page

The Homepage is the main access screen for all services.

A tile shows for each service you can use. The number of tiles displayed depends on your permissions. If you do not see a tile that you need, contact your SAP Traceability Hub administrator who sets up users and permissions. If a tile is missing, check the App Finder in your profile.

Personalize Homepage

You can personalize the Home page by selecting the Personalize Home Page option in the user profile drop down menu at the top left of the screen. You can create new groups and move tiles between groups.

Filtering Display

On some screens, you can use filter features. You can refine your search using the filter bar:

- Select a screen element.
- Select Go.
- To clear the filter, select Clear.
- To hide the filter bar, select Hide Filter Bar.

Note

To return to the Home page, select the Home icon at the top left of your screen.

Apps

App	Role	Purpose
Manage Products	responder only	Use to define Connectivity Information (CI) which will be used for routing verification requests
View Lookup Directory	responder only	Use to review the content of the Lookup Directory, including CI from third-party VRS
Write Log	responder only	Verify that messages are successfully written to the verification repository
Configure Verification Responses	responder only	Configure responses based on product pack disposition, PI expiry and requester GLN
Verify Product Pack	responder and requester	Verify PI
Verification Log	responder and requester	Review verification requests. As an MAH, you can check verification requests from different requesters. As a wholesaler or dispenser, you can review all requests for different MAHs.
Upload Product Data	responder only	Used to bulk upload GTINs to the Lookup Directory
Configure Alert Creation Rules	responder and requester	Configure conditions and recipients for alert creation
Manage Verification Settings	Responder and requester	Responder only: Configure alert issue and alert resolution types All: configure contact data, telephone and email All: configure DIDs for each GLN for ATP check
Manage Alerts	responder and requester	Manage received alerts

4.4.4 Lookup Directory

The Lookup Directory contains the connectivity information (CI) of a responder's repository that fulfills verification requests. Connectivity information is stored by product ID (GTIN). The Lookup Directory (LD) is an integral part of any Verification Routing Service (VRS) as it determines the destination for a verification request. Data in each LD is exchanged with other LDs in the eco system. Therefore, each LD contains all Connectivity Information (CI) maintained in the ecosystem.

For details of the Lookup Directory, see the Service Description on the [Help page](#).

4.4.4.1 Manage Products App

The Manage Products web app allows:

- Manual creation of CI by defining GTIN, GTIN description, start and end date, and labeler code. A new CI is always created with status active.
- Bulk creation of CI from a file. You can download a template, and populate the file with GTINs, description, start and end date, and then upload the file.
- Edit CI description, status, start and end dates
- Bulk Update of CI status, start and end dates
- Delete a CI. A deleted entry remains in status deleted. A deleted entry cannot be changed again.
- View synchronization status of each CI
- Review change log for all or selected entries
- Search and filter the list of products

GTIN

GTINs must follow the GS1 standard (13 digits numeric, correct check digit) and must match a customer GCP stored in SAP Traceability Hub.

Start and End Date

Start and End data define the validity period for the connectivity information (CI) referring to the expiry date of the verified product identifier (PI). Because the dates are transferred to other LDs in YYMMDD format, dates must not be more than 50 years in the past or more than 50 years in the future.

Labeler Code

The labeler code is a 4-6 digit numeric value and identifies the owner of the GTIN and related CI.

When the assigned labeler code matches the GTIN and embedded GCP, and therefore the embedded labeler code, the GCP is considered a primary GCP. For example, GTIN 00363391100200 matches the SAP Customer's GCP 0363391 and the SAP Customer's labeler code 63391.

The user can select From GTIN, and the labeler code is assigned based on the labeler code embedded in the GTIN.

In cases where the GTIN is transferred or there is co-marketing of the GTIN, the labeler code in the GTIN is owned by another MAH. In such cases, the related GCP is considered a secondary GCP. However, you need to assign your own labeler code to the CI and the labeler code must match a primary GCP. You can assign the labeler code from the drop down list. In this case, the labeler code you assign does not match the labeler code in the GTIN.

Example:

	Own GTIN	GTIN transferred from third party
SAP Customer primary GCP	0363391	0363391
SAP Customer labeler code	63391	63391
GTIN	00363391100200	00363322100200
Embedded GCP	0363391 (primary GCP)	0363322 (secondary GCP)

	Own GTIN	GTIN transferred from third party
Assigned labeler code	63391 (own labeler code)	63391 (own labeler code)

Limits

- GTIN description can include any character and is limited to 5000 characters.
- Maximum file size for bulk creation is 1MB.
- Maximum number of GTINs in the upload file is 2000.

Sync Status

The sync status depicts the status for synchronizing the CI to all connected LDs:

- Sync in process: a recent creation or change is still synchronizing. It can take several minutes for this process to finish.
- Synced: the new or changed CI has successfully synchronized with all connected LDs.
- Out of Sync: the new or changed CI failed to synchronize with at least one connected LD.

4.4.4.2 View Lookup Directory App

The View Lookup Directory web app allows you to view the entire Lookup Directory including any connectivity information (CI) synchronized from third-party VRS LDs.

4.4.5 Sending Product Information to SAP Verification Repository

A responder can send Product Identifier (PI) data to the SAP verification repository using an EPCIS file. The Write Log app allows you to check that data has been written correctly.

4.4.5.1 Write Log App

The Write Log app allows you to review details of sent EPCIS messages. It provides a summary of the PI sent by message ID, GTIN, Lot, Expiration Date and Disposition. Therefore, one message containing multiple GTINs or several events with different dispositions creates several entries in the write log.

You can filter the write log by Message ID, Message Time, Event Time, Disposition, GTIN, Lot and other details. To view details, select the row.

The Write Log overview and detail screens include:

Message ID

The message ID identifies a message.

Message Time (UTC)

Message Time refers to the EPCIS file creation time.

EPCIS files contain multiple events, and the time of these events refers to the event creation times. Therefore, an event creation time may be earlier than the EPCIS file creation time.

If you upload a message using the web app, the message time may be significantly earlier than the time you uploaded the message.

Event Time (UTC)

The event time refers to the time the event was captured. The last event is used to determine the current disposition.

Disposition

The disposition reflects the status of an item. The disposition is used to determine the response based on the response configuration. See section 4.1.

GTIN, Lot, Expiry Date

GTIN, lot and expiry date are the key identifiers of a product pack together with the serial number. The serial number is not shown in the write log.

Sender GLN

The sender GLN defines the sender of the message. Sender GLN from the message header is used as responder GLN when responding to a verification request.

EPCs Received

Number of EPCs (GTIN and serial number combination) received for writing to the verification repository for the given combination of GTIN, batch, expiry date, disposition and message ID.

Each EPC is received into a queue, and then written to the verification repository. Therefore, there can be more EPCs received than written.

EPCs Written to Repository

Number of EPCs (GTIN and serial number combination) written to the verification repository for the given combination of GTIN, batch, expiry date, disposition and message ID. When all received EPCs are written to the verification repository, the number of queued and written EPCs are equal.

Percentage Received Written to Repository

The percentage of EPCs written of the total number of EPCs received.

When all EPCs received have been written, the value changes to 100%.

Time Message Received

The time when the message was received for writing to the verification repository.

Time EPC Written to Repository

The time when the last EPC was written to the verification repository for this combination of GTIN, batch, expiry date, disposition and message ID.

Download Data

You can download data to an MS EXCEL or PDF file.

All data that matches your filter is downloaded.

The PDF that can be downloaded from the write log also contains:

- The timestamp of the download is added in the header
- The information "Confidential" is added to the header
- The filter criteria are added to the header
- Pages are numbered in the footer as "Page x of xx"
- The information "SAP Traceability Hub", indicating the source system, is added to the footer

Repository Explorer

From the details screen, you can navigate to the repository explorer.

4.4.6 Verification

SAP Traceability Hub provides the following apps for the verification process.

App	Role(s)	Purpose
Configure Verification Responses	MAHs only	As a responder, you can customize verification responses and provide additional information.
Verify Product Pack	All	For an MAH, verification is only performed against the MAH's own data in the verification process. Wholesale distributors or dispensers can use the app to verify any product identifier. Verification requests are routed to the responder defined in the Lookup Directory. To perform a verification, you enter PI data manually or by scanning with a camera enabled on your mobile device.
Verification Log	All	As a requester, you can review all verification requests made B2B and through the web interface. As a responder, you can review all verifications of your products.

4.4.6.1 Configuring Verification Responses

As an MAH, you can define verification responses for requests about your product identifiers (PI).

The GS1 LWMS R1.3 defines all possible responses. To comply with GS1 LWMS R1.3, the SAP Traceability Hub provides response configuration capabilities that allow you to configure all parameters in the response (verified/additionalInfo/verificationFailureReason), and limit possible responses to those defined in the standard.

Note

Default Setting: By default, every PI that is found returns a verification response with verified=true and no additional information. If you do not configure responses, the default response is verified=true for all PIs found.

4.4.6.1.1 Response Options

GS1 LWMS R1.3 restricts responses to the certain scenarios. The standard explicitly does not allow any other combinations of "verified", "verificationFailureReason" and "additionalInfo" beyond the defined scenarios. For example, a response containing "verified=true" and "additionalInfo=Suspect" is non-compliant.

For details of response scenarios, see the Verification Responses section of:

- [GS1 Healthcare US Implementation Guideline Applying the GS1 Lightweight Messaging Standard for DSCSA Verification of Returned Product Identifiers](#) ➡

The standard documentation is available on the relevant GS1 web page:

- [GS1 US DSCSA Implementation Suite](#) ➡

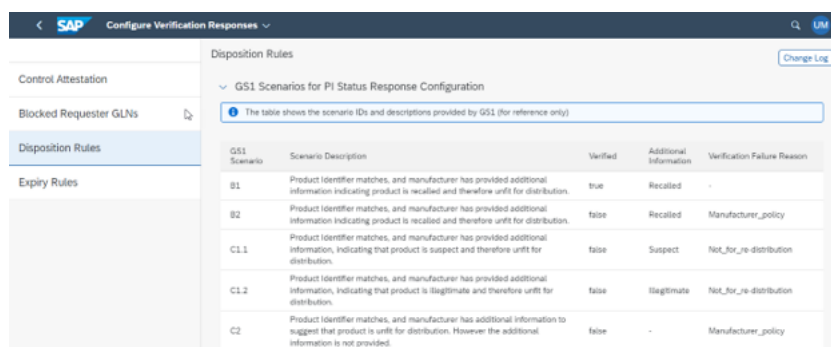
4.4.6.1.2 Configuring Responses based on Disposition

You can define the response scenario for each disposition in the Configure Verification Responses web app.

The five valid response scenarios (B1, B2, C1.1, C1.2 and C2) are predefined, and you can choose one option for a disposition. Dispositions configured in the app can be GS1 standard or custom.

The app uses the GS1 Scenario IDs to define response content for "verified", "verificationFailureReason" and "additionalInfo".

To view the GS1 Scenarios for PI Status Response Configuration, select Forward Caret >



The screenshot shows the 'Configure Verification Responses' web app interface. On the left, there is a sidebar with navigation options: 'Control Attestation', 'Blocked Requester GLNs', 'Disposition Rules' (selected), and 'Expiry Rules'. The main area is titled 'Disposition Rules' and contains a section 'GS1 Scenarios for PI Status Response Configuration'. Below this, a table lists predefined scenarios. A 'Change Log' button is visible in the top right corner of the main area.

GS1 Scenario	Scenario Description	Verified	Additional Information	Verification Failure Reason
B1	Product Identifier matches, and manufacturer has provided additional information indicating product is recalled and therefore unfit for distribution.	true	Recalled	-
B2	Product Identifier matches, and manufacturer has provided additional information indicating product is recalled and therefore unfit for distribution.	false	Recalled	Manufacturer_policy
C1.1	Product Identifier matches, and manufacturer has provided additional information, indicating that product is suspect and therefore unfit for distribution.	false	Suspect	Not_for_re-distribution
C1.2	Product Identifier matches, and manufacturer has provided additional information, indicating that product is illegitimate and therefore unfit for distribution.	false	Illegitimate	Not_for_re-distribution
C2	Product Identifier matches, and manufacturer has additional information to suggest that product is unfit for distribution. However the additional information is not provided.	false	-	Manufacturer_policy

Changes to response configuration are recorded in the Change Log.

You can download the current configuration of disposition rules to PDF.

The following table shows an example response configuration.

Disposition	Selected Scenario
Recalled	B1
Inactive	C1.1
XX_illegitimate	C1.2

Disposition	Selected Scenario
Destroyed	C2
Custom_disposition_XY	B1

4.4.6.1.3 Configuring Responses based on Expiry Date

GS1 LWMS R1.3 allows for sending a dedicated response for expired PI, that is, a product pack that is expired.

You can define the response scenario for expired PI in the Configure Verification Responses web app. The two valid response scenarios (B1 and B2) are predefined, and you can choose one option. In addition, a "default" option is available in case you choose not to check for expired PI.

Changes to response configuration are recorded in the Change Log.

Note

When a response is determined based on disposition, the check for expired PI is skipped. Therefore, for a product pack that is recalled or suspect and expired, the service only uses the recalled or suspect information in the response.

AdditionalInfo=suspect or additionalInfo=recalled therefore supersedes additionalInfo=expired.

Configuration changes may take up to ten seconds to become effective.

Configuration for Extended Expiration

The service supports the definition of extended expiration dates for certain lots and the ability to respond to verification requests accordingly.

You can define GTIN lot combinations and the associated extended expiry date in the Configure Verification Responses app.

When determining the response for a verification request with an expired PI, the service checks the list of lots, and if the lot is in the list, takes the extended expiry date into account.

- If the extended expiry date is in the past, that is the PI is expired even though the expiry was extended, a response is sent according to scenario B1 or B2 depending on the expiry rule configuration.
- If the extended expiry date is today or in the future, a response is sent according to scenario A2, that is with verified=true and additionalInfo=ExpirationExtended.

Changes to extended expiration configuration are recorded in the Change Log.

4.4.6.1.4 Block or Allow Requester GLNs

As a Responder, you can choose to block or allow certain requesters based on GLN.

You must choose to block OR allow.

Blocklist

You can reject requests from certain requesters. The Configure Verification Responses app allows you to add GLNs to a Blocklist.

A verification request that includes a GLN on the Blocklist is rejected. The requester receives a 403 HTTP error.

All other GLNs not on the Blocklist are permitted to make a request.

Allowlist

You can allow verifications from certain requesters. The Configure Verification Responses app allows you to add GLNs to an Allowlist. A verification request from a GLN that is not on the Allowlist is rejected.

Caution

Only GLNs on the Allowlist can make a request.

4.4.6.2 Verifying Product Pack

MAH

You can use the Verify Product Pack app:

- As an MAH acting as requester to perform verification requests
- To test verification responses are working in the way you configured in the Configure Verification Responses app

For testing, you can use "context = SAPdscsaSelfTest".

Verifications made from the app show in the verification log .

You can only verify GTINs owned by your organization and stored in the Lookup Directory.

Verification requests are not routed to other solution providers but performed on the SAP verification repository or your backend system, for example, SAP Advanced Track and Trace for Pharmaceuticals.

Wholesaler or Dispenser

As a Wholesaler or Dispenser, you can use the Verify Product Pack app for verifications as an alternative to verifications from your backend system.

Verifications initiated by wholesalers or dispensers are routed based on the Lookup Directory.

To verify, you can:

- Enter PI data manually from a laptop or PC
- Use a mobile device that has a camera
- Use a mobile device that does not have a camera

As well as PI information, you can select the context (default: dscsaSaleableReturn) and control attestation (default: true).

In the contact data section, you can enter Requester GLN (default: first GLN in the list), as well as email and telephone (default from configuration).

4.4.6.2.1 Verifying by Manual Entry

To verify using a laptop or PC, you manually enter the PI. You can use the Decoded Data tab or the GS1 Element String tab.

Context

The process begins at the Web App Home page.

Procedure

1. Select the Verify Product Pack app.
2. You can enter a code on the Decoded Data tab or on the GS1 Element String tab.
3. If using the Decoded Data tab, enter a GTIN, Batch Number, Expiration Date and Serial Number. If the details are valid, the GS1 field is auto filled with the corresponding GS1 element string. If the details are not valid, you cannot verify the Product Pack.
4. If you use the GS1 Element String tab, enter a GS1 element string in bracketed format including the application identifiers (AIs). If the GS1 element string is valid, the other fields are auto filled. For example, enter (01)00305970040705(10)747031X(17)210630(21)20011686496500

Table

Application Identifier	Refers to	Example
01	GTIN	00305970040705
10	Batch Number	747031X
17	Expiration Date	210630
21	Serial Number	20011686496500

Checks include the following:

GTIN

- Must be 14 digits
- Must be numeric
- Check Digit must be correct

Batch

- No blanks
- 20 digits maximum

Serial Number

- No blanks
- 20 digits maximum

Expiration date

- Must be a valid date entered in the format YYMMDD with the following exceptions:
 - An entry in the form YYMM, that is omitting the day of the date indicating the last day of the month as the expiry date, is supported. The app automatically adds the last day of the month in the GS1 element string.
 - You can explicitly enter a date with DD=00, such as 230600. In this example, the expiry date in the GS1 element string and verification request is 230600. The verification log shows the expiry date accordingly.
 - Expired product packs show a warning.
5. As well as the PI, the following information must be provided, some of which is filled by default.
1. Attestation that requester has possession or control of the product pack being verified. For this, the tag ctrlPossessAtt is provided in the request. Default is true but user can change to false.
 2. Contact information, telephone number or email. These values are prefilled from configuration, but a user can change them.
 3. Context of the verification request. Depending on your role, you must pick: dscsaStatusCheck, dscsaExceptionVerification, dscsaSuspectIllegitimate, or dscsaSaleableReturn
- If details are not valid or missing, a warning displays and you are prevented from verifying.
- If you cannot verify, check the verification request details.
6. If the details are valid, choose Verify. The result depends on whether the PI is present, and the response configured by the responder. See section 4.

4.4.6.2.2 Verifying on a Mobile Device with Camera

Context

The process begins on your mobile device using the web browser.

Procedure

1. Enter the Web App URL in your web browser.
2. Open the Verification app.
3. If you have a camera set up, the camera starts, and you can scan the 2D matrix barcode on a package.
4. Scan the pack code to verify the pack code validity. The result depends on whether the PI is present, and the response configured by the responder. See section 4.
5. If you temporarily lose access to the camera, select Home or use the menu drop down to return to the Web App home screen, and select the Verification app.
6. To exit, select Sign Out from the profile menu.

4.4.6.2.3 Verifying on a Mobile Device Without Camera

If you do not have a camera on a mobile device, you can enter data manually. The process for verifying on a mobile device is the same as in a browser, see section .

The result depends on whether the PI is present, and the response configured by the responder. See section .

4.4.6.3 Verification Log App

As a responder, you can view the verification requests that have been made about your products. As a requester, you can review all verification requests that you sent, and corresponding responses.

The tile shows how many responses with "verified = false" occurred in the last seven days.

4.4.6.3.1 Screen Personalization

To choose which columns to display, and define the sequence of columns, select the cogwheel.

Note

After a new release of SAP Traceability Hub, you may not be able to see all new fields. To view all fields, personalize the view using the cogwheel.

The screen uses a multi-line layout that shows a second line if you select more than nine columns.

4.4.6.3.2 Filter Display

To filter a list, choose Filters, then choose relevant fields such as:

- Request Time
- GTIN
- Lot
- Serial Number
- Verified (true, false, all)
- Additional Information
- Requester GLN (identifies the wholesaler or dispenser who sent the request by its GLN)
- Responder GLN (identifies the MAH who responded to the request by its GLN)
- UUID
- linkType
- Requester Company (identifies the wholesaler or dispenser who sent the request by its company name)
- Responder Company (identifies the MAH who responded to the request by its company name)

- Status
- Response code
- Alert email status
- Context
- Verification Failure Reason
- Execution Duration (ms)
- Credentials
- Control Attestation (true, false, all)

4.4.6.3.3 Display Company Name

In verification requests and responses, parties are identified by their respective GLN. The service provides a match between GLN and company name. The company name is displayed for requesters and responders.

SAP maintains company names centrally by Global Company Prefix used for each GLN based on the GS1 GEPIR service. GLNs for which no company name could be retrieved from the GS1 GEPIR service are displayed as "unknown". An unknown company name is not an indication of an invalid requester as not all GCPs may be published in the GS1 service.

The company name is determined asynchronously, that is, not as part of the actual verification, by calling the GS1 GEPIR service at regular intervals. This may result in cases where a GLN is initially unknown and shows a valid company name later.

4.4.6.3.4 Verification Request Fail Codes

The verification log includes verification requests that fail, that is, HTTP Response Codes other than 200 (400, 401, 403, 404, 408, 500, 502). Failed verification requests are mainly visible to requesters. In exceptional cases, they are shown in the responder verification log.

The Verification Log Application contains:

- Response Code: the error code, such as 500
- Response Code Description: a detailed description of the error
- Status (Success/Error): requests with http=200 show "Success". All other response codes show "Error".

You can filter verifications based on Response Code and Status.

Note

Error descriptions for the same error code can vary. The following tables provide an overview of potential error codes and related error text for various cases.

E
r
r
o
r
e
d
i
c
t
e
d
p
o
s
s
e
d
e
d
u
n
e
d
s
s
f
u
l
l
y

E
r
r
e
d
i
c
t
e
d
G
e
n
e
r
i
c
E
r
r
o
r
s

E
C
O
n
o
m
i
c
B
N
D
n
o
t
f
o
u
n
d
f
o
r
l
o
g
g
e
d
u
s
e
r

E
C
o
n
f
i
d
e
n
t
i
a
l
i
z
e
d
i
n
f
o
r
m
a
t
i
o
n
r
e
c
e
i
v
e
d
f
r
o
m
a
n
d
d
o
e
s
n
o
t
h
a
v
e
g
t
i
n
/
{
}
/
l
o
t
/
{
}
/
s
e
r
/

E
C
o
n
o
m
i
c

{
}

G
O
D
N
v
a
l
u
e
i
n
s
u
s
t
a
i
n
a
b
l
e
d
e
v
e
l
o
p
m
e
n
t

B
O
O
p
a
s
a
m
e
h
g
r
m
i
s
s
i
o
n
g
:

:

E
C
e
d
e
B
O
O
W
a
m
b
e
m
i
s
B
i
a
g
k
:
S
e
e
p
a
s
t
a
m
e
t
h
i
n
s
s
i
n
g
g
:

Electronic Serial Number
Availability
Remarks
Sign
Opp
Assessment
Requirements
Sign
g
:

Exotic Bopriyative blamssing BDDKKYppasamethgrimsissingg:

E
C
o
n
o
m
i
c
B
O
D
k
T
y
p
e
i
n
a
b
l
e
m
k
s
s
i
n
g
B
O
D
h
e
e
k
p
a
s
a
m
e
h
g
r
m
i
s
s
i
n
g
:

E
C
e
d
e

b
o
o
h
e
e
k
v
a
v
a
e
m
e
s
s
m
n
g
s
i
n
g
:

b
e
o
q
G
L
N
p
a
r
a
m
e
t
e
r
m
s
m
s
s
s
g
n
g
:

E
C
O
n
t

R
e
q
u
e
s
t
e
r
G
L
N
m
a
t
e
r
i
a
l
s
o
n
g
n
o
t
p
r
e
s
e
n
t
:

E
C
O
n
t

R
e
q
u
e
s
t
e
r
G
L
N
h
e
n
t
h
e
t
h
e
w
e
w
e
d
:

E **e** **e** **d** **e** **b** **o** **r** **U** **U** **D** **p** **a** **s** **t** **a** **m** **e** **n** **g** **i** **r** **m** **s** **s** **i** **n** **g** **:** **b** **o** **r** **U** **U** **I** **D** **i** **v** **a** **b** **l** **a** **m** **k** **s** **s** **i** **n** **g**

E
T
e
e
M
A
E
h
e
h
o
w
h
b
e
o
w
G
E
r
N
f
G
T
I
N
:
A
u
t
h
o
r
i
z
a
t
i
o
n
R
e
s
p
o
n
s
e
C
o
d
e
s

Ende der Organisation ist es nicht MAH or WHO (Web App)

E
C
O
n
t
r
o
l
l
e
d
g
o
v
e
r
n
m
e
n
t
s
r
e
s
p
o
n
s
i
b
l
e
f
o
r
t
h
e
i
r
o
u
t
r
e
a
t
m
e
n
t
s
o
f
t
h
e
d
r
u
g
s
u
p
p
l
y
c
h
a
i
n
.

E
C
e
d
e

C
D
e
d
e
e
d
e
a
t
s
a
b
s
p
d
o
v
t
d
e
d
e
o
u
fi
d
d
o
t
b
e
v
e
r
i
fi
e
d

E **C** **e** **d** **e** **O** **t** **h** **e** **r** **E** **r** **r** **o** **r** **C** **o** **d** **e** **s** **E** **D** **4** **N** **B** **n** **R** **e** **t** **c** **e** **u** **m** **d** **i** **n** **t** **E** **D** **O** **4** **:**

E
C
O
n
t
e
n
t
s
4
0
8
:
B
O
B
p
o
r
t
e
e
S
y
e
t
e
n
d
O
n

4.4.6.3.5 Display Verification Response Times

The service provides the verification response times on the verification log overview and detail screens. You can filter and sort the verification log overview screen by verification response times using ranges.

Note

Response time is only visible for verification requests made after Release 2008.

Response Times are only shown for verification requests that are initiated in the service. Therefore, requesters will always see the response duration, while responders only see the response duration in the log when the request was created inside the service. In other cases, the time the verification request spent outside the service is unknown and a total verification duration cannot be derived.

4.4.6.3.6 Download Data

You can download data to an MS EXCEL or PDF file.

All data that matches your filter is downloaded.

Note

The service doesn't limit the number of lines to download. However, the service may take considerable amount of time to execute for large volumes of data. Test showed, that download of 100.000 rows of data may take up to one minute to complete.

4.4.6.3.7 Verification Details

To view details of a verification request, select the row.

Note

Details about a request and response are only available to the MAH who owns the product or the wholesaler or dispenser who made the request.

Repository Explorer

From the details screen, you can open the repository explorer, see section 6.

4.4.7 Managing Alerts

Requesters and Responders can generate and manage alerts for verification requests that require follow up. You can:

- Define conditions for generating an alert
- Define to receive an alert by email or through the web app
- Manage alerts received

4.4.7.1 Configure Alert Creation Rules App

The app allows you to define under which conditions alerts are generated.

You can define if an alert is displayed in the Manage Alerts app, or sent by email to specified recipients, or both in the app and by email.

When you create a new rule, you provide a rule name and description. The rule is initially inactive. You can activate rules or leave them as inactive.

When you create a rule, you can add one or more conditions that must be fulfilled to trigger an alert.

If you want alerts sent by email, you enter email recipients.

If you want the alert to show in the Manage Alerts app, set Alert in App to ON.

The following table shows conditions supported:

Field	Operators	Values	Input Type/ Restrictions
VERIFIED_STATUS	is equals to	true	Select input
	is not equals to	false	
ADDITIONAL INFO	is equals to	Recalled	Select input
	is not equals to	Expired	
		Suspect	
		Illegitimate	
VERIFICATION FAILURE REASON	is equals to	Manufacturer_policy	Select input
	is not equals to	Not_for_re-distribution	
		No_reason_provided	
LINKTYPE	is equals to	verificationService	Select input
	is not equals to		
REQUESTER GLN	is in list	comma separated values in text input, for example:	Text input: Only ten GLNs are allowed
	is not in list	0363391100002, 1100001002641	
RESPONDER GLN	is in list	comma separated values in text input, for example:	Text input: Only five GLNs are allowed.
	is not in list	0363391100002, 1100001002641	

Field	Operators	Values	Input Type/ Restrictions
GTIN	starts with	Initials of a GTIN in free text. Wildcards asterisk and dot: * - asterisk- more than one character . - dot- any single character *3708 matches 103708, 400003708 .03708 matches 103708,203708	Multivalue Text
CONTEXT	is in list	dscsaStatusCheck dscsaExceptionVerification dscsaSuspectIllegitimate dscsaSaleableReturn SAPdscsaSelfTest	Multi select
HTTP RE- SPONSE CODE	is in list	403, 500, 502 and 504	Multi select
Control Attes- tation	is equals to	True, false	Select Input
Credentials	is equals to	None Request only Response only Request and Response	Select Input

4.4.7.2 Manage Alerts App

The Manage Alerts app lists alerts generated based on the rules you configured.

4.4.7.2.1 Filter Display

To filter a list, choose Filters, then choose relevant fields such as:

- Request Time
- GTIN
- Lot
- Serial Number

- Verified (true, false, all)
- Additional Information
- Requester GLN (identifies the wholesaler or dispenser who sent the request by its GLN)
- Responder GLN (identifies the MAH who responded to the request by its GLN)
- UUID
- linkType
- Requester Company (identifies the wholesaler or dispenser who sent the request by its company name)
- Responder Company (identifies the MAH who responded to the request by its company name)
- Status
- Response code
- Alert email status
- Context
- Verification Failure Reason
- Execution Duration (ms)
- Credentials
- Control Attestation (true, false, all)

4.4.7.2.2 Managing one or more alerts

To process one alert, select the alert, then you can:

- Assign an issue, a resolution, or both.
- Add a comment
- Change the status

You can group alerts, for example for a given batch, set issue, resolution, and status for all alerts related to the batch.

All changes to an alert are shown in the alert history.

4.4.8 Verification Repository Explorer

You can view verification repository information using the Verification Repository Explorer app, which is accessible from the Write Log and Verification Log apps.

- The Write Log app displays product and batch information. The Verification Repository Explorer app displays the related batch information, that is the GTIN, batch number and expiry date as well as the PI Count for the GTIN and batch. To display related event information stored in the verification repository, enter a Serial Number to complete the PI.
- The Verification Log app displays the full product batch and serial number. The Verification Repository Explorer app displays the related batch information and the event information for the serial number.

Note

Verification repository details are only visible to responders who make their PI data available in the verification repository.

4.4.9 Manage Verification Settings

4.4.9.1 Define Issues

You can define issues that are used in Manage Alert apps to assign to alerts. An issue is a problem that leads to certain verification responses and triggers alerts. You can use an issue for example to group alerts and assign a common resolution.

You can delete an issue, and you can edit an issue that is not assigned to an alert.

4.4.9.2 Define Resolutions

You can define resolutions that you can assign to alerts in the Manage Alerts app.

You cannot edit a resolution. You can delete a resolution that is not assigned to an alert.

4.4.9.3 Manage Request and Response Contact Details

You can manage the contact information transmitted to other parties in verification requests and responses.

You can set default contact information, or enter contact information for each GLN.

Requester or responder role is automatically assigned depending on your role.

You can edit name, email and telephone number. Email and telephone number are transmitted in the request or response.

4.4.9.4 Manage ATP Credentials

You can choose from the following wallet providers:

- Spherity
- LedgerDomain

You can define if a GLN requires credentials and an ATP check. In the ATP Credentials section of the Manage Verification Settings web app, you can enter the Decentralized Identifier (DID) that credentials are assigned to in the wallet, and then assign that DID for requester and responder roles, and for each GLN. You can also define whether credentials are required in messages from other parties.

See ATP Credentials in section.

4.5 About US Drug Supply Chain Security

Purpose and Scope

This document provides an overview of the service provided by the SAP Traceability Hub to meet the requirements for drug supply chain security. The service enables pharmaceutical manufacturers providing products for the U.S. market, as well as U.S. wholesale distributors and U.S. Dispensers to comply with the regulations of the U.S. Drug Supply Chain Security Act, especially requirements for verification, and exchange of transaction information and transaction statements.

Target Audience

This document is for:

- Supply Chain Managers
- Integration Engineers
- Implementation teams
- Compliance teams

Assumptions and Prerequisites

To use the service of the SAP Traceability Hub, participants must be onboarded to the SAP Traceability Hub. For further information about onboarding see the SAP Traceability Hub Help Page.

Some information is only available to SAP customers and partners.

4.5.1 Trace Request Management

SAP offers a Trace Management option which provides the ability for a trading partner to manage Trace Requests acting as an Initiator, and Trace Responses acting as a Responder.

Trace requests are received from Initiators such as regulators, agencies, or other trading partners in case of investigation of pharmaceutical drugs.

You can create and manage trace requests, respond to a trace request, include attachments, and there is an optional approval process.

A Change Log records all trace management actions.

4.5.1.1 ATTP Integration

The service provides the ability to integrate with SAP Advance Track and Trace for Pharmaceuticals (ATTP) to retrieve transaction information (TI) relevant to the product identifier in a trace request.

For companies acting as buyer and seller, such as a U.S. Wholesaler, the service responds with two types of file, one for inbound and one for outbound.

4.5.1.2 Manual Upload

You can also upload transaction information in the form of EPCIS XML files.

4.5.2 Web Apps

Write Log

Web App that allows MAHs to confirm that messages have been successfully written to the SAP verification repository.

Configure Verification Responses

Web App that allows MAHs to configure verification responses

Verify Product Pack

Web App to perform verifications

Verification Log

Shows the number of verifications that returned a false response in the past week and provides access to:

- Verifications initiated (wholesalers/requesters)
- Verifications responded (MAHs/responders)

Upload Product Data to Lookup Directory

Web App that allows MAHs to mass upload GTINs and related descriptions to the Lookup Directory, and the ability to download a complete list to PDF

Configure Alert Creation Rules

Web App that allows MAHs to configure rules for alerts sent by email or displayed in the Manage Alerts app

Manage Verification Settings

Web App that allows:

- MAHs to configure issue and resolution categories for alerts
- Verification requester and responders to enter contact information

Manage Alerts

Web App that allows MAHs to manage alerts by assigning issue and resolution categories and status

Manage Messages

Web App that allows MAHs to view message logs and message

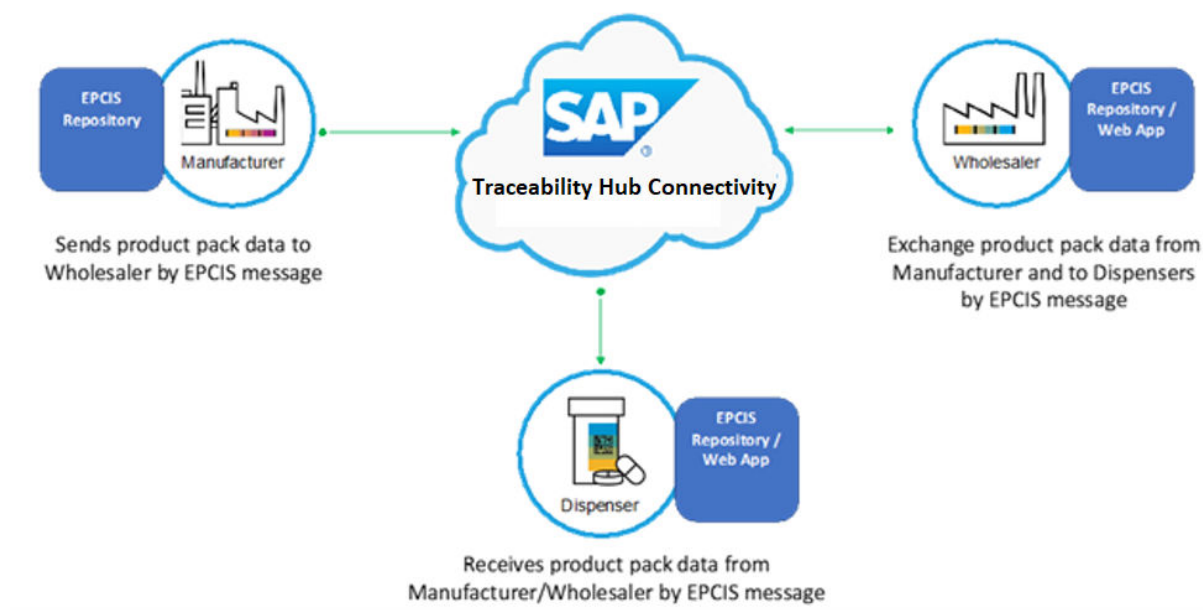
4.5.2.1 Supply Chain Notification -TI/TS Exchange

The service allows MAHs and U.S. Wholesalers to send product pack data to their customers to meet the requirements for exchange of transaction information (TI) and transaction statement (TS) according to DSCSA requirements. Suppliers can exchange TI/TS messages B2B with their customers using GS1 EPCIS 1.2 U.S. Healthcare Implementation Guideline as a standard (EPCIS 1.2 USHC). TI/TS Messages must be sent for every shipment and require full serialization aggregation.

SAP customers can send Lot level information according to HDA EDI Guidelines for 856 Advance Ship Notice to meet lot level requirements of U.S. DSCSA. A partner can receive information through B2B, TPI or web app.

Suppliers who are customers of the SAP Traceability Hub invite their customers to connect to the SAP Traceability Hub. For customers who cannot establish a B2B connection, SAP provides a Web App to receive the EPCIS file and download the original file or download TI/TS as a TI PDF report.

Wholesalers or Dispensers who are customers of the SAP Traceability Hub can invite their suppliers to onboard. For suppliers who cannot establish a B2B connection, SAP provides a Web App to upload and send EPCIS files.



4.5.2.1.1 Onboarding

SAP customers have access to Web Apps to invite their customers to self-onboard.

The SAP Onboarding team onboards suppliers and partners of SAP customers.

4.5.2.1.2 Web Apps

The SAP Launchpad provides access to a number of Web Apps each represented as a tile. Access to these apps is managed by the Web App Administrator in your organization. Contact SAP in case none of the users in your organization is set up as Web App Administrator.

4.5.2.1.2.1 Send Transaction Information

A Web App allows suppliers to send an EPCIS message that contains TI/TS information to customers if B2B connection is not available.

4.5.2.1.2.2 View Transaction Information

A Web app allows SAP Customers and their invited business partners to:

- Review messages sent or received in TI/TS exchange
- Search for a TI/TS message, for example, based on delivery, purchase order, product, batch or product identifier
- Download a TI/TS message as a PDF
- Download original message in XML
- Export all or a selection of messages to MS Excel

4.5.2.1.3 Exception Management

The Exception Management option allows you to process exceptions during exchange of transaction information (TI) between trading partners, including analysis and integration to serialization repositories.

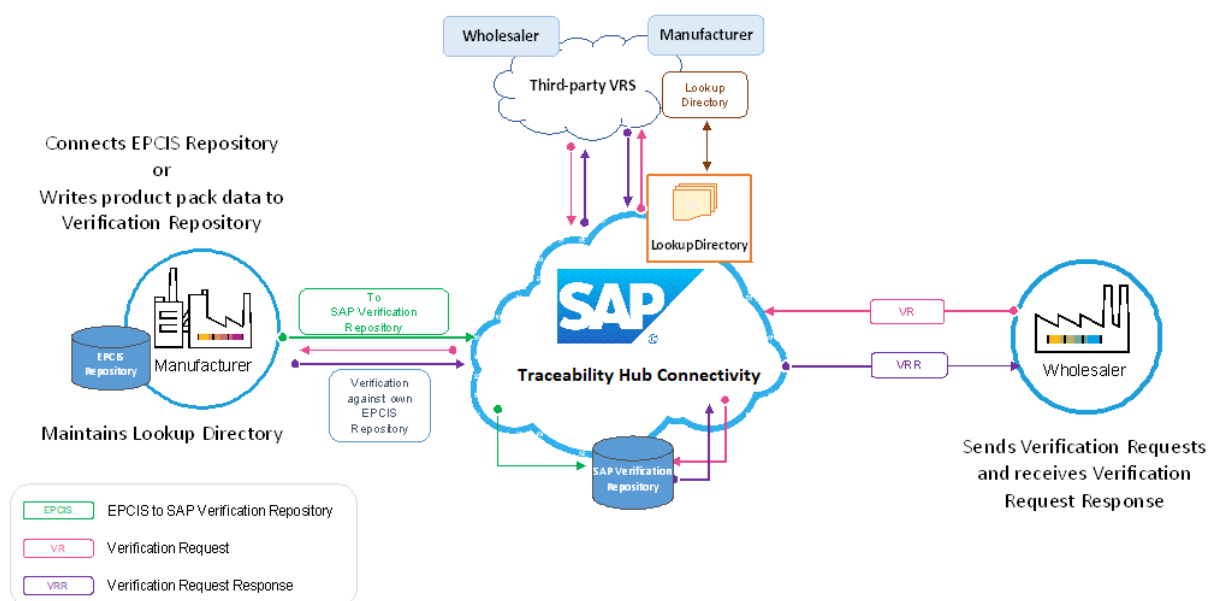
- A Web App allows SAP Customers to:
 - Create and manage exceptions
 - Collaborate internally and externally with business partners by transferring an exception. Onboarded partners access the web app.
 - Add notes and attachments to an exception, and make them visible only within your organization or externally as well

4.5.3 Verification

SAP Traceability Hub supports Verification as required by U.S. DSCSA.

To enable Verification MAHs make data available for verification:

- MAHs can connect their own EPCIS repository to the service or send product pack data to a verification repository using messages that follow the GS1 EPCIS standard.
- MAHs enter information about their products (GTINs) in a Lookup Directory (LD). The LD contains the Connectivity Information (CI) of the MAH's repository. Connectivity information is stored by product ID (GTIN). Connectivity Information stored in a Lookup Directory is automatically exchanged with other Lookup Directories managed by other solution providers. SAP Traceability Hub now uses its own LD.



Wholesalers can send verification requests to the SAP Traceability Hub. The verification request is typically triggered by scanning the Data Matrix code on the product pack that encodes the product identifier (PI) which includes GTIN, lot, expiration date, and serial number.

When a Verification Request is received from a wholesaler, the Lookup Directory in the SAP Traceability Hub determines the endpoint where verification is executed based on the GTIN in the verification request. The service routes the verification request to one of the following:

- SAP verification repository
- SAP customer's EPCIS repository
- Third-party solution

A response is then sent to the wholesaler.

4.5.3.1 Writing Product Pack Data to the Verification Repository

Note

This section is not relevant for MAHs who offer verification against their own EPCIS repository.

MAHs send product pack data to a verification repository by sending an EPCIS message. The message format is similar to that of the U.S. Supply Chain Notification with no aggregation required.

A message can contain multiple batches. An MAH can send data to the verification repository through a B2B connection or by using an SAP Web App. The status of a pack can be set using dispositions. To confirm that data was written to verification repository, an MAH can use the Write Log Web App.

4.5.3.2 Managing the Lookup Directory

The Lookup Directory contains the Connectivity Information (CI) of the responders (MAH) repository to respond to verification requests. CI is stored by product ID (GTIN). The LD is therefore an integral part of any Verification Routing Service (VRS) because it determines the destination for a verification request issued by a requester (wholesaler). The content in the LD is exchanged with other LDs in the ecosystem. Therefore, every LD contains all GTIN information maintained in the ecosystem.

4.5.3.3 Verification

Verification Requests

Requesters send a verification request. The response is sent back to the requester.

To create verification requests, SAP provides a B2B option as well as Web App and mobile access. In all cases, the verification request and response follow the GS1 US Implementation Guideline V1.2 of the GS1 Lightweight Messaging Standard for DSCSA Verification of Returned Product Identifiers .

The Web App is available on any device. On a mobile device, the app allows a user to scan the 2D Matrix Barcode, decode the barcode and send a verification request to SAP. On devices that do not have a camera, a user can enter the GS1 element string or the four data elements separately.

How a verification request is processed depends on the requester role, such as wholesaler, manufacturer, logistics service provider or dispenser. For example, a request sent by a wholesaler is routed through the entire VRS ecosystem to the responder, while manufacturers can only verify their own GTINs against the verification repository with no routing executed.

SAP Customer Role	Usage	Capability	Checks
Wholesaler	B2B	Full routing	Requester GLN
Wholesaler	SAP Web App	Full routing	Requester GLN
MAH	SAP Web App	Verification repository only	MAH GTIN Ownership
3PL on behalf of MAH	B2B	Verification repository only	Requester GLN, MAH GTIN Ownership
Any organization through an MAH Customer Web Site	B2B	Verification repository only	MAH GTIN Ownership

Verification Response

When a verification request reaches the repository, the service checks if the PI is present, then determines the response based on disposition, expiry date and customer-specific response configuration.

SAP provides a Web App to customers to configure responses as defined in V1.1 of the GS1 verification standard.

Verification Credentials

You can choose to use verifiable credentials for each GLN. Credentials are always verified when credentials are included in a request or a response, and the GLN matches the SAP customer's responder GLN or requester GLN.

Verification Request and Response Logs

Every verification request and response is stored for analysis in a verification log. This is required for an MAH (responder) to recognize a verification request occurred and is a prerequisite for investigation of a suspect product. It also provides wholesalers (requesters) with a history of all verifications.

Verification Alerts

The service provides an Alert Configuration app that allows responders (manufacturers, MAHs) to define conditions when alerts are created. Alerts can be sent by email or managed in a web app.

4.5.4 Introduction

The service supports the requirements of the U.S. Drug Supply Chain Security Act (DSCSA) regarding interaction between marketing authorization holders (MAHs) who provide prescription drugs to the U.S. market, U.S. wholesale distributors and U.S. dispensers.

This includes:

- Verification
- Supply Chain Notification from supplier to wholesaler or dispenser, also known as Transaction Information and Transaction Statement Exchange (TI/TS Exchange)
- Trace Request Management
- Exception Management

5 Manage Users - Introduction

As an Administrator, you can:

- Add, edit, and delete users and administrators
- Give users access to apps, and define the rights and actions each user can perform in each app
- Reset password of users

5.1 View Users

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.

The Manage Users screen displays user details, including the following:

- Display Name
 - Email address
 - User Type: Administrator or User
 - Last Login
 - Changed on & Created on details
 - Status: Active or inactive
2. To search the list, enter text in the search field, and press [Enter](#).
 3. To clear the search field, select [X](#).
 4. To sort the list based on Display Name or Changed Date, click the [Sort](#) icon .
 5. To view details of a user, click the user name in the list.

The User Details screen displays the details along with the list of applications that the user has access to.

5.2 View Apps and User Access

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Click [Applications](#) from the Left Navigation Menu .
A list of apps displays, and active users display.
3. To view users of an app, select the app.

5.3 Add User

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Click [Add](#).
3. Select User Type whether Administrator or User .
An Administrator has access to the Manage Users app.
4. Select the applications as required.
5. Click [Add](#).
The user receives an activation email.

5.4 Copy User

Context

To add a new user, you can copy one user and edit the app details as required. The user type and permitted apps are copied.

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Select a user you wish to copy.
The User Details screen displays.
3. Click [Copy](#).
The New User screen displays. The User Type and permitted apps are copied to a new user.
4. Enter First Name, Last Name, Email of new user . You can change User Type, and add or remove app access.
5. Click [Save](#).
The new user is created with input details.

5.5 Edit User

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the Manage Users tile.
2. Select a user.
The User Details screen displays.
3. Click [Edit](#). You can change the First Name, Last Name, Status, User Type and add or remove app access.
4. Click [Save](#). For changes to take effect, the user must log out and log in again.

5.6 Delete User

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Select a user.
The User Details screen displays.
3. Click [Delete](#).
A Confirmation dialog box displays.
4. Click [OK](#) to confirm deletion.

5.7 Approve User Request

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Click [User Request](#) from the Left Navigation Menu.
New User Request for Approval or Rejection will be available.
3. Choose the User Type , to Approve (or) reject the request with a comment.

5.8 Export or Delete Personal Data

To export or delete personal data, contact SAP Support. See also, [Security Policy and Procedures](#).

6 Web Apps Introduction

You access all Web Apps through a browser. Use the Chrome browser for best results.

6.1 Permitted Apps

You access all Web Apps through a browser. You must use Chrome.

When you log in, you see the apps that you are authorized to use.

If you do not see an app for which you need access, contact the SAP Web App Administrator in your company.

6.2 Technical Pre-requisites

The following are required to use the Web App.

- High speed Internet connection > 1 Mbps
- Chrome browser which includes the following enabled:
 - Downloads - for downloading serial numbers in a file
 - base64 decoder
 - Certificate-based authentication
 - SAP trusted certificates - certificates are probably trusted already
 - Pop ups - for selecting items, and uploading commissioned serial numbers
 - Browser redirect
- Hostname provided by SAP allowlisted on your firewall
- Network configured to allow resolution of URLs provided by SAP using public DNS
- Email addresses must be on a corporate domain, and you must manage the validity of email addresses
- Your internal network and firewall are configured to allow outbound SSL calls from your network to the Internet using port 443

Note

If you are unsure about some of these technical details, contact your IT team.

6.3 Test Area

SAP offers a Test Area for users before beginning to use the Productive environment. The Test Area displays message transmission in the Staging environment and can be identified by the URL.

ⓘ Note

Test data is not transferred to the Productive environment.

6.4 Home Page

The Homepage is the main access screen for all apps. A tile shows for each app you can use.

6.4.1 Personalize Homepage

You can personalize the Homepage by selecting the *Personalize Home Page* option in the user profile drop down menu at the top right of the screen. You can create new groups and move tiles between groups.

6.5 Filter Data Displayed

You can use filter features on the overview screen. You can refine your search using the filter bar.

- To view, filtered results, choose *Go*.
- To clear the filter, select *Clear*.
- To hide the filter bar, select *Hide Filter Bar*

6.6 View Change Logs

You can view change logs in all apps for all actions performed by users of your organizations.

- To view change logs, select *Change Log*.
- To search for a particular log, use the search field and press *Enter*.

7 Manage Users - Introduction

As an Administrator, you can:

- Add, edit, and delete users and administrators
- Give users access to apps, and define the rights and actions each user can perform in each app
- Reset password of users

7.1 View Users

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.

The Manage Users screen displays user details, including the following:

- Display Name
 - Email address
 - User Type: Administrator or User
 - Last Login
 - Changed on & Created on details
 - Status: Active or inactive
2. To search the list, enter text in the search field, and press [Enter](#).
 3. To clear the search field, select [X](#).
 4. To sort the list based on Display Name or Changed Date, click the [Sort](#) icon .
 5. To view details of a user, click the user name in the list.

The User Details screen displays the details along with the list of applications that the user has access to.

7.2 View Apps and User Access

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Click [Applications](#) from the Left Navigation Menu .
A list of apps displays, and active users display.
3. To view users of an app, select the app.

7.3 Add User

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Click [Add](#).
3. Select User Type whether Administrator or User .
An Administrator has access to the Manage Users app.
4. Select the applications as required.
5. Click [Add](#).
The user receives an activation email.

7.4 Copy User

Context

To add a new user, you can copy one user and edit the app details as required. The user type and permitted apps are copied.

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Select a user you wish to copy.
The User Details screen displays.
3. Click [Copy](#).
The New User screen displays. The User Type and permitted apps are copied to a new user.
4. Enter First Name, Last Name, Email of new user . You can change User Type, and add or remove app access.
5. Click [Save](#).
The new user is created with input details.

7.5 Edit User

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the Manage Users tile.
2. Select a user.
The User Details screen displays.
3. Click [Edit](#). You can change the First Name, Last Name, Status, User Type and add or remove app access.
4. Click [Save](#). For changes to take effect, the user must log out and log in again.

7.6 Delete User

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Select a user.
The User Details screen displays.
3. Click [Delete](#).
A Confirmation dialog box displays.
4. Click [OK](#) to confirm deletion.

7.7 Approve User Request

Procedure

1. Log on to the SAP Traceability Hub Connectivity, navigate to the [Manage Users](#) tile.
2. Click [User Request](#) from the Left Navigation Menu.
New User Request for Approval or Rejection will be available.
3. Choose the User Type , to Approve (or) reject the request with a comment.

7.8 Export or Delete Personal Data

To export or delete personal data, contact SAP Support. See also, [Security Policy and Procedures](#).

8 Manage Messages - Introduction

Customers of the SAP Traceability Hub invite business partners to exchange messages relating to pharmaceutical products.

The service includes a number of web apps available to customers. Some apps are available to invited partners.

This document describes the Manage Messages app which allows an SAP Customer and Business Partner onboarded B2B or through a Third-Party Integrator to access message processing logs for all messages you send and receive, including:

- View error details
- Download message payload
- Review messages
- Retriggler failed messages
- Upload new messages for certain scenarios

For more information, see the [SAP Traceability Hub Help page](#).

Web App Administrator

Your organization has a nominated SAP Web app administrator who can:

- Give administrator rights to colleagues
- Give users access to apps

If you do not have access to an app, contact your administrator who can use the Manage Users app to give you access.

Assumptions

This guide assumes you are familiar with the pharmaceutical industry and serialization terminology.

Data Protection and Privacy

To have user data removed, contact your SAP team.

9 Manage Company Data - Prerequisites

The Manage Company Data app allows you to add, edit and delete information about your organization, which is required for sending invitations and messages exchange.

Pre-requisites

You must be authorized to use the Manage Company Data app. If you do not have access to the app, contact your organization Web App Administrator.

Administrator can assign the application to other users of the organization with following role-based access:

- Full Access: User can add, edit, delete the company data
- Display Only: User can only view the company data.

9.1 Add Company Data

Context

Learn how to create and maintain company identifiers, such as GLN or CNPJ, that are required for invitation management and message exchange.

Procedure

1. Logon to the SAP Traceability Hub Connectivity portal, navigate to General > Manage Company Data.
2. Select Add.
3. Select Code Type either CNPJ or GLN. CNPJ is a Brazilian tax identifier for legal entities. GLN is a global location identifier used in GS1/EPCIS standards.
4. Enter the 13 digit GLN code in Company Code field.
5. Enter your Company Name.
6. Enable 'Relevant for Verification' if GLN is used in USDSCSA scenario also.
7. Save.

9.2 Edit Company Data

Context

This section explains how to update existing company information, including company name, verification relevance, and status.

Procedure

1. Logon to the SAP Traceability Hub Connectivity portal, navigate to General > Manage Company Data.
2. Select a row or rows.
3. Click Edit. You can change the Company Name, Relevant for Verification, Status whether Active or Inactive.
4. Save.

9.3 Delete Company Data

Context

This section details the steps to remove company records and highlights restrictions that may prevent deletion of records already in use.

Procedure

1. Logon to the SAP Traceability Hub Connectivity portal, navigate to General > Manage Company Data.
2. Select a row or rows.
3. Click Delete.
4. Confirm deletion.

Note

If the company code is used in an invitation, you cannot delete the company code.

9.4 Global Company Prefix

Context

This section explains how to view Global Company Prefix information maintained for your organization and track associated creation details.

Procedure

1. Log on to the SAP Traceability Hub Connectivity and navigate to General > Manage Company Data.
2. Select Global Company Prefix button . You can check all the Global Company Prefixes maintained for your organization and added on dates.

9.5 View Change Log

Context

This section describes how to access audit records and review when changes were made, by whom, and what actions were performed.

Procedure

1. Logon to the SAP Traceability Hub Connectivity portal, navigate to General > Manage Company Data.
2. Click Change Log to view a log of all the events performed in the application in Change Log, performed by whom and when.

10 Manage Company Data - Partners

Customers of the SAP Traceability Hub Connectivity invite business partners to exchange messages relating to pharmaceutical products. The service includes Web Apps that allow each organization to onboard to the service and to exchange messages with other organizations.

Assumptions

This guide assumes you are familiar with the pharmaceutical industry and serialization terminology.

Data Protection and Privacy

To have user data removed, contact your SAP team.

For more information see the Service Description on the [SAP Traceability Hub Connectivity U.S. Drug Supply Chain Security Help page](#).

11 Manage Certificates - Introduction

This document describes the security certificate process for connecting to the SAP Information Collaboration Hub for Life Sciences including a list of approved Certificate Authorities.

This document also describes the features and use of the Manage Certificates app which allows you to upload and download certificates and download certificates and monitor upcoming certificate replacement dates.

Target Audience

This document is for all stakeholders including:

- Security Officers
- Integration engineers
- Implementation engineers and partners

Related Information

- [SAP Traceability Hub Connectivity help pages](#).

12 Certificate based Authentication

Context

In the interest of securing your data, the SAP Traceability Hub Connectivity uses certificate-based authentication. To comply with security best practices, all certificates must be signed by one of the SAP Trusted Certificate Authorities, in .cer or .crt format. Self-signed certificates are not accepted.

📘 Note

Transport Layer Security version must be TLS 1.2.

📘 Note

SAP Traceability Hub Connectivity security certificates are available in the Security section of the [Help page](#).

Procedure

1. To begin, you need to generate a keypair on your system. At this point, the keypair is self-signed, that is, you trust your own certificate!
2. You now raise a Certificate Signing Request. This is a block of text, which contains a thread of:private key some public key materials
3. Next you choose a Certificate Authority if you don't already have one.
4. Then you log onto the Certificate Authority's secure website to upload your Certificate Signing Request.
5. Enter information such as: proof of domain ownership, names, email addresses, physical addresses.
6. The Certificate Authority then investigates to ensure the request is from an authentic source. The investigation may include emails, phone calls, correspondence.
7. After the Certificate Authority confirms the authenticity of the request, the Certificate Authority provides a signed certificate response.
8. You import this into your keystore.
9. At this point, your self-signed key is promoted to a signed keypair, which you can share with SAP and all business partners who will be happy that you are using a trusted certificate.

For more information see

https://sapvideo.cfapps.eu10-004.hana.ondemand.com/?entry_id=1_5yu1np2e

12.1 SAP Certificates

SAP Traceability Connectivity certificates are available in the Security section of the [Help page](#).

13 Trusted Certificate Authorities

This list may contain links to foreign (i.e. non SAP group of companies) sites. SAP is not responsible for the privacy practices or the content of other websites outside the SAP Group of companies. Therefore, we recommend that you carefully read the privacy statements of such foreign sites. Please refer to the SAP Privacy Statement here: <https://www.sap.com/about/legal/privacy.html>

See also [2801396 - SAP Global Trust List - SAP for Me](#)

Certificate Authority	DN	Serial Number	Expiration Date MM-DD-YYYY
Baltimore CyberTrust Root	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	02 00 00 b9	05-13-2025
Entrust Root Certification Authority	CN = Entrust Root Certification Authority OU = (c) 2006 Entrust, Inc. OU = www.entrust.net/ CPS is incorporated by reference O = Entrust, Inc. C = US	45 6b 50 54	11-27-2026
Entrust Root Certification Authority - G2	CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US	4a 53 8c 28	12-07-2030

Entrust.net Certification Authority (2048)	CN=Entrust Root Certification Authority, OU=(c) 2006 Entrust\, Inc., OU= www.entrust.net/CPS is incorporated by reference,O=Entrust\, Inc., C=US	38 63 de f8	07-24-2029
Go Daddy Root Certificate Authority - G2	CN = Go Daddy Root Certificate Authority - G2 O = GoDaddy.com , Inc. L = Scottsdale S = Arizona C = US	00	01-01-2038
DigiCert Global Root CA	CN = DigiCert Global Root CA OU = www.digicert.com O = DigiCert Inc C = US	08 3b e0 56 90 42 46 b1 a1 75 6a c9 59 91 c7 4a	11-10-2031
DigiCert High Assurance EV Root CA	CN=DigiCert High Assurance EV Root CA, OU= www.digicert.com , O=DigiCert Inc, C=US	2A C5 C26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	11-10-2031
COMODO RSA Certification Authority	CN = COMODO RSA Certification Authority O = COMODO CA Limited L = Salford S = Greater Manchester C = GB	4c aa f9 ca db 63 6f e0 1f f7 4e d8 5b 03 86 9d	01-19-2038

USERTrust RSA Certification Authority	CN = USERTrust RSA Certification Authority O = The USERTRUST Network L = Jersey City S = New Jersey C = US	01 fd 6d 30 fc a3 ca 51 a8 1b bc 64 0e 35 03 2d	01-19-2038
QuoVadis Root CA 2 G3	CN = QuoVadis Root CA 2 G3 O = QuoVadis Limited C = BM	44 57 34 24 5b 81 89 9b 35 f2 ce b8 2b 3b 5b a7 26 f0 75 28	01-12-2042
SAP Global Root CA	CN = SAP Global Root CA O = SAP AG L = Walldorf C = DE	5d 03 d9 3d 31 61 5d 8f 48 8b 39 70 c7 8f 1b 99	04-26-2032
Roche G3 Root CA	CN=Roche G3 Root CA, O=F. Hoffmann-La Roche Ltd	1B 10 29 15 BC 10 2B B8 4C E3 16 59 C2 02 CB 93	06-15-2038
GlobalSign Root CA	CN = GlobalSign Root CA OU = Root CA O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 15 4b 5a c3 94	01-28-2028
DigiCert Global Root G2	CN = DigiCert Global Root G2 OU = www.digicert.com  O = DigiCert Inc C = US	03 3a f1 e6 a7 11 a9 a0 bb 28 64 b1 1d 09 fa e5	01-15-2038
SAP Cloud Root CA	CN=SAP Cloud Root CA, O=SAP SE,L=Walldorf, C=DE	18 77 0F BE 65 06 6B BF 4C EA 93 38 D9 B1 85 62	02-13-2039

DigiCert Assured ID Root CA	CN = DigiCert Assured ID Root CA OU = www.digicert.com 📁 O = DigiCert Inc C = US	0ce7e0e517d846fe8fe560fc1bf03039	11-10-2031
Amazon Root CA 1	CN=Amazon Root CA 1 O=Amazon C=US	06 6c 9f cf 99 bf 8c 0a 39 e2 f0 78 8a 43 e6 96 36 5b ca	01-17-2038
Atos TrustedRoot 2011	CN = Atos TrustedRoot 2011 O = Atos C = DE	5c 33 cb 62 2c 5f b3 32	01-01-2031
Certum CA	CN=Certum CA O=Unizeto Sp. z o.o. C=PL	01 00 20	06-11-2027
COMODO Certification Authority	CN=COMODO Certification Authority O=COMODO CA Limited L=Salford SP=Greater Manchester C=GB	20 a4 c4 7f dd df e1 c7 53 63 07 13 88 77 60 12	01-01-2031
COMODO ECC Certification Authority	CN = COMODO ECC Certification Authority O = COMODO CA Limited L = Salford S = Greater Manchester C = GB	1f 47 af aa 62 00 70 50 54 4c 01 9e 9b 63 99 2a	01-19-2038
GlobalSign Root CA - R3	CN=GlobalSign O=GlobalSign OU=GlobalSign Root CA - R3	04 00 00 00 00 01 21 58 53 08 a2	03-18-2029
Go Daddy Class 2 Certification Authority	OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US	00	06-29-2034

GTS Root R1	C = US O = Google Trust Services LLC CN = GTS Root R1	02 03 e5 93 6f 31 b0 13 49 88 6b a2 17	06-22-2036
GTS Root R2	C = US O = Google Trust Services LLC CN = GTS Root R2	02 03 e5 ae c5 8d 04 25 1a ab 11 25 aa	06-22-2036
GTS Root R3	C = US O = Google Trust Services LLC CN = GTS Root R3	02 03 e5 b8 82 eb 20 f8 25 27 6d 3d 66	06-22-2036
GTS Root R4	C = US O = Google Trust Services LLC CN = GTS Root R4	02 03 e5 c0 68 ef 63 1a 9c 72 90 50 52	06-22-2036
ISRG Root X1	CN=ISRG Root X1 O=Internet Security Re- search Group C=US	00 82 10 cf b0 d2 40 e3 59 44 63 e0 bb 63 82 8b 00	06-04-2035
QuoVadis Root CA 2	CN=QuoVadis Root CA 2 O=QuoVadis Limited C=BM	05 09	11-24-2031
Starfield Class 2 Certification Authority	OU=Starfield Class 2 Certifi- cation Authority O=Starfield Technologies, Inc. C=US	00	06-29-2034

Starfield Services Root Certificate Authority - G2	CN=Starfield Services Root Certificate Authority - G2 O=Starfield Technologies, Inc. L=Scottsdale S=Arizona C=US	00	01-01-2038
SwissSign Gold CA - G2	CN=SwissSign Gold CA - G2 O=SwissSign AG C=CH	00 bb 40 1c 43 f5 5e 4f b0	10-25-2036
SwissSign Platinum CA - G2	CN=SwissSign Platinum CA - G2 O=SwissSign AG C=CH	4e b2 00 67 0c 03 5d 4f	10-25-2036
SwissSign Silver CA - G2	CN=SwissSign Silver CA - G2 O=SwissSign AG C=CH	4f 1b d4 2f 54 bb 2f 4b	10-25-2036
T-TeleSec GlobalRoot Class 2	CN=T-TeleSec GlobalRoot Class 2 OU=T-Systems Trust Center O=T-Systems Enterprise Services GmbH C= DE	01	10-02-2033
Autoridade Certificadora Raiz Brasileira v10	CN=Autoridade Certificadora Raiz Brasileira v10 OU=Instituto Nacional de Tecnologia da Informacao – ITI O=ICP-Brasil C=BR	d2 d5 8b 44 bf 81 93 42	07-01-2032

Autoridade Certificadora Raiz Brasileira v11	CN=Autoridade Certificadora Raiz Brasileira v11 OU=Instituto Nacional de Tecnologia da Informacao – ITI O=ICP-Brasil C=BR	24 2b 60 d4 cd 43 69 7f	07-01-2032
Autoridade Certificadora Raiz Brasileira v2	CN=Autoridade Certificadora Raiz Brasileira v2 OU=Instituto Nacional de Tecnologia da Informacao – ITI O=ICP-Brasil C=BR	01	06-22-2023
Autoridade Certificadora Raiz Brasileira v5	CN=Autoridade Certificadora Raiz Brasileira v5 OU=Instituto Nacional de Tecnologia da Informacao – ITI O=ICP-Brasil C=BR	01	03-03-2029
AAA Certificate Services	CN=AAA Certificate Services O=Comodo CA Limited L=Salford ST=Greater Manchester C=GB	01	01-01-2029
GeoTrust Primary Certifica- tion Authority - G2	CN=GeoTrust Primary Certif- ication Authority - G2 OU=(c) 2007 GeoTrust Inc. - For authorized use only O=GeoTrust Inc. C=US	3c b2 f4 48 0a 00 e2 fe eb 24 3b 5e 60 3e c3 6b	01-19-2038

SAP Internet of Things CA	CN=SAP Internet of Things CA	00	07-18-2040
	O=SAP IoT Trust Community II		
	C=DE		

14 Manage Certificates App

The Manage Certificates app allows you to:

- Upload and activate a certificate to replace an expiring certificate
- View the number of days before a certificate expires
- View and download your TLS and MLS certificates
- Delete unused certificates
- View changes made by different users
- Download SAP certificates

You must be authorized to use the Manage Certificates app. If you do not have access to the app, contact your company Web App Administrator.

The app sends email notifications when a certificate is due to expire.

14.1 View your company Certificates

Context

This feature enables users to access and review company certificates, helping ensure secure and uninterrupted communication with SAP systems.

Procedure

1. Log on to the Traceability Hub Connectivity portal and navigate to General > Manage Certificates tile.
2. The Manage Certificates screen displays your TLS and MLS certificate details, including: Certificate Status: Active, Inactive or Expired Environment: Dev, QA, Staging Number of days before certificate expires with expiry Date <https://me.sap.com/notes/>  The Environment refers to your backend system's environment connected to SAP.
3. To search the list, enter text in the search field, and press Enter.
4. To clear the search field, select X.
5. To Sort the list based on Certificate Name, Status, Alias Name, Expiry Date or Last Modified, select Sort.
6. To view details of a certificate, select the certificate. The Certificate Details screen displays.

14.2 Download your company certificates

Context

The process starts at the Homepage. It allows users to securely download their organization's TLS and MLS certificates for backup, validation, or configuration purposes, ensuring continued secure communication with SAP systems.

Procedure

1. Log on to the Traceability Hub Connectivity portal and navigate to General > Manage Certificates.
2. Click the Download Certificate icon for the certificate you want to download.

14.3 Replace Expiring Certificate

Context

The process starts at the Homepage. It enables users to upload and activate a new certificate before the existing one expires, ensuring uninterrupted secure communication and compliance with SAP's certificate requirements

Procedure

1. Log on to the Traceability Hub Connectivity portal and navigate to General > Manage Certificates.
2. Upload your Client certificate in .cer or .crt format. This is used for authentication when you send messages to SAP. Self-signed certificates are not accepted. The certificate must be from an SAP Certificate Authority.<https://me.sap.com/notes/>  The Web App allows you to upload a maximum of five certificates, with only one active.
3. To activate the certificate, select the certificate and click Activate. The status of the certificate changes to Active and In Use for sending messages to SAP.

14.4 Delete Unused Certificate

Context

The process starts at the Homepage. It allows users to remove inactive or obsolete certificates that are no longer required, helping maintain an organized and secure certificate repository.

Procedure

1. Log on to the Traceability Hub Connectivity portal and navigate to General > Manage Certificates.
2. Select a certificate. The certificate details screen displays.
3. Select an unused certificate.
4. Click Delete. Note: You cannot delete a certificate that is in use.

14.5 Download SAP Certificates

Context

The process starts at the Homepage. It allows users to download SAP certificates required for establishing secure and trusted connectivity with SAP systems.

Procedure

1. Log on to the Traceability Hub Connectivity portal and navigate to General > Manage Certificates.
2. Select Download SAP Certificates. This downloads SAP's TLS and MLS certificates for sending to SAP and receiving from SAP in a Zip file.
3. Import these certificates into your backend system.

14.6 Notification of Expiring Certificates

Context

Customers receive email alerts for TLS and MLS certificates due to expire within 30 days. An email is sent to all administrators and users of the Manage Certificates app.

The email is sent 30 days, 15 days, 7 days, 6 days, 5 days, 4 days, 3 days, 2 days and 1 day before expiry of a certificate.

Procedure

To add and remove administrators, use the Manage Users app.

Caution: Customers are responsible for monitoring, managing and updating valid certificates. Failure to do so can result in disruption of message exchange.

15 Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines/strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: <http://help.sap.com/disclaimer>)

2026 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
 - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
 - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.

