DriveLock Self-Service Portal

Dokumentation 2021.2

DriveLock SE 2021

Inhaltsverzeichnis

1 Willkommen zum DriveLock Self-Service Portal

Das DriveLock Self-Service Portal (SSP) bietet Endbenutzern die Möglichkeit, auf ihre mit DriveLock Disk Protection oder BitLocker Management verschlüsselten Computer wieder zugreifen zu können, wenn sie ihr Kennwort für die Anmeldung an der DriveLock-PBA vergessen haben (oder den Wiederherstellungsschlüssel für eine mit BitLocker verschlüsselte Festplatte benötigen). Dies geschieht mittels eines Challenge-Response-Verfahrens.

Mit dem SSP ist bei diesem Prozess keine Unterstützung seitens eines Administrators notwendig. Dieser Vorgang kann rund um die Uhr und von jedem internetfähigen Gerät aus durchgeführt werden.

Das Modul besteht aus zwei Teilen:

- Self-Service Portal: webbasiertes Frontend für die Authentifizierung und den Empfang der Notfallanmeldeinformationen.
- Enrollment Wizard zur Registrierung: Endbenutzeroberfläche zur Angabe der Ersatz-Informationen für die Authentifizierung. Hiermit wird auch die Zuordnung zwischen dem Benutzer an einem Computer mit DriveLock Agenten und dem Computer an sich festgelegt. Der Assistent prüft im Hintergrund den Status und beendet sich automatisch, sobald die initiale Registrierung erfolgt ist.

Hinweis: Das Self-Service Portal benötigt keine eigenständige Lizenz, sondern ist in den Lizenzen für BitLocker Management oder Disk Protection bereits enthalten.

2 Self-Service Portal

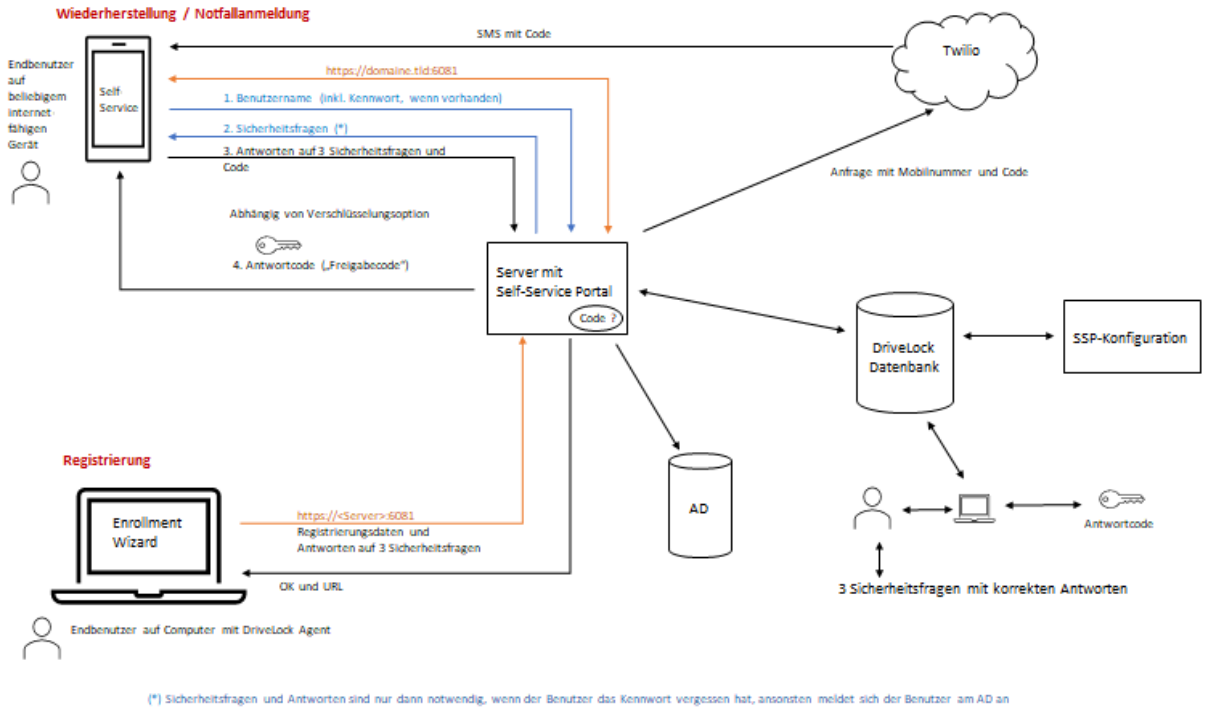
2.1 Voraussetzungen

Die Verwendung des Self-Service Portals (SSP) setzt folgendes voraus:

- Installation des SSP-Dienstes auf einem Server
- Externe URL und Port für den Server: der Endbenutzer greift mittels URL auf das Web-Portal zu, um die Wiederherstellungsinformationen zu erhalten
- Verbindung des SSP-Dienstes zur zentralen DriveLock Datenbank: hier werden die Informationen des Endbenutzers gespeichert und der jeweilige Computer mit dem DriveLock Agenten muss hier registriert sein
- Verbindung des SSP-Dienstes zum Active Directory
- Wiederherstellungszertifikate müssen in der DriveLock Datenbank vorhanden sein (BitLocker/Disk Protection)

2.2 Übersicht über die Kommunikationswege des SSP-Dienstes

Die Zwei-Faktor-Authentifizierung über die Plattform Twilio funktioniert folgendermaßen:



2.3 Einrichtung des Self-Service Portals (SSP)

Das SSP wird als eigenständiger Dienst (DriveLock Self-Service Portal.msi) installiert und mit dem DriveLock-ISO ausgeliefert.

Da das Portal eine Internet-Verbindung benötigt, können Sie es auf jedem Server installieren (innerhalb der DMZ), der über das Internet von außen erreichbar ist. Das Portal ist unabhängig vom DriveLock Enterprise Service (DES) und von anderen DriveLock Diensten.

Nach erfolgreicher Installation erfolgt die Konfiguration des Portals. Nach Zuweisung der entsprechenden Richtlinieneinstellungen auf den DriveLock Agenten, kann sich der Endbenutzer für den Self-Service registrieren und eigene Einstellungen vornehmen.

2.3.1 Installation

Um das SSP zu installieren, gehen Sie folgendermaßen vor:

1. Starten Sie zunächst den DriveLock Self-Service Portal Setup Wizard, indem Sie die Datei **DriveLock Self-Service Portal.msi** doppelklicken.

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

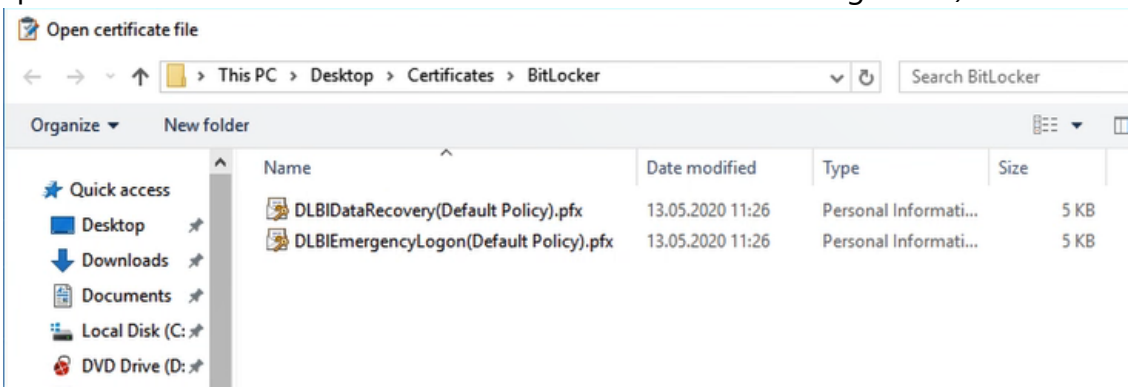
2. Nach Begrüßungsdialog und EULA geben Sie das Service-Konto an, das eine Verbindung zur DriveLock Datenbank hat, und das dazugehörige Kennwort.
3. Im nächsten Dialog wählen Sie das SSL-Zertifikat für die Kommunikation aus. Sie können hier entweder ein bereits vorhandenes Zertifikat oder ein Zertifikat Ihrer eigenen Zertifizierungsstelle wählen oder ein neues Zertifikat erstellen.
4. Wenn Sie ein vorhandenes Zertifikat auswählen wollen, wird Ihnen im nächsten Schritt eine Liste aller vorhandenen Zertifikate angezeigt. Wählen Sie das entsprechende aus.
5. Starten Sie im nächsten Schritt die Installation, damit der Dienst für das SSP eingerichtet wird (hierbei werden auch die Firewall-Regeln entsprechend angepasst).
6. Beenden Sie den Setup Wizard und führen Sie anschließend die Konfiguration durch.

2.3.2 Konfiguration

Die Konfiguration des SSP kann über den entsprechenden Startmenüeintag oder durch Doppelklicken der `DlSspPortalConfig.exe` im Installationsverzeichnis gestartet werden.

1. Im ersten Dialog wird die Datenbankverbindung festgelegt. Dazu geben Sie als erstes den **Server** (mit Instanznamen) an, auf dem die Datenbank läuft. Testen Sie die Verbindung. Ist dieser Test erfolgreich, wird auch die Verbindung zur **Datenbank** überprüft, wobei die Datenbank inklusive der Versionsnummer angezeigt wird.
2. Klicken Sie auf **Weiter**, um die Angaben zu bestätigen.

3. Im nächsten Dialog wählen Sie die Zertifikate für die Wiederherstellung bzw. Notfall-Anmeldung, je nachdem ob Sie mit Disk Protection oder BitLocker Management arbeiten.
   - Öffnen Sie dazu den Ablageort der Zertifikate und importieren Sie diese (im Beispiel unten handelt es sich um Zertifikate für BitLocker Management).



> Hinweis: Beachten Sie, dass Sie auch das entsprechende Kennwort zum jeweiligen Zertifikat eingeben müssen.

4. Im nächsten Schritt können Sie optional konfigurieren, wie die Endbenutzer zusätzlich zur Beantwortung der Sicherheitsfragen verifiziert bzw. benachrichtigt werden. DriveLock arbeitet mit der Kommunikationsplattform Twilio zusammen, bei der Sie sich ganz einfach ein Konto erstellen können und die Angaben dann entsprechend in den Dialog eingeben können. Der Endbenutzer erhält dann zusätzlich per SMS einen Code, um sich zu verifizieren. Alternativ oder zusätzlich können Sie auch eine Verifizierung per E-Mail auswählen. Geben Sie die entsprechenden Informationen im Dialog an.
5. Zuletzt können Sie angeben, wie viele Anmeldeversuche Endbenutzer durchführen dürfen bzw. wie lange sie von der Anmeldung ausgeschlossen werden. Diese Angaben tragen dazu bei, ein Ausspionieren von Kennwörtern zu verhindern.
6. Speichern Sie Ihre Angaben und schließen Sie Ihre Konfiguration ab.

> Hinweis: Diese initiale Anmeldung an der Webseite des Self-Service Portals dient gleichzeitig auch als Überprüfung, ob der Dienst korrekt installiert wurde. Wenn dies der Fall ist, müssen sich lediglich noch die Endbenutzer über den Enrollment Wizard registrieren. Dazu sind Einstellungen für den DriveLock Agenten notwendig.

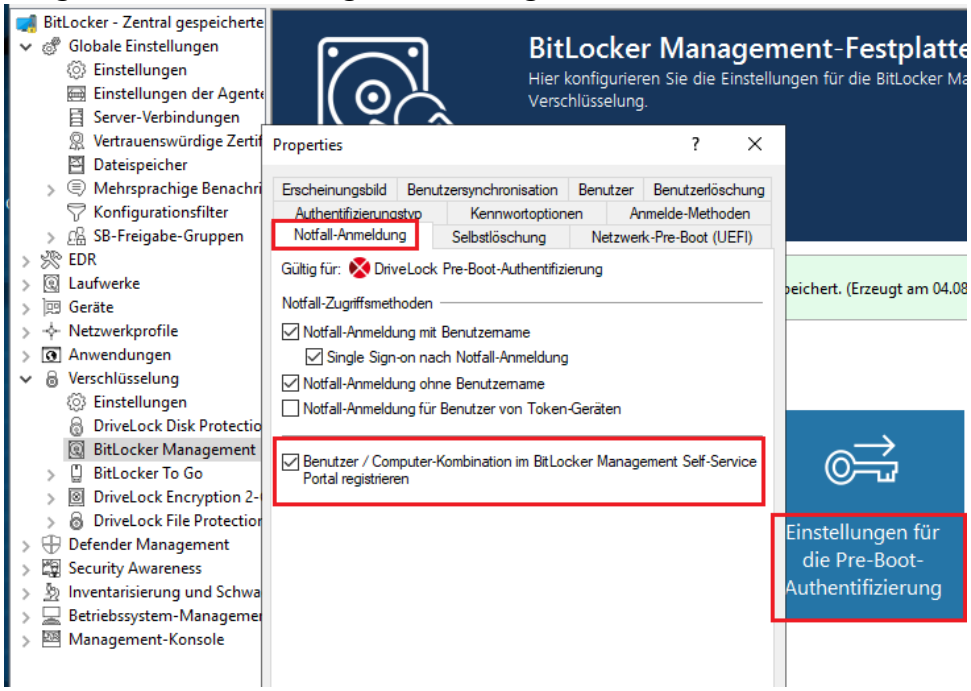
2.3.2.1 SSP für den DriveLock Agenten einrichten

Bevor sich Endbenutzer automatisch für das Self-Service Portal registrieren können, müssen entsprechende Einstellungen in der Richtlinie gesetzt werden, die den jeweiligen Agenten dann zugewiesen wird. Je nachdem, ob Sie für Ihre DriveLock Agenten BitLocker Management oder Disk Protection als Verschlüsselungsoption verwenden, befindet sich die Einstellung für die Notfall-Anmeldung an anderer Stelle in der DMC. Außerdem muss eine Einstellung in der Richtlinie für den Server gesetzt werden.

2.3.2.2 Einstellung für die Notfall-Anmeldung

Je nachdem welche Verschlüsselungsoption Sie verwenden, gehen Sie folgendermaßen vor:

1. Öffnen Sie in der DriveLock Management Konsole (DMC) im Knoten **Verschlüsselung** entweder den Unterknoten **BitLocker Management** oder **Disk Protection** und dann die **Einstellungen für die Pre-Boot-Authentifizierung** (s. Abbildung am Beispiel BitLocker Management)
2. Auf dem Reiter **Notfall-Anmeldung** können Sie durch Auswahl der Option **Benutzer / Computer-Kombination im BitLocker Management Self-Service Portal registrieren** (bei Disk Protection lautet die Option DriveLock Disk Protection) die Benutzung des SSP auf dem Agenten ermöglichen.



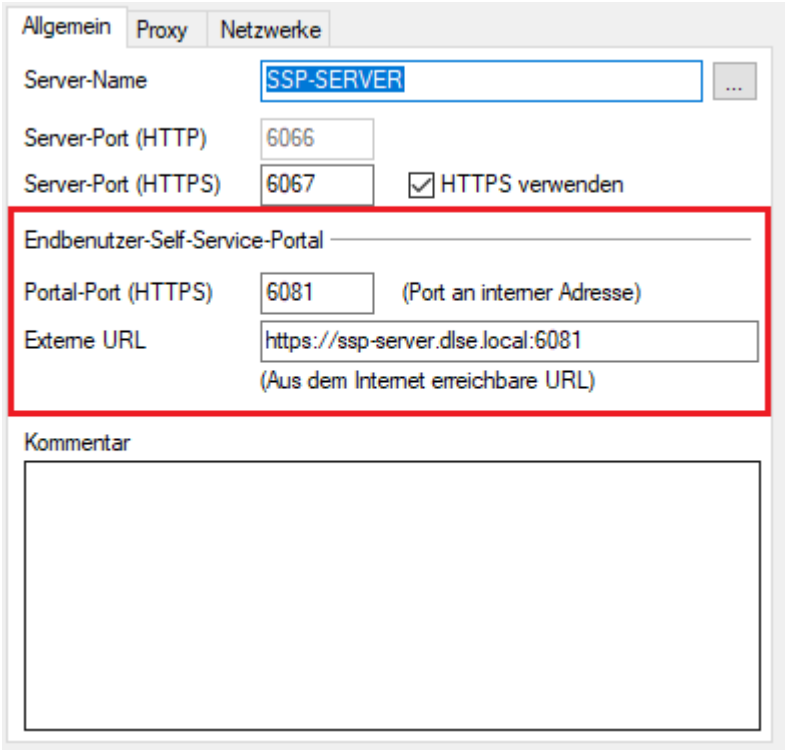
3. Speichern Sie die Richtlinie. Nehmen Sie anschließend die Server-Verbindungseinstellungen vor und weisen Sie danach die Richtlinie zu.

Hinweis: Wenn diese Einstellung aktiviert ist, wird der Enrollment Wizard bei jedem Benutzer gestartet, der sich an dem Computer anmeldet.

2.3.2.3 Einstellungen für die Benutzerregistrierung

Um die Einstellungen für den Port und die Internet-Adresse anzugeben, über die Endbenutzer auf das Portal zugreifen können, gehen Sie folgendermaßen vor:

1. Öffnen Sie in Ihrer Richtlinie den Knoten **Server-Verbindungen** und wählen Sie hier den Server aus, auf dem das SSP installiert ist.
2. In den **Server-Eigenschaften** geben Sie auf dem Reiter **Allgemein** folgendes an (s. Abbildung):
   - **Server-Name**: Name Ihres Servers, auf dem das SSP läuft, oder ein entsprechendes DNS-Alias.
   - **Portal-Port (HTTPS)**: Der Port 6081 wird automatisch eingetragen.
   - **Externe URL**: Die externe URL wird dem Endbenutzer nach Durchlaufen des Enrollment Wizards angezeigt. Hier meldet sich der Endbenutzer an, um den Wiederherstellungsprozess durchzuführen.



3 Enrollment Wizard

3.1 Benutzerregistrierung über den DriveLock Agenten

Sobald die Richtlinie mit den SSP-Einstellungen auf dem DriveLock Agenten zugewiesen und dort wirksam ist, startet der Enrollment Wizard beim Endbenutzer automatisch.

Alternativ kann der Assistent über die `DLSelfServiceEnrollment.exe` auch per Kommandozeile aus dem Installationsverzeichnis des DriveLock Agenten gestartet werden. Damit können Sie Benutzer manuell registrieren oder die Registrierung mit Software-Verteilungslösungen automatisieren.

Der Endbenutzer gibt dann initial in dem Assistenten die für ihn relevanten Informationen ein:

- 3 Sicherheitsfragen und deren Antworten
- Mobilnummer für Empfang von SMS und/oder E-mail-Adresse (je nach Konfiguration)

Zum Schluss wird die Verbindung zum Server überprüft und die Anmeldeadresse (URL) für das SSP angezeigt.

Hinweis: Weisen Sie den Endbenutzer darauf hin, sich die Anmeldeadresse zu notieren, um im Notfall auch von anderen Geräten auf das Wiederherstellungsverfahren zugreifen zu können.

Hinweis: Die Informationen können auch in der DriveLock PBA konfiguriert werden.

4 Verwendung des Self-Service durch den Endbenutzer

Sobald sich der Endbenutzer über den Enrollment Wizard für das Self-Service Portal (SSP) registriert hat, steht der Dienst für den Notfall zur Verfügung. Hat der Benutzer sein Kennwort vergessen und kann sich nicht mehr an seinem Computer (an der DriveLock-PBA) anmelden, werden folgende Schritte durchgeführt:

1. Der Benutzer ruft den DriveLock Self-Service über die URL auf, die im letzten Dialog des Enrollment Wizards genannt wurde. Dies kann von jedem internet-fähigen Gerät aus erfolgen.
2. Dann folgt die Anmeldung mit Benutzername und Kennwort (die Daten werden dabei mit dem AD abgeglichen). Bei fehlendem Kennwort wird die Schaltfläche **Kennwort vergessen** ausgewählt.
3. Als nächstes erscheinen die drei Sicherheitsfragen. Sobald die korrekten Antworten eingegeben und überprüft worden sind, erhält der Benutzer bei konfigurierter Zwei-Faktor-Authentifizierung über SMS oder E-Mail einen Code, der zunächst eingegeben werden muss. Ansonsten reicht auch nur die korrekte Beantwortung der Fragen.
4. Ist der Endbenutzer auf mehreren Computern für das SSP registriert, wird eine entsprechende Auswahl angezeigt.
5. Anschließend wählt der Benutzer gegebenenfalls das Wiederherstellungsszenario aus (Anmeldung an der DriveLock-PBA oder BitLocker-Wiederherstellung).
6. Wenn das Kennwort für die Anmeldung an der DriveLock-PBA vergessen wurde, muss als nächstes der Challenge-Code eingegeben und verifiziert werden. Dieser wird bei der Notfall-Anmeldung in der Anmeldemaske der PBA angezeigt.
7. Zuletzt erhält der Endbenutzer den Freischaltcode, der dann in die Anmeldemaske eingegeben wird, um den Computer zu entsperren.

Copyright