Authentication Methods

Single Factor Authentication

E-Mail Login

Authentication with E-Mail address and password is available for all entitlement users and is mainly used from the internet. Due to the low authentication strength of this method, this authentication method is only recommended as an alternative to any of the other stronger authentication methods such as PKI. For most applications, a stronger authentication method is required. Therefore the user will be prompted for a second-step authentication (e.g. one-time password per SMS) or an even stronger authentication method such as PKI.

1) In the login box "E-Mail Login" enter your e-mail address in the field "My e-mail address". You can activate "Remember me" to remember your e-mail address for future logins.

2) Enter your entitlement password. This password is NOT your Windows password.

3) Click "login" in the login box "E-Mail Login" on the login page.

4) After successful authentication you will be automatically forwarded to the application, that was originally called.
PKI Smartcard Login

The most secure authentication method is the Siemens PKI (or public key infrastructure). Should you have your own personalized PKI card, you will be able to authenticate directly to most Siemens entitlement protected applications. Before you start: Please make sure, that your smart card is working and inserted successfully in your smart card reader.

Right-click the cardOS api symbol on the right bottom of your screen.

Should you not have the cardOS api installed on your PC, please install it from the UCMS basket on your desktop. Should you wish to use the cardOS api on a non-Siemens PC, please request the CardOS api here: https://intranet.for.siemens.com/wll/0015/en/lscc/sol/pki/Pages/card_os_api.aspx

For Entitlement PKI authentication:

1) Click "login" in the login box "Smart Card PKI Login" on the login page.
2) In the next dialog please enter your personal smart card PIN and click OK.
3) After successful authentication you will be automatically forwarded to the application, that was originally called.

Network Smart Card Login

For more information on using the Network Smartcard with Entitlement, please refer to the NSC user guide: IT HR User Guide - NSC#NSC-InsertingyourNetworkSmartcard

Windows Login

Within the Siemens network, this authentication method offers a very comfortable way to authenticate to many applications, as there is no input required to proceed. Depending on the security requirements of some of the connected applications, you will be requested to re-authenticate by using a stronger authentication method (e.g. PKI or OTP SMS).

Note: This authentication method is only available from within the Siemens intranet and requires that you are logged in to Windows with a valid user account.

1) Optional: Activate "Always use Windows Login" to automatically use Windows Login, whenever calling a protected application. Disabling this option can be done in the Entitlement Self Service tool.
2) Click "Windows Session" on the login page.
3) After successful authentication you will be automatically forwarded to the application, that was originally called.
Soft-PKI Login

Another way of using PKI, is that of a software certificate. You can request a soft authentication certificate on the PKI Self Services (Internet Explorer only) website. Installation is described here.

1) Click "Soft PKI" on the login page.
2) In the next dialog please enter your personal PIN / password.
3) After successful authentication you will be automatically forwarded to the application, that was originally called.

OTP SMS Login Multi Factor Authentication

One-time Password via SMS is only a 2nd step of the authentication.

The 1st step of the authentication is a "weak" authentication method such as Windows or E-Mail login. When the OTP SMS login step (2nd authentication) is successfully completed, the authentication level is at it's highest. As an exception, there are some applications that only allow PKI as the strongest authentication method.

The login process is equal to E-Mail Login, except for an additional step of requesting the one-time password, which will be sent to your pre-configured mobile device in the Entitlement Self Service.

1) Complete the first authentication step (e.g. E-Mail Login or Windows Login)
2) Depending on whether the requested web application requires a higher level of authentication, you will be redirected to an additional login page
3) A one time password (OTP) message is now sent out to your mobile device. (The ID in the Loginmask must match the ID in your SMS).
4) Enter the received one-time password in the following page to finish the login process
5) After successful authentication you will be automatically forwarded to the application, that was originally called.

Eventhough SMS might seem a cheap and interesting 2nd authentication method, it's not always the best solution. In many countries, SMS is a rather instable solutions and our experiences with the SMS technology have not always been very good (in some countries). For those affected countries, we recommend configuring the Entrust IdentityGuard app or Threema instead.

ginlo

The ginlo app is available for use with the corporate entitlement service. ginlo is a freely available app for IOS and Android. More information on ginlo can be found here.

Unfortunately ginlo will only be available until December 31st, 2019 due to insolvency proceedings.

Threema

Threema is a paid app and will be charged upon download from the app store. Usage however will not be charged (e.g. per message). More information from Threema can be found here.

Threema is a public service provider for secure messaging services (similar to Whatsapp). When Threema is configured for a mobile number, our external SMS provider attempts to send the message to the Threema channel first. Should that fail, an SMS is sent. This means, that as soon as Threema is configured, all OTP messages will be sent to the Threema app on the mobile device.

In order to use this service for receiving OTP messages from Siemens, you will need:

- A Threema account
The Threema app (available for different mobile platforms, like iOS and Android)
Your mobile phone number activated in the Entitlement Self Service
Your Threema account associated with the same mobile phone number as was activated in your Entitlement account.

To register the Siemens contact in your Threema account you can scan the following QR-code with your Threema app.

Please note that the mobile phone number configured for OTP SMS must exactly match the mobile phone number that is configured and published in your Threema account. More information about Threema availability and purchase price for platform of choice can be found on the Threema homepage.

Entrust IdentityGuard App

The Entrust app authentication is only a 2nd step of the authentication. The 1st step of the authentication is a “weak” authentication method such as Windows or E-Mail login. When the Entrust app login step (2nd authentication) is successfully completed, the authentication level is at its highest. As an exception, there are some applications that only allow PKI as the strongest authentication method.

1) Complete the first authentication step (e.g. E-Mail Login or Windows Login)
2) Select the "Mobile app" login method
3) Start the Entrust IdentityGuard app on your mobile device
4) Enter the code from the Entrust app into the correct input field on the Entitlement webpage
5) After successful authentication you will be automatically forwarded to the application, that was originally called.

It is possible to use the touch ID feature on supporting mobile phones. This feature is deactivated by default and can be activated in the configuration settings of Entrust IdentityGuard Mobile

Users and Data

User Types

In the Siemens Infrastructure there are multiple known user types. Following are the main user types:

- Internal Employee – Internal Employee (Z-GID)
- Known Business Partner (KBP) – External Employee / Contractor (Z-GID)
- General Business Partner (GBP) – Business Partner / Extranet User (X-GID)

Important: Each person has an intransmissible GID (General Identifier) that identifies him/her within Siemens Infrastructure. By reporting an issue to the Support Contact the GID of the affected person should always be mentioned.

You can check your type of user on the SCD (Siemens Corporate Directory) under the following link: https://scd.siemens.com/
Note: General Business Partner (X-GIDs) are not visible in SCD. X-GIDs are delivered by their responsible Data Supplier and are only visible on the application from which they were delivered. Each Data Supplier has its own interface to register and work on X-GID data. Please refer to the Entitlement XGID user guide for more information.

## SCD Data

Most of the data in the SCD is delivered from external (HR) applications (e.g. Colorado, Fusion).

<table>
<thead>
<tr>
<th>SCD Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>GID</td>
<td>Global Identifier</td>
<td>Z0001234</td>
</tr>
<tr>
<td>C</td>
<td>Country name</td>
<td>DE</td>
</tr>
<tr>
<td>O</td>
<td>Organization</td>
<td>SIEMENS</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational unit (SCD-OU)</td>
<td>GS IT 7092</td>
</tr>
<tr>
<td>L</td>
<td>Locality</td>
<td>MCH P</td>
</tr>
<tr>
<td>LastNam</td>
<td>Last name</td>
<td>Mueller</td>
</tr>
<tr>
<td>GN</td>
<td>Given name without national special characters</td>
<td>Joerg</td>
</tr>
<tr>
<td>SNamPre</td>
<td>Surname prefix</td>
<td>von,van</td>
</tr>
<tr>
<td>SNamAdd</td>
<td>Surname suffix</td>
<td>Baron</td>
</tr>
<tr>
<td>SNamNat</td>
<td>Surname national</td>
<td>Müller</td>
</tr>
<tr>
<td>GNamNat</td>
<td>Given name national</td>
<td>Jörg</td>
</tr>
<tr>
<td>CNamNat</td>
<td>Given name and surname with national spelling</td>
<td>Baron Jörg von Müller</td>
</tr>
<tr>
<td>I</td>
<td>Initials</td>
<td>Jmu</td>
</tr>
<tr>
<td>Gender</td>
<td>Gender</td>
<td>M</td>
</tr>
<tr>
<td>PersonalTitle</td>
<td>Personal title</td>
<td>Herr</td>
</tr>
<tr>
<td>GraduateTitle</td>
<td>Graduate title</td>
<td>Dr.</td>
</tr>
<tr>
<td>UserType</td>
<td>User type</td>
<td>I</td>
</tr>
<tr>
<td>RecordType</td>
<td>Record type</td>
<td>H</td>
</tr>
<tr>
<td>ContractStat</td>
<td>Contract status</td>
<td>A</td>
</tr>
<tr>
<td>Mail</td>
<td>Internet address / SMTP address</td>
<td><a href="mailto:joerg.mueller@siemens.de">joerg.mueller@siemens.de</a></td>
</tr>
<tr>
<td>Department</td>
<td>Department designation</td>
<td>GS IT HR 7 2</td>
</tr>
<tr>
<td>DepartmentText</td>
<td>Department text</td>
<td>Technology &amp; Infrastructure</td>
</tr>
<tr>
<td>MainFunc</td>
<td>Group-internal function designation</td>
<td>Administrator</td>
</tr>
<tr>
<td>Building</td>
<td>Building</td>
<td>MAIN</td>
</tr>
<tr>
<td>RoomNumber</td>
<td>Room number</td>
<td>410</td>
</tr>
<tr>
<td>PostOfficeBox</td>
<td>Postbox</td>
<td>Box 1234</td>
</tr>
<tr>
<td>TelNumber</td>
<td>Telephone number</td>
<td>+49 (89) 636-1234</td>
</tr>
<tr>
<td>Mobile</td>
<td>Mobile telephone number</td>
<td>+49 (171) 1234567</td>
</tr>
<tr>
<td>GIDSec</td>
<td>GID Secretary</td>
<td>ZZ004321</td>
</tr>
<tr>
<td>GIDRep</td>
<td>GID Representation</td>
<td>ZZ001234</td>
</tr>
<tr>
<td>Sponsor</td>
<td>Sponsor</td>
<td>ZYDH0002</td>
</tr>
<tr>
<td>PersRemark</td>
<td>Personal remark</td>
<td>maternity leave</td>
</tr>
</tbody>
</table>
### SCD Attribute

<table>
<thead>
<tr>
<th>SCD Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>UrlPers</td>
<td>Personal WEB-site</td>
<td><a href="https://intranet.siemens.com">https://intranet.siemens.com</a></td>
</tr>
<tr>
<td>PersIDNum</td>
<td>Personnel number</td>
<td>123998877</td>
</tr>
<tr>
<td>LeaveDate</td>
<td>Leave Date</td>
<td>43100</td>
</tr>
<tr>
<td>ValidDate</td>
<td>Valid date</td>
<td>38000</td>
</tr>
<tr>
<td>ExpireDate</td>
<td>Expire Date</td>
<td>43100</td>
</tr>
<tr>
<td>OrgID</td>
<td>Org-ID</td>
<td></td>
</tr>
<tr>
<td>NickNam</td>
<td>Nickname</td>
<td>Bob</td>
</tr>
<tr>
<td>Manager1</td>
<td>GID of the In-Country Manager</td>
<td></td>
</tr>
<tr>
<td>MailPriv</td>
<td>Private email address</td>
<td><a href="mailto:example@siemens.com">example@siemens.com</a></td>
</tr>
<tr>
<td>MobilePriv</td>
<td>Private mobile number</td>
<td></td>
</tr>
</tbody>
</table>

**Source:** [https://scd.siemens.com/luz/AttrDesc?lang=de&format=AdrV31](https://scd.siemens.com/luz/AttrDesc?lang=de&format=AdrV31) *(Some data was left out for readability reasons)*

This means, the SCD only stores what is delivered to it. Therefore, changes in SCD data (e.g. mobile number) can't be done by neither Entitlement nor SCD support. Please refer to the [SCD HELP](#) for more information.

### LeaveDate and Validity

Each SCD account has a so-called "Leave Date". This date determines, whether the SCD record of the employee is still valid. Put in other words: if the employee is still actively in the company. Should the LeaveDate have passed, the entitlement account is automatically disabled for security reasons. Please refer to the [SCD HELP](#) for more information on what to do in case your LeaveDate (or that of your sponsee) had expired.

### Mobile

The SCD's "Mobile" attribute plays an important role for the Entitlement account. The mobile number is exported automatically into the secure directory. After this synchronization was completed, the number must be activated in the Entitlement User Self-Service.

### E-Mail and LTE

The SCD's "Mail" attribute plays an important role for the Entitlement account. The e-mail address is exported automatically into the secure directory. Should your e-mail address have disappeared from the SCD, this could have great consequences for the authentication procedure. Most e-mail addresses are delivered from the so-called LTE (lifetime e-mail) database.

In the LTE database, each e-mail address is listed and is provided with a "SCD Export" attribute (or flag). Should your e-mail address be available in the database, but the SCD export flag have a "FALSE" value, the e-mail address is not exported to the SCD. This could be the root cause for severe authentication issues with Entitlement. You can check the LTE database as follows:

1. Visit [https://email.siemens.net/Web/SearchEmailAddress.aspx](https://email.siemens.net/Web/SearchEmailAddress.aspx)

   ![Search for LTE email addresses](image)

   - Please insert the e-mail address under the 'From' for which you would like to search within the LTE database and within the Siemens Corporate Directory (SCD). @siemens.com will be automatically added if no domain is given.

2. Should a red cross be displayed on the "SCD export" attribute, we'd advise you to open a ticket

   ![Table showing LTE email addresses](image)

<table>
<thead>
<tr>
<th>E-Mail Entry</th>
<th>Status</th>
<th>Grid</th>
<th>Sponsor Grid</th>
<th>SPem Filter</th>
<th>Expire Date</th>
<th>IMC Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:johndoe@siemens.com">johndoe@siemens.com</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>z9000093F</td>
<td>Z9000949W</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Z90009810W</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   If you think the data stored in LTE database is not correct, please inform the helpdesk!

### Private Data

As soon as one of the following SCD attributes are set, the Entitlement behaves differently than normal.

<table>
<thead>
<tr>
<th>SCD Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
The private attributes were designed for centralized data management. People that don't have regular access to a computer (e.g. factory worker) also want to benefit from the e-mail authentication method with a non-Siemens e-mail address and the OTP SMS authentication method. In these exact cases, a centralized (mostly HR) department can manage the so-called "private data" in SCD. This will have the following effects for an Entitlement user account:

1. The private e-mail address is added directly as a valid authentication method for the e-mail login method
2. The private mobile number is added directly as a valid authentication method for OTP SMS without having to activate the number in the self-service portal

This feature is beneficial to some, but can cause issues for others. Improper use of this mechanism can cause the self-managed mobile number to be overwritten or even disappear altogether.

**Case:** Only private mail is set and private mobile is empty

**Result:** The self managed mobile will be disabled and the private mobile (which is empty) will be activated automatically. Inversely, this causes the self managed mobile number to de-activate and no new number to activate, basically disabling the OTP SMS functionality altogether.

**Resolution:** Always make sure, that when the private data is used, both attributes (private mail AND private mobile) are populated in the SCD. Another option is to have this data removed from the SCD (by your HR department in most cases) and to manage the data yourself in the self-service portal.

### Active Directory Data

The Active Directory data is used when performing the Windows Login authentication method. This goes for both person's as well as functional accounts. There are some key points to consider:

- On which domain is my account located (e.g. ad005, ad001)
- Which value does the attribute UserPrincipleName contain? And is it equal to the e-mail address in the connected SCD record?

To browse your active directory data, do the following:

1. **Download** the Microsoft Active Directory Explorer (Executable provided by Microsoft)
2. From the package AdExplorer.zip, run AdExplorer.exe
3. A window like such should open:

   ![Active Directory Explorer](image)

4. Click "File" > "Connect" and fill out the correct connection data
   - a. ad001.siemens.net for Siemens Domain AD001 / ad005.onehc.net for Healthineers Domain AD005
   - b. User is your own Siemens GID (in most cases)
   - c. Password: Your personal Windows Password
   - d. Save the connection for easy future access
   - e. Click OK

   ![Connect to Active Directory](image)

5. A tree should automatically open, like so:
6. Click "Search" > "Search Container". A menu should open:
   a. Class stays unchanged (–common classes–)
   b. Attribute: Type in "siemens-gid" and the program will autocomplete
   c. Value: Type your GID
   d. Click "Add" to add your search criterion to the search query
   e. Hit Search at the bottom of the window to start the search
   f. Your Data record will appear in the bottom half of the window
   g. Double click your record to open (this could take a while, please be patient)
   h. As soon as the search completes, click cancel to close the dialog window

7. On the right hand side of the window, you will find all your record's attributes
   a. You want to search for the "userPrincipleName" attribute.
   b. This e-mail address MUST match the e-mail address in the SCD. If not, the Windows Login authentication method will not work

Should the Windows Login authentication method not work and you're having trouble connecting the Active Directory, please open a Ticket in MyIT.

Entitlement Account Data

The entitlement account data is stored in the so-called "secure directory". Most of it's information is received from the SCD. There are however some attributes that only live inside the secure directory:

- Self Managed Mobile
- Alternative E-Mail (used for password reset only)
- Registration data for the Entrust IdentityGuard app
- Your GetAccess roles (e.g. Access to the GA ServiceTool)
- The authentication methods allowed for use

Apart from the data listed above, no other data can either be created nor altered by the Entitlement service.
E-Mail Notifications

E-mail notifications will be sent to users in the following cases:

1. SCD Data that affects the Entitlement account was modified
2. Data was changed in the Entitlement account directly
3. The password of your Entitlement account is about to expire
4. When you request a one time password link from the forgot password mechanism
5. A general business partner was successfully onboarded

The reason for the e-mails 1 to 3 are for security reasons. E-Mails 4 and 5 are triggered by either a user, or a workflow. Should you receive an e-mail message, please follow the steps described in the e-mail.

User Self-Service

Production System: https://entitlement.siemens.com/myprofile
Reference System: https://rs.entitlement.siemens.com/myprofile

These are the main functionality of the user self-service:

- Viewing the available user data that was transferred from other systems to the Entitlement
- Configuring standard login behavior, such as the ‘Always use windows login’ feature
- Administration of the self managed mobile number
- Reviewing the status of the mobile app login method

Depending on individual account conditions the Entitlement User Self-Service may appear slightly different.

Auto-Windows Login Feature

Auto-Windows login allows you to access the applications that have the Windows login authentication method enabled, automatically.

On the login screen you are able to enable the feature:

![Windows Session](image)

You can disable the feature in the Entitlement Self-Service:

![Preferred Login Methods](image)

Or by using the following URL: https://entitlement.siemens.com/SSO/autoWindowsOff

Enabling/Disabling the Auto-OTP Feature

The Auto-OTP Feature sets your 2nd Factor Method to OTP, this means the System sends out an OTP automatically as soon as you need a stronger Authentication.

On the login screen you are able to enable the feature:
You can activate/deactivate this Feature by checking/unchecking the box.

**Activation of the (SCD) mobile number**

To activate your mobile number for SMS OTP, click the activate button:

Then, please check if the number to be activated is correct.

---

** CES OTP Activation **

Antonio Roldao

Please select your mobile number for activation

+351

Activate

Click "activate" and proceed with the following steps to verify your mobile device.

- **Check your mobile for the activation code received from Siemens.**
- **The received 4-digit code needs to be entered in the mask to finalize activation.**

---

You are done, if the successful activation is confirmed by the following screen.
The activation was completed successfully.

Registration and Activation of "Self-Managed Mobile"

Find the following section in the Entitlement Self-Service and click "edit".

The Corporate Entitlement Service provides an One-time password (OTP) login with a SMS delivery.

You have to add an OTP delivery number to use this login method. After that you will get the OTP login method option for according protected applications. Furthermore you can edit and reset your OTP delivery number here.

Please click on "edit" to continue.

Please note that this enforces a PKI login.

You will be prompted for additional PKI authentication for security reasons. Should you not have PKI and you still want to manage this number, please contact your Siemens sponsor and proceed here. After successful PKI authentication:

After this step, activation of your mobile number might still be needed.

Should an unexpected error occur, chances are that your number was already registered for another user. Please proceed to the chapter "Mobile number Deactivation / Deletion".

Mobile number Deactivation / Deletion

Follow the steps described in the previous chapter (Registration and Activation of "Self-Managed Mobile") and instead of save, click the "delete" button. This will remove the self-managed mobile number from your profile.

Please note: The mobile number is deleted from the Entitlement account, but is not deactivated. Should another user try to activate this number, the activation will fail. Should you wish to hand over this number to another colleague, please open a service desk ticket to have the number deactivated from the original Entitlement account.

Registration of the Entrust Mobile App

Please note: For security reasons, you MUST have activated OTP SMS first, before you can continue with the mobile app activation.

Another note: You can only associate the app configuration with one device. This means you need to decide which device you want to configure for your Entitlement account. Should you change devices in the meantime, the setup (starting from step 5) will have to be repeated for the new device.

1. Download the app from the Google Play or Apple app store and install

2. You will have to then register the Entrust Mobile app here.

3. You will be prompted for an additional SMS login, even after having performed PKI login.

4. Type in your OTP code and click login
5. On the first screen, click yes

![Image of IdentityGuard Self-Service]

6. Name: Siemens Entitlement
   Serial Number: Serial Number as displayed on the webpage
   Activation Code: Activation Code as displayed on the webpage

7. On the mobile phone app, save the configuration and provide a app PIN. Please remember the app PIN carefully! The app PIN will be requested each time the app is used.

![Image of app PIN screen]

8. To confirm your registration (Serial Number and Activation Code) please enter the Registration Code from your mobile phone app to the dialog box of your desktop screen.

![Image of Registration Code input]

9. After entering the Registration Code please continue on your mobile phone app with “OK” and the following dialog is shown. Please confirm with “Yes”.

![Image of confirmation dialog]
10. On the desktop dialog press "Next" to finish.

(Re)setting the Entitlement Password

You can change your password here: https://entitlement.siemens.com/SSO/Login?GASF=UserPassword

You will be prompted to enter you e-mail address. **For externals:** Please enter your Siemens e-mail address and NOT your alternative e-mail address. An additional copy of the e-mail is sent to your alternative e-mail address (when configured).

Click on the link in the e-mail that you’ve received and set your new password.
Eventhough all Checkmarks are set, you might want to review the Entitlement Password Rules. The newly implemented password requirements listed below weren't fully implemented in the checkmarks of the webform. This could cause an error setting the password, eventhough all checkmarks are set. A change request for this was already opened for the Entitlement development team.

**Entitlement Password Rules**

<table>
<thead>
<tr>
<th>Rule</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD_ATTEMPTS_BEFORE_LOCK</td>
<td>3</td>
<td>Attempts wrong password before account is locked</td>
</tr>
<tr>
<td>PASSWORD_LOCK_TIME</td>
<td>10</td>
<td>Time in Minutes the account is locked after entering the wrong password</td>
</tr>
<tr>
<td>Password_Expiry_Time</td>
<td>180 days</td>
<td>Password Expiry Time enforced by the system. User is asked to change password at login, if expiry time is reached.</td>
</tr>
<tr>
<td>PASSWORD_MINIMUM_LENGTH</td>
<td>12</td>
<td>Minimum password length</td>
</tr>
<tr>
<td>REQUIRE_LOWER_CASE_CHARACTER</td>
<td>YES</td>
<td>If enabled, the password must contain lower cases</td>
</tr>
<tr>
<td>REQUIRE_UPPER_CASE_CHARACTER</td>
<td>YES</td>
<td>If enabled, the password must contain upper cases</td>
</tr>
<tr>
<td>REQUIRE_NUMERIC_CHARACTERS</td>
<td>YES</td>
<td>If enabled, the password must contain numeric characters</td>
</tr>
<tr>
<td>REQUIRE_NON_ALPHANUMERIC_CHARACTERS</td>
<td>YES</td>
<td>If enabled, the password must contain special characters *1)</td>
</tr>
<tr>
<td>NO_USR_LOGIN_PASSWORD_LENGTH</td>
<td>YES</td>
<td>If enabled, the password must not contain parts of the login name</td>
</tr>
<tr>
<td>NO_CHARACTER_PASSWORD_LENGTH</td>
<td>YES</td>
<td>If enabled, the password must not contain recurring characters (like xxxxxxxx)</td>
</tr>
<tr>
<td>NO_USER_FIRST_NAME</td>
<td>YES</td>
<td>If enabled, the password may not contain the users' first name</td>
</tr>
<tr>
<td>NO_USER_LAST_NAME</td>
<td>YES</td>
<td>If enabled, the password may not contain the users' last name</td>
</tr>
<tr>
<td>CHECK_AGAINST_PASSWORD_HISTORY</td>
<td>8</td>
<td>Number of history passwords, which must not be reused</td>
</tr>
</tbody>
</table>

Allowed special characters in password management and for registration of external users - XGID:

```
: ; , - _ / \ ( ) < > @ * $ % & + = ! ? ' "
```

Additionally, a password blacklist was implemented to prevent choosing potentially weak passwords.

- Alphabetical (a-z, A-Z, wrap = true)
- Numerical (0-9, wrap = true)
Qwerty, ignore case (English keyboard layout, wrap = true, like qwertyuiop[])
Qwertz (German keyboard layout, wrap = true)
Repeated character, ignore case (like 11111, aAaAa or BBBB)
and dictionary rules, including popular but trivial passwords like company names, politicians, artists, and several other words

Should you have trouble setting the password of your choice, please try another password instead using the above rules and regulations to avoid any violations.

Delegated User Administration

Production System: https://entitlement.siemens.com/useradmin
Reference System: https://rs.entitlement.siemens.com/PasswordManagement/delegated/adm

The delegated user administration allows a sponsor of externals (known business partners) to modify the following data

- An alternative email address (e.g. external company address), which is used ONLY for the Entitlement password reset process
- The mobile number of the "self-managed mobile"

Note: Due to restrictions of the Siemens Information Security Policy administration of external XGID users (General Business Partners) is not possible to use the delegated administration service.

After a successful authentication of the sponsor, a search can be performed using the following data of the sponsee:

- the surname / given name
- the GID
- e-mail address

Wildcard searches are not supported.

Modify Sponsee Data

The alternative mail address must be of an external domain (e.g. somemail@somedomain.com). Siemens internal e-mail addresses are not allowed to be used as alternative mail address. The OTP delivery number has to follow international standardization regulations. Make sure that you enter the phone number with the country code attached, e.g. +4917212345678 or +49 (172) 12345678

To prevent misuse, a confirmation mail is sent to the primary mail address of the affected user and a CC (copy) is sent to the alternative mail address (if configured). To delete the currently configured alternative mail address or the OTP delivery number, simply use one of the available reset buttons.

Please note: The mobile number is deleted from the Entitlement account, but is not deactivated. Should another user try to activate this number, the activation will fail. Should you wish to hand over this number to another external, please open a service desk ticket to have the number deactivated from the original Entitlement account.

ServiceTool

Productive System: https://entitlement.siemens.com/serviceTool
Reference System: https://rs.entitlement.siemens.com/serviceTool/userService

The Entitlement ServiceTool allows verifying the status of an employee in

- the SCD (Siemens Corporate Directory)
- the Secure Directory (Entitlement GetAccess repository)
- the Siemens Active Directory (siemens.net).

The Entitlement ServiceTool is used by IT Servicedesk and Entitlement support to perform Entitlement account troubleshooting. The Entitlement ServiceTool can only be accessed with the correct role assignment. Access is granted to authorized support staff only. For acquiring access to the ServiceTool, please open a service request in MyIT.

General

Identification and Authentication

Identification

There is a difference between identification and authentication. Identification is the means to and end (getting yourself authenticated). Identification can be provided in these forms

- Windows Account
- Siemens e-mail address
- (Soft) PKI certificate

When presenting one of these identification types, the system was able to identify who you are. The following step is authentication, which also has multiple types.

Single- and Multi-Factor Authentication

A direct access authentication method is any authentication method, that can be used to directly access an application (regardless of the authentication strength). A step-up authentication method is an combination of 2 authentication methods (at least!), to achieve a higher level of authentication. This is typically achieved through additional evidence of user authenticity.
Example 1: Direct access authentication method

- step 1: enter PKI smartcard
- step 2: enter PIN

Example 2: Step-up authentication method

- step 1: enter username/password
- step 2: enter OTP SMS was sent to the user's mobile device

Another situation in which a step-up authentication can occur, is when a user already has a valid session, the authentication strength of that session is not sufficient to access the affected application.

Example: the user is already authenticated with username + password, but the application requires a stronger authentication, the user will be prompted to authenticate using one of the available stronger authentication methods (such as smartcard PKI). The user's session is updated from "weak authenticated" to "strong authenticated" and the user will be able to access more secure applications, too.

The two-factor authentication is an approach of identification and authentication, that requires the presentation of two different kinds of evidence (identification) to guarantee that someone is who he says he is. It is a part of the broader family of multi-factor authentication, which is a defensive in depth approach to security, since it is more unlikely, that an attacker is in possession of more than one of the possible factors:

- What You Know: can be a combination of username + password, a password for a keystore or the PIN of a smartcard
- What You Have: can be a smartcard, a mobile phone
- What You Are: can be biometrics, e.g. fingerprint

Within the Siemens environment, both internal Employees and business partners have the following options for authentication.

<table>
<thead>
<tr>
<th>Security Level (ACP) 1 - &quot;Restricted&quot;</th>
<th>Security Requirement</th>
<th>Authentication Standard (Minimum Requirement)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Simple proof of identity</td>
<td>E-Mail login</td>
</tr>
<tr>
<td></td>
<td>Single factor authentication</td>
<td>Windows login</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Level (ACP) 2 - &quot;Confidential&quot;</th>
<th>Security Requirement</th>
<th>Authentication Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unambiguous proof of identity with resistance against &quot;skilled&quot; attacks</td>
<td>PKI soft-certificate plus TransportPin</td>
</tr>
<tr>
<td></td>
<td>Strong authentication - two &quot;soft factors&quot;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Level (ACP) 3 - &quot;Strictly confidential&quot;</th>
<th>Security Requirement</th>
<th>Authentication Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Non-repudiatable proof of identity with resistance agains &quot;professional&quot; attacks</td>
<td>Corporate ID card plus PIN</td>
</tr>
<tr>
<td></td>
<td>True two-factor authentication</td>
<td>One-Time password (OTP) via SMS plus username / password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Entitlement Entrust mobile app login</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Smartcard</td>
</tr>
</tbody>
</table>

Second Factor One-Time Password (OTP) Rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Current</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD_ATTEMPTS_BEFORE_LOCK</td>
<td>3</td>
<td>Attempts wrong password before account is locked</td>
</tr>
<tr>
<td>PASSWORD_LOCK_TIME</td>
<td>10</td>
<td>Time in Minutes the account is locked after entering the wrong password</td>
</tr>
<tr>
<td>OTP Lifetime</td>
<td>300s = 5min</td>
<td>One Time Password Expiry Time enforced by the system. User gets a new password, if expiry time is reached or the password was used before.</td>
</tr>
<tr>
<td>OTP Length</td>
<td>8</td>
<td>OTP length</td>
</tr>
<tr>
<td>Cell Alphabet</td>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td>The password will be created with these chars.</td>
</tr>
<tr>
<td>Rule</td>
<td>Current</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>New OTP for each request</td>
<td>yes</td>
<td>If enabled, each request will generate a new OTP. Otherwise an OTP is valid until the OTP lifetime is reached or the OTP was used.</td>
</tr>
</tbody>
</table>

### Web Browsers

Basically there are no known functional restrictions regarding the chosen browser when using the Entitlement, except for the Firefox browser. Firefox needs additional settings in order to work with the Entitlement authentication system. The chosen browser must be compatible to W3C standardization of html, css and JavaScript. Please make sure to always use up-to-date versions of common browsers:

- Google Chrome
- Internet Explorer
- Firefox
- Safari

Please note, that there may be additional requirements for a selected login method to work properly, e.g. CA certificates installed in the browser.

#### Firefox

In order to use older versions of Firefox with the Entitlement authentication system, the following settings must be applied.

Follow these steps for setting up the PKI login feature:

1. Start your Firefox browser and open the Advanced Options menu (Firefox button → Options → Options → Advanced)
2. Select the tab Certificates and click on „Security Devices“
3. Then click on „Load“
4. Choose a name for your new module (for example CardOS)
5. 32bit Browser: Select the file C:\Windows\system32\siecap11.dll resp. cardos11.dll for newer versions of CardOS API or
6. 64bit Browser: Select the file C:\Windows\System32\siecap11_64.dll resp. cardos11_64.dll or cardos15_64.dll for newer versions of CardOS API
7. Insert your smartcard in the cardreader, click on „Log In“, enter the PIN and then close the Device Manager

To enable the Soft-PKI login feature:

1. Start your Firefox browser and open the Advanced Options menu (Firefox button → Options → Options → Advanced)
2. Select the tab Certificates and click on „Security Devices“
3. Open View Certificates → Your Certificates and start the import of your certificate
4. On the subsequent dialog select the location of your certificate (p12 or pfx file)
5. You will immediately be asked for a password after selecting the certificate file. Please enter the password, that is used to protect the certificate file. This is either the transport PIN, which was communicated to by Siemens Trust Center, when the certificate has been delivered to you, or a password, which you have provided, if the certificate file was exported to a file by you.

To enable the Windows login feature:

1. Insert about:config into the address bar and press return
2. Accept the security warning and insert network.automatic-ntlm-auth.trusted-uris into the filter field
3. Now just one entry should be presented in the list, please double click the entry
4. Double click on the filtered result and insert siemens.com and click ok

And some additional settings:

1. Insert about:config into the address bar and press return
2. Accept the security warning and insert security.ssl.renego_unrestricted_hosts into the filter field
3. Now just one entry should be presented in the list, please double click the entry
4. Double click on the filtered result and insert entitlement.siemens.com, mspki.entitlement.siemens.com, xauth.entitlement.siemens.com

### Session Management

After successful user authentication a global session is generated. This session is used to authtenticate the user to all web applications connected to the Siemens Entitlement Authentication Service (through a process called "application integration"). The global session information is stored as a cookie on the client / the browser. On each access attempt to a new web application (connected to the Siemens Entitlement Authentication Service) this global session is used to autthomatically authenticate the user without the need for additional user interaction. This is possible as long as the global session is valid and the cookie is present on the client's browser.

In short, a Session Management System, in which the user has to authenticate only once and can then – as long as the session has not expired – use the existing valid session for further authentication to other applications.

#### Entitlement Session Timeouts:

1. General Timeout: 480 minutes
2. Idle Timeout: 120 minutes

This means that a session will be invalidated after 120 minutes (on-idle), if the user does not perform any activities in the active browser session of the protected web application. The general timeout will invalidate the user session after
480 minutes and the user has to re-authenticate to continue working with the protected application.

Diagram A: A basic session

Diagram B: Application requires a higher level of authentication from the start
The user is prompted for a 2nd authentication step immediately when opening the session

Diagram C: A step-up is required during the session
The user authenticated with E-Mail Login (Level 1) followed by the dedicated step-up method OTP SMS Login. In combination, the user is authenticated with level 3.

Diagram D: A forced authentication during the session
This feature is typically used for implementing a workflow-like process to enforce the user to actively commit particular workflow steps by performing a login

As soon as the session expires, the login procedure restarts from the beginning.