



DriveLock Self-Service Portal

Documentation 2021.2

DriveLock SE 2021



Table of Contents

1 WELCOME TO THE DRIVELOCK SELF-SERVICE PORTAL	3
2 SELF-SERVICE PORTAL	4
2.1 Requirements	4
2.2 Outline of communication channels for the SSP	4
2.3 Setting up the Self-Service Portal (SSP)	4
2.3.1 Installation	5
2.3.2 Configuration	5
2.3.2.1 Setting up the SSP for the DriveLock Agent	6
2.3.2.2 Setting for emergency logon	7
2.3.2.3 Settings for user enrollment	7
3 ENROLLMENT WIZARD	9
3.1 User registration via DriveLock Agent	9
4 HOW END USERS WILL USE THE SELF SERVICE	10
COPYRIGHT	11

1 Welcome to the DriveLock Self-Service Portal

The DriveLock Self-Service Portal (SSP) allows end users to regain access to their computers encrypted with DriveLock Disk Protection or BitLocker Management in the event that they forget their password for logging into the DriveLock PBA (or need the recovery key for a BitLocker-encrypted hard drive).

The challenge-response procedure the SSP initiates does not require any support from an administrator or help desk. End users can perform recovery around the clock and from any device with internet access.

The module consists of two parts:

- Self-Service Portal: Web-based front end designed to authenticate users and receive emergency logon credentials.
- Enrollment Wizard: Interface for the end user to provide the backup information required for authentication. It also maps the user to the computer running the DriveLock Agent. The wizard checks the status in the background and stops automatically once the initial enrollment is complete.



Note: The Self-Service Portal doesn't require a separate license; it's included with BitLocker Management or Disk Protection licenses.

2 Self-Service Portal

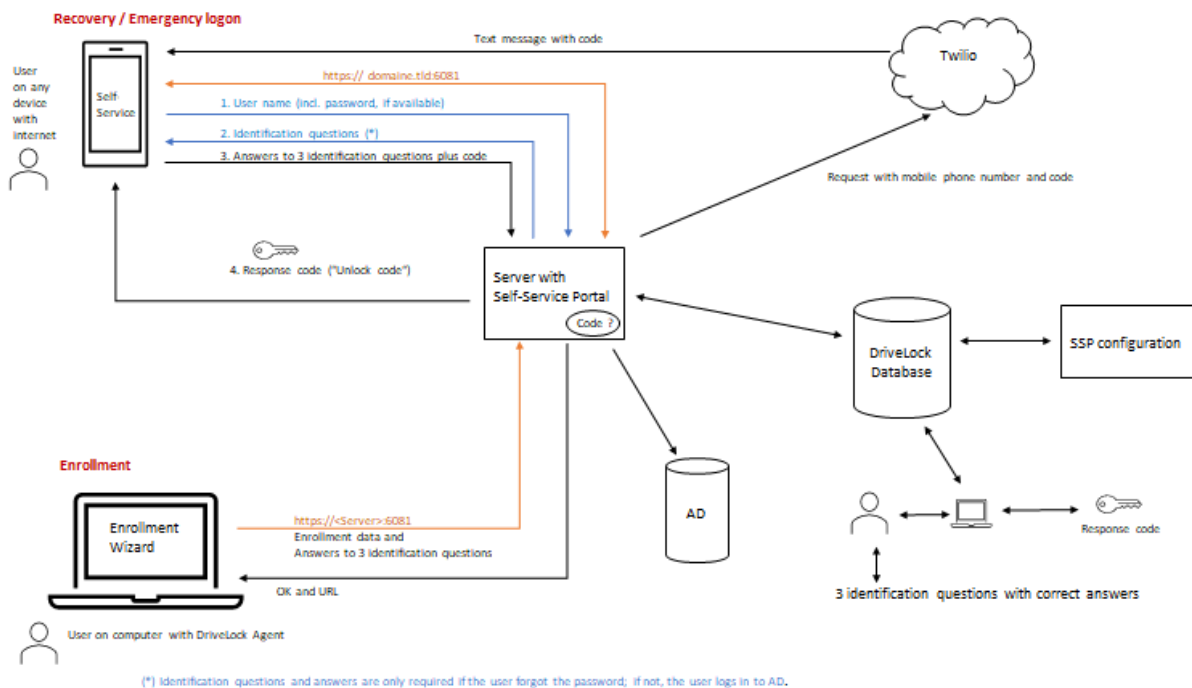
2.1 Requirements

To use the Self-Service Portal (SSP), the following is required:

- Install the SSP service on a server
- Specify an external URL and port for the server: the end user accesses the web portal via URL to get the recovery information
- Connect the SSP service to the central DriveLock database: this is where the end user's information is stored and where the specific computer with the DriveLock Agent must be registered
- Connect the SSP service to the Active Directory
- Provide the recovery certificates in the DriveLock database (BitLocker/Disk Protection)

2.2 Outline of communication channels for the SSP

This is how two-factor authentication via the Twilio platform works:



2.3 Setting up the Self-Service Portal (SSP)

The SSP is installed as a standalone service (DriveLock Self-Service Portal.msi) and comes with the DriveLock ISO.

Since the portal requires an Internet connection, you can install it on any server (inside the DMZ) that can be reached from the outside via the Internet. The portal is independent of the DriveLock Enterprise Service (DES) and other DriveLock services.

Once you have successfully [installed](#) the portal, you can start [configuring](#) it. Once the appropriate policy settings are assigned to the DriveLock Agent, the [end user](#) can enroll in the self-service and define custom settings.

2.3.1 Installation

To install the SSP, follow these steps:

1. First, start the DriveLock Self-Service Portal Setup Wizard by double-clicking the **DriveLock Self-Service Portal.msi** file.



Note: Das MSI-Paket sollte mit einem angemeldeten Benutzer gestartet werden, der Datenbankrechte hat.

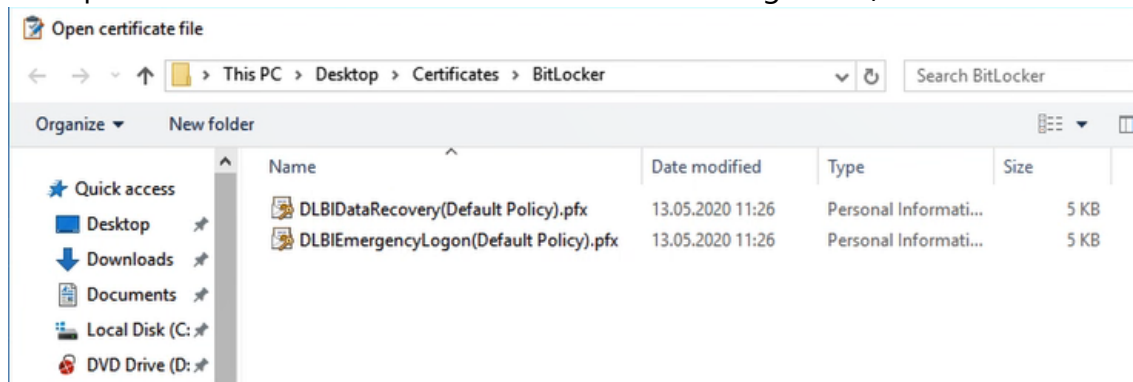
2. After the welcome dialog and an EULA, specify the service account that will connect to the DriveLock database and enter the associated password.
3. In the next dialog, select the SSL certificate for communication. Here you can either select an existing certificate or a certificate from your own certification authority or create a new certificate.
4. If you want to select an existing certificate, the next step will show you a list of all existing certificates. Select the appropriate one.
5. Next, start the installation to set up the service for the SSP (this will also adjust the firewall rules accordingly).
6. Exit the DriveLock Self-Service Portal Setup Wizard and continue with the [configuration](#).

2.3.2 Configuration

Start the configuration of the SSP by selecting the appropriate start menu item or by double-clicking the `DlSspPortalConfig.exe` in the installation directory.

1. In the first dialog, specify the database connection. Start by entering the **server** (with instance name) hosting the database. Test the connection. If this test is successful, the system also checks the connection to the **database**, displaying the database including the version number.
2. Click **Next** to confirm the information.

3. In the next dialog, select the certificates for recovery or emergency logon, depending on whether you are working with Disk Protection or BitLocker Management.
 - Open the location where the certificates are stored and import them (in the example below, the certificates are for BitLocker Management).



Note: You will also be asked to enter the appropriate password for the certificate.

4. In the next step, you can optionally configure how end users are verified and/or notified in addition to answering the recovery questions. DriveLock uses the Twilio communication platform. You can easily create a Twilio account and then enter the required information in the dialog. In addition, the end user then also receives a code via text message for authentication. As an alternative or in addition, you can also select e-mail notification. Specify the appropriate information in the dialog.
5. And finally, you can specify a maximum number of login retry attempts or a login lock-out delay. This information helps to prevent password spying.
6. Save your settings and finish your configuration.

Note: By logging in to the Self-Service Portal website for the first time, you can also verify that the service has been installed correctly. If so, the only remaining step is to have the end users enroll via the Enrollment Wizard. For this purpose, you need to specify settings for the DriveLock Agent.

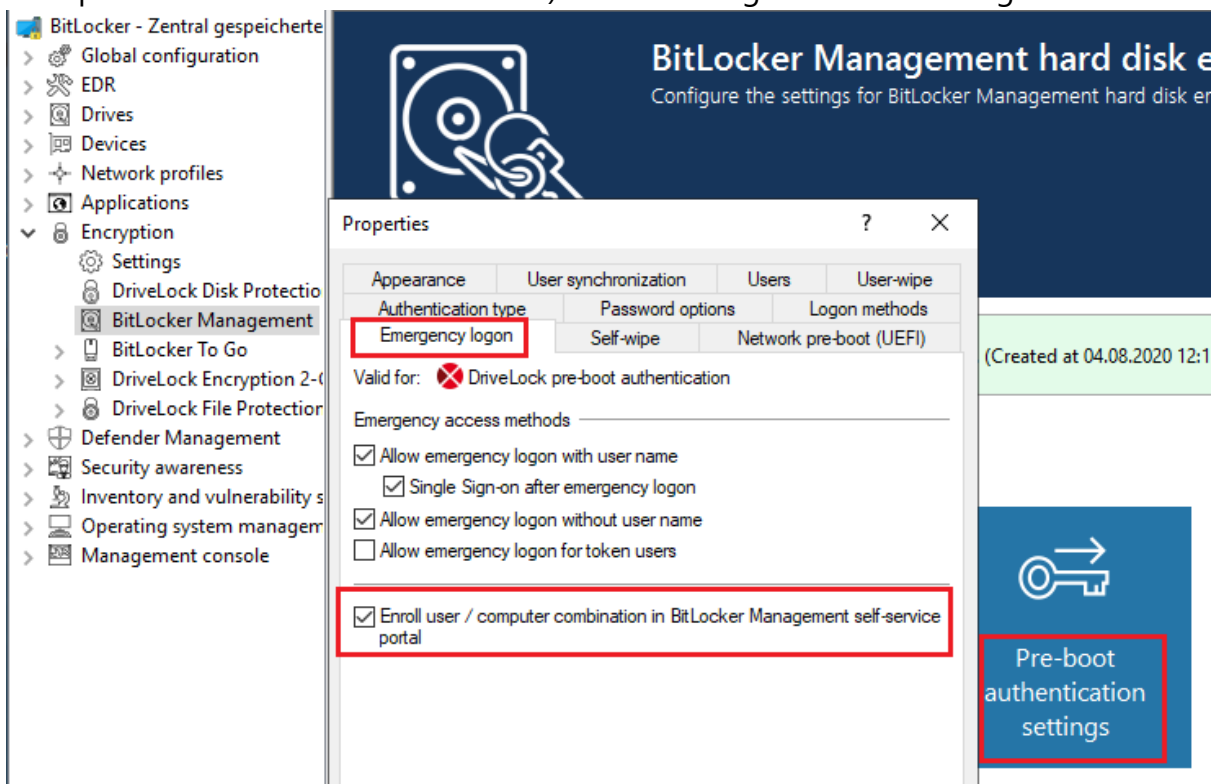
2.3.2.1 Setting up the SSP for the DriveLock Agent

Before end users can automatically enroll in the self service, you must configure settings in the policy that will be assigned to the agents. Depending on whether you are using BitLocker Management or Disk Protection as the encryption option for your DriveLock Agents, the [setting](#) for emergency logon is in a different location in the DMC. Also, please specify a [setting](#) for user enrollment.


2.3.2.2 Setting for emergency logon

Depending on the encryption method you are using, proceed as follows:

1. In the DriveLock Management Console (DMC), in the **Encryption** node, open either the **BitLocker Management** or **Disk Protection** subnode, and then open the **Pre-Boot Authentication settings** (see figure with BitLocker Management as example)
2. On the **Emergency logon** tab, you can choose the **Enroll user / computer combination in BitLocker Management Self-Service Portal** option (for Disk Protection, the option is DriveLock Disk Protection) to allow using the SSP on the agent.



3. Save the policy. Next, configure the [server connection settings](#) and then assign the policy.

 Note: With this setting enabled, the Enrollment Wizard is launched for each user who logs on to the computer.

2.3.2.3 Settings for user enrollment

To specify the port and Internet address settings used by end users to access the portal, proceed as follows:

1. Go to the **Server connections** node in your policy and select the server where the SSP is installed.

2. Enter the following information on the **General** tab in the **server properties** (see example):
- **Server name:** Name of your server running the SSP, or a corresponding DNS alias.
 - **Portal port (HTTPS):** Port 6081 is entered automatically.
 - **External URL:** The external URL is displayed to the end user after going through the enrollment wizard. And this is where the end user logs in to run the recovery process.

The screenshot shows the 'General' tab of a configuration window. The 'Server name' is 'SSP-SERVER'. The 'Server port (HTTP)' is '6066' and the 'Server port (HTTPS)' is '6067' with the 'Use HTTPS' checkbox checked. The 'End-user self service portal' section is highlighted with a red box and contains the following fields: 'Portal port (HTTPS)' is '6081' (Port on internal address) and 'External URL' is 'https://ssp-server{dlse.local:6081' (URL accessible from the internet). The 'External URL' field is highlighted with a blue box. Below this section is a 'Comment' text area.

3 Enrollment Wizard

3.1 User registration via DriveLock Agent


Once the policy with the SSP settings is assigned and effective on a DriveLock Agent, the Enrollment Wizard starts automatically for the respective end user.


Alternatively, you can also start the wizard manually by adding the `DLSelfServiceEnrollment.exe` from the DriveLock Agent installation directory to the command line. This way you can enroll users manually or automate the enrollment with software deployment solutions.

At the beginning, the end user enters the required information in the wizard:

- 3 recovery questions plus answers
- Mobile number for receiving text messages and/or e-mail address (depending on your configuration)

The final step is to verify the connection to the server and display the login address (URL) for the SSP.

 Note: Remind end users to make a note of the login address so that they can access the recovery procedure from other devices when necessary.

 Note: The information can also be configured in the DriveLock PBA.

4 How end users will use the self service

Once the end user has enrolled in the self service via the Enrollment Wizard, the service is available in case an emergency logon is required. If the user forgets the password to log in to the DriveLock PBA, the following steps should be performed:

1. The user calls the DriveLock Self Service via the URL provided in the last dialog of the Enrollment Wizard. This can be done from any device with internet access.
2. Next, the user logs in with user name and password (the data is synchronized with the AD). If the password is missing, the user clicks **I forgot my password**.
3. Then, the three recovery questions are displayed. Once the correct answers are typed in and verified, the user will receive a code via text message or email if the two-factor authentication has been configured; this code must first be entered. In all other cases, simply answering the questions correctly will suffice.
4. If the end user is enrolled for the service on more than one computer, a corresponding choice will be displayed.
5. After that, the user chooses the recovery scenario if applicable (logging in to DriveLock PBA or BitLocker recovery).
6. In the event that the password for logging into the DriveLock PBA is missing, the next step will be to enter and verify the challenge code. This is displayed in the PBA login screen during emergency logon.
7. Finally, the end user receives the recovery code and enters it into the logon screen to unlock the computer.



Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

© 2021 DriveLock SE. All rights reserved.

DriveLock and others are either registered trademarks or trademarks of or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

