SCM STAR Zugriff gesicherte Anmeldung

<u>Lieferantenportal</u>

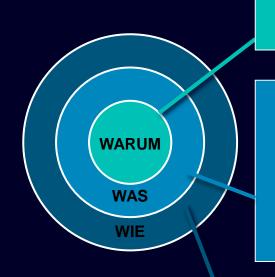


Lieferantenstammdatenverwaltung (SMDM) Inhalt

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



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 <u>Link</u> (Anmeldung mit Multi-Faktor-Authentifizierung via Siemens-ID)
- Tragen Sie Ihre Mail-Adresse und Ihr Passwort ein. (Falls Sie die Multi-Faktor-Aufhentifizierung noch nicht erstellt oder Ihr Passwort vergessen naben, klicken Sie bitte auf "Passwort vergessen" und folgen Sie den hier / gegebenen Anweisungen.)
- Danach werden Sie aufgefordert, sich noch mit der zweiter Authentifizierungsmethode anzumelden

Bei technischen Problemen wenden Sie sich bitte an den technischen Support s2c support.scm@siemens.com

Bitte loggen Sie sich möglichst bald ein, um Ihren Zugang zu testen und die Nutzungsbedingungen zu akzeptieren ("Terms of Use" - Sie können die Spr. che Genechts auf "Deutsch" ändern). Eventuell erfordern auch weitere Lieferantenqualifizierungsfragen Ihren input.

Da Ihr Nutzerkonto der "Hauptkontakt" ist, haben Sie das besondere Recht, weitere Nutzer im SCM STAR- Modul "Benutzerverwaltung" anzulegen und zu verwalten.

In unserem <u>Download Center</u> girl es weitere User Guides, um Ihnen die Nutzung von SCM STAR zu erleichtem. Bitte beachten Sie dass das System Sie immer per E-Mail informieren wird, falls Sie eine Aufgabe, wie B. die Beantwortung eines Fragebogens oder eine Einladung zur Angebotsaus ber oekommen.

Vielen Dank für Ihre Unterstützung. Siemens AG / Supply Chain Management



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 <u>Video</u> oder in dieser <u>Benutzeranleitung</u>. 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.



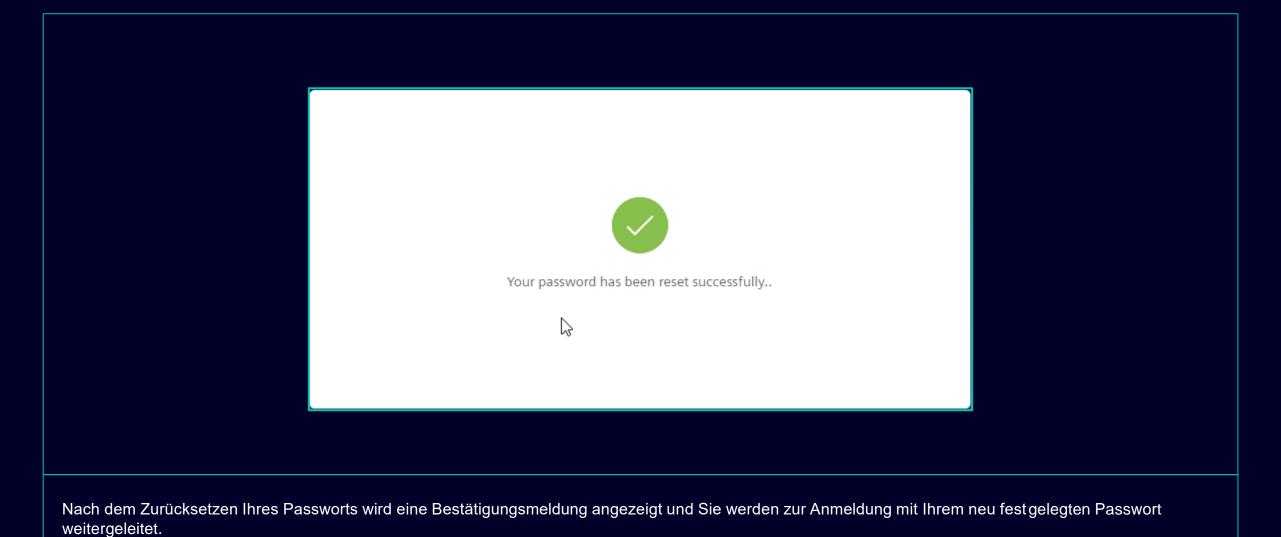
Fragen?

- 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.

Januar 03, 2024 At least 12 characters in length Vendor Upper case letters (A-Z) Numbers (i.e. 0-9) Supplier Master Data Management - SCM STAR Special characters (e.g. I@#\$%^&*) No more than 2 identical characters in a row (e.g., "aaa" not allowed) Enter a new password for Diese E-Mail wird automatisch generiert. Bitte antworten Sie nicht auf diese E-Mail-Adresse. training1612de@yahoo.com Sehr geehrter Geschäftspartner, vielen Dank für die Registrierung in unserer strategischen Einkaufsplattform SCM your new password STAR und die Zusammenarbeit mit Siemens. Um sich in SCM STAR einzuloggen, gehen Sie bitte wie folgt vor: confirm your new password Klicken Sie auf diesen Link (Ahmeldung 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 Reset Password Sie bitte auf "Passwort vergessen" und folgen Sie den hier gegebenen Anweisungen.) Danach werden Sie aufgefordert, sich noch mit der zweiten Authentifizierungsmethode anzumelden

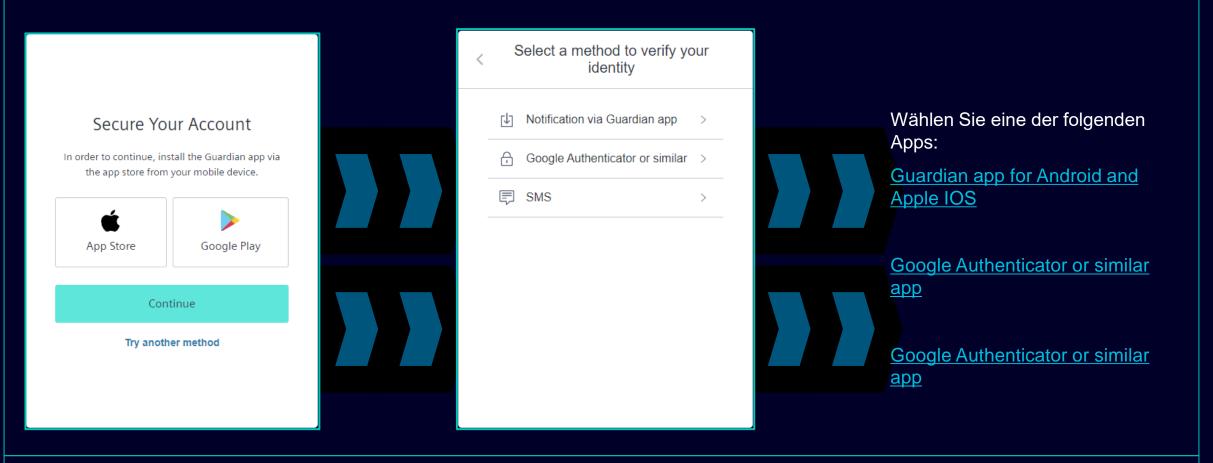
Nachdem Sie auf den Initiierung Link geklickt haben, werden Sie zur Siemens-Login-Webseite weitergeleitet. Richten Sie zunächst ein sicheres Passwort ein, das auf den Passwortrichtlinien basiert. Sobald Sie Ihr Passwort eingegeben haben, klicken Sie auf "Reset Password".





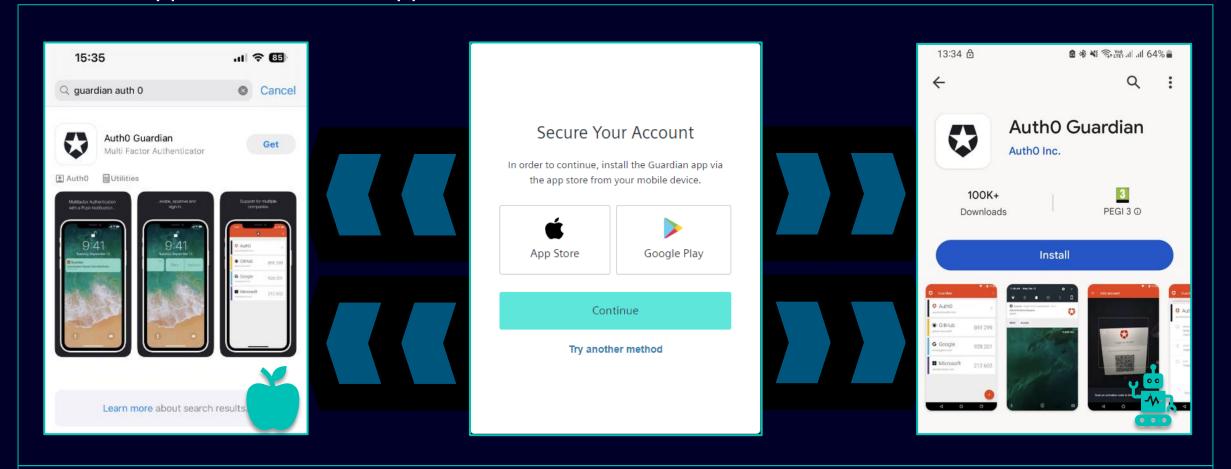
Falls Sie Ihr neues Passwort vergessen haben, klicken Sie bitte auf "Don't remember your password?" und hier weitermachen.

Erste Aktivierung der Multi-Faktor-Authentifizierung Wählen Sie Ihre bevorzugte zweite Authentifizierungsmethode



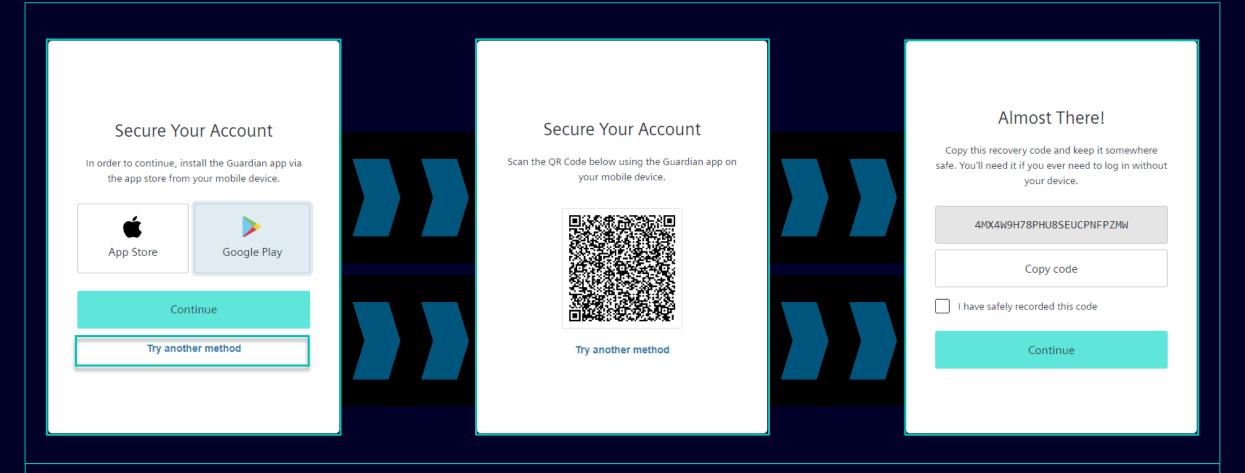
Nachdem Sie Ihr Passwort festgelegt haben, werden Sie weitergeleitet, um die zweite Authentifizierungsmethode auszuwählen. Sie können zwischen der Guardian-App, dem Google Authenticator oder einer ähnlichen App und der Authentifizierung der Mobiltelefonnummer wählen. Bitte wählen Sie Ihre bevorzugte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

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



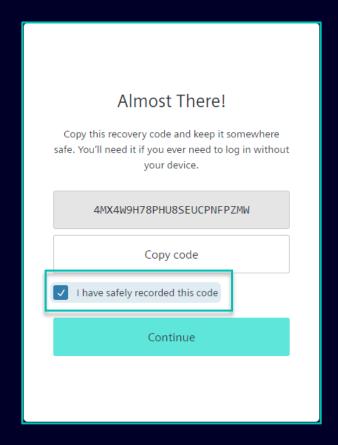
Wenn Sie Ihr Android- oder Apple IOS-Gerät für die zweite Authentifizierungsmethode verwenden möchten, sollten Sie die **Guardian-App** auswählen. Sie können den direkten Link verwenden, indem Sie auf das Google Play-Symbol oder das App Store-Symbol klicken. Suchen Sie auf Ihrem Mobiltelefon/Tablet nach 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



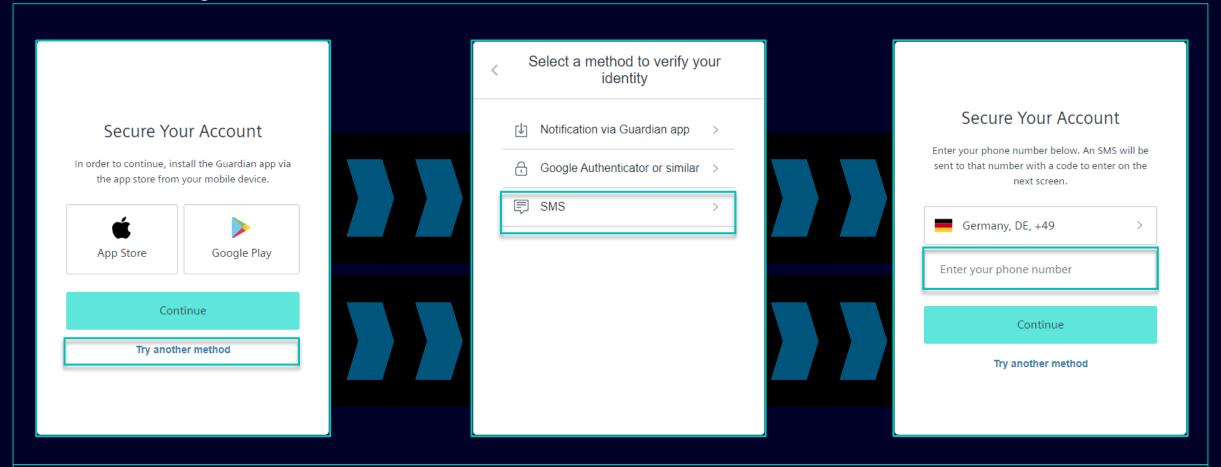
Sobald die Guardian-App erfolgreich auf Ihrem Andorid-Gerät installiert wurde, wählen Sie "Continue". Es wird ein eindeutiger QR-Code generiert. Öffnen Sie die Guardian-App auf Ihrem Mobiltelefon/Tablet und scannen Sie den QR-Code. Sobald der QR-Code gescannt wurde, werden Sie aufgefordert, diesen-entweder zu bestätigen oder einen sicheren Satz in der Guardian-App zu erstellen. Im Siemens Login werden Sie aufgefordert, den Wiederherstellungscode zu hinterlegen.

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



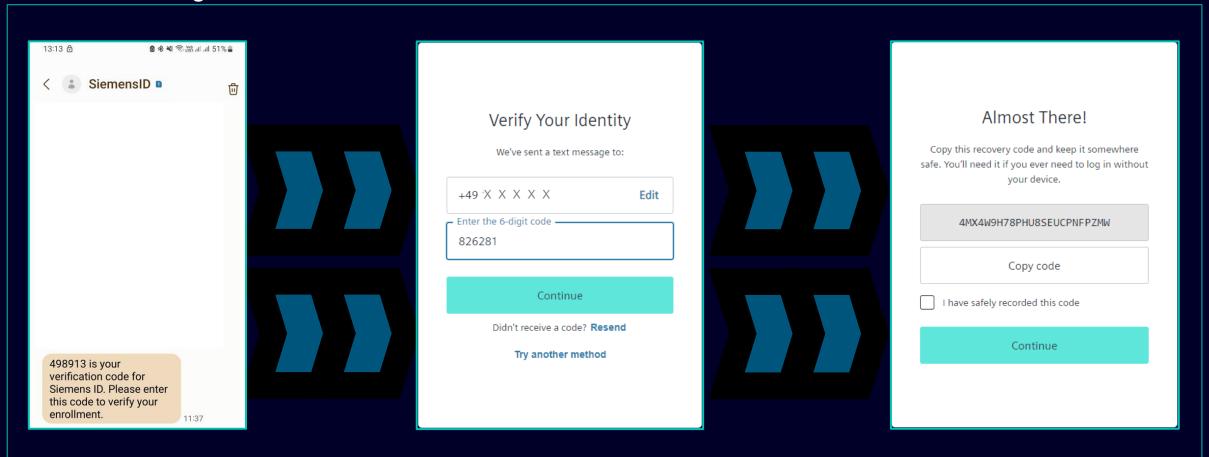
Nachdem Sie den Wiederherstellungscode gespeichert haben, bestätigen Sie bitte die Speicherung und wählen Sie "Continue". Nachdem Sie auf "Continue" geklickt haben, werden Sie zum GMDM PEGA-Tool weitergeleitet. Bei allen zukünftigen Anmeldungen wird nach Eingabe Ihrer E-Mail-Adresse und Ihres Passworts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

Authentifizierung der Mobiltelefonnummer



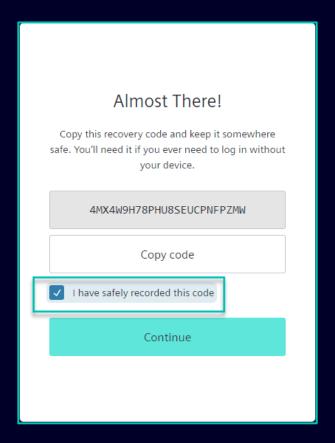
Für die Authentifizierung der Mobiltelefonnummer (SMS-Code) wählen Sie bitte "Try another method" und dann "SMS". Wählen Sie die Vorwahl Ihres Landes und geben Sie Ihre Mobilfunknummer (ohne "0" am Anfang) ein.

Authentifizierung der Mobiltelefonnummer



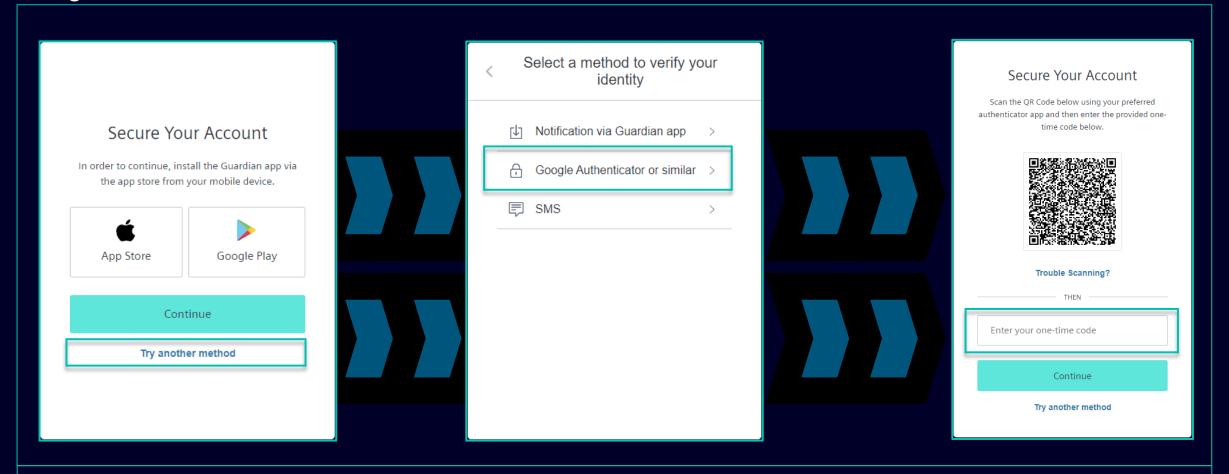
Nach Eingabe Ihrer Mobilfunknummer erhalten Sie eine SMS mit einem 6-stelligen Code. Klicken Sie nach Eingabe des erhaltenen Codes auf "Continue". Falls Sie den Code nicht erhalten haben, klicken Sie bitte auf "Erneut senden". Nach erfolgreicher Validierung des 6-stelligen Codes werden Sie aufgefordert,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

Authentifizierung der Mobiltelefonnummer



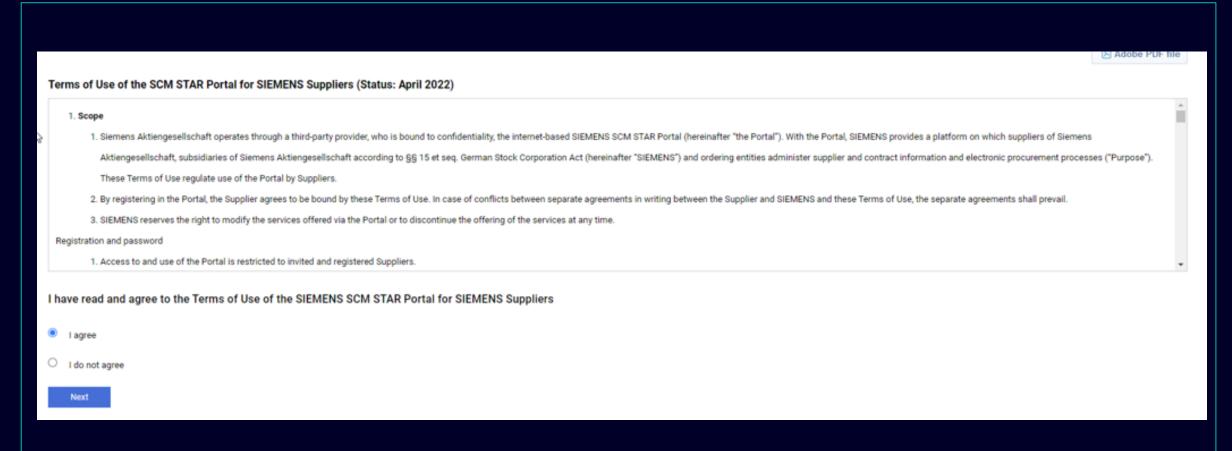
Nachdem Sie den Wiederherstellungscode gespeichert haben, bestätigen Sie bitte die Speicherung und wählen Sie "Continue". Nachdem Sie auf "Continue" geklickt haben, werden Sie zum GMDM PEGA-Tool weitergeleitet. Bei allen zukünftigen Anmeldungen wird nach Eingabe Ihrer E-Mail-Adresse und Ihres Passworts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

Google Authenticator oder ähnliches



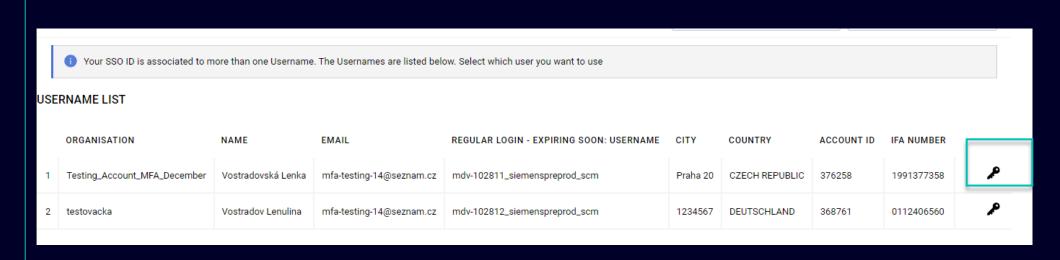
Google Authenticator oder ähnliches kann verwendet werden, wenn der Benutzer bereits den Google Authenticator oder eine ähnliche Authentifizierungs-App auf seinem Gerät installiert hat. Nach Nutzung dieser Option wird ein QR-Code gescannt, um den Einmalcode zu erstellen.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung SCM STAR view – first time login



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 – Emailaddresse ist in mehreren Konten vorhanden



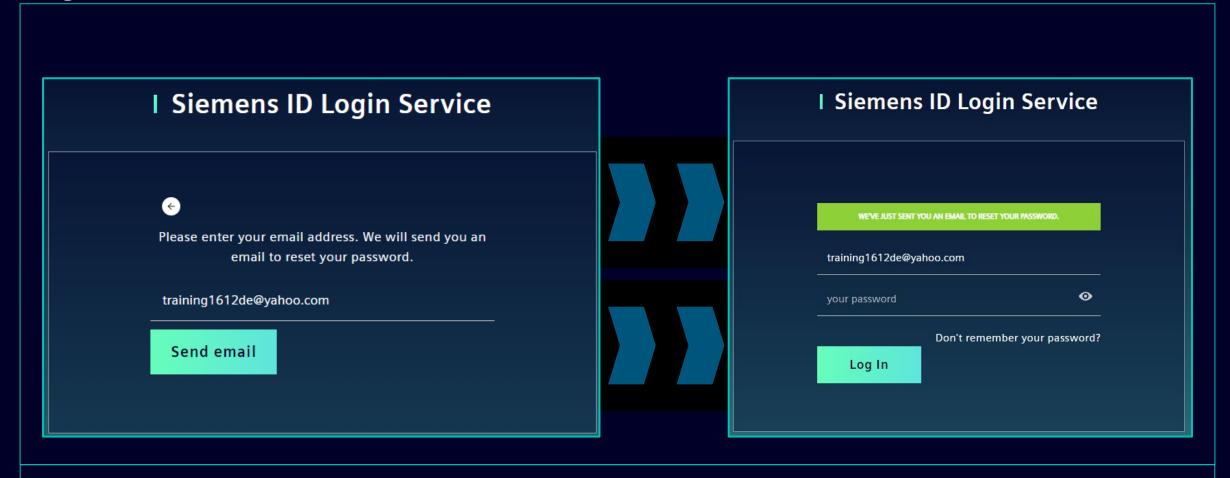
Wenn die Lieferanten-Emailadresse mit mehreren Konten in SCM STAR verbunden ist, werden alle Konten auf einmal angezeigt, nachdem sich der Lieferant mit der Multi-Factor-Authentifizierung anmeldet. Der Lieferant kann entscheiden, zu welchem Konto er sich anmelden möchte.

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

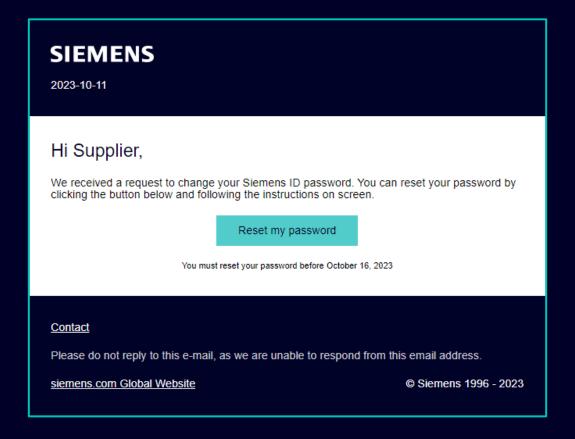


Erstmalige Aktivierung der Multi-Faktor-Authentifizierung – Passwort vergessen

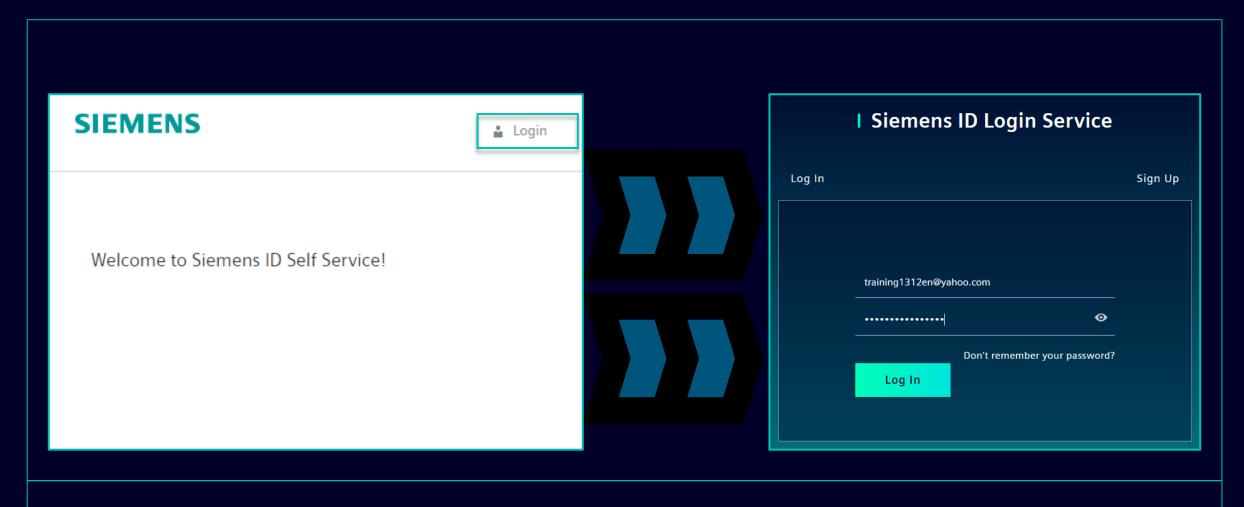


Geben Sie Ihre E-Mail-Adresse ein (dieselbe E-Mail-Adresse wie auf der Seite 6 angezeigt) und klicken Sie auf "Send Email". Sie erhalten eine E-Mail, um Ihr Passwort erneut zurückzusetzen.

Erstmalige Aktivierung der Multi-Faktor-Authentifizierung – Passwort vergessen

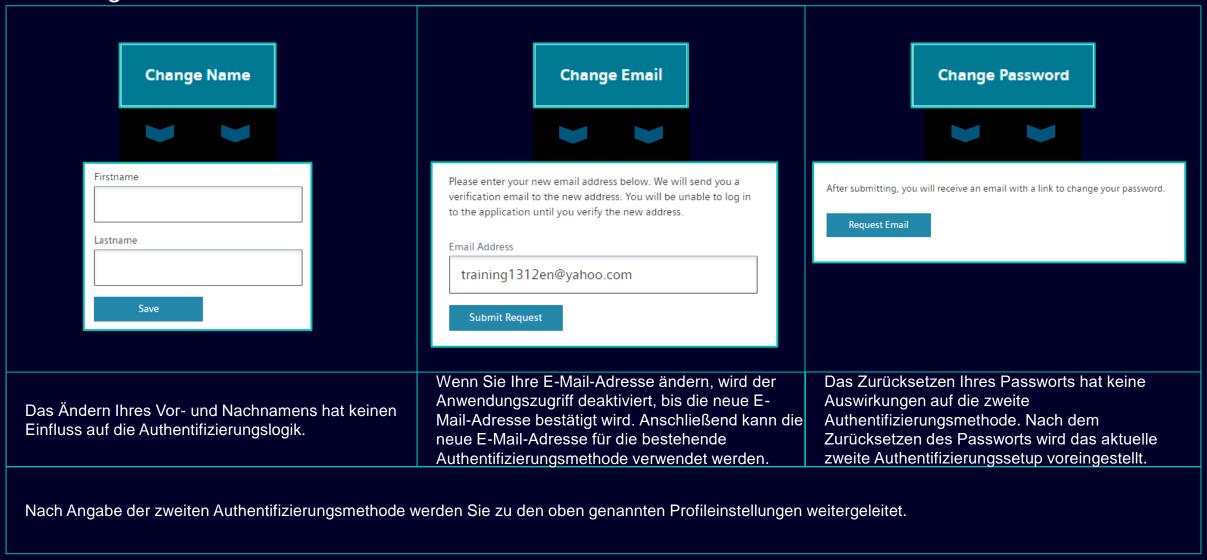


Öffnen Sie die E-Mail und klicken Sie auf "Reset my password". Sie werden zur ersten Siemens-Anmeldeseite weitergeleitet, wo Sie Ihr neu festgelegtes Passwort zurücksetzen können. Dann fahren Sie hier fort.

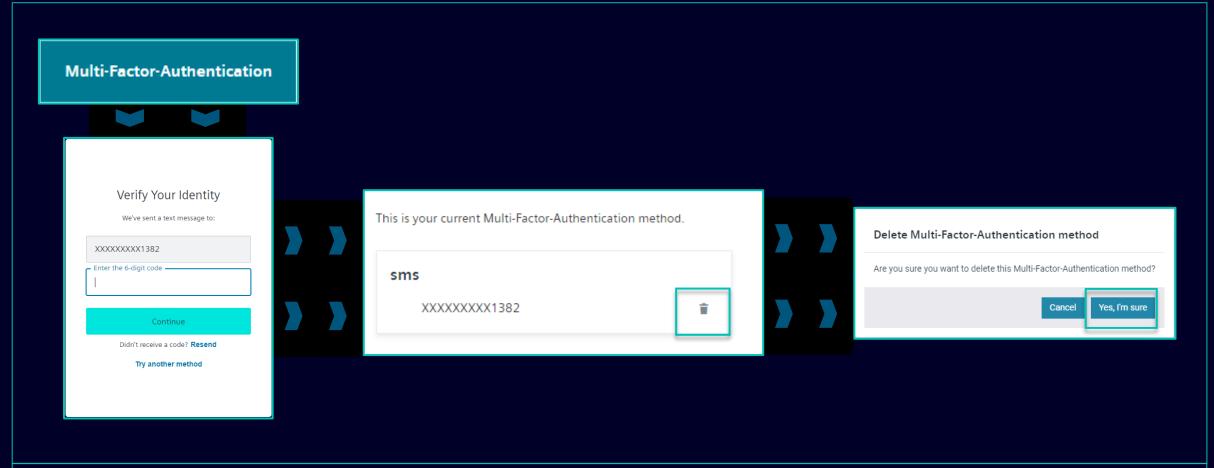


Bitte gehen Sie auf https://uss.login.siemens.com und klicken auf "Login"; Geben Sie auf der nächsten Seite Ihre E-Mail-Adresse und Ihr Passwort ein und klicken Sie auf "Login".

Änderung der Kontoinformationen

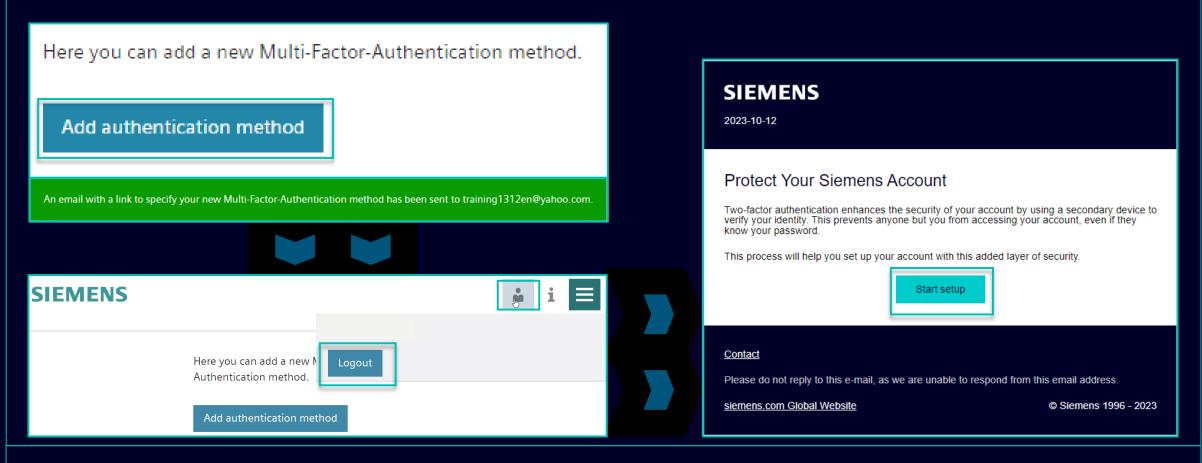


Änderung der Multi-Faktor-Authentifizierungsmethode



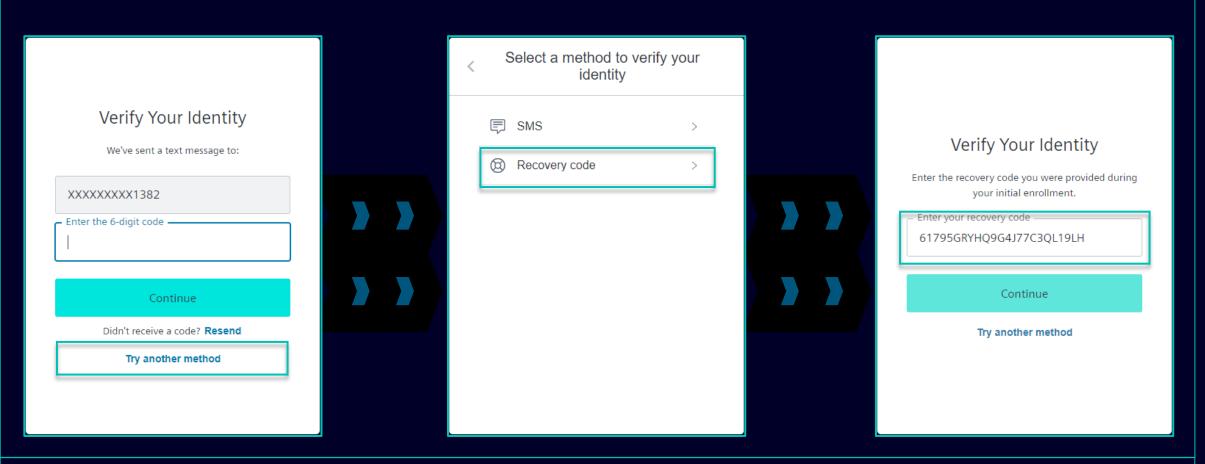
Um Ihre Multi-Faktor-Authentifizierungsmethode zurückzusetzen, klicken Sie auf "Multi-Factor-Authentication" – Sie werden weitergeleitet, um die aktuell eingestellte Authentifizierungsmethode anzugeben. Wählen Sie nach der Anmeldung das Löschsymbol aus und bestätigen Sie das Zurücksetzen. Falls Sie versuchen, 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



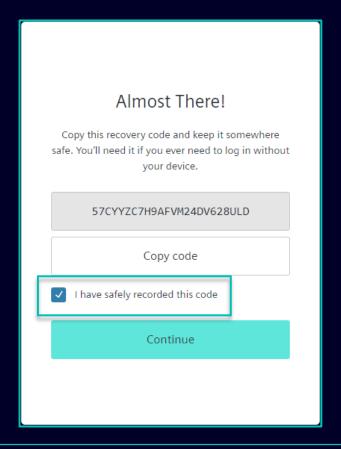
Nachdem Sie die aktuelle Authentifizierungsmethode gelöscht haben, müssen Sie eine neue Multi-Faktor-Authentifizierungsmethode festlegen. Klicken Sie auf "Add authentication method" und Sie erhalten eine E-Mail. **Es ist wichtig, dass Sie sich von Ihrem Konto abmelden, bevor Sie mit der Einrichtung einer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

Anmeldung über Wiederherstellungscode



Wenn Sie die zweite Authentifizierungsmethode ändern müssen oder die zweite Authentifizierung derzeit nicht bereitstellen können, können Sie sich mit dem Wiederherstellungscode 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 Wiederherstellungscode und klicken auf "Continue".

Anmeldung über Wiederherstellungscode



Sie erhalten einen neuen Wiederherstellungscode. Bitte stellen Sie sicher, dass Sie den neuen Wiederherstellungscode durch den Alten ersetzen. Der alte Wiederherstellungscode wird deaktiviert, nachdem Sie einen neuen Code erhalten haben. Nachdem Sie Ihren neuen Wiederherstellungscode 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

Supplier Portal

SCM STAR

ured login Forgotten password (secured login)

→

SCM STrategy And Realization -

- Informationen zu SCM STAR im Allgemeinen
- Neuigkeiten und Informationen, um Sie auf dem Laufenden zu halten
- Zugriff auf Schulungsmaterial (<u>Download Center</u>)

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

