

SCM STAR Zugriff gesicherte Anmeldung

[Lieferantenportal](#)

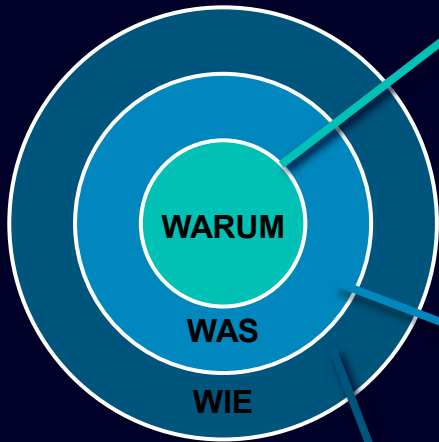
Lieferantenstammdatenverwaltung (SMDM)

Inhalt

- | | |
|--|-----------------|
| 1. Einführung | Seite 2 |
| 2. Wie wähle ich die Authentifizierungsmethode aus? | Seite 4 |
| 3. Wie kann ich meine Anmeldedaten/ Authentifizierungsmethode zurücksetzen? | Seite 19 |
| 4. Weiteres Kommunikationsmaterial | Seite 28 |

Lieferanten-Zugangsberechtigung

Hintergrund, Zielsetzung, Vorgehensweise



Anforderungen an die Informationssicherheit zum Schutz vor Cyberangriffen durch externe Benutzer machen einen sicheren Anmeldemechanismus erforderlich.

Supplier Entitlement ist ein Zugangssystem für Lieferanten, um über eine einzigartige 2-Faktor-Authentifizierung Zugriff auf Siemens-Anwendungen zu erhalten:

- Faktor 1: Berechtigungs-E-Mail-Adresse + Passwort
- Faktor 2: Ein zusätzlicher Faktor, der dem jeweiligen Benutzer zur Verfügung gestellt wird

Basierend auf der ausgewählten zweiten Authentifizierungsmethode erhalten Lieferanten

- Option 1: eine Push-Benachrichtigung auf dem Mobiltelefon (Guardian-App)
- Option 2: Ein Einmalpasswort (OTP) per Textnachricht (SMS) auf dem Mobiltelefon
- Option 3: Einen Code, der nach dem Scannen des QR-Codes über die Authentifizierungs-App generiert wird

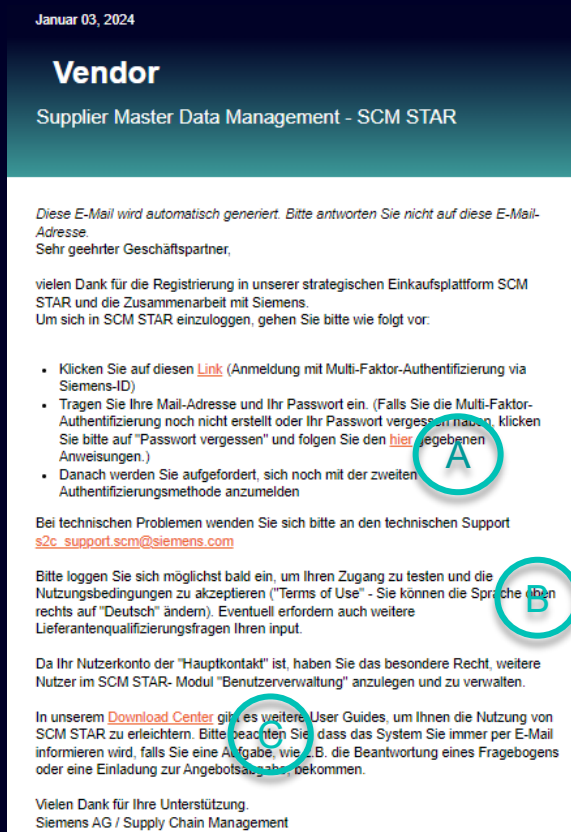
Nach erfolgreicher Bestätigung wird der Anwendungszugriff gewährt.

Lieferantenstammdatenverwaltung (SMDM)

Inhalt

- | | |
|---|----------|
| 1. Einführung | Seite 2 |
| 2. Wie wähle ich die Authentifizierungsmethode aus? | Seite 4 |
| 3. Wie kann ich meine Anmeldedaten/ Authentifizierungsmethode zurücksetzen? | Seite 19 |
| 4. Weiteres Kommunikationsmaterial | Seite 28 |

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung



Bitte klicken Sie [hier](#), um den Antrag zu vervollständigen.

Loggen Sie sich zum ersten Mal ein?

Wie Sie sich in wenigen Schritten einloggen können, erfahren Sie in diesem [Video](#) oder in dieser [Benutzeranleitung](#). Sie müssen ein gesichertes Single-Sign-On-Konto erstellt haben, um diesen Antrag abzuschließen. Dies ist ein einmaliger Vorgang zum Erstellen einer geschützten Benutzerverbindung im Siemens Authentifizierungsservice. Wenn Sie noch kein aktives Benutzerkonto haben, werden Sie auf die Siemens Authentifizierungsseiten weitergeleitet. Nachdem Sie Ihr Benutzerkonto aktiviert haben, werden Sie zu dem Lieferantenstammdatenantrag weitergeleitet.

Fragen?

- Email: s2c_support.scm@siemens.com
- Internetseiten für Lieferanten (beinhaltet User Guides im Download Center): <http://www.siemens.com/supplierportal>

Sie erhalten eine Benachrichtigungs-E-Mail von star.scm@siemens.com mit einem Aktivierungslink – bitte klicken Sie auf Link (A), um zum Aktivierungsprozess der Multi-Faktor-Authentifizierung weitergeleitet zu werden. Als unterstützendes Material können Sie eine Videoanleitung oder ein Benutzerhandbuch (B) verwenden. Bei Fragen wenden Sie sich bitte an das Support-Team, E-Mail-Kontakt: s2c_support.scm@siemens.com. Dokumente können im Supplier Portal über das Download Center (C) eingesehen werden.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

Januar 03, 2024

Vendor

Supplier Master Data Management - SCM STAR

Diese E-Mail wird automatisch generiert. Bitte antworten Sie nicht auf diese E-Mail-Adresse.

Sehr geehrter Geschäftspartner,

vielen Dank für die Registrierung in unserer strategischen Einkaufsplattform SCM STAR und die Zusammenarbeit mit Siemens.

Um sich in SCM STAR einzuloggen, gehen Sie bitte wie folgt vor:

- Klicken Sie auf diesen [Link](#) (Anmeldung mit Multi-Faktor-Authentifizierung via Siemens-ID)
- Tragen Sie Ihre Mail-Adresse und Ihr Passwort ein. (Falls Sie die Multi-Faktor-Authentifizierung noch nicht erstellt oder Ihr Passwort vergessen haben, klicken Sie bitte auf "Passwort vergessen" und folgen Sie den [hier](#) gegebenen Anweisungen.)
- Danach werden Sie aufgefordert, sich noch mit der zweiten Authentifizierungsmethode anzumelden

At least 12 characters in length

Contain at least 3 of the following 4 types of characters:

Lower case letters (a-z)

Upper case letters (A-Z)

Numbers (i.e. 0-9)

Special characters (e.g. !@#%&*)

No more than 2 identical characters in a row (e.g., "aaa" not allowed)

Enter a new password for
training1612de@yahoo.com

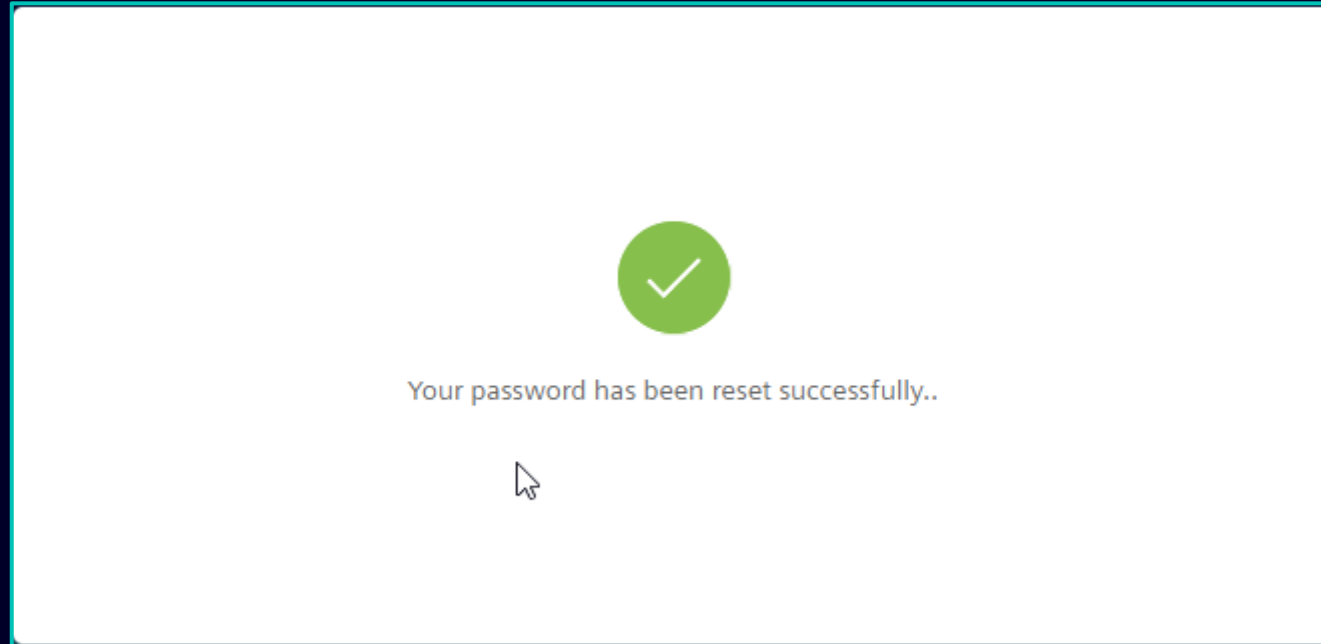
your new password

confirm your new password

Reset Password

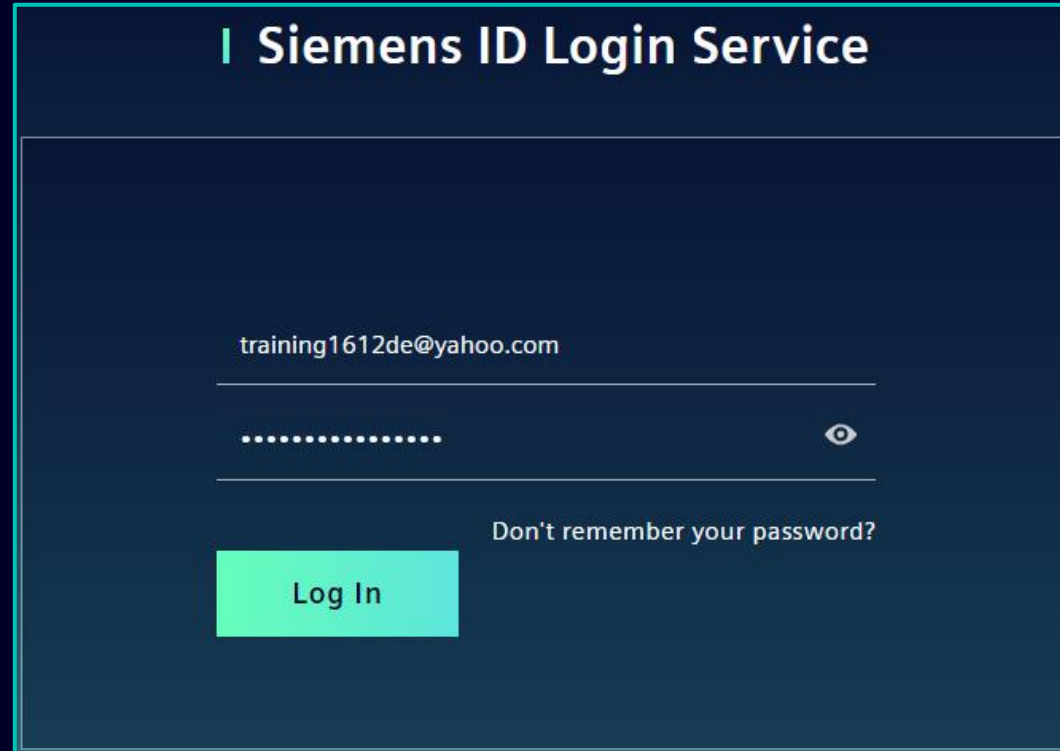
Nachdem Sie auf den Initiierung Link geklickt haben, werden Sie zur Siemens-Login-Webseite weitergeleitet. Richten Sie zunächst ein sicheres Passwort ein, das auf den Passwortrichtlinien basiert. Sobald Sie Ihr Passwort eingegeben haben, klicken Sie auf „Reset Password“.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung



Nach dem Zurücksetzen Ihres Passworts wird eine Bestätigungsmeldung angezeigt und Sie werden zur Anmeldung mit Ihrem neu festgelegten Passwort weitergeleitet.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

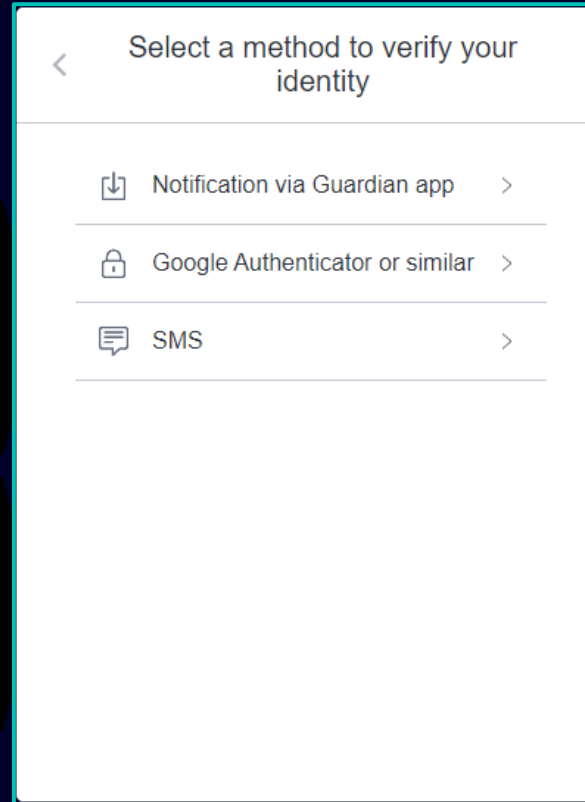
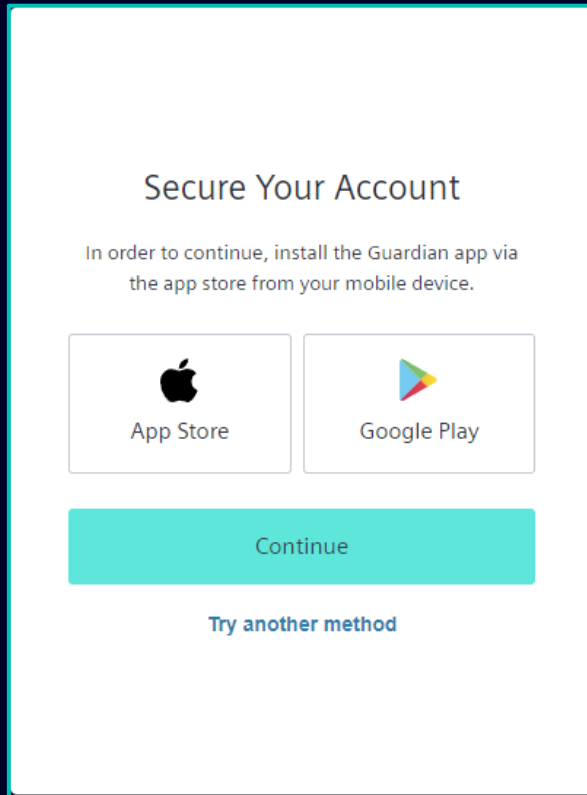


The screenshot displays the Siemens ID Login Service interface. At the top, the title 'Siemens ID Login Service' is shown. Below it, there is a login form with two input fields: the first contains the email address 'training1612de@yahoo.com', and the second contains a masked password represented by dots. To the right of the password field is an eye icon for toggling visibility. Below the password field is a blue button labeled 'Log In'. To the right of the 'Log In' button is a link that says 'Don't remember your password?'.

Falls Sie Ihr neues Passwort vergessen haben, klicken Sie bitte auf „Don't remember your password?“ und [hier](#) weitermachen.

Erste Aktivierung der Multi-Faktor-Authentifizierung

Wählen Sie Ihre bevorzugte zweite Authentifizierungsmethode



Wählen Sie eine der folgenden Apps:

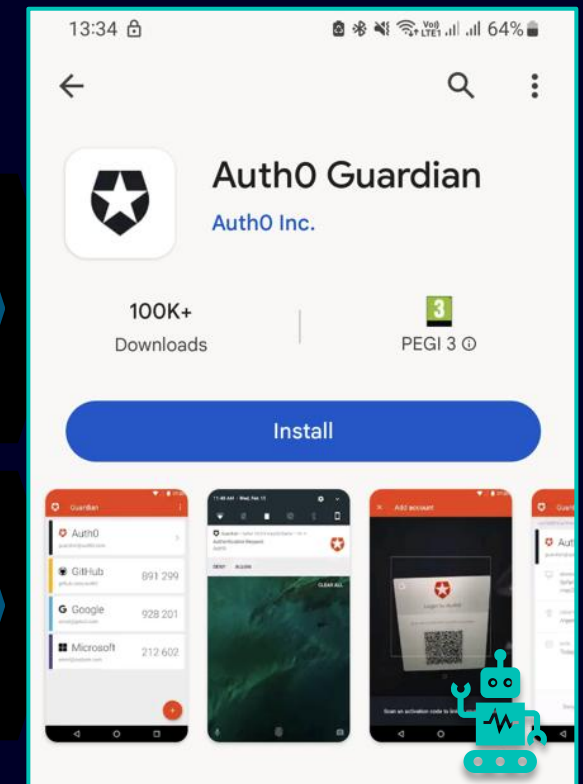
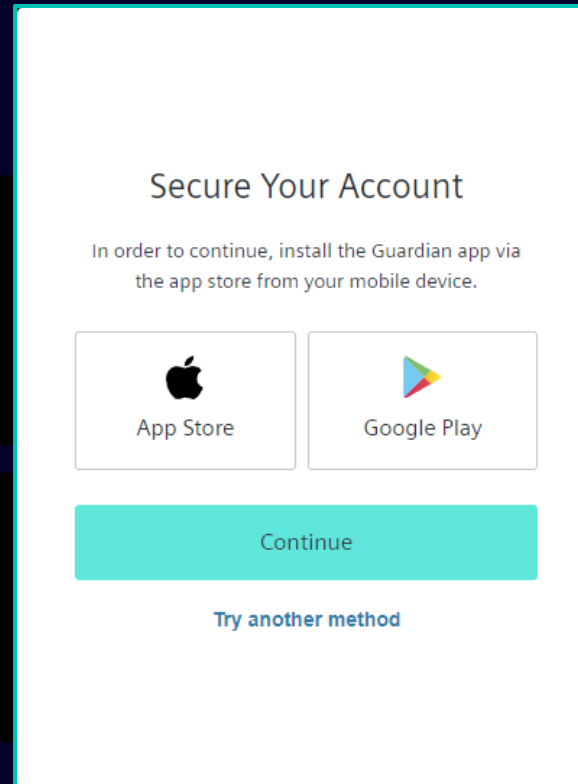
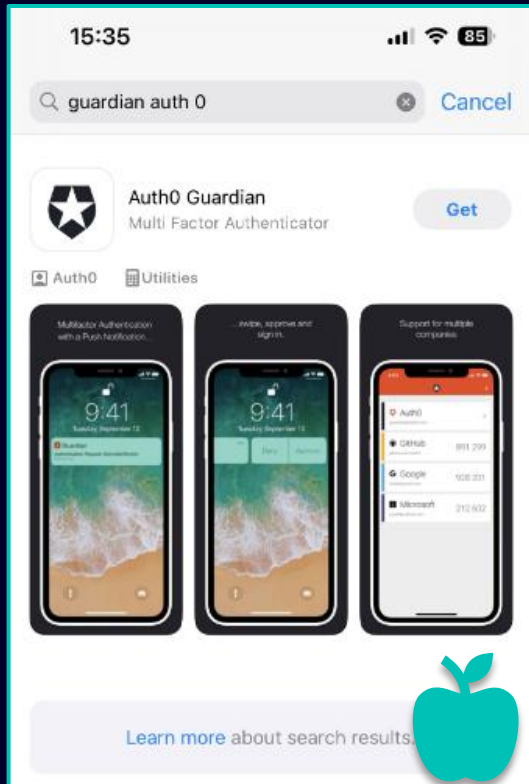
[Guardian app for Android and Apple IOS](#)

[Google Authenticator or similar app](#)

[Google Authenticator or similar app](#)

Nachdem Sie Ihr Passwort festgelegt haben, werden Sie weitergeleitet, um die zweite Authentifizierungsmethode auszuwählen. Sie können zwischen der Guardian-App, dem Google Authenticator oder einer ähnlichen App und der Authentifizierung der Mobiltelefonnummer wählen. Bitte wählen Sie Ihre bevorzugte zweite Authentifizierungsmethode aus und verwenden die Links für [Guardian app for Android and Apple IOS](#), [Google Authenticator or similar app](#), [mobile phone number authentication](#).

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung Guardian-App für Android und Apple IOS

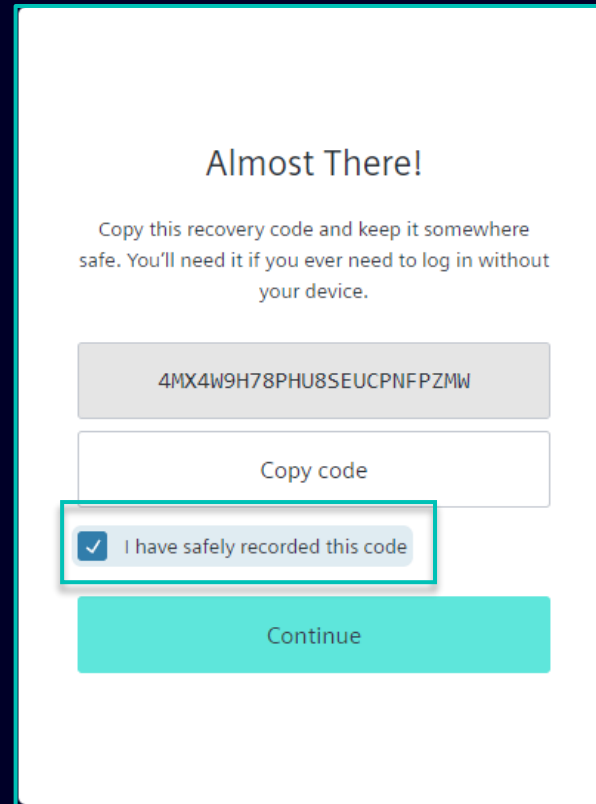


Wenn Sie Ihr Android- oder Apple IOS-Gerät für die zweite Authentifizierungsmethode verwenden möchten, sollten Sie die **Guardian-App** auswählen. Sie können den direkten Link verwenden, indem Sie auf das Google Play-Symbol oder das App Store-Symbol klicken. Suchen Sie auf Ihrem Mobiltelefon/Tablet nach der App „Auth0 Guardian“. Fahren Sie nach erfolgreicher Installation der App mit dem nächsten Schritt fort.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung Guardian-App für Android und Apple IOS



Erstmalige Aktivierung der Multi-Faktor-Authentifizierung Guardian-App für Android und Apple IOS



Almost There!

Copy this recovery code and keep it somewhere safe. You'll need it if you ever need to log in without your device.

4MX4W9H78PHU8SEUCPNFPZMW

Copy code

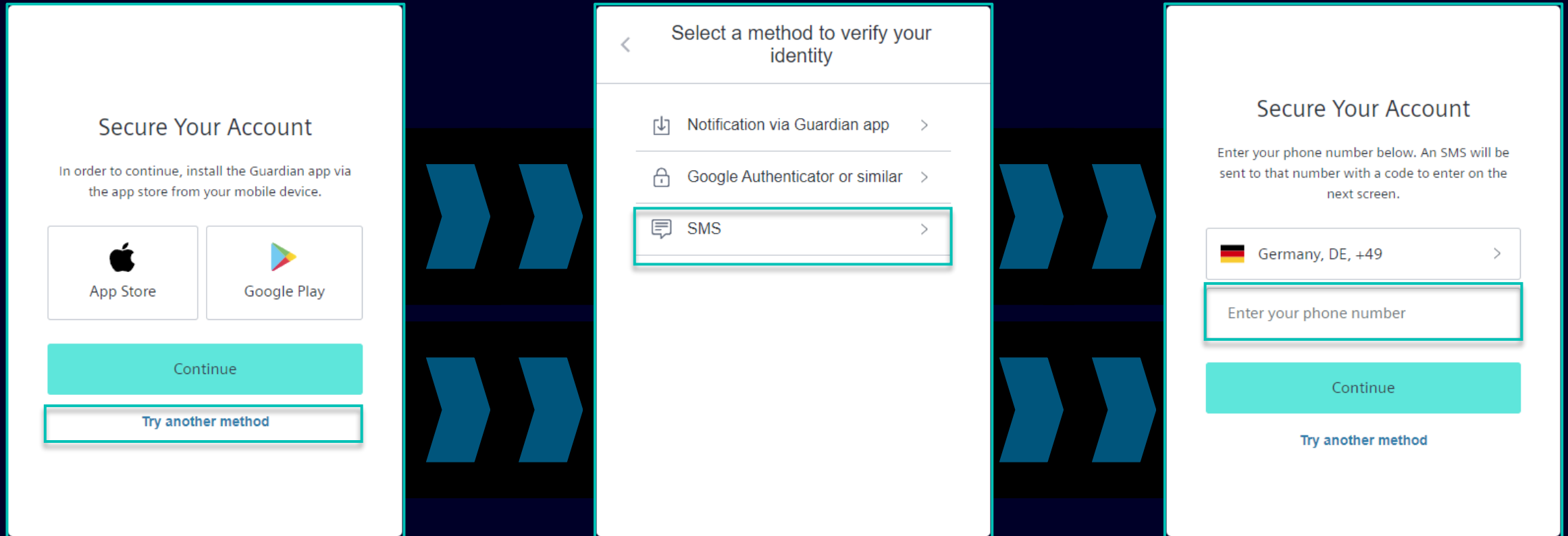
☒ I have safely recorded this code

Continue

Nachdem Sie den Wiederherstellungscode gespeichert haben, bestätigen Sie bitte die Speicherung und wählen Sie „Continue“. Nachdem Sie auf „Continue“ geklickt haben, werden Sie zum GMDM PEGA-Tool weitergeleitet. Bei allen zukünftigen Anmeldungen wird nach Eingabe Ihrer E-Mail-Adresse und Ihres Passworts (wie [hier](#) im Beispiel) die Guardian-App automatisch als standardmäßige zweite Authentifizierungsmethode festgelegt.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

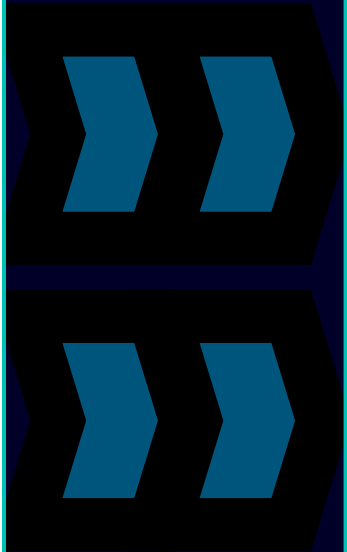
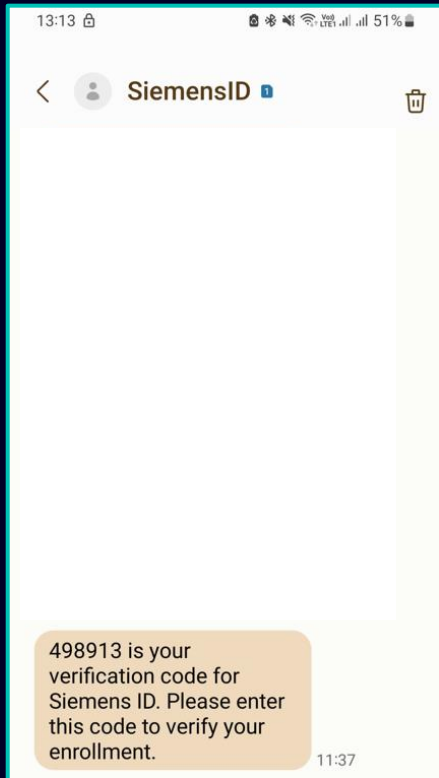
Authentifizierung der Mobiltelefonnummer



Für die Authentifizierung der Mobiltelefonnummer (SMS-Code) wählen Sie bitte „Try another method “ und dann „SMS“. Wählen Sie die Vorwahl Ihres Landes und geben Sie Ihre Mobilfunknummer (ohne „0“ am Anfang) ein.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

Authentifizierung der Mobiltelefonnummer



Verify Your Identity

We've sent a text message to:

+49 X X X X X [Edit](#)

Enter the 6-digit code

826281

[Continue](#)

Didn't receive a code? [Resend](#)

[Try another method](#)



Almost There!

Copy this recovery code and keep it somewhere safe. You'll need it if you ever need to log in without your device.

4MX4W9H78PHU8SEUCPNFPZMW

[Copy code](#)

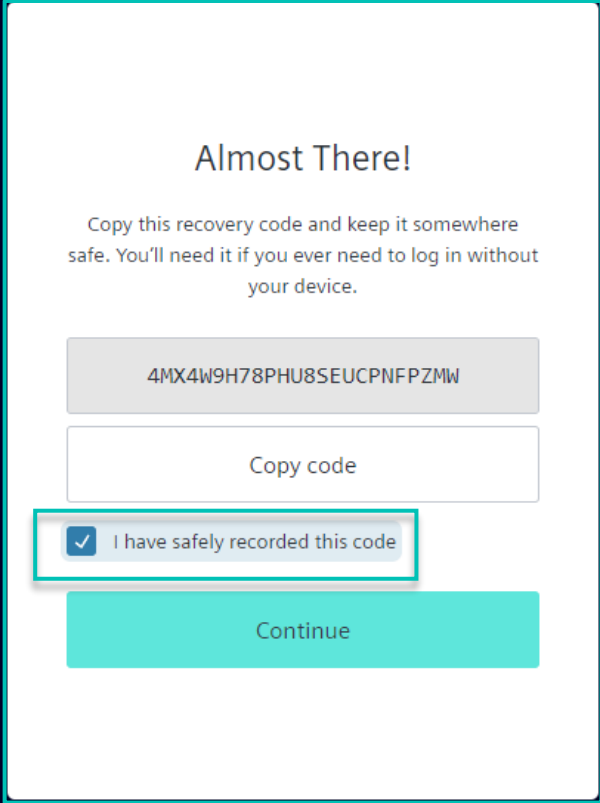
☐ I have safely recorded this code

[Continue](#)

Nach Eingabe Ihrer Mobilfunknummer erhalten Sie eine SMS mit einem 6-stelligen Code. Klicken Sie nach Eingabe des erhaltenen Codes auf „Continue“. Falls Sie den Code nicht erhalten haben, klicken Sie bitte auf „Erneut senden“. Nach erfolgreicher Validierung des 6-stelligen Codes werden Sie aufgefordert, den Wiederherstellungscode zu speichern.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

Authentifizierung der Mobiltelefonnummer



Almost There!

Copy this recovery code and keep it somewhere safe. You'll need it if you ever need to log in without your device.

4MX4W9H78PHU8SEUCPNFPZMW

Copy code

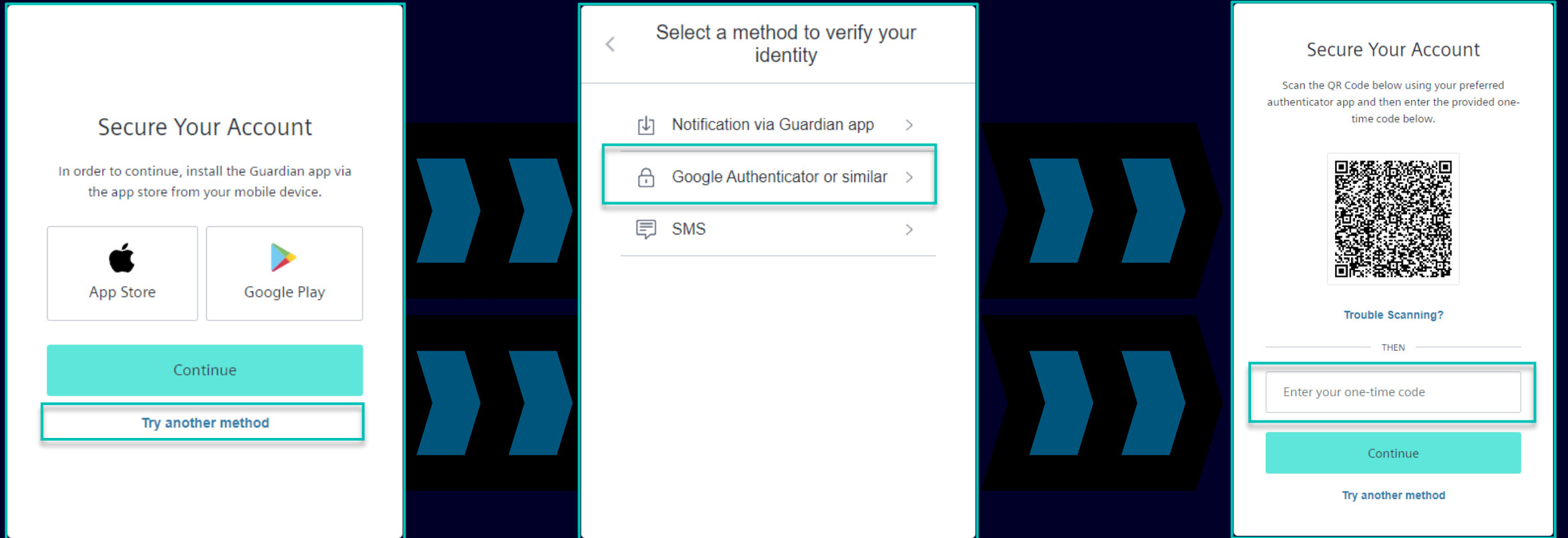
☒ I have safely recorded this code

Continue

Nachdem Sie den Wiederherstellungscode gespeichert haben, bestätigen Sie bitte die Speicherung und wählen Sie „Continue“. Nachdem Sie auf „Continue“ geklickt haben, werden Sie zum GMDM PEGA-Tool weitergeleitet. Bei allen zukünftigen Anmeldungen wird nach Eingabe Ihrer E-Mail-Adresse und Ihres Passworts (wie [hier](#) im Beispiel) die SMS-Authentifizierung automatisch als standardmäßige zweite Authentifizierungsmethode festgelegt.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

Google Authenticator oder ähnliches



Google Authenticator oder ähnliches kann verwendet werden, wenn der Benutzer bereits den Google Authenticator oder eine ähnliche Authentifizierungs-App auf seinem Gerät installiert hat. Nach Nutzung dieser Option wird ein QR-Code gescannt, um den Einmalcode zu erstellen.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

SCM STAR view – first time login

 Adobe PDF file

Terms of Use of the SCM STAR Portal for SIEMENS Suppliers (Status: April 2022)

1. Scope

1. Siemens Aktiengesellschaft operates through a third-party provider, who is bound to confidentiality, the internet-based SIEMENS SCM STAR Portal (hereinafter "the Portal"). With the Portal, SIEMENS provides a platform on which suppliers of Siemens Aktiengesellschaft, subsidiaries of Siemens Aktiengesellschaft according to §§ 15 et seq. German Stock Corporation Act (hereinafter "SIEMENS") and ordering entities administer supplier and contract information and electronic procurement processes ("Purpose"). These Terms of Use regulate use of the Portal by Suppliers.
2. By registering in the Portal, the Supplier agrees to be bound by these Terms of Use. In case of conflicts between separate agreements in writing between the Supplier and SIEMENS and these Terms of Use, the separate agreements shall prevail.
3. SIEMENS reserves the right to modify the services offered via the Portal or to discontinue the offering of the services at any time.

Registration and password

1. Access to and use of the Portal is restricted to invited and registered Suppliers.

I have read and agree to the Terms of Use of the SIEMENS SCM STAR Portal for SIEMENS Suppliers

☒ I agree

☐ I do not agree

[Next](#)

Wenn Sie zum ersten Mal sich ins SCM STAR anmelden, müssen Sie die Nutzungsbedingungen akzeptieren

Die volle Version der Nutzungsbedingungen ist in dem Download Center in Supplier Portal hinterlegt

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung

SCM STAR Ansicht – Emailadresse ist in mehreren Konten vorhanden

 Your SSO ID is associated to more than one Username. The Usernames are listed below. Select which user you want to use

USERNAME LIST

	ORGANISATION	NAME	EMAIL	REGULAR LOGIN - EXPIRING SOON: USERNAME	CITY	COUNTRY	ACCOUNT ID	IFA NUMBER	
1	Testing_Account_MFA_December	Vostradovská Lenka	mfa-testing-14@seznam.cz	mdv-102811_siemenspreprod_scm	Praha 20	CZECH REPUBLIC	376258	1991377358	
2	testovacka	Vostradov Lenulina	mfa-testing-14@seznam.cz	mdv-102812_siemenspreprod_scm	1234567	DEUTSCHLAND	368761	0112406560	

Wenn die Lieferanten-Emailadresse mit mehreren Konten in SCM STAR verbunden ist, werden alle Konten auf einmal angezeigt, nachdem sich der Lieferant mit der Multi-Faktor-Authentifizierung anmeldet. Der Lieferant kann entscheiden, zu welchem Konto er sich anmelden möchte.

Lieferantenstammdatenverwaltung (SMDM)

Inhalt

- | | |
|---|----------|
| 1. Einführung | Seite 2 |
| 2. Wie wähle ich die Authentifizierungsmethode aus? | Seite 4 |
| 3. Wie kann ich meine Anmeldedaten/ Authentifizierungsmethode zurücksetzen? | Seite 19 |
| 4. Weiteres Kommunikationsmaterial | Seite 28 |

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung – Passwort vergessen

Siemens ID Login Service



Please enter your email address. We will send you an email to reset your password.

training1612de@yahoo.com

Send email



Siemens ID Login Service

WE'VE JUST SENT YOU AN EMAIL TO RESET YOUR PASSWORD.

training1612de@yahoo.com

your password

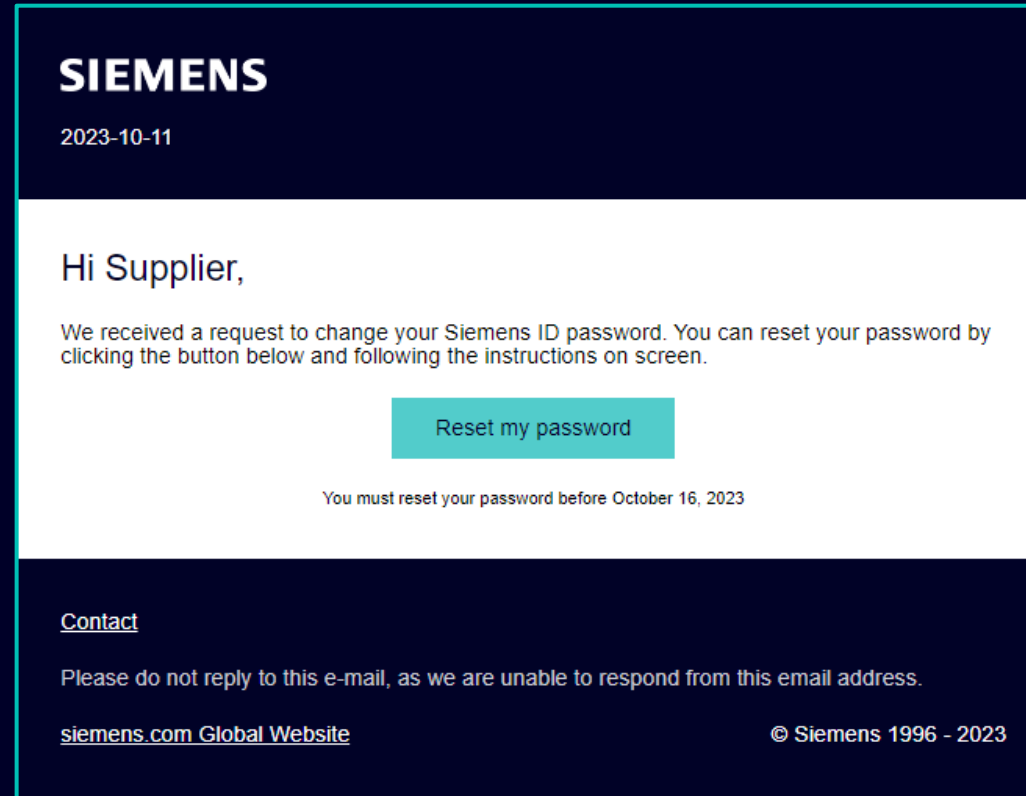


Don't remember your password?

Log In

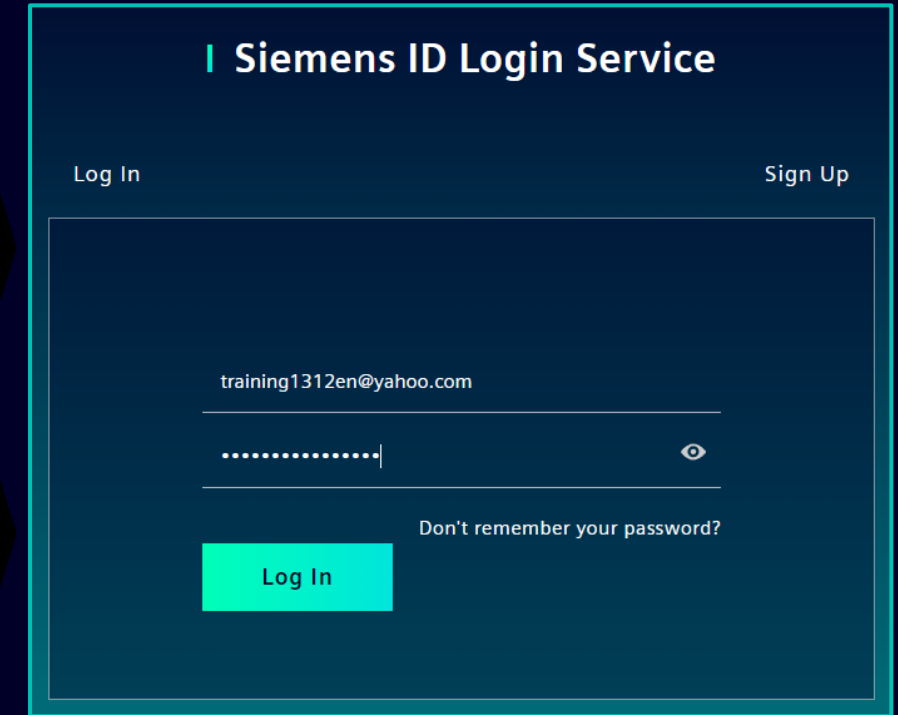
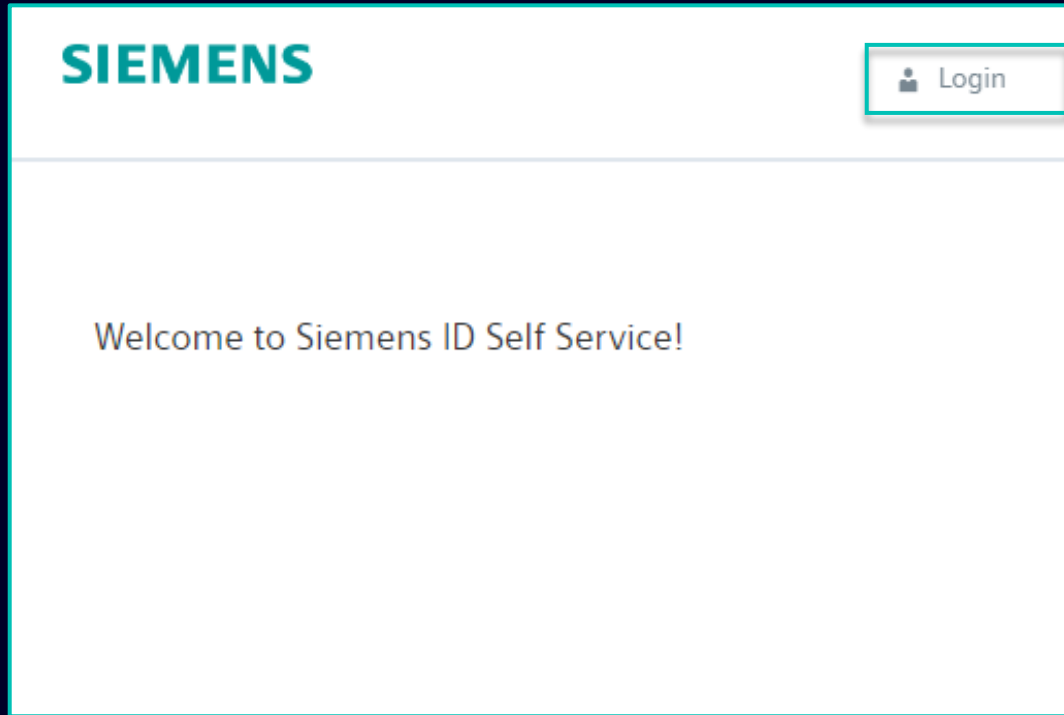
Geben Sie Ihre E-Mail-Adresse ein (dieselbe E-Mail-Adresse wie auf der Seite 6 angezeigt) und klicken Sie auf „Send Email“. Sie erhalten eine E-Mail, um Ihr Passwort erneut zurückzusetzen.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung – Passwort vergessen



Öffnen Sie die E-Mail und klicken Sie auf „Reset my password“. Sie werden zur ersten Siemens-Anmeldeseite weitergeleitet, wo Sie Ihr neu festgelegtes Passwort zurücksetzen können. Dann fahren Sie [hier](#) fort.

So setzen Sie die Authentifizierungsmethode zurück



Bitte gehen Sie auf <https://sp.login.siemens.com/> und klicken auf „Login“; Geben Sie auf der nächsten Seite Ihre E-Mail-Adresse und Ihr Passwort ein und klicken Sie auf „Login“.

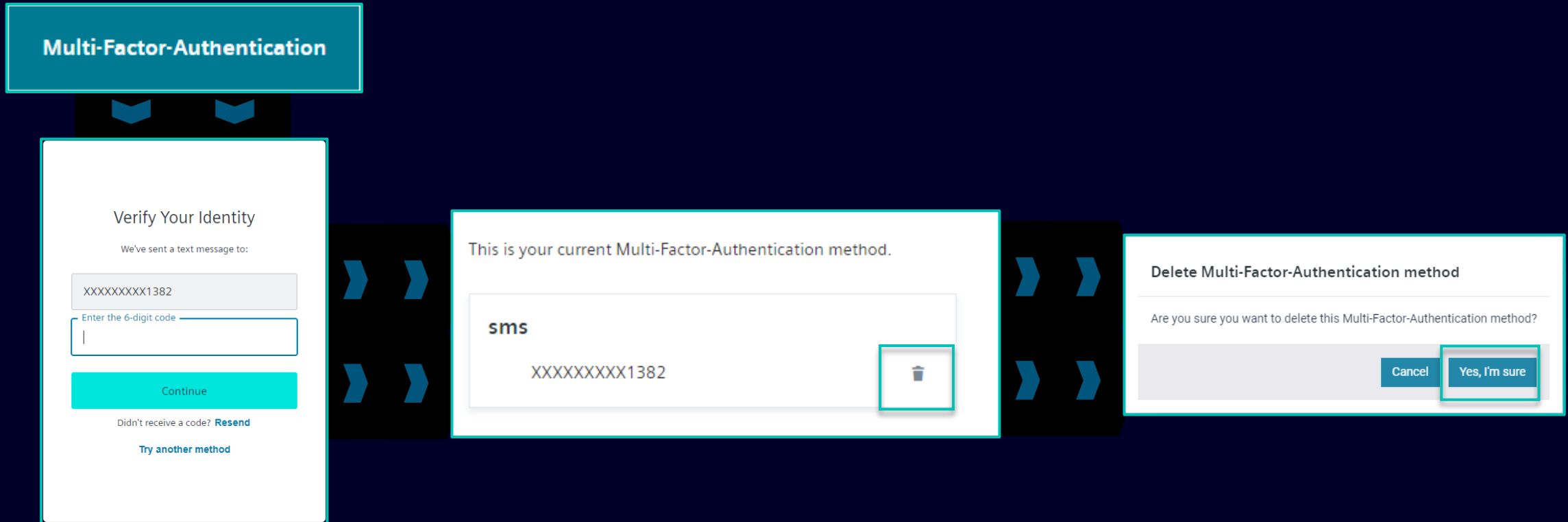
So setzen Sie die Authentifizierungsmethode zurück

Änderung der Kontoinformationen

Change Name Firstname Lastname Save	Change Email Please enter your new email address below. We will send you a verification email to the new address. You will be unable to log in to the application until you verify the new address. Email Address training1312en@yahoo.com Submit Request	Change Password After submitting, you will receive an email with a link to change your password. Request Email
Das Ändern Ihres Vor- und Nachnamens hat keinen Einfluss auf die Authentifizierungslogik.	Wenn Sie Ihre E-Mail-Adresse ändern, wird der Anwendungszugriff deaktiviert, bis die neue E-Mail-Adresse bestätigt wird. Anschließend kann die neue E-Mail-Adresse für die bestehende Authentifizierungsmethode verwendet werden.	Das Zurücksetzen Ihres Passworts hat keine Auswirkungen auf die zweite Authentifizierungsmethode. Nach dem Zurücksetzen des Passworts wird das aktuelle zweite Authentifizierungssetup voreingestellt.
Nach Angabe der zweiten Authentifizierungsmethode werden Sie zu den oben genannten Profileinstellungen weitergeleitet.		

So setzen Sie die Authentifizierungsmethode zurück

Änderung der Multi-Faktor-Authentifizierungsmethode



Um Ihre Multi-Faktor-Authentifizierungsmethode zurückzusetzen, klicken Sie auf „Multi-Factor-Authentication“ – Sie werden weitergeleitet, um die aktuell eingestellte Authentifizierungsmethode anzugeben. Wählen Sie nach der Anmeldung das Löschsymbol aus und bestätigen Sie das Zurücksetzen. Falls Sie versuchen, die zweite Authentifizierungsmethode zurückzusetzen, weil die zweite Authentifizierungsmethode für Sie nicht verfügbar ist (z. B. Telefon verloren, Zugriff auf die Guardian-App oder andere zweite Authentifizierungs-Apps verloren), klicken Sie [hier](#) für die Anleitung.

So setzen Sie die Authentifizierungsmethode zurück

Änderung der Multi-Faktor-Authentifizierungsmethode

Here you can add a new Multi-Factor-Authentication method.

Add authentication method

An email with a link to specify your new Multi-Factor-Authentication method has been sent to training1312en@yahoo.com.

SIEMENS



Here you can add a new Multi-Factor-Authentication method.

Logout

Add authentication method

SIEMENS

2023-10-12

Protect Your Siemens Account

Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. This prevents anyone but you from accessing your account, even if they know your password.

This process will help you set up your account with this added layer of security.

Start setup

Contact

Please do not reply to this e-mail, as we are unable to respond from this email address.

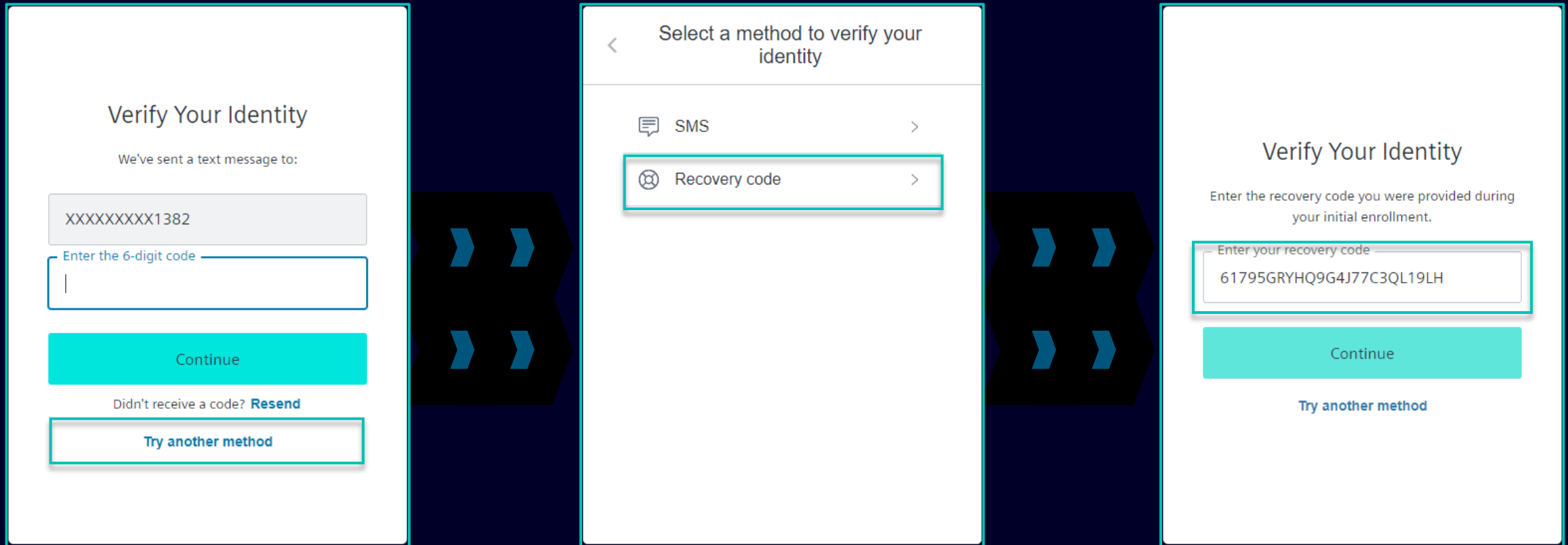
[siemens.com Global Website](https://www.siemens.com)

© Siemens 1996 - 2023

Nachdem Sie die aktuelle Authentifizierungsmethode gelöscht haben, müssen Sie eine neue Multi-Faktor-Authentifizierungsmethode festlegen. Klicken Sie auf „Add authentication method“ und Sie erhalten eine E-Mail. **Es ist wichtig, dass Sie sich von Ihrem Konto abmelden, bevor Sie mit der Einrichtung einer neuen zweiten Authentifizierungsmethode fortfahren.** Gehen Sie dann zu Ihrem E-Mail-Posteingang, klicken Sie auf „Start setup“ und fahren Sie wie [hier](#) fort.

So setzen Sie die Authentifizierungsmethode zurück

Anmeldung über Wiederherstellungscodes



Wenn Sie die zweite Authentifizierungsmethode ändern müssen oder die zweite Authentifizierung derzeit nicht bereitstellen können, können Sie sich mit dem Wiederherstellungscodes anmelden, den Sie bei Ihrer ersten Anmeldung erhalten haben. In diesem Fall, wenn Sie nach der zweiten Authentifizierung gefragt werden, wählen Sie „Andere Methode ausprobieren“ und wählen Sie die Option „Recovery code“. Kopieren Sie Ihren Wiederherstellungscodes und klicken auf „Continue“.

So setzen Sie die Authentifizierungsmethode zurück

Anmeldung über Wiederherstellungscodes

Almost There!

Copy this recovery code and keep it somewhere safe. You'll need it if you ever need to log in without your device.

57CYYZC7H9AFVM24DV628ULD

Copy code

☒ I have safely recorded this code

Continue

Sie erhalten einen neuen Wiederherstellungscodes. Bitte stellen Sie sicher, dass Sie den neuen Wiederherstellungscodes durch den Alten ersetzen. Der alte Wiederherstellungscodes wird deaktiviert, nachdem Sie einen neuen Code erhalten haben. Nachdem Sie Ihren neuen Wiederherstellungscodes gespeichert haben, klicken Sie auf „Continue“.

Lieferantenstammdatenverwaltung (SMDM)

Inhalt

- | | |
|---|----------|
| 1. Einführung | Seite 2 |
| 2. Wie wähle ich die Authentifizierungsmethode aus? | Seite 4 |
| 3. Wie kann ich meine Anmeldedaten/ Authentifizierungsmethode zurücksetzen? | Seite 19 |
| 4. Weiteres Kommunikationsmaterial | Seite 28 |

Further communication material and wrap-up

Multimedia touch points

1 Supplier Portal



- Informationen zu SCM STAR im Allgemeinen
- Neuigkeiten und Informationen, um Sie auf dem Laufenden zu halten
- Zugriff auf Schulungsmaterial ([Download Center](#))

2 First level support

User Help Desk

The User Help Desk is available from Monday to Friday, 07.00 a.m. – 08.00 p.m. CET. Supported Languages: English and German.

GBS Portal: [Open a ticket here](#)

Call-back service for suppliers: +49 (89) 780 52 7450

- Eröffnen Sie ein Ticket per E-Mail – klicken Sie [hier](#)

Vielen Dank

