



## BitLocker Management

Manual 2020.2

DriveLock SE 2021



## Table of Contents

1 DRIVELOCK BITLOCKER MANAGEMENT	6
1.1 General information	6
1.1.1 System Requirements	6
1.1.2 Algorithms for DriveLock BitLocker Management	
1.1.3 Licensing BitLocker Management	
1.2 BitLocker policy configuration	
1.2.1 Encryption settings	
1.2.1.1 Encryption certificates	
1.2.1.1.1 Create encryption certificates	
1.2.1.2 Deployment settings	
1.2.1.3 Hard disk encryption settings	15
1.2.1.3.1 The General tab	15
1.2.1.3.2 The Recovery tab	20
1.2.1.3.3 The Execution options tab	20
1.2.1.4 Pre-boot authentication settings	
1.2.1.4.1 The Authentication type tab	22
1.2.1.4.2 The Password options tab	24
1.2.2 Decryption	27
1.2.2.1 Decrypting encrypted drives	27
1.2.3 Override policy settings (BitLocker)	29
1.3 Sample configuration	
1.4 Recovery	32
1.4.1 Recovering encrypted hard disks	32
1.4.2 Recovery process	34
1.5 Taking over native BitLocker	
1.5.1 Integrating existing BitLocker environments	

1.5.2 Additional modifications of BitLocker policies	
1.6 DriveLock Agent	41
1.6.1 BitLocker pre-boot authentication	41
1.6.2 BitLocker Management on client computers (DriveLock Agent)	41
1.6.3 Encrypting client computers	42
1.6.3.1 Delay encryption	44
1.6.4 Integrating data partitions with existing BitLocker	46
1.7 DriveLock Control Center	
1.7.1 BitLocker Management in the DCC	49
1.7.1.1 Assigning a computer-specific BitLocker password	50
1.7.1.2 Allowing a user-defined BitLocker password	52
1.7.2 BitLocker event report	54
1.7.2.1 Customizing the BitLocker event report	54
1.7.2.2 Listing of BitLocker-relevant events	55
1.8 Tracing BitLocker actions	55
2 DRIVELOCK PRE-BOOT AUTHENTICATION	
2.1 Policy configuration with pre-boot authentication settings	57
2.1.1 License DriveLock PBA	57
2.1.2 Pre-boot authentication settings	57
2.1.2.1 Authentication type	57
2.1.2.2 Logon methods	59
2.1.2.3 Users	60
2.1.2.4 User synchronization	60
2.1.2.5 User wipe	60
2.1.2.6 Appearance	61
2.1.2.7 Network pre-boot (UEFI)	61
2.1.2.8 Emergency logon	61

	2.1.2.9 Self-wipe	62
2	.1.3 Override policy settings (DriveLock PBA)	63
2.2	Network pre-boot authentication (UEFI)	.65
2	.2.1 Network pre-boot (UEFI)	.66
2	.2.2 Use case 1: Automatic logon	.68
2	.2.3 Use case 2: Network login for all AD users	69
2	.2.4 Network PBA settings in the DOC	.71
2.3	Settings for emergency logon	.72
2.4	DriveLock Agent	.75
2	.4.1 Installing the DriveLock PBA on the DriveLock Agent	.75
2	.4.2 Login to the DriveLock PBA	75
2	.4.3 Network pre-boot authentication	78
2	.4.4 Emergency logon with recovery code	.80
2.5	DriveLock PBA command line tool	82
3 DR	IVELOCK BITLOCKER TO GO	85
3.1	BitLocker To Go policy configuration	85
3		00
-	.1.1 General settings for BitLocker To Go	86
3	.1.1 General settings for BitLocker To Go	.86 .87
3	.1.1 General settings for BitLocker To Go .1.2 Recovering encrypted drives 3.1.2.1 Administrative password	.86 .87 .87
3	<ul> <li>1.1 General settings for BitLocker To Go</li> <li>1.2 Recovering encrypted drives</li> <li>3.1.2.1 Administrative password</li> <li>3.1.2.2 Certificate-based recovery</li> </ul>	.86 .87 .87 .88
3	<ul> <li>1.1 General settings for BitLocker To Go</li> <li>1.2 Recovering encrypted drives</li> <li>3.1.2.1 Administrative password</li> <li>3.1.2.2 Certificate-based recovery</li> <li>1.3 Settings for enforced encryption</li> </ul>	.86 .87 .87 .88 .88
3 3 3.2	<ul> <li>1.1 General settings for BitLocker To Go</li> <li>1.2 Recovering encrypted drives</li> <li>3.1.2.1 Administrative password</li> <li>3.1.2.2 Certificate-based recovery</li> <li>1.3 Settings for enforced encryption</li> <li>Sample configuration for BitLocker To Go encryption</li> </ul>	.86 .87 .87 .88 .88 .88
3 3 3.2 3	<ul> <li>1.1 General settings for BitLocker To Go</li> <li>1.2 Recovering encrypted drives</li> <li>3.1.2.1 Administrative password</li> <li>3.1.2.2 Certificate-based recovery</li> <li>1.3 Settings for enforced encryption</li> <li>Sample configuration for BitLocker To Go encryption</li> <li>2.1 Create drive whitelist rule</li> </ul>	86 .87 .87 .88 .88 .88 .88 .89
3 3.2 3.3	<ul> <li>1.1 General settings for BitLocker To Go</li> <li>1.2 Recovering encrypted drives</li> <li>3.1.2.1 Administrative password</li> <li>3.1.2.2 Certificate-based recovery</li> <li>1.3 Settings for enforced encryption</li> <li>Sample configuration for BitLocker To Go encryption</li> <li>2.1 Create drive whitelist rule</li> <li>BitLocker To Go recovery</li> </ul>	86 .87 .87 .88 .88 .88 .89 .90
3 3.2 3.3 3.3 3.3	<ul> <li>1.1 General settings for BitLocker To Go</li> <li>1.2 Recovering encrypted drives</li> <li>3.1.2.1 Administrative password</li> <li>3.1.2.2 Certificate-based recovery</li> <li>1.3 Settings for enforced encryption</li> <li>Sample configuration for BitLocker To Go encryption</li> <li>2.1 Create drive whitelist rule</li> <li>BitLocker To Go recovery</li> <li>3.1 Recovery procedure</li> </ul>	86 .87 .87 .88 .88 .88 .89 .90 .91 .92
3 3.2 3.3 3.3 3 3	<ul> <li>1.1 General settings for BitLocker To Go</li> <li>1.2 Recovering encrypted drives</li> <li>3.1.2.1 Administrative password</li> <li>3.1.2.2 Certificate-based recovery</li> <li>1.3 Settings for enforced encryption</li> <li>Sample configuration for BitLocker To Go encryption</li> <li>2.1 Create drive whitelist rule</li> <li>BitLocker To Go recovery</li> <li>3.1 Recovery procedure</li> <li>3.2 Recovery in the DriveLock Operations Center (DOC)</li> </ul>	86 .87 .87 .88 .88 .88 .90 .91 .92 .92

COPYRIGHT	
INDEX	
3.5.2 Encryption rules	
3.5.1 Administrative password rules	96
3.5 Use cases	95
3.4.1 BitLocker To Go on the DriveLock Agent	

### 1 DriveLock BitLocker Management

BitLocker Management offers you a number of advantages when compared to the standard usage of Microsoft BitLocker:

- Manage encryption with BitLocker technology from a central location
- Keep track of all client computers whose hard disks are encrypted with BitLocker
- Easily integrate native BitLocker environments in DriveLock BitLocker Management
- In addition to the common authentication methods, BitLocker Management also supports smartcard and token.
- Monitor the encryption and decryption states of individual client computers in the DriveLock Control Center
- BitLocker Management provides a secure and central administration of recovery keys
- Quickly decommission devices when they are lost or stolen in case they are re-connected to the network
- BitLocker Management prohibits unauthorized access to decommissioned or recycled devices
- DriveLock pre-boot authentication for BitLocker allows you to unlock the system partition using your Windows login. This eliminates the need to enter the computer-specific BitLocker password.

#### **1.1 General information**

#### **1.1.1 System Requirements**

Note: For information on general system requirements (hardware and operating system requirements), see the latest Release Notes at DriveLock Online Help.

Warning: In some cases, it may be necessary to prepare the hard disk with the boot partition prior to using it with BitLocker. In this case, please perform the following steps: Check the status using "manage-bde -status c:" If the following error message pops up, "ERROR: The volume C: could not be opened

by BitLocker. This may be because the volume does not exist, or because it is not a valid BitLocker volume." make sure to prepare the hard disk. See https://docs.microsoft.com/de-de/windows-server/administration/windows-com-

mands/bdehdcfg. In an admin command line, you can prepare it by using "bdehdcfg.exe -target default" or "bdehdcfg.exe -target default -restart -quiet" (without prompting for scripting)



#### DriveLock BitLocker Management supports the following operating systems:

- Windows 7
  - Starting with Windows 7 SP1 (version 6.1.7601)
  - only 64 bit operating system
  - only Ultimate and Enterprise Editions
  - an existing Trusted Platform Module (TPM chip or vTPM) is mandatory

#### • Windows 8

- starting with Windows 8.1, Update 1 (version 6.3.9600)
- 32 bit and 64 bit operating systems
- only Professional and Enterprise Editions
- no TPM required (recommended for security reasons)

#### • Windows 10

- starting with Windows 10 1607 (version 10.0.14393)
- 32 bit and 64 bit operating systems
- only Professional, Enterprise and Education Editions
- no TPM required (recommended for security reasons)

Warning: Please note that the BitLocker feature for server operating systems is not installed by default.

# DriveLock PreBoot Authentication (DriveLock PBA) for Bitlocker only supports the following operating systems:

- Windows 10
  - UEFI firmware required
  - 64 bit operating systems
  - only Professional, Enterprise and Education Editions
  - no TPM required (recommended for security reasons)

#### 1.1.2 Algorithms for DriveLock BitLocker Management

BitLocker Management uses the following algorithms that are based on the operating systems in use. The methods of the relevant previous versions are also supported. See System requirements.

Operating system	Algorithm			
	• AES 128 bit with diffuser			
	• AES 256 bit with diffuser			
Windows 7	• AES 128 bit			
	• AES 256 bit			
	• AES 128 bit			
Windows 8.1	• AES 256 bit			
Windows 10	• AES XTS 128 bit			
	• AES XTS 256 bit			

Note: The default algorithm for data drives is AES 128 (this is the most compatible algorithm for almost all operating systems).

Note: Make sure to select the right algorithm. The above standard algorithms are the best choice in this case. When you integrate existing BitLocker environments, choosing the right one will affect how fast DriveLock can decrypt and re-encrypt the environment.

#### **1.1.3 Licensing BitLocker Management**

#### To license BitLocker Management, please follow these steps:

- 1. Select the policy where you want to license BitLocker Management.
- 2. Select Global configuration, then Settings and then click License.
- 3. This opens the License Properties; go to the General tab.
- 4. Click **Add license file...** and follow the instructions.
- 5. Next, select your **license file**(BitLocker license).

6. In the following dialog, please specify how to activate your license file. We recommend online activation.

Mote: Make sure that you are connected to the Internet.

- 7. Finally, confirm that your license for BitLocker Management will be added to DriveLock Enterprise Service.
- 8. Confirm your settings in the final dialog to activate BitLocker Management.
- 9. Your license appears in the license properties on the **General** tab.
- Next, open the Licensed computers tab. Select All computers on which you want to use BitLocker Management. You can also add individual computers, groups or organizational units by clicking Add.
- 11. Check the BitLocker Management box.

Warning: If you have already licensed Disk Protection (DriveLock FDE), BitLocker Management cannot be used in the same policy at the same time.

12. Apply your changes by clicking OK.

Note: If you have purchased the separate license for DriveLock PBA for BitLocker, you can also license it here. See also Licensing DriveLock PBA.

#### **1.2 BitLocker policy configuration**

#### **1.2.1 Encryption settings**

BitLocker Management allows you to manage the encryption of the client computers with BitLocker in your network from a central point.

Once you have licensed BitLocker Management, saved the policy and reopened it, you will see the new BitLocker Management sub-node in the **Encryption** node. Open the new sub-node to specify the settings for encryption, installation and authentication and to generate the encryption certificates.

Note: If you are using BitLocker Management for the first time, start by creating the certificates.



#### 1.2.1.1 Encryption certificates

To use BitLocker Management to encrypt hard drives, you first need encryption certificates. DriveLock requires these certificates for both encryption and recovery (to provide the recovery key and for a possible emergency logon).

DriveLock automatically adds the encryption certificates to the Windows Certificate Store where it also stores the passwords.

Note: It is absolutely necessary to store the encryption certificates in another secure location in the file system or on a smartcard.

BitLocker encryption certificates consist of two parts, the actual certificate (see figure below **DLBiDataRecovery.cer**) and the private key (see figure below **DLBiDataRecovery.pfx**):

DLBIDataRecovery.cer	04.12.2018	Security Certificate
DLBIDataRecovery.pfx	04.12.2018	Personal Information Exchange

The certificate for emergency logon consists of the following parts:

🔄 DLBIEmergencyLogon.cer	04.12.2018	Security Certificate
DLBIEmergencyLogon.pfx	04.12.2018	Personal Information Exchange

Warning: Prevent these certificates from being overwritten, as they are required for the clients' system recovery.

When you create a new policy to use for controlling BitLocker Management (BitLocker policy), always generate new certificates first. Proceed as described in chapter Creating encryption certificates for BitLocker Management.

#### **1.2.1.1.1 Create encryption certificates**

#### Please do the following:

1. When you are finished creating the BitLocker policy and licensing BitLocker Management, save and reopen the policy. Then the BitLocker Management subnode appears in the policy tree.

Note: A text message indicates that no encryption certificates have been generated yet:

- 2. Click the **Encryption certificates** option or open the link in the text message.
- 3. In the Encryption certificate Properties dialog, select the Generate certificates button.

You can import any existing certificates by clicking the **Manage certificates** button. If you do so, make sure that you do not overwrite any existing certificates because otherwise recovery will be impossible.

4. Follow the wizard and specify a **certificate backup location**. This can either be a folder in the file system or a smart card.

Note: Please make sure that the appropriate security requirements regarding storage location and access are met. 5. In the next step, define the passwords for the private keys (see figure).

Ø	Note: In this dialog, you specify the password for both the emergency logon
	certificate and the recovery certificate.

Encryption Certificate Creation X			
Certificate protection Type the password to			
Private keys for th Passwords are no need the passwor and recovery. Please save these	e certificates are protected by passwords. t stored as part of the DriveLock policy. You will ds to access private keys for emergency logon e passwords in a secure location.		
Emergency logon certi	ficate password		
Password	•••••		
Confirm password	•••••		
Recovery certificate p	assword		
Password	•••••		
Confirm password	•••••		
	,		
	< Back Next > (	Cancel	

6. Next, DriveLock generates the encryption certificates in the location you specified.

#### 1.2.1.2 Deployment settings

When BitLocker Management or the DriveLock PBA for BitLocker is installed on a DriveLock agent, the users are informed by default and their client computer is restarted after 30 seconds after the installation. You can change these settings if necessary.

#### **Installation tab**

Deployment	t settings Properties	?	×	
Installation	Options			
Display u	user information / confirm computer restarts			
Disp Disp	ay notification area icon while configuring the comp lav notification area icon while encrypting local hard	uter I disks		
⊡ Disp	lay user information before installing updates			
🗹 Auto	matically confirm all message boxes after 6	🚔 mir	nutes	
When BitLo	cker Management installation is finished			
Restart the system after     30     seconds				
ODon	ot restart the computer (wait until manual restart)			
	lun program after installation is finished			
5	Run as the currently logged-on user			
	Run also after deinstallation			
	OK Cancel	Ar	opły	

On this tab you can decide whether notifications are displayed or not, and you can also choose when they appear in the notification area: during configuration, during encryption and/or before installing updates.

Select **Do not restart the computer (wait until manual restart)** if you want to control the reboot. This allows you to start your own installation script, for example, with a shell command after the installation.

Two options are available:

- **Run as the currently logged on user**: The script runs with the rights of the user who is currently logged on. Normally it would run under the local system account.
- Run also after uninstall: The script runs during installation and uninstallation.



#### **Options tab**

**Show BitLocker Management logon messages**: Select this option if you want the preboot authentication information to appear in the notification area of the client computer after logon to Windows.

A message with detailed information will appear on the client computer (see figure):



#### 1.2.1.3 Hard disk encryption settings

#### 1.2.1.3.1 The General tab

On this tab you set the values for encryption and decryption with BitLocker.

Propertie	s						?		×
General	Recovery	Execution o	ptions						
Encrypt local hard disks on agent computers									
Encr	yption algorit	nm priority (to	pmost has	high	est priori	ty)			
AES AES AES	6 (256 bit key 5-XTS (256 b 6 (128 bit key 5-XTS (128 b	length) t key length) length) t kev lenath)				<b>^</b>	Mo Mov	ve u e do	ip iwn
	onfigure enc	yption setting	gs per driv	e	Setting	js			
Initia	encryption								- 1
	ncrypt only u isplay warnin	sed disk spa g when disks	ce (fast ini s are not fi	tial er ully er	ncryption ncrypted	)			
Settings for native BitLocker						-			
Manage native BitLocker environment									
ΜH	ide native Bi	Locker cont	ext menu (	entrie	s				
Insta	llation protec	tion ———							- 1
E	Encrypt only if pre-boot login succeeded at least once								
Response to configuration changes									
🔿 Delay decryption by 3 🌲 days									
۲	Do not decr	/pt							
			ОК		Cance			Appl	ly

The following options are available:

- 1. Encrypt local hard disks on Agent computers:
  - Select this option to start the **encryption** of the hard disks with BitLocker. Before you do so, make sure that all other encryption settings (see below) are specified.

Warning: As soon as you check this option and the policy has been assigned and updated on the client, the encryption process starts.

• To allow **decryption** (see detailed description in chapter decryption), uncheck the option and, if necessary, specify a delay in days.

Warning: Once you uncheck the option and do not specify a delay (and the policy is assigned and synchronized by the client), the decryption process will start.

#### 2. Encryption algorithm priority:

The list of the different encryption methods is processed from top to bottom.
 Once BitLocker Management finds a suitable algorithm that can be applied to the client, it will use it for encryption.

Mote: We recommend placing the strongest algorithm at top level.

- You can also sort the algorithms manually according to your requirements.
- Hardware encryption algorithm:

This is a special algorithm some producers build in to their hard disks. If you want to use this algorithm, please move it to the top of the list.

• Example:

You may want to move the **AES with Elephant diffuser (128 or 256 bit key length)** entry up if you have many computers with Windows 7 systems to encrypt, so that this algorithm is preferred.

#### 3. Configure encryption settings per drive:

 Select the required encryption algorithm for the system drive and the data drives by clicking the **Settings** button or choose 'Not encrypted' if no encryption is required.

Note: Please ensure that the drive letter and system partition assignment is the same for all computers this BitLocker policy is assigned to.



Encryption per drive			
Encryption set	ings for each local drives		
Drive	Encryption	^	
C:	AES (256 bit key length)		
💽 D:	AES (256 bit key length)		
🤇 E:	Not encrypted		
💽 F:	Not encrypted		
💽 G:	Not encrypted		
💽 H:	Not encrypted		
🤇 I:	Not encrypted		
🤇 J:	Not encrypted		
🧲 K:	Not encrypted		
L:	Not encrypted		
M·	Not encrypted	*	
Change	ОК	Cancel	

#### 4. Initial encryption

#### • Encrypt only used disk space (fast initial encryption):

- Select this option if you want to encrypt only the used disk space.
- Background:

With Windows 8, BitLocker introduced a feature that the hard disk does not have to be fully encrypted, but only the part where data is stored. Encryption is much faster for this reason.

• Issue:

Data that has been deleted from the hard disk and that is no longer visible in the Explorer may actually still exist and the original data can be accessed with special tools.

Note: We recommend that you only enable this option if you want to encrypt new hard disks, for example. Make sure that there is no old sensitive data on the hard disk. Likewise, this option is recommended for all SSDs.



#### • Display warning when disks are not fully encrypted

Each time the system is rebooted or the DriveLock Agent is restarted, the system checks whether all hard disks are already fully encrypted according to the settings. If this is not the case, the user is notified accordingly.

#### 5. Settings for native BitLocker

#### Manage native BitLocker environment

Select this option if you want to manage existing (native) BitLocker environments with DriveLock BitLocker Management. Please refer to chapter Integrating existing BitLocker environments for more information.

Note: Once you select this option and assign the policy accordingly, a wizard opens on the client computers with native BitLocker-encrypted (and thus locked) data drives; this wizard prompts the user to take over the drives. This is where you must provide the passwords for the locked partitions before they can be taken over.

#### • Hide native BitLocker context menu entries

This option is enabled by default. It hides all BitLocker options in the Windows Start menu or in the Explorer so that the native BitLocker dialogs are not displayed. This limits the chance of accidentally encrypting a hard disk or a drive with BitLocker but without DriveLock.

#### 6. Installation protection

#### • Encrypt only if pre-boot logon succeeded at least once

This is a preventive measure that keeps encryption separate from the initial logon to the PBA. Encryption is delayed until the first logon is successful.

#### 7. Response to configuration changes

#### • Delay decryption by [x] days:

This setting delays the decryption for the specified number of days. This may be useful so that the client computers and their users can be properly prepared for decryption.

The default value is **3** days. This value provides additional protection against misconfiguration. If you want to perform decryption immediately, change the setting to 0 days.

#### • Do not decrypt:

This option is enabled by default. Its purpose is to prevent unintentional decryption of BitLocker encryption when the configuration is changed, for example, after



0

DriveLock Agent updates, if group memberships are changed, or if the policy is no longer used by the DriveLock Agent.

Warning: Note that decryption is triggered only by disabling the **Encrypt local disks on agent computers** option described above. Decryption starts once the DriveLock Agent receives the configured policy with the mandatory decryption setting.



#### 1.2.1.3.2 The Recovery tab

On this tab you specify where the encrypted recovery data should be stored. These are the settings you need when you start the recovery process.

#### The following option is currently available:

1. DriveLock Enterprise Service:

Select this option if you want to send the encrypted recovery data to the DriveLock Enterprise Service (DES).

#### 2. File server (UNC path)

If you select this option, your encrypted recovery data is stored on a server, for example. When you select this option, you can specify a user name and password under the **Log in to file server** option.

#### 3. Local folder on Agent computers (not recommended)

We recommend this option only if you store the key files on a secure storage medium (e.g. USB device) or move them to a secure location later.

#### 1.2.1.3.3 The Execution options tab

On this tab you can select options for starting and delaying the encryption.

You can configure whether BitLocker encryption on the DriveLock Agent should start depending on certain events, or whether the user can delay the encryption. The objective is to disturb the user as little as possible and to keep the computer performance constant without compromising the protection provided by the encryption.

In the top section of the **Execution options** tab, check the **Start encryption only in the following events:** option to specify conditions that determine when encryption is allowed to start. For example, if you want to specify that encryption should start only on a client computer if no users are logged in, check the option as illustrated in the figure below:



Note: When selecting the option when no application is running in full screen mode, make sure that the application is actually running in full screen mode and not just maximized. This option is particularly important when running CAD/CAM applications, for example.

In the lower section, you specify the maximum number of hours users are allowed to delay encryption. A value of up to 9000 hrs. is possible here. You also specify how long the delay notification is displayed to the user. Once this time has expired and the user has taken no action on their client computer, the encryption will start automatically. The same applies if no user is logged in.

Note: As soon as the user receives the delay notification, encryption will start and the protectors will be created automatically. Immediately after that, encryption is paused and then resumes once the user clicks Encrypt in the notification or the delay time expires (without user interaction). Then encryption continues. The system is already protected at that point, and the user must enter a password (or PIN in the case of TPM) when rebooting.

Properties					?	×
General Re	ecovery	Execution options				
Start end	ryption o	nly in the following e	vents:			
when	the scre	en saver is configure	d and acti	ve		
✓ when	no users	are logged in				
outsid	de the tim	es specified in Wind	ows Focus	assist		
when	no appli	cation is running in fu	ill screen n	node		
Users ca	n delay ti	he encryption by a m	aximum of	12	hou	urs.
A corres	ponding r	notification appears f	or 2	mir	nutes; aft	er
this time	the encry	ption process starts	immediatel	у.		
		ОК	C	ancel	Ap	ply

#### **1.2.1.4 Pre-boot authentication settings**

#### 1.2.1.4.1 The Authentication type tab

Your choice of pre-boot authentication type (PBA) differs depending on whether the computers whose hard disks you want to encrypt contain a Trusted Platform Module (TPM) or not.

In the example below, the BitLocker pre-boot authentication is explicitly used. For information about DriveLock pre-boot authentication for BitLocker, refer to the corresponding chapter.

#### The following options are available on the Authentication type tab:

Properties					?	×		
Appearance	Use	r synchronization	Users	s	User-v	vipe		
Emergency log	on	Self-wipe	Netwo	rk pre-bo	oot (UE	FI)		
Authentication type Password options Logon methods								
Pre-boot authentic	ation typ	e				_		
O No pre-boot au	thentica	tion						
BitLocker requ computers. On additional auth	ires an a ly the sy enticatio	ictive Trusted Platfo stem partition will b on required to boot t	orm Module e encrypted the comput	e (TPM) d d, there is er.	on all s no			
BitLocker pre-b	oot auth	entication 📒						
The BitLocker password is required to boot the client computer. All users of this computer must use this password to log in. A recovery key is provided in case of emergencies.								
O DriveLock pre-	boot aut	hentication 🔀						
User authentic authenticate th authentication	ation is r ne user, t can be i	equired to boot the the user name and used. All emergence	client com password o y logon me	puter. To or 2-facto thods are	o or e availa	able.		
The BitLocker PBA is used instead of the DriveLock PBA when there is a BIOS system in place and/or no DriveLock PBA license available.								
Global options								
<ul> <li>Automatically unlock all data partitions</li> <li>Mitigate TPM security to eliminate repeated entry of a recovery key (e.g. in connection with a docking station)</li> </ul>								
		ОК	Canc	el	Ap	ply		

- 1. Select the first option No pre-boot authentication,
  - if there is a TPM built in on the hard disks you want to encrypt. In this case, an additional authentication when booting the computer is not required.



Mote: The protector DriveLock uses is called **TPM only**.

- Here, BitLocker accesses a TPM which has to be activated first in BIOS.
- If you chose this option, you can close the dialog and continue because you do not need to specify a password on the next tab.
- 2. Select the second option BitLocker pre-boot authentication (see figure),
  - if there is no TPM built in on the hard disks you want to encrypt or if you are not sure whether it is active.
  - In this case, DriveLock uses the original Windows BitLocker PBA.
  - Open the **Password options** tab to specify a password or to select one of the other options.
- 3. In both cases, we recommend checking the **Automatically unlock all data par-titions** check box. With this option set, both the system partition and all data partitions are unlocked after authentication on the computers you assign the BitLocker policy to.
  - Note: Unlike Microsoft, DriveLock unlocks the data partitions automatically for all users of a computer. The unlocking process by DriveLock BitLocker Management works independently of the Windows Bitlocker functionality; this means, for example, that the call manage-bde -status still returns "Automatic Unlock: Disabled" for drives that DriveLock unlocks.
- 4. The **Mitigate TPM security** ... option can be used to customize the TPM platform validation. The option is useful, for example, when BitLocker-encrypted laptops keep requesting the recovery key whenever the laptop is not connected to its docking station. The new option affects all types of pre-boot authentication, as DriveLock uses TPM-based protection mechanisms where TPM is available (TPM only, TPM/PIN, TPM/StartupKey). The option is disabled by default.

#### **1.2.1.4.2 The Password options tab**

There are different options available:

Note: The options on this tab are only available if you have selected BitLocker pre-boot authentication the authentication type.

In this case, none of the other tabs are active, because the options on these tabs refer exclusively to the authentication type **DriveLock pre-boot authen-tication**.

Properties					?	$\times$
Appearance	Use	er synchronization	Users	s	User-v	vipe
Emergency log	on	Self-wipe	Netwo	rk pre-b	oot (UE	FI)
Authentication	Logo	on metho	ods			
Valid for: == BitL BitLocker passwo Password Confirm User cannot Vser must ch	ocker p rd: change nange p	e password	on			
Password mu Allow onl Allow nur Minimum pass A valid pass 1 1 Treat	ust meet y numbe sword k word mu lower c upper c numbers	t the following requirers and Latin based char ength 8 ist contain at least case letters 1 case letters 1 s as special charact	ements: acters charactur numl specers	ers bers sial char	acters	
		ОК	Cano	el	Ap	ply

- 1. You specify a **BitLocker password** and select none of the other options in the in the top part of the dialog:
  - The encryption process starts when you activate it and/or assign the policy. The user of the client computer is allowed to change the password later or continues to use the password you specified.



Note: Please note that you are responsible for communicating the password to the users over a secure channel.

- 2. You check the **User cannot change password** box:
  - Please specify a fixed password which the user can never change. The initial encryption process starts automatically even without the user being logged on to the client computer, after you activate it and/or assign the policy.
  - As soon as the user starts the computer, the BitLocker password must be entered to unlock the encrypted hard disks.

Note: Please provide users with the appropriate password information over a secure channel.

- The password is entered independently of the encryption progress, i.e. as soon as encryption is started, the BitLocker password must be entered in the PBA.
- 3. You check the **User must change password** option (see figure):
  - The user can specify a password, you do not enter a password here.
  - If required, you can define the requirements the user password must meet.
  - The encryption process starts as soon as the user specifies the password.
  - The password may be changed later.

The options below **Password must meet the following requirements:** provide precise criteria that a password assigned by the user must meet. The option is selected by default.

1. You can select the **Allow numbers only** option if all client computers are equipped with a TPM which means that 6 characters are allowed.

Warning: If there is no TPM on client computers or non-system partitions need to be encrypted as well, the default is still at least 8 characters. (Microsoft default for passwords on data partitions).

- The Allow numbers and Latin based characters option restricts the usage of allowed characters. Special characters can no longer be used with this setting.
   Please note the information in the BitLocker pre-boot authentication chapter.
- 3. With the A valid password must contain at least... options you define the



number of letters, numbers and special characters:

- The password may be between 8 and 20 characters long. A number below 8 or higher than 20 leads to an error message.
- Define the minimum requirements (number of letters, number, special characters etc.).
- If you select the **Treat numbers as special characters** option, numbers count as numbers and also as special characters. Please make sure that the numbers and special characters correspond.

If you want to set individual passwords for individual client computers, you can do so in the DriveLock Control Center. Here you can also monitor the encryption progress. Please refer to BitLocker Management in the DriveLock Control Center (DCC) for more information.

#### 1.2.2 Decryption

Decryption is triggered with a single setting that is specified in the **Harddisk encryption settings** on the **General** tab.

You can monitor the decryption process (same as the encryption process) in the DriveLock Control Center (DCC), see below:

5	Verschlüsselte Festplatten Verschlüsselte Festplatten: Verschlüsselte Festplatten - DriveLock Control Center 7.9. 1. 21488								×				
Start	Aktionen	Einstellun	gen										?
(J) Neu laden	Spalten	<b>↓</b> Sortieren	Gruppieren	Suche	Filter	Computersp	ezifisches Benutzerde	îniertes					
Allcomoin	- For	Tieren / Cru	T	Suchan /	Filtern	BitLocker Ke	nnwort • BitLocker-Ke	nnwort					
Aligement	scelte Festo	latten: Vers	blüccelte Fe	stolatten V			Computer						
versenius	ssente i esip	atten. verst	and a server re										
Ziehen Sie ein	ne Spaltenüb	perschrift in	diesen Berei	ch, um nach die	eser zu grupp	pieren							
ComputerNam	ne Zeitster	npel	Laufwer	Label	Größe	Algorythm	nus Verschlüsselter Ant	eil Status	Methode \	/ersion	Protektoren		
	27.11.2	2018 10:41:0	08 C:	System	39,8 G	B XTS AES 2	256 27 %	Wird entschlüsselt	BitLocker	10.0.17134.319	TPM and PIN, Recovery	Key	
MLO-1803-BL	27.11.2	2018 10:37:3	84 E:	BitLockerNat	tive 9,98 G	B XTS AES 1	128 100 %	Verschlüsselt	BitLocker :	10.0.17134.319	Passphrase, Recovery K	≥y	
	27.11.2	2018 10:40:3	88 D:	Data	19,5 G	в -	0 %	Entschlüsselt	-				
MLO-WIN7-BL	L 27.11.2	2018 10:40:5	60 C:		59,6 G	B AES 256	57 %	Wird entschlüsselt	BitLocker 6	5.1.7600.16385	TPM and PIN, Recovery	Key	
<						٢ >							
Verschlüsselte Festplatten: 4 🚦 DLSE Vadministrator 🚦 DLSERVER. DLSE. local 🦼													
verschlusseite	erestplattel	n: 4								DLSE\Adminis	strator 📄 DLSERVER.	DLSE.loca	al _:
verschlusselte	er esipiattei	1: 4								DLSE\Adminis	strator 🧮 DLSERVER.	OLSE.loca	al <sub>.e</sub> :
o la	Encrypted	n: 4 Disks				Encrypted [	Disks: Encrypted Disks - Dr	iveLock Control Center 7	7.9.1.21488	DLSE\Adminis	strator 📕 DLSERVER.	-	ند. <sup>اه</sup> ×
Start A	Encrypted I	n: 4 Disks Options				Encrypted [	Disks: Encrypted Disks - Dr	iveLock Control Center 7	7.9.1.21488	DLSE \Adminis	strator 📓 DLSERVER.	- 🗆	Ie × ?
Start A	Encrypted I Actions (	Disks Options		<b>Y</b>		Encrypted [	Disks: Encrypted Disks - Dr	iveLock Control Center 7	7.9.1.21488	DLSE \Adminis	strator 📕 DLSERVER.	- 🗆	⊪. <sup>I</sup> i × ?
Start A Refresh	Encrypted Actions	Disks Options	p Find	Filter B	Computer -sp itLocker pass	Encrypted [ becific l	Disks: Encrypted Disks - Dr	iveLock Control Center 7	7.9.1.21488	DLSE \Adminis	strator 📕 DLSERVER.	- 🗆	:. It × ?
Start A Refresh General	Encrypted I Actions ( Columns Sort	Disks Options U 2 Sort Grou / Group	p Find Find	Filter / Filter	Computer-sp itLocker pass	Encrypted [ becific l word + BitL Computer	Disks: Encrypted Disks - Dr The Disks - Dr Disks - Dr User-defined ocker password	iveLock Control Center 7	7.9.1.21488	DLSE \Admini:	strator 📕 DLSERVER.	- 🗆	⊧. <sup>∣</sup> ⊧ × ©
Start A Refresh General	Encrypted I Actions ( Columns Sort	Disks Dptions U A Sort Group / Group pted Disks	p Find Find	Filter /Filter	Computer-sp itLocker pass	Encrypted [ becific t word + BitL Computer	Disks: Encrypted Disks - Dr	iveLock Control Center 7	7.9.1.21488	DLSE (Adminis	strator 📕 DLSERVER.	- 🗆	: la × ?
Start A Start A Refresh General Drag a column	Encrypted Actions Columns Sort i Disks: Encry	Disks Diptions U 2 Group / Group / Jeted Disks to group by	p Find Find X	Filter Filter / Filter	Computer-sp itLocker pass	Encrypted [ becific l word * BitL Computer	Disks: Encrypted Disks - Dr	iveLock Control Center 7	7.9.1.21488	DLSE (Adminis	strator DLSERVER.	- D	al .: × ?
Start A Start A Start A Refresh General Orag a column ComputerName	Encrypted I Actions ( Columns Sort : Hoisks: Encry header here e   Timestam	Disks Diptions U 2 (Group / Group / Group ppted Disks to group by	p Find Find Find Tind DriveLetter	Filter / Filter Label	Computer-sp (Locker pass	Encrypted [ beafic t word + BitL Computer	Disks: Encrypted Disks - Dr	iveLock Control Center 7	7.9.1.21488	DLSE (Adminis	Protectors	- 🗆	al .: × ! ?
Start A Start A Start A Refresh General Drag a column ComputerName	Encrypted I Actions Columns Sort I Disks: Encry header here Timestam 27, 11, 20:	Disks Diptions U22 Sort Grou / Group pted Disks to group by p 18 10:41:08	p Find Find Find Tind Tind C:	Filter Filter / Filter Label System	Computer-sp (Locker pass	Encrypted [ bedfic t word * BitL Computer Ngorithm 1 TS AES 256	Disks: Encrypted Disks - Dr	iveLock Control Center 7	7.9.1.21488	DLSE\Adminis	Protectors 9 TPM and PIN, Recover	-	× ?
Start A Start A Refresh General Drag a column ComputerName MLO-1803-BL	Encrypted I Actions Columns Sort I Disks: Encry header here e Timestam 27.11.20 27.11.20	Disks Diptions Sort Group / Group pted Disks to group by p P Ba 10:41:08 Ba 10:37:34	p Find Find X DriveLetter C: E:	Filter Filter / Filter Label System BitLockerNative	Computer-sp itLocker pass	Encrypted I becific I word * BitL Computer Igorithm 1 TS AES 256 TS AES 256	Disks: Encrypted Disks - Dr	iveLock Control Center 7 State Decryption In Progress Fully Encrypted	Method BitLock	DLSE\Adminis	Protectors PTM and PIN, Recovery Passphrase, Recovery	-	× × • ?
Start A Start A Refresh General General Orag a column ComputerName MLO-1803-BL	Encrypted I Actions Columns Sort I Disks: Encry header here e Timestam 27.11.20 27.11.20 27.11.20	Disks Diptions Sort Group / Group pted Disks to group by p 18 10:41:08 18 10:37:34	p Find Find X DriveLetter C: E: D:	Filter Filter /Filter Label System BitLockerNative Data	Computer-sp itLocker pass 99,8 GB X 9,98 GB X 19,5 GB -	Encrypted I becific I word * BitL Computer Igorithm I TS AES 256 TS AES 128	Disks: Encrypted Disks - Dr	State Decryption In Progress Fully Encrypted Fully Decrypted	Methoc BitLock	DLSE\Adminis	Protectors Passphrase, Recovery Passphrase, Recover	-	<u>, le</u> × •
Start A Start A Refresh General General Orag a column ComputerName MLO-1803-BL MLO-WIN7-BL	Encrypted I Actions Columns Sort I Disks: Encry header here e Timestam 27.11.20 27.11.20 27.11.20	Disks Diptions Sort Group / Group ppted Disks to group by p 18 10:41:08 18 10:40:38 18 10:40:50	p Find Find X DriveLetter C: E: D: C:	/Filter /Filter Label System BitLockerNative Data	Disk size A 39,8 GB X 19,5 GB X 19,5 GB A	Encrypted I becific I word * BitL Computer Igorithm I TS AES 256 TS AES 128 ES 256	Disks: Encrypted Disks - Dr	State Decryption In Progress Fully Encrypted Fully Decrypted Decryption In Progress	Methoc BitLock BitLock BitLock	DLSE\Adminis	Protectors	-	њ <sup>I</sup> ер
Start A Start A Start A Refresh General Drag a column ComputerName MLO-1803-BL MLO-WIN7-BL	Encrypted Actions Columns Sort I Disks: Encry header here e Timestam 27.11.20 27.11.20 27.11.20	Disks Deptions Sort Grou / Group pted Disks to group by p 18 10:41:08 18 10:40:50	p Find Find Find C: E: D: C:	Filter Filter / Filter Label System BitLockerNative Data	Computer-sp (tLocker pass 39,8 GB X 9,98 GB X 19,5 GB A 59,6 GB A	Encrypted I becific U word * BitL Computer Ugorithm I TS AES 256 TS AES 128 ES 256	Disks: Encrypted Disks - Dr	State Decryption In Progress Fully Encrypted Fully Decrypted Decryption In Progress	Method BitLock BitLock	DLSE (Adminis Version er 10.0.17134.33 er 10.0.17134.33 er 6.1.7600.1638	Protectors PTPM and PIN, Recovery TPM and PIN, Recovery PTPM and PIN, Recovery	-	±. Ie
Start A Start A Refresh General General ComputerName MLO-1803-BL MLO-WIN7-BL	Encrypted I Actions Columns Columns Sort I Disks: Encry header here e Timestam 27.11.20 27.11.20 27.11.20	Disks Doptions Sort Group rpted Disks to group by p 18 10:41:08 18 10:40:50	p Find Find Find Find Find Find Find C: C:	Filter Filter Jabel System BitLockerNative Data	Computer-sp itLocker pass 39,8 GB X 9,98 GB X 19,5 GB A 59,6 GB A	Encrypted I bedfic I word * BitL Computer IS AES 256 TS AES 128 AES 256	Disks: Encrypted Disks - Dr	State Decryption In Progress Fully Encrypted Fully Decrypted Decryption In Progress	Methor BitLock BitLock	DLSE\Adminis	Protectors	-	<u>ن</u> اد ج ۲

The Event report (BitLocker events) also provides information on the decryption/encryption of individual computers.

#### 1.2.2.1 Decrypting encrypted drives

#### To start decrypting encrypted drives, proceed as follows:

- 1. Open the respective BitLocker policy.
- 2. Open the General tab in the Harddisk encryption settings dialog.



3. Uncheck the Encrypt local hard disks on Agent computers option.



4. Set a value for the **Delay decryption by** *x* days setting. The default value is **3**, which means that decryption starts after 3 days. Depending on the value you enter, the decryption will be delayed by x days.

Note: In order to start the encryption process immediately, enter the value 0 here.

- 5. **Do not decrypt** is the default setting, which is intended to prevent unwanted decryption. It is deactivated as soon as you enter a value for the delay.
- 6. Click **OK** to confirm your settings.
- 7. The following message appears in the status bar of the client computer that is being decrypted.





#### 1.2.3 Override policy settings (BitLocker)

To disable specific encryption settings on individual client computers, you can override the respective policy settings.

Warning: Note that the policy settings will not be re-enabled until you undo the reconfiguration.

Please do the following:

- 1. Open the **Agent remote control** in the **Operating** node of the DriveLock Management Console.
- 2. Select the DriveLock Agent you want to change the policy settings for.
- 3. From the context menu, select the menu item **Disk encryption properties...**.

Note: Please note that a connection between DES and DriveLock Agent must exist to display the encryption properties.

- 4. On the **General** tab you can see information about DriveLock Agent encryption. Click the **Reconfigure agent...** button.
- If you select the Override policy settings option and keep the Override general deployment settings option checked (default), the DriveLock Agent will be decrypted immediately and BitLocker will be disabled (see figure below).



_	<u>^</u>		1					
CriveLock	Remote computer	Logged-on user	Last contact	D	riveLock Versi	Agent configuration	Comment	
Device Scanner	DLCLIENT01	DLSE\User1	29.04.2020 16:58:45	20	0.1.0	Zentral gespeichert		
Groups				_		2.1		
✓ Policies Encr	yption Properties		? >	<	Reconfigure B	itLocker Management		×
Centrally stored policies								
Computer-specific policy cus	ieral Users				You can overrid	de BitLocker Management	settings in your comp	any policy on
🕞 Active Directory / Local comp 🛛 Dis	c encryption status	Encryption in progres	s		is applied to the	e agent computer.	area nere with the con	nparty policy triat
Configuration files		Pre-boot authenticati	on not active					
Policy assignments Inst	alled Version	20.1.0.28328			✓ Override po	licy settings	$\sim$	
> E DriveLock Enterprise Services [dls Red	coverv kev status	Envelope: Not create	ed		✓ Ovemde	general deployment settin	gs	
> P DriveLock Cloud	,,	Key backup: Not cre	ated			ypt local hard disks		
> 🚳 DriveLock File Protection 🛛 🛛 Mar	nual reconfiguration	Not active				o not decrypt in case of c	onfiguration changes	
✓ ₿ Operating	j				Pre-boot aut	thentication settings		
🚡 Agent remote control					Pre-b	oot authentication type		
Retwork pre-boot computers Tru	sted Platform Module	Not present			0 N/	n pre-boot authentication		
Shadowed files	e encryption status					t ocker Pre-Root Authenti	eation	
D	rive Size	Encryption state	Protection			ivel ook Pre-Root Authent	ication	
	C 244GB	Not encounted			0.01	IVELUCK THE-DOUL AULITERI	ication	
	0. 24,400	Not choryptou			Override	authentication methods		
							Windows	Preboot
					Local us	eraccess		
					Domain	user access (with passwor	d) 📃	
< .					Domain	user access (with token)	····· 🛄 ·····	
					Enab	le logon using "password	tokens"	
	Re-uplo	ad recovery keys	Reconfigure agent			lequire token PIN on Wind	lows logon	
					Override	emergency access metho	ds	
			OK Cancel		Allow	emergency logon with us	ername	
	1				S	ingle Sign-on after emerge	ency logon	
					Allow	emergency logon without	user name	
					Allow	emergency logon for toke	en users	
							ОК	Cancel

- 6. By checking the **Encrypt local hard disks** option, the encryption settings from the policy (e.g. algorithm or fast encryption) are applied.
- 7. If you select the **Do not decrypt in case of configuration changes** option, the corresponding policy option (Do not decrypt) is overwritten.
- 8. If you click **OK** now, your settings will be applied to the selected client computer with immediate effect.

#### 1.3 Sample configuration

Please find below a sample configuration for encryption involving the user entering a password on the client computer.

To quickly and easily encrypt the drives on your client computers, follow the instructions below in the specified order.

This sample process starts with the licensing of DriveLock BitLocker Management and ends with the encryption of the drives on the client computers.

Mote: For more information on the individual steps, see the cross-references.

- Create a new policy or use an existing one. In this document, the policy is referred to as the 'BitLocker Policy'.
- 2. Enter the appropriate licenses in the policy and license all computers.
- 3. In the policy, open the **Encryption** node and select **Hard disk encryption** in the **BitLocker Management** sub-node. Read more here.
- 4. First, create the encryption certificates.
- 5. Open the Deployment settings and specify the notifications you want the user to get.
- 6. Next, specify the Pre-boot authentication settings.
  - On the Authentication type tab, select BitLocker pre-boot authentication. Check the Automatically unlock all data partitions box.
  - On the **Password options** tab, select the **User must change password** option and specify the complexity requirements you want for the password.

Apply your changes by clicking OK.

- 7. Specify the following in the Hard disk encryption settings:
  - Open the General tab.
    - 1. First of all, check the **Encrypt local hard disks on Agent computers** option.
    - 2. Then set the entry **AES-XTS (256 bit key length)** to the highest position in the encryption algorithm priority.
    - 3. Optionally check the **Configure encryption settings per drive** box and select the encryption algorithm mentioned above for the drives C: and the



expected data drives via the **Settings** button. You can also specify **Not encrypted** if you do not require encryption.

- 4. Click **OK** to close the dialog.
- 5. In the Initial encryption section, check the **Encrypt only used disk space** (fast initial encryption) option; in the Initial protection section, select '0' for the number of days the decryption will be delayed.
- Next, open the Recovery tab and select the first option DriveLock Enterprise Service.

Click **OK** to close the dialog.

- 8. Save and publish the policy.
- 9. Your settings will be activated the next time the client computer's configuration is updated.
- 10. Depending on the setting, the hard disk encryption is executed immediately on the client computers or after the user enters the password.
  - Note: For more information on installing the DriveLock Agent or on policy management in general, please refer to the DriveLock Installation or Administration Guide at https://drivelock.help/.

#### 1.4 Recovery

#### **1.4.1 Recovering encrypted hard disks**

If users can no longer access their hard disk (system partition) encrypted with BitLocker Management, for example because they have forgotten their BitLocker password, the recovery certificate and the associated private key must be used to provide access.

Note: The upload of the recovery data starts when all drives that are needed for encryption have begun encrypting.

In this case, please start the recovery process. For this purpose, DriveLock offers you two possibilities:

1. In the **DriveLock Control Center**, open **HelpDesk** and click the **BitLocker recovery** button.(see figure).



	DriveLock Control Center 7.9.1.21488	- 🗆 ×
Start		
Overview	Helpdesk Open Helpdesk views to see the state of the Agents, or use the operating buttons to solve problems direct.	DLSE\Administrator
E Helpdesk	Temporarily unlock agents Temporarily unlock agents Temporarily unlock agents Temporarily unlock agents	]
Statistic report	Image: Construction of the protection recovery     Image: Construction of the protection recovery     Image: Construction of the protection recovery       Image: Construction of the protection recovery     Image: Construction of the protection recovery     Image: Construction of the protection recovery	J
Event report	Unlock Terminal Service drives Create volume identification file Disk Protection recovery tools	
b Forensic	Recently used Entities	
inventory	Leipdesk Encrypted Disks	
Plug-in		
Settings	Disk Protection Helpdesk	
About		

2. In the **DriveLock Management Console**, select the **Operating** node and open the context menu for **Agent remote control** to select the **BitLocker Management recovery** menu item (see figure).

🦪 DriveLock - [DriveLock\Operating\Agent r	emote control]				
File Action View Help					
🗢 🔿 🙍 🗐 🕼					
<ul> <li>DriveLock</li> <li>Device Scanner</li> <li>Product updates and support</li> <li>Policies         <ul> <li>Centrally stored policies</li> <li>Computer-specific policy customiz</li> <li>Active Directory / Local computer p</li> <li>Configuration files</li> <li>Policy assignments</li> <li>DriveLock Enterprise Services [dlserver]t</li> <li>DriveLock Cloud</li> <li>OpriveLock File Protection</li> <li>Operating</li> </ul> </li> </ul>	Remote computer	Logged-on user DLSE\User1	Last contact 28.09.2018 07:53:57 27.08.2018 14:18:10 25.10.2018 14:15:06	DriveLock Versi 7.8.1.19933 7.9.21166	Agent configuration
🚡 Agent remote control					
Network preb Connect					
Shadowed file Temporary unloss	ock	>			
Encryption reco	overy	>			
BitLocker Mana	gement recovery	>	BitLocker Manageme	nt recovery / emerg	ency logon
DriveLock Disk	Protection recovery and	tools >			
Additional help	desk tools	>			
All Tasks		>			
View		>			
Refresh					
Export List					
Properties					
Help					

In both cases, the Recovery Wizard will open and guide you through the steps.



#### 1.4.2 Recovery process

To recover access to an encrypted hard disk, Please do the following::

- 1. Open the Disk Recovery wizard either from the DriveLock Control Center or the DriveLock Management Console.
- 2. In the first dialog, select the **BitLocker recovery key** option.

Disk Recovery	×
Recovery type and source Select the type of recovery to perform and the source of recovery information.	
Select the type of recovery to be performed: C Emergency logon Use this option when a user needs to log on and does not have a password for the Pre-Boot Authentication or forgot the password. BitLocker recovery key Use this option if a computer with an encrypted hard disk does not start and you need to recover data from the hard disk. Recovery information is retrieved from: C Recovery files (copied from the client computer) DriveLock Enterprise Service	
< <u>B</u> ack <u>N</u> ext > C	ancel

Note: For information on emergency logon to the DriveLock PBA, refer to the corresponding chapter.

#### Select where the **recovery information is retrieved from:**.

Note: Which option you select, depends on your settings in the encryption settings dialog. We recommend the DriveLock Enterprise Service option.

3. In the next dialog, select the location of the certificate and/or private key (\*.PFX file).



Disk Recovery X
Certificate private key file Select the required certificate private key file and password.
Encryption certificates and private keys are needed for BitLocker Management recovery. Please specify where certificates and private keys are stored.
O Windows certificate storage
◯ Smart card
File system (PFX files)
Data recovery certificate private key file (PFX)
Private key file password
< <u>B</u> ack <u>N</u> ext > Cancel

You can also access the information stored in the Windows Certificate Store.

Note: If you specified earlier in the encryption settings dialog that the recovery information resides in the file system, please enter the matching password for the private key here.

- 4. Next, select the client computer that needs recovery from the list. Use a filter, if required.
- 5. Continue by requesting a recovery key in the next dialog.

Mote: The challenge-response feature will be fully available in the next version.

- 6. Wait a moment while DriveLock retrieves the recovery information.
- 7. The next dialog issues the recovery key.

Mote: Select the drive defined as system partition on the client computer.



Disk Recovery	×
Creating recovery information Creating recovery information	
The recovery data was retrieved successfully. Please forward the data retrieved to the end user or use the key directly.	
Drive to be recovered: C ~ Recovery key 304117-478742-036190-637087-061743-	]
423313-076505-639540	
< <u>B</u> ack Finish	Cancel

8. Provide the user with the recovery key.

Note: Please note that you are responsible for communicating the recovery key to the users over a secure channel.

9. Last, the user enters this key in the **BitLocker recovery** dialog when starting the client computer.


BitLocker recovery
Enter the recovery key for this drive
137313-565466-109802-034243-223377-384714-547921-146223
For more information on how to retrieve this key, go to http://windows.microsoft.com/recoverykeyfaq from another PC or mobile device.
Use the number keys or function keys FI-F10 (use FIO for 0).
Recovery key ID: E3279388-A77E-4842-8835-29AE5D944618
Press Enter to continue Press Esc for more recovery options

- Note: Note that this recovery key represents a major security risk. For this reason, BitLocker Management immediately initiates a password change by the user and replaces the recovery key with a new one.
- 10. The Change BitLocker Password wizard starts on the client computer and the user must specify a new password.





11. As soon as this is done, the user can enter this password when starting up the client computer.

### **1.5 Taking over native BitLocker**

### **1.5.1 Integrating existing BitLocker environments**

It is now simple to include hard disks and data drives from client computers that have already been encrypted in advance with native BitLocker into DriveLock BitLocker Management. DriveLock BitLocker Management allows you to control encryption and decryption from a central point without having to deal with the encryption state of individual client computers.

Enable the **Manage existing BitLocker environment** option in your BitLocker policy to specify that DriveLock can start the integration. By assigning the policy to the respective client computers, BitLocker Management is activated.

Note: If you do not enable this option and there are drives in your environment that have been encrypted with BitLocker before, DriveLock ignores these drives. They remain encrypted but cannot be managed with DriveLock BitLocker Management.

System drives differ from data drives:

• **System drives:** DriveLock automatically takes over system drives that have been encrypted before with native BitLocker; they do not necessarily have to be re-

encrypted. In the background, DriveLock adapts the algorithms and exchanges protectors (even External keys are deleted and re-created). If the encryption algorithms match, this is a very quick process; if they do not match, DriveLock re-encrypts the drives. Depending on the system and partition size, this may take a longer time. Since users unlock the system drive directly by logging on to the system or entering their BitLocker password, no further action is required from the user.

 Data drives: Data drives are neither unlocked nor integrated in DriveLock BitLocker Management automatically. Users will have to take action here: A wizard pops up on the client computer where the user selects the partitions that need to be unlocked. Then, the user enters the original BitLocker password and specifies a new one. Note that a password entry is only required if the User must change password option has been enabled in the Password options dialog before. However, if this option is not selected and a password is preset, make sure to let the users know. In this case, a password change is not required; the users simply select the drives that need to be unlocked and enter their original BitLocker password.

**Recovery keys:** DriveLock BitLocker Management creates new recovery keys when it integrates the native BitLocker environments.

**Encryption algorithms:** If you adhere to the Windows default settings for encryption algorithms, DriveLock BitLocker Management can take over native BitLocker environments easily and quickly.

### 1.5.2 Additional modifications of BitLocker policies

You will need to modify an existing BitLocker policy in the following cases:

- if the client computers the existing BitLocker policy is assigned to have changed (e.g. drive changes) or
- if the settings for encryption or decryption have changed, or
- if you upgrade your DriveLock agents to a higher version. For more information about updating the DriveLock Agent, refer to the Release Notes.

The encryption behavior changes depending on the setting in the respective policy.

Mote: Policy changes are applied in the next configuration update.

These are the different scenarios:



### Re-encrypt already encrypted partitions

If the encryption algorithm is changed in the policy, the system will decrypt the partition first and then immediately encrypt it again using the newly set algorithm. For example, if you had specified the algorithm AES 128 bit key length and changes it to AES-XTS 128 bit key length, encryption restarts.

• Exchange protectors of already encrypted partitions without new encryption If the encryption algorithm already corresponds to the algorithm specified in the policy, this approach is followed.

There are two possible reasons for such a behavior:

- In the first case, a change from TPM/PIN to TPM (and vice versa) leads to the exchange of protectors.
- In the second case, DriveLock is to integrate existing BitLocker partitions that have already been encrypted with the algorithm specified in the policy.

### • Decrypting partitions

Decryption is always triggered if either

- the Encrypt local hard disks on agent computers option has been unchecked or
- a drive is set to not encrypted in the Configure encryption settings per drive option, or
- the **Bitlocker Management** option is disabled in the License Options under **Licensed Computers**.

# • Encrypt newly added partitions

The encryption should always be triggered when new hardware or a new drive are added (in the **Configure encryption settings per drive** option). By doing so, you ensure that all data on new computers and drives is protected by BitLocker.

# 1.6 DriveLock Agent

### **1.6.1 BitLocker pre-boot authentication**

Please note that **an English keyboard layout** may be enabled when logging on to the BitLocker PreBootAuthentication (see figure below). Use the INSERT key to display the entered password if in doubt.

Warning: Please inform the users of this information and point out that special characters on an EN-US keyboard are occupied by other key combinations and that Y and Z are interchanged.



# 1.6.2 BitLocker Management on client computers (DriveLock Agent)

When your BitLocker policy is assigned to the appropriate client computers, disk encryption is initiated. Depending on the settings you specified in the Pre-Boot authentication settings dialog, encryption starts with or without the user having to enter a password.

Mote: Please provide users with the appropriate password information.



The user may also redefine the password later. The **DriveLock Agent** on the client computer provides the **Change BitLocker password** button on the **Encryption** tab for this purpose.

<b>X</b> Drive <b>Lock</b>	
💮 Home 💧 Encryption 🔥 Status 🕐 Help	
******       Image: State of the state of t	

# **1.6.3 Encrypting client computers**

# On the client computers, the hard disk encryption and the corresponding password entry are carried out as follows:

- 1. In one case, the user starts the (unencrypted) client computer and logs on to Windows as usual. In the other case, the user is already logged in and the DriveLock Agent has just been assigned the new BitLocker policy.
- 2. Two options are available:
  - a. If you specified a set password, the encryption process starts automatically and immediately without the user's interaction (no password entry or definition required).

The user can only follow the encryption process in the status bar.



When the encryption process is finished, DriveLock issues the message described in item 5.

b. If the user must specify their own password, a wizard starts where the user defines an authentication password.

BitLocker encryption		Х
Ω	Authentication password	
	Your hard disk will be encrypted by Windows BitLocker. To log on to your computer a password is required.	
0	This wizard guides you through creating this password.	
OriveLock		
< <u>B</u> ack	Next > Cancel Help	

- 3. In case b. the user now assigns a password. The policy requirements are checked and only valid passwords are accepted.
- 4. As soon as the password has been defined and confirmed, the encryption process starts.
- 5. When this process is complete, the following notice appears on the user's screen:



BitLocker Disk	Protection	
	DriveLock BitLocker Management Installation	
DriveLock Bit	Locker Management has finished encrypting your hard disk.	
Continuing in	4:35	Close

6. The next time the client computer starts up, the user enters the BitLocker password as pre-boot authentication thus unlocking the encrypted system partition (and the data partitions, where applicable).

In case a. the client computer starts without the user having to enter a password.

### 1.6.3.1 Delay encryption

Users can delay the encryption by selecting the appropriate time in the notification (see figure). Depending on how many hours are specified as the maximum value on the Execution options tab, the user can specify the time until the dialog is displayed again in the **Delay by** dropdown list. Encryption is then delayed for that long. When the specified maximum time is used up, encryption starts. It also starts if the user does nothing while the dialog is displayed or clicks on **Encrypt**.



DriveLock	VE <b>Lock</b>				
Your computer will be	encrypted.		1000		à
Encryption may affect the encryption process (depending on your a To start encryption im	your compute is. Select a de dministrator's p mediately, clici	er perform lay time fr preference k the Enc	ance. om the es) and rypt bu	If required, yo dropdown lis d click Later. utton.	u can delay st
Start encryption in 4:53	Delay by	10min	~	Later	Encrypt

# 1.6.4 Integrating data partitions with existing BitLocker

There are two settings in the **Password options** of the BitLocker policy that determine how to unlock data partitions that have been encrypted with native BitLocker and that are to be integrated in DriveLock BitLocker Management:



#### or

• the BitLocker password is preset.

Pre-boot authenti	Pre-boot authentication settings Properties ? $\times$											
Authentication type	Authentication type Password options											
Valid for: 📒 BitLocker pre-boot authentication												
BitLocker passwo	BitLocker password:											
Password	Password ••••••											
Confirm	Confirm											
User cannot	User cannot change password User must change password											

Depending on the selected option, a different wizard opens on the client computer.



• One wizard prompts the user to change the password on the following dialog pages.



• The other wizard only contains information on how to integrate the native BitLocker environment:



The second wizard dialog is the same in both cases; here, you are asked to select the data partition you want to unlock.



Select the drive (or the drives) you want to unlock and enter the original BitLocker **password**. Then you can click **Next**.

Data partition: The followin BtLocker.	with native BitLocker a data partitions were already locked in adv	ance with
Before you can r unlocked. Select Bitlocker passwo	anage these partitions with DriveLock, the which partitions you want to unlock. Enter d and click 'Unlock'.	y must first be your native
Partition	State	
L.	Locked	
	2	
Password:		Unlock
		7.72 C 227975

If a new password is required, a further dialog appears where a new password must be assigned.

Complete the final dialog by clicking **Finish**.

Note: In the background, DriveLock BitLocker Management implements the integration by replacing protectors and taking over encryption algorithms.

# **1.7 DriveLock Control Center**

# **1.7.1 BitLocker Management in the DCC**

In the DriveLock Control Center's **Helpdesk** view, click **Encrypted Disks** to view all computers with encrypted and/or decrypted hard drives.

5	Encry	ted Disks	Encrypted Disks: EncryptedDisks - DriveLock Control Center 2019.1 (19.1.0.22197)											-		×
Start	Actions	Options														?
<b>(5</b> )		₽		60	Y			-								
Refresh	Column	s Sort	Group	p Find	Filter	Comp BitLock	puter-spec er passwo	tific User-define ord * BitLocker pass	ed word							
General		Sort / Group		Find	Find / Filter Computer											
P Helpdesk: Helpdesk 😽 Encrypted Disks: EncryptedDisks 🗴																
Drag a column header here to group by that column																
Computer	🔺 Time	stamp		DriveLetter	Label		Disk size	Algorithm	Percentage of en	State	Managed by	Version	Protectors			
CERTTEST	17.1	2.2018 15:56	5:46	C:			59,4 GB	XTS AES 256	100 %	Fully Encrypted	DriveLock BitLocker	10.0.15063.0	Passphrase, Recovery Key			^
	04.1	2.2018 15:5	3:58	C:			24,4 GB	XTS AES 256	100 %	Fully Encrypted	DriveLock BitLocker	10.0.14393.0	Passphrase, Recovery Key			
	04.1	2.2018 08:3	3:19	E:	FAT32_E		2,92 GB	-	0 %	Fully Decrypted	-					
DLCLIENT01	04.1	2.2018 08:3	3:19	F:	FAT32_F		2,92 GB	-	0 %	Fully Decrypted	-					
	04.1	2.2018 08:3	3:19	G:	NTFS_G		6,30 GB	-	0 %	Fully Decrypted	-					
	04.1	2.2018 15:5	2:57	D:	NTFS_D		2,92 GB	XTS AES 128	100 %	Fully Encrypted	DriveLock BitLocker	10.0.14393.0	Passphrase, Recovery Key			
<															3	Þ
Encrypted D	Encrypted Disks: 44 🔮 DLSE\Administrator 🛼 root 💈 DLSERVER.D												ER.DLS	E.loca		

The following information, among others, is displayed here:

- **Algorithm**: this column shows the algorithm used to encrypt the respective drive and which you set in the **Harddisk encryption settings** dialog.
- **Percentage of encryption**: if the drive is completely encrypted, the percentage shows 100%. During the encryption or decryption process, you can see how much of the data is encrypted in percent.
- State of encryption with the following values:
  - Fully Decrypted: the drive is decrypted. The data is not protected.
  - Fully Encrypted: the drive is encrypted.
  - **Encryption In Progress**: the drive is currently being encrypted. See how much of the drive is already encrypted in the Percentage of encryption column.
  - **Decryption In Progress**: the drive is currently being decrypted. The percentage refers to the portion that is still encrypted.
  - Locked: This state shows that a drive has already been encrypted with native BitLocker before being managed with DriveLock BitLocker Management (i.e. before the installation of the DriveLock Agent and before assigning a BitLocker policy).

Please find more information in the topic Integrating existing BitLocker environments.

• Managed by shows whether DriveLock is already managing the encryption or still

native BitLocker.

- DriveLock BitLocker: DriveLock BitLocker Management is already managing the drive.
- **BitLocker**: Native BitLocker is still locking the drive (see above). The drive has to be unlocked so that it can be accessed by the DriveLock Agent, re-encrypted and managed by DriveLock BitLocker Management.

Protectors:

- **Passphrase**: If the Trusted Platform Module (TPM) is missing or not enabled on the computer, a passphrase can be used for authentication. Users must enter this passphrase each time they start their computer in the Windows pre-boot environment.
- **Recovery Key** (also Numerical Password): The recovery key is always used as a protector for encryption.
  - Note: Microsoft uses two protectors by default for the original encryption of a system or data partition with BitLocker. These are either TPM, TPM and PIN or Passphrase and Numerical Password.
- **TPM**: This protector only works on drives with a built-in TPM ('TPM only'). Entering a PIN (BitLocker password) is not required.
- **TPM and PIN**: A built-in TPM is also required in this case. Here the TPM and a PIN (BitLocker password) are used for authentication. Users must enter this password each time they start their computer in the Windows pre-boot environment.
- External Key: DriveLock uses this protector if the auto-unlock option is specified for the drive (Automatically unlock all data partitions in the Authentication type dialog).
  - Note: DriveLock also provides the recovery key for data partitions. Even without the auto-unlock option, this external key allows you to access a data partition that is not protected with a password. This ensures that data partitions can also be unlocked using the recovery key, even if **TPM** is used as the protector.

### 1.7.1.1 Assigning a computer-specific BitLocker password

You can assign a password for selected computers in the **HelpDesk** views of the DriveLock Control Centers (DCC).

Warning: Note that you can only change a computer-specific password if the client user has not already assigned a user-specific password.

### To specify the password, Please do the following::



- 1. Click BitLocker password
- 2. Select In the password dialog.

Enter BitLocker password	
Enter the new BitLocker password for the selected confirm.	clients here and
Password	
Assign BitLocker password for the selected clients:          DLCLIENT03         TESTPC003         COMPNAME2         COMPNAME1         COMPNAME	Select all Select none
OK	Cancel

- a. Enter and confirm a password.
- b. Select the computers you want to assign the password to from the list. You can also use the buttons next to the list.
- c. Click **OK**.

# 3. Select Import password from CSV file.

a. Enter the **path** to the CSV file, see figure below:



Specify the CSV file you want to import the BitLocker passwords from.  Path to the CSV file:  Assign BitLocker password for the selected clients:  Select all Select none  Please note that the names of the clients in the CSV file must appear with the corresponding BitLocker passwords in the following form. Example: Client01;Password01 Client02;Password02 Client03;"Password;03"	Import BitLocker password from CSV file		
Path to the CSV file: Assign BitLocker password for the selected clients: Select all Select none	Specify the CSV file you want to import the BitLocker from.	passwords	
Assign BitLocker password for the selected dients: Client01;Password01 Client02;Password02 Client03;"Password;03" Select all Select none	Path to the CSV file:		Please note that the names of the clients in the CSV file must appear with the corresponding BitLocker passwords in the following form. Example:
Select none	Assign BitLocker password for the selected dients:	Select all	Client01;Password01 Client02;Password02 Client03;"Password;03"
	OK	Select none	

- b. Select the computers you want to assign the password to from the list. You can also use the buttons next to the list.
- c. Click **OK**.

### 1.7.1.2 Allowing a user-defined BitLocker password

In the DriveLock Control Center's (DCC) **Helpdesk** view, you can enable users of individual computers to assign their own BitLocker password.

Note: The users are asked to specify a BitLocker password for their computer. When the users assign this password, DriveLock overwrites the respective setting in the BitLocker policy originally assigned to these computers.

### To enable users to change their password, Please do the following::



2. In the next dialog, click **Yes**. You confirm that the original password will be overwritten.

Note: This setting is only available if the original BitLocker policy supports password changes.

3. Click **OK**.





- 4. A dialog asking the user to change their password appears on the respective computer.
- 5. The Event report in the DCC issues the following event:

0	Event	Event Report Event Report								port: BitLocker events - DriveLock Control Center 7.9.4.21788				
Start	Actions	Options	5											
() Refresh	Columns	Columns Sort Group Find Find Filter New Forensic Analysis Start / end								1 I I I I I	5 Days			
General	So	Sort / Group Find / Filter Drill down								je				
🔒 Encrypte	🗞 Encrypted Disks: Encrypted Disks 🖉 Forensics: Users and groups 🚳 Event Repo								BitLocker events	x				
Drag a colum	Drag a column header here to group by that column													
Type [Events	s] Descript	Description [Events]								User [Events]	Computer n	Date / Time [Events] 👻		
(i) Inform	. Sent age	Sent agent action to change BitLocker password from DriveLock Control Center								DLSE\Admi	DLSERVER	21.01.2019 14:26:46		
(i) Inform	. Sent age	Sent agent action to change BitLocker password from DriveLock Control Center							811	DLSE\Admi	DLSERVER	21.01.2019 14:20:23		

### **1.7.2 BitLocker event report**

DriveLock BitLocker Management logs all activities, events and errors that occur with BitLocker actions.

To view these events, open the BitLocker event report in the DriveLock Control Center (DCC). You can customize the view to suit you best.

6	Event F	Report					Event	Report: BitLocker ev	vents - DriveLock Con	trol Center 7.9.1.21488			-	
Start	Actions	Options												
(J) Refresh	Columns	<b>↓</b> A Sort	Group	Find	Filter	L) New Forensic Analysis	Range Start / en	d	<mark>0</mark> All					
General	So	rt / Group		Find /	Filter	Drill down		Time range						
🔒 Event R	eport: BitLo	:ker even	ts x											
Drag a column header here to group by that column														
Type [Events] Description [Events]								Event ID [Events]	User [Events]	Computer name [Events]	Date / Time [Events] 🔻			
Inform New initial BitLocker password from DriveLock Control Center								810	DLSE\Administrator	DLSERVER	15.11.2018 09:15:00			
<ol> <li>Inform</li> </ol>	(i) Inform New initial BitLocker password from DriveLock Control Center							810	DLSE\Administrator	DLSERVER	15.11.2018 09:14:59			
<ol> <li>Inform</li> </ol>	. New initi	al BitLock	er passw	ord from Driv	eLock Cor	trol Center		810	DLSE\Administrator	DLSERVER	15.11.2018 09:14:59			
<ol> <li>Inform</li> </ol>	. Sent age	ent action	to chang	je BitLocker j	bassword f	rom DriveLock Co	ntrol Center	811	DLSE\Administrator	DLSERVER	15.11.2018 09:14:39			
<ol> <li>Inform</li> </ol>	. Sent age	ent action	to chang	je BitLocker j	bassword f	rom DriveLock Co	ntrol Center	811	DLSE\/MHA	DEVCLIENT01	14.11.2018 16:17:32			
<ol> <li>Inform</li> </ol>	. Sent age	ent action	to chang	je BitLocker j	bassword f	rom DriveLock Co	ntrol Center	811	DLSE\/MHA	DEVCLIENT01	14.11.2018 16:16:38			
<ol> <li>Inform</li> </ol>	. New initi	al BitLock	er passw	ord from Driv	eLock Cor	trol Center		810	DLSE\/MHA	DEVCLIENT01	14.11.2018 16:12:03			
<ol> <li>Inform</li> </ol>	. New initi	w initial BitLocker password from DriveLock Control Center						810	DLSE\/MHA	DEVCLIENT01	14.11.2018 16:12:03			
<ol> <li>Inform</li> </ol>	. New initi	al BitLock	er passw	ord from Driv	eLock Cor	trol Center		810	DLSE\/MHA	DEVCLIENT01	14.11.2018 16:12:03			
<ol> <li>Inform</li> </ol>	. New initi	al BitLock	er passw	ord from Driv	eLock Cor	trol Center		810	DLSE\/MHA	DEVCLIENT01	14.11.2018 16:12:03			
<ol> <li>Inform</li> </ol>	. New initi	al BitLock	er passw	ord from Driv	eLock Cor	trol Center		810	DLSE\/MHA	DEVCLIENT01	14.11.2018 16:12:03			
<ol> <li>Inform</li> </ol>	. New initi	al BitLock	er passw	ord from Driv	eLock Cor	trol Center		810	DLSE\/MHA	DEVCLIENT01	14.11.2018 16:10:35			
– Details –									1	1	1			
Set new initia	al BitLocker p	assword	for client	COMPNAME	1 from Driv	eLock Control Cer	nter						^	

For more details on the individual events, refer to the BitLocker event list.

### 1.7.2.1 Customizing the BitLocker event report

# Please proceed as follows to customize the event report in the DriveLock Control Center:

- 1. On the **Start** tab, open the **Event report** area.
- 2. In the **Entities** section, select **BitLocker events**.
- 3. The **Actions** tab provides a table with all the BitLocker events.
- 4. Customize the table according to your needs by specifying filters or grouping columns, for example.

Note: For more information, please refer to the DriveLock Control Center User Guide at DriveLock Online Help, chapter Working area.

- 5. Save your changes.
- 6. If you reopen the event report, the **BitLocker events** button appears in the **Recently used** section.

# 1.7.2.2 Listing of BitLocker-relevant events

For the current table of all DriveLock events, see the DriveLock Events documentation at DriveLock Online Help.

### **1.8 Tracing BitLocker actions**

You can track all BitLocker actions in the Events section in the DriveLock Control Center and the DriveLock Operations Center (DOC).

You can also use tracing in detailed diagnostic logs. For example, this is important in order to trace errors during the import of original BitLocker environments. The tracing file is called DlSvcBitLocker.log, see figure below. Here you can easily identify the actions DriveLock performs when taking over existing BitLocker environments.

DISvcBitLocker.log - Notepad	
File Edit Format View Help	
16.05.2019 10:29:55.318 1656 3540 Exit	0 CBitLockerController::GetLockedNativeBlDriveString {BitLockerWorkflow.cpp @2772}
16.05.2019 10:29:55.318 1656 3540 Entry	CBitLockerController::GetVolumeIndexDelta {BitLockerWorkflow.cpp @1315}
16.05.2019 10:29:55.318 1656 3540 Entry	CBitLockerController::GetSystemStatus {BitLockerController.cpp @2085}
16.05.2019 10:29:55.318 1656 3540 Entry	CBitLockerController::GetBLMStatus {BitLockerController.cpp @1888}
16.05.2019 10:29:55.475 1656 3540 Exit	1 CBitLockerController::GetBLMStatus {BitLockerController.cpp @2074}
16.05.2019 10:29:55.475 1656 3540 Exit	CBitLockerController::GetSystemStatus {BitLockerController.cpp @2113}
16.05.2019 10:29:55.475 1656 3540 Entry	CBitLockerController::VerifyBitLockerAlgorithm {BitLockerController.cpp @3716}
16.05.2019 10:29:55.475 1656 3540 Exit	1 CBitLockerController::VerifyBitLockerAlgorithm {BitLockerController.cpp @3758}
16.05.2019 10:29:55.475 1656 3540 Msg	CBitLockerController::GetVolumeIndexDelta: Drive C: is BitLocker encrypted but not managed by DriveLock. It will be adopted now. {BitLockerWorkflow.cpp @1461
16.05.2019 10:29:55.475 1656 3540 Msg	CBitLockerController::GetVolumeIndexDelta: Protector TpmAndPin needs to be replaced by TpmAndPin for drive C:. {BitLockerWorkflow.cpp @1515}
16.05.2019 10:29:55.475 1656 3540 Entry	CBitLockerController::VerifyBitLockerAlgorithm {BitLockerController.cpp @3716}
16.05.2019 10:29:55.475 1656 3540 Exit	1 CBitLockerController::VerifyBitLockerAlgorithm {BitLockerController.cpp @3758}
16.05.2019 10:29:55.475 1656 3540 Msg	CBitLockerController::GetVolumeIndexDelta: Drive E: is BitLocker encrypted but not managed by DriveLock. It will be adopted now. {BitLockerWorkflow.cpp @1461
16.05.2019 10:29:55.475 1656 3540 Msg	CBitlockerController::GetVolumeIndexDelta: Protector Passphrase needs to be replaced by Passphrase for drive E:. {BitlockerWorkflow.cpp @1515}

You can enable the creation of trace logs via the command line, with the help of the DriveLock Management Console or via the DriveLock Support tool DLSupport.exe (which resides in the DriveLock installation directory).

Please refer to the DriveLock Administration Guide for further information on creating trace files, in chapter 21.5. **DriveLock Support tools** on our website.

# 2 DriveLock Pre-Boot Authentication

The 2019.2 release introduces a new DriveLock Pre-Boot Authentication (PBA) that can be used for both DriveLock encryption technologies, BitLocker Management and Disk Protection (Full Disk Encryption, FDE). A separate license is required for DriveLock Pre-Boot Authentication for BitLocker.

Warning: Note that the new PBA only works on UEFI systems in Windows 10 environments.

The older BIOS PBA can only be used in Windows 7 or 8.1 environments, it is no longer updated and is only used for DriveLock Disk Protection (FDE). When you implement BitLocker Management on BIOS systems, the native BitLocker PBA is used.

Note: For information on the PBA with DriveLock Disk Protection, see the corresponding chapter in the Administration Guide in the Product Documentation section on the DriveLock.Help website.

# DriveLock Pre-Boot Authentication for BitLocker Management includes a range of benefits:

- Login with user name / password
- Recovery using Challenge-Response procedure
- Single sign-on (SSO) for Windows logon
- Login with Smartcard
- Support for other keyboard layouts and virtual keyboard
- Exchangeable PBA background images

# 2.1 Policy configuration with pre-boot authentication settings

Note that the DriveLock PBA for BitLocker Management requires a separate license, which is based on the BitLocker Management license.

# 2.1.1 License DriveLock PBA

License **DriveLock PBA for BitLocker** as described in the chapter Licensing BitLocker Management.

Mote: Please make sure to select both licenses as indicated in the figure below.

BitLocker-Richtlinie - Centrally stored DriveLoc	Setting		Value				
V 🛷 Global configuration	Jetting						
Settings	License		Perpetual license and option	ns			
User interface settings	License Properties					?	×
Server connections	Constant						
R Trusted certificates	General Licenses Licensed compute	rs Excluded computers					
File storage	License usage	• •					
> > Multilingual notification messages	Number of licensed computers	10 🥑 Y	our license covers the computers	in the list.			
> 🔆 EDR	Computers in Active Directory	3					
> 🗵 Drives							
> 図 Devices	License summary						
> 🔶 Network profiles	Product ID / Condition	License type	Number of licenses	Description			
>      Applications	DriveLock Device control	Perpetual license	10				
✓ B Encryption	DriveLock Encryption 2-Go	Perpetual license	10				
Settings	Application control	Perpetual license	10				
> DriveLock Encryption 2-Go	La ITerminal and Virtual License	Not licensed	0				
> B DriveLock File Protection	DriveLock Disk Protection	Not licensed	0				
DriveLock Disk Protection	DriveLock File Protection	Not licensed	0				
✓  S     BitLocker Management	Eegacy US support	Not licensed	0				
Hard disk encryption	Egg Security Education	Not licensed	U				
> 🖞 BitLocker To Go	Bit ocker Management	Perpetual license	10				
> 🛱 Security awareness	Brivel ock PBA for Bitlocker	Pemetual license	10				
> 🦻 Systems management		repetadricense	10				
> Management console	License configuration						
	License is not configured in this polic	y vill be enabled and can be con	figured. An appropriate license b	as to be present in one	e of the policies that form		
	the resultant set of policies on each	Agent.					
				0	)K Cancel	Ap	ply

# 2.1.2 Pre-boot authentication settings

To configure the DriveLock PBA for BitLocker, open the **Encryption** node, then select **BitLocker Management** and then **Hard disk encryption**. Start by configuring the **authen-tication type**.

### 2.1.2.1 Authentication type

Open the **Pre-boot authentication settings** and select **DriveLock pre-boot authentication** on the **Authentication type** tab.

Note: If this option is not available, verify that the DriveLock PBA option is correctly licensed and that you saved and reopened the policy after activating the license option.

Properties				?	×	
Appearance	Use	r synchronization	Users	User-v	vipe	
Emergency log	on Self-wipe Network p			e-boot (UEFI)		
Authentication t	ype	Password optic	ons Lo	ogon metho	ods	
Pre-boot authentic	ation typ	e				
○ No pre-boot authentication						
BitLocker requires an active Trusted Platform Module (TPM) on all computers. Only the system partition will be encrypted, there is no additional authentication required to boot the computer.						
O Bit Locker pre-b	oot auth	entication 📒				
The BitLocker password is required to boot the client computer. All users of this computer must use this password to log in. A recovery key is provided in case of emergencies.						
DriveLock pre-	poot aut	hentication 🔀				
User authentication is required to boot the client computer. To authenticate the user, the user name and password or 2-factor authentication can be used. All emergency logon methods are available.						
A The BitLocker PBA is used instead of the DriveLock PBA when there is a BIOS system in place and/or no DriveLock PBA license available.						
Global options						
Automatically unlock all data partitions  Mitigate TPM security to eliminate repeated entry of a recovery key (e.g. in connection with a docking station)						
		ОК	Cancel	Ap	ply	

Warning: This option is only supported for computers running Windows 10 and UEFI firmware. We do not support server systems, older systems or systems with legacy BIOS.

Please note the following:

- If the client computer does not meet the requirements, the **BitLocker pre-boot authentication** option is automatically used.
- The **Automatically unlock all data partitions** option has no effect on DriveLock pre-boot authentication because data drives are generally unlocked automatically.

You cannot select any options on the **Password options** tab. If you want to configure settings on this tab (e.g., for computers where DriveLock pre-boot authentication cannot be used), you must temporarily enable the **BitLocker pre-boot authentication** option.

# 2.1.2.2 Logon methods

The following options are available on this tab:

Select the **Enable single sign-on for Windows** option so that users only need one logon to the client computer. The Windows login screen will no longer appear.

The following authentication methods are available:

- Local user access: This option is enabled by default. This method allows local Windows users to authenticate to the system using their local Windows user name, password, and local system name.
- **Domain user access (with password)**: This method allows Windows domain users to authenticate themselves to the system with their Windows domain user name, password and domain name.

Warning: Users can only log on to the domain at all if the Windows and Preboot options are set.

• **Domain user access (with token)**: This method allows Windows domain users to authenticate themselves with a smartcard/token and PIN.

**Enable logon using password tokens**: This method allows the pre-boot authentication for a password token user. If you check this option, then you need to select at least one more Windows authentication.

Warning: Prior to configuring the DriveLock PBA for token access only, make sure that a valid token exists for both the PBA and the Windows logon (unlock).

Other options in the dialog:

- The **Maximum number of logins before lockout** option causes a user to be locked for a certain period of time after the specified number of failed logins to protect the system from a brute force attack with automatic logon scripts. Change the default values according to your corporate security policies.
- If you are using certificates for authentication, you can specify the number of days after which DriveLock alerts users before certificates expire.
- The **Count failed logons globally for all users** option is enabled by default. Instead of counting up failed attempts for a single user, the failed attempts counter is incremented independently of users.

# 2.1.2.3 Users

On this tab, you specify the settings for DriveLock PBA users.

BitLocker Management adds all users who have successfully logged on to Windows to the pre-boot authentication database. For this reason, the option **Automatically add Windows users to pre-boot authentication on logon** is set by default. If you deselect this option, users are no longer added automatically. You can add users manually using the **Add** button.

If you activate the option **Always use downlevel logonnames during single sign-on**, the user logon is only possible with the so-called downlevel logon names. They take the format "DOMAIN\username". Logon with User Principal Names such as benutzername@domain.org is not permitted anymore.

# 2.1.2.4 User synchronization

The option **Synchronize Active Directory users to pre-boot authentication** is not enabled by default because AD users are automatically entered into the PBA database when they log on to the PBA.

Use this option only if you want to preconfigure the PBA by manually adding users from AD to the PBA user database before they log on.

In this case, add the appropriate AD groups and users that you want to synchronize to the PBA database.

As an initial password, you can assign a **fixed password** (identical for all users), the **user name**, or any available **AD property value**.

Note: Please note that the members of the "Domain Users" group will not be synchronized. This group employs a mechanism based on the user's "primary group ID" to determine membership, and does not typically store members as multi-value linked attributes.

# 2.1.2.5 User wipe

To configure user wipe, select the **User-wipe** tab, check **Enable user-initiated wipe**, and enter a wipe suffix.

Enabling this option allows a valid PBA user to make the system inaccessible.

# 2.1.2.6 Appearance

On this tab you can define how the DriveLock PBA is displayed to users on their client computers.

- There are several **background images** to chose from. Choose one of them.
- You can also select your own **custom background image** by selecting one from the file system or the policy file storage.
- The **Show password** option allows the user to briefly view the entered password in plain text. Currently, this option is not yet available for the Drivelock PBA, but only for BitLocker Management.
- If required, you can enter your own display test in the text box below the **Show pre-boot user information message** option.

# 2.1.2.7 Network pre-boot (UEFI)

For more information on this tab, please click here.

### 2.1.2.8 Emergency logon

Use these settings to specify which logon methods are available in case a user is no longer able to log on to the DriveLock PBA (for example because the password is missing).

We recommend using the default settings.

- Allow emergency logon with user name: This default option lets users log on in an emergency by entering their name. This applies to Windows domains or local Windows user password accounts added to the PBA user database. It permits a one-time preboot access to the system.
  - Note: Note that a user must have successfully logged in to pre-boot authentication at least once before this feature is available to that user. Users who have never logged in before, must use the Emergency logon without user name procedure.
- **Single sign-on after emergency logon** allows users to log on to Windows and work with it if they forget their password even if an administrator has not yet reset the password.
- Emergency logon without user name allows a one-time pre-boot access to the system for all users who have never been logged into the system before. Single sign-on (SSO) is not possible in this case.

• If you enable the **Emergency logon for users of token devices** option, make sure you set the appropriate settings for logon with tokens on the **Logon methods** tab.

# 2.1.2.9 Self-wipe

Self-wipe has two main application scenarios. Either you want to protect the data on a lost PC that no longer connects to the DES and/or you want to force mobile users to connect to the corporate network on a regular basis.

To configure self-wipe, select the **Self-wipe** tab, check **Enable self-wipe when computer is offline** and configure the appropriate settings as described in the dialog.

After the specified offline time expires, DriveLock deletes the PBA database.

### 2.1.3 Override policy settings (DriveLock PBA)

To disable specific pre-boot authentication settings on individual client computers, you can override the respective policy settings.

Warning: Note that the policy settings will not be re-enabled until you undo the override option.

Please do the following:

- 1. Open the **Agent remote control** in the **Operating** node of the DriveLock Management Console.
- 2. Select the DriveLock Agent you want to change the policy settings for.
- 3. From the context menu, select the menu item **Disk encryption properties...**.
- 4. On the **General** tab you can see information about DriveLock Agent encryption. Click the **Reconfigure agent...** button.
- 5. Set the **Override policy settings** option and leave the **Override general deployment settings** option checked (default).



Reconfigure BitLocker Management	×
You can override BitLocker Management settings in your company policy on agents. This replaces the settings configured here with the company policy th is applied to the agent computer.	nat
Override policy settings     Override general deployment settings     Encrypt local hard disks     Do not decrypt in case of configuration changes	
Pre-boot authentication settings Pre-boot authentication type No pre-boot authentication BitLocker Pre-Boot Authentication O DriveLock Pre-Boot Authentication	
Override authentication methods Windows Preboot	
Local user access          Domain user access (with password)          Domain user access (with token)          Enable logon using "password tokens"          Require token PIN on Windows logon	
Override emergency access methods     Allow emergency logon with user name     Single Sign-on after emergency logon     Allow emergency logon without user name     Allow emergency logon for token users	
OK Cancel	

6. Select the appropriate PBA in the Pre-boot authentication settings section.

Note: If there is no TPM, the No pre-boot authentication option is automatically grayed out (see figure above).

- The Override authentication methods and Override emergency access methods options are active only if you selected DriveLock pre-boot authentication. Both options override the corresponding settings in the policy. For more information, see the Logon methods and Emergency logon chapters.
- 8. If you click **OK** now, your settings will be applied to the selected client computer with immediate effect.

### 2.2 Network pre-boot authentication (UEFI)

This add-on to the DriveLock pre-boot authentication enables simplified management of client computers (Drivelock Agents) in network environments.

Upon reboot, the operating system drive of a client computer can be automatically unlocked if it is connected to a corporate network via cable. In this way, client systems that meet the hardware requirements can be booted in Windows without user interaction.

You can, for example, configure the feature so that client computers can be booted automatically only when they are on the network. Booting without a network is not possible!

If no network connection is available, alternatives may be permitted (e.g. emergency logon requiring user and password entry).

This also makes it easier for administrators to roll out software patches to unattended client computers, for instance.

### Note the following limitations:

- Only UEFI firmware is supported (The network PBA for BIOS will remain functional only when using DriveLock Disk Protection)
- Only wired network is supported
- Only network adapters that UEFI offers for PXE boot are supported
- The DriveLock network PBA does not provide any network drivers of its own

### The following rules apply:

- The network PBA and the DriveLock Enterprise Service (DES) must have the same date / time
- To negotiate the key pairs, the secure network connection under Windows to the DES is required (HTTPS/SSL)
- Connections via proxy are not supported in the network PBA
- In the DriveLock Operations Center (DOC), automatic logon can be temporarily disabled for each DriveLock agent (more information can be found here )

Warning: To ensure that the network PBA works, a server connection must be specified in the policy in the Server connections subnode in the Global settings.

# 2.2.1 Network pre-boot (UEFI)

Note: The settings on the Network pre-boot (UEFI) tab are available for both DriveLock Disk Protection and DriveLock BitLocker Management (depending on the license) as the DriveLock pre-boot authentication is used for both features.

The following settings are possible on the tab:

- Check the Enable network pre-boot authentication option to enable the feature. However, you must also select at least one of the two options below (automatic or AD logon).
- 2. The **Allow automatic logon to the network** option enables authentication to the client computer without any user interaction, provided that a network connection is available.

Once the policy with this setting is assigned to the DriveLock Agent (client computer), this is what happens in the background:

- a special network user is created in the PBA database ('AutoLogon user') along with an auto-generated user password
- an RSA key pair is exchanged between the DriveLock Agent and the DriveLock Enterprise Service (DES)
  - Note: Automatic logon to the PBA will only occur if this key exchange is successful.

Warning: Note that the client operating system can only be started if there is a network connection between DriveLock Agent and DES.

See this use case for more information.

3. When you select the automatic login, the **Allow other logon methods** option is always also selected by default. This option will guarantee that the authentication is still possible even without a network connection.

Warning: If you remove the checkmark here, the possibility of a local logon or logon via challenge response method no longer exists. In the event that the configuration becomes invalid, the system cannot be booted any longer. All user accounts are automatically deleted from the PBA, AD synchronization and user import are no longer enabled!

4. The Number of network logons to be successfully completed before disabling failsafe option is set to the default value of 3.

Context: An additional local AutoLogon user is configured in the network PBA to serve as a failsafe in case the network PBA is unable to boot over network.

When the specified successful network logons have been performed, the local AutoLogon user is deleted and after that it is only possible to boot via the network autologon.

Warning: This option can only be set initially, it has no effect on systems that are already running. For safety reasons, make sure not to select a number too high.

- 5. Allow logon via Active Directory (AD): Select this option to obtain credentials from the AD.
- Allow network logon for all AD users: Select this option to ensure that users can be logged on who are already known in the AD but not yet in the PBA database. See this use case for more information.
- 7. **User logon must only occur via network authentication**: The network PBA only allows logons if the user credentials can also be verified online against AD. This means that a network logon is a prerequisite; without a network, only a challenge-response procedure is available.
- 8. **Number of automatic retries until the network connection is established**: Specify how often the system should automatically try to establish a network connection.
- 9. **Time between retries**: Specify the seconds that may elapse between retries. Default value is 5 seconds.

Example: To ensure that a router has enough time to establish a network connection, you can increase the number of automatic retries and adjust the pause accordingly. If the pause is set to 0, the process will be repeated immediately.

### 2.2.2 Use case 1: Automatic logon

Certain use cases require that the operating system of a client computer may only be started if there is a network connection, e.g. ATMs or special notebooks that may be used exclusively in the corporate network. In the event that this type of computer is stolen, the operating system can no longer be started without a network connection and the hard disks cannot be decrypted accordingly.

Follow these steps for configuration (the settings on the other tabs are explained in the corresponding descriptions):

Pre-boot authentication settings Properties ? X						×
Appearance	User synchronization Use				User-wi	ipe
Authentication	type	Password optic	ons	Logon	Logon method	
Emergency log	on	Self-wipe	Netwo	rk prebo	ot (UEF	-I)
Enable network pre-boot authentication Select either automatic or Active Directory logon or both if you want the client operating system to start automatically when the client is connected to the network.						
Allow autom [V] (No user int	natic logo eraction	on to the network required)				
Allow other logon methods Number of network logons to be successfully completed before disabling failsafe						
Note that logging on without a network connection is no longer possible once the specified number of successful network logons is reached!						
<ul> <li>Allow logon via the Active Directory (AD)</li> <li>Allow network logon for all AD users         This allows users to log on even if they have not previously logged             on to the client operating system     </li> <li>User logon must only occur via network authentication</li> </ul>						jged
Number of automatic retries until the network 3						
Time between retries: 5 econds						
		ОК	Cance	el	Арр	bly

- 1. Select the basic setting Enable network pre-boot authentication.
- 2. Select Allow automatic logon to the network.
- 3. Remove the checkmark at Allow other logon methods.

- 4. Leave the default value for failsafe at 3. This way you can make sure that only after 3 successful network logins there is no other way to log on. This option is intended for both testing purposes and as a failsafe.
- 5. Leave the default value 3 at Number of automatic retries until network connection is established.
- 6. Likewise, you can leave the pauses between retries at 5 seconds.
- 7. Apply your changes by clicking OK.

# 2.2.3 Use case 2: Network login for all AD users

Two use cases:

- An employee (new user) needs to log on to a particular client computer in Windows, even though the user has never logged on there before. The client computer is connected to the corporate network.
- A user has forgotten or changed their password. No challenge-response procedure needs to be performed when the client computer is connected to the network. The administrator can reset the Windows password and the user can log in to the network PBA via AD. If the AD logon is successful, a single sign-on into Windows takes place and the new user credentials are synchronized back into the PBA.

Follow these steps for configuration (the settings on the other tabs are explained in the corresponding descriptions):

Appendic	the sector tests to the sector tests				Llace	wine
Appearance	User	Synchronization	Use	ers	User	wipe
Authentication	type	Password optic	ons N-t	LO	gon metr	nods
Emergency log	on	Self-wipe	Iver	work pr		EFI)
Enable network Select either au client operating connected to the	c pre-boo utomatic o system t he netwo	t authentication or Active Directory I o start automatically rk.	ogon or / when t	both if y the clier	you want nt is	the
Allow autom (No user int	natic logo eraction i	n to the network required)				
🗹 Allow ot	her logon	methods				
Number of before disal	network lø bling failsi	ogons to be succes afe	sfully co	omplete	d 3	▲ ▼
Allow logon Allow ne This allo on to the User log	via the A stwork log ws users e client op ion must (	active Directory (AD gon for all AD users to log on even if th perating system only occur via netw	) ey have ork auth	e not pre	eviously l	ogged
Number of puts	matic rat	ries until the networ	۰ –		. 1	
connection is established						
Time between retries: 5 seconds						
		OK	(	ncel	Δ	oolu

- 1. Select the basic setting Enable network pre-boot authentication.
- 2. Select Allow automatic logon to the network.
- 3. Keep the check mark at **Allow other logon methods**.
- 4. Leave the default value for failsafe at 3. This way you can make sure that only after 3 successful network logins there is no other way to log on. This option is intended for both testing purposes and as a failsafe.
- 5. Select Allow logon via the Active Directory (AD).
- 6. Select Allow network logon for all AD users.
- 7. Based on whether or not you want to enforce network logon, select or uncheck the **User logon must only occur via network authentication** option.
- 8. Leave the default value 3 at Number of automatic retries until network connection is established.

- 9. Likewise, you can leave the pauses between retries at 5 seconds.
- 10. **Apply** your changes by clicking **OK**.

# 2.2.4 Network PBA settings in the DOC

To configure network pre-boot authentication settings in the DriveLock Operations Center, proceed as follows:

- 1. Select the **Computer** section and open the BitLocker dashboard.
- 2. Select the DriveLock Agent you want to change the settings for.
- 3. In the detail view on the right side, open the drop-down menu and select Configure view.

TESTPC01		:
△ Compliance s <sup>1</sup>	4	Delete computer
	ŀ	Unlock computer
		Run actions on computers
	-	PBA emergency logon
-		BitLocker
	***	Set password
	<u>P</u>	Reset password
	•	Show recovery key
		View
	ැටි	Configure detail view
Click to navigate to the r	222	

- 4. Select **Network Pre-Boot Authentication** and check **Show** and optionally **Expand** (depending on whether you want to display the item open right away).
- 5. The Allow automatic logon to the network option can only be enabled or disabled.

Note: The policy with this setting must have been assigned to the DriveLock Agent (client computer) and applied there.

### 2.3 Settings for emergency logon

If users are no longer able to log on to pre-boot authentication (for example, because they forgot their password), you will need to configure the emergency logon settings.

Please do the following:

- To start the recovery/emergency wizard, open the **Operating** node in the **DriveLock** Management Console and right-click the **Agent remote control** sub-node to open the context menu.
- 2. Here you select **BitLocker Management recovery** and then **BitLocker Management recovery / emergency logon** (see figure).



3. The recovery wizard opens.

Select **Emergency logon**. If your recovery keys are sent to the DriveLock Enterprise Service, do not change the default setting **DriveLock Enterprise Service**. To specify the path to the required recovery keys later, select **Recovery files (copied by agent computer)**.
Disk Recovery	×
Recovery type and source Select the type of recovery to perform and the source of recovery information.	
Select the type of recovery to be performed:	
Emergency logon Use this option when a user needs to log on and does not have a password for the Pre-Boot Authentication or forgot the password.	
O BitLocker recovery key Use this option if a computer with an encrypted hard disk does not start and you need to recover data from the hard disk.	
Recovery information is retrieved from:	
<ul> <li>Recovery files (copied from the client computer)</li> </ul>	
DriveLock Enterprise Service	
< <u>B</u> ack <u>N</u> ext > Can	cel

- 4. For the emergency logon procedure you need the private key of the recovery certificate. In the second dialog, specify the storage location, either Windows certificate store, a smart card or a PFX file together with the respective password. For more information on certificates, please click here. Click **Next**.
- The third dialog provides a list of computers where you can select the computer to restore. Check the option only show the most recent entry for each computer. Click Next.
- Next, you will see the dialog for entering the user's request/recovery code.
   Enter the code in the appropriate text boxes (see figure). You can optionally specify the name of the user.

Warning: The recovery code provided by the user is mandatory.



Disk Recovery	Х
<b>Specify recovery code</b> Select user to enable to log on and type the recovery code from the PBA screen.	
Users must initiate a request for a one-time password from the Pre-Boot Authentication (PBA) screen by selecting "Emergency" or pressing F3. Then after entering the user name a recovery code is generated. Recovery for specific user	
Recovery code as specified by the user       Z+SGJ     N4G-R     Y+3	
< <u>B</u> ack <u>N</u> ext >	Cancel

7. Click **Next** to generate the response code.

Disk Recovery X	
Recovery completed Please review the results of the recovery operation.	
The user must enter the Response Code on the Pre-Boot Authentication screen in the "Enter reponse below:" field and then press ENTER.	
Response code	
CZ2C. NQ6OF RZ*K+ JW3VR KF*CK 3	
< <u>B</u> ack <b>Finish</b> Cancel	

- 8. Tell the user the **response code**.
- 9. Click Finish.

#### 2.4 DriveLock Agent

#### 2.4.1 Installing the DriveLock PBA on the DriveLock Agent

#### Please note the following:

- 1. Once the client computer has started, a message appears indicating that the DriveLock PBA is being installed.
- 2. When confirmed, the computer is restarted.

Mote: In case no user is logged in, the computer is restarted immediately.

3. After restarting the client computer and logging on, another dialog box appears (see figure), informing the user that DriveLock PBA is now active.

DriveLock BitLocker Mana	gement
	/eLock
DriveLock	PBA Installation
Print Lock	From now on you need to authenticate in the DriveLock PBA at every system start or reboot before you can access your hard disk. You can authenticate using your Windows credentials. As soon as the computer restarts, enter your Windows user name and your password. Choose the correct domain.
Continuing in 5:57	Close

4. At the same time the encryption starts; restarting or shutting down the computer is now possible at any time.

# 2.4.2 Login to the DriveLock PBA

#### Please consider the following when logging in:

- 1. As soon as the client computer is booted, a short text is displayed indicating that DriveLock pre-boot authentication is active.
- 2. Immediately after the text display and even before the start screen is displayed, hot keys can be used.
- 3. The login page opens when you press any key or click the mouse button.





Using function keys is not required anymore, but possible.

4. Please enter the Windows credentials on the login page.

Warning: The most recently logged on user is not saved or displayed for security reasons.

Please note the following:

- Please note that the user must have previously logged on to Windows if you have selected the option "Synchronize Windows users automatically". For more information, refer to the chapter User synchronization.
- You can also import users from Active Directory beforehand with a policy setting. For more information, refer to the chapter Users.
- 5. Click **Select another** to select the domain. A list of the available domains is displayed.

If no keyboard is available (for example, on a tablet computer), an on-screen keyboard can be displayed by clicking the **keyboard icon** in the lower right corner.
 A green checkmark is displayed on the keyboard icon. The keyboard appears when the cursor is in a text field.



The speech bubble icon allows you to set the language of the login interface.

- 7. You can reach all fields and options also using <Tab>, <Shift-Tab> and the arrow keys, if there is no mouse available.
- 8. By selecting the language (in the figure '**GER**') in the lower right corner, you can select a different keyboard layout.
- 9. You can log in either by clicking the arrow next to the password or by pressing <Return>.
- 10. By default, the user is also logged on to Windows (Single Sign On). You can disable this feature in the policy.

#### 2.4.3 Network pre-boot authentication

Once the policy containing the network PBA settings is assigned to the client computer and the computer is started, the following scenarios are possible:

#### 1. The client computer is connected to the corporate network

When booting the client computer, a notification appears that DriveLock pre-boot authentication is active.

Then the following login screen appears, see the figure:

Mote: No user interaction is required.



Note: By clicking the key icon within 10 seconds it is possible to switch to the PBA login mode with user name and password entry, if enabled.

The next step shows the Windows login screen where the Windows credentials are entered.

#### 2. The client computer cannot connect to the corporate network

As soon as the client computer is booted, the notification indicating that DriveLock preboot authentication is active also appears. However, the login screen now indicates that the automatic network login has failed. Depending on the configuration in the policy, the system will try to connect automatically a few times.



# If no connection can be established, the user has the following options according to the policy settings:

• Try to re-establish the network connection

The following options are available from the **network icon menu** in the taskbar:



• Select another login method (user name/password entry), if enabled. Here, single sign-on is active and logging in to the DriveLock PBA is required only once.



Warning: Unless another login method is allowed, it is not possible to start the client computer's operating system without a network connection.

Note: For more information, including how to use shortcut and function keys, see the Login to the DriveLock PBA chapter.

#### 2.4.4 Emergency logon with recovery code

**Scenario:** A user of a DriveLock Agent has forgotten their password and cannot authenticate to the DriveLock PBA. The user asks the administrator for help.

User and administrator now perform the following actions:

#### 1. User action:

1. Select the Lost username or password option on the left side of the login screen.



2. A new login screen will then appear, displaying your request or recovery code.



Lost ü	ser name	or passwo	ord	
	Stgn in to: I Select and	DLSE	5	
Machine MI 0-1803-BI				
Recovery code				
Z+SGJ	N4G-R	Y+3		
Response code				
			$ \rightarrow $	
	Sign in ont	lions		
	Sign in opi	ions		

3. Inform the administrator of the recovery code and machine name, including the user name if necessary.

Note: You must provide the machine name and recovery code while the user name is optional.

#### 2. Administrator action:

- 1. You immediately launched the Recovery Wizard after the user notified you and now you have reached the input mask for the recovery code.
- 2. Enter the **recovery code** to generate the **response code**.
- 3. Now communicate the **response code** to the user.

Warning: The request code and the response code are both generated once and can only be used once.

#### 3. User action:

 Enter the **response code** in the appropriate text boxes in the DriveLock PBA. In case you make a mistake while entering the code, you will be shown error digits in different colors.

If you have entered everything correctly, you can log back into the system by clicking the arrow button.

Lost u	ser name or passwor	rd
Uset	Sign in to: DLSE Select another	5
Machine MLO-1803-BL Recovery code Z+SGJ Response code	N4G-R Y+3	
CZ2C. NQ60	F RZ*K+ JW3VR KF*CK Sign in options	3 →

2. Sign in to Windows.



# 2.5 DriveLock PBA command line tool

The DriveLock PBA command line tool DLFDEcmd can be employed with both BitLocker Management and DriveLock Disk Protection (Full Disk Encryption, FDE). Use this tool, for

example, to view the status of the PBA or to initiate an automatic logon (autologon) to the client computer whenever Windows system updates are required.

Note: The display text is adapted accordingly depending on the preferred encryption method (Disk Protection - FDE or BitLocker Management).

Help on how to use the individual commands is available when you use the 'help' parameter to call the DLFdeCmd.exe program.

Please find below the detailed description of the individual parameters:

- SHOWSTATUS: Displays the current status of the encryption method you are using.
- CRYPTSTATUS: Displays information about the encryption status, such as the number of encrypted disks.
- ENABLEAUTOLOGON: Enables automatic logon as part of disk encryption for the next number of logons.

Enter the following:

- <user>: PBA user for automatic logon
- <domain>: Domain of the specified PBA user
- <password>: Password of the specified PBA user (\* to enter the password, # to enter in a dialog)
- <count>: Number of reboots where automatic logon is activated. Specify 'forever' if you want the automatic logon to be activated indefinitely.
- [sso]: Add "sso" only if you want automatic login with Single Sign On.

Example: If you enter enableautologon hans dlse \* 2, the user 'hans' from the domain 'dlse' will be automatically logged in at the next '2' reboots and the pass-word will be entered in the command line.

Note: For automatic login with a smartcard or token, specify "token" for <user> and <domain>.

- DISABLEAUTOLOGON: Disables automatic logon.
- SHOWAUTOLOGON: Shows the settings for automatic logon
- ENABLERESETSP: Activates resetting the system protection interrupt vector list after the next reboot. Use this option after updating the system BIOS to store new interrupt

vector values and suppress the PBA warning messages. A single automatic logon is required to reset the interrupt vector list.

Please enter the information in <user> <domain> <password> here as well.

- DISABLERESETSP: Disables resetting the system protection interrupt vector
- SHOWRESETSP: Displays the current settings for resetting system protection
- ENABLEDELAYINST: Delays the installation of the hard disk encryption until "DisableDelayInst" is executed.
- DISABLEDELAYINST: Disables the delay and performs the disk encryption installation as configured in the policy
- SHOWDELAYINST: Displays the current status of the delayed installation

In the figure below, the autologon for BitLocker Management is disabled and the ENABLEAUTOLOGON command has not been set here.

```
C:\WINDOWS\system32>DlFdeCmd SHOWAUTOLOGON
DriveLock 19.2.0 : Data protection, encryption, and more
DLFdeCmd
                : Full disk encryption command line tool
                  (C) Copyright 2004-2019 DriveLock SE.
BitLocker Management auto-logon is currently disabled.
C:\WINDOWS\system32>DlFdeCmd SHOWRESETSP
DriveLock 19.2.0 : Data protection, encryption, and more
                : Full disk encryption command line tool
DLFdeCmd
                  (C) Copyright 2004-2019 DriveLock SE.
BitLocker Management system protection reset is not active.
C:\WINDOWS\system32>DlFdeCmd SHOWDELAYINST
DriveLock 19.2.0 : Data protection, encryption, and more
DLFdeCmd
                : Full disk encryption command line tool
                  (C) Copyright 2004-2019 DriveLock SE.
BitLocker Management installation will execute as configured.
C:\WINDOWS\system32>
```

# 3 DriveLock BitLocker To Go

DriveLock BitLocker To Go includes the following features:

- Enforced encryption of external USB storage media with BitLocker To Go
- Enforced encryption of external drives (e.g. eSATA hard drives)
- DriveLock detects USB drives already encrypted with BitLocker To Go and does not reencrypt them during enforced encryption
- User-defined passwords
- A corporate password can be assigned ensuring that data can only be accessed internally within a company
- Recovery of encrypted data
- Centralized management
- DriveLock BitLocker To Go does not require a separate license other than the license for DriveLock BitLocker Management

# 3.1 BitLocker To Go policy configuration

Before DriveLock can encrypt an unencrypted USB storage device with BitLocker To Go, you need to configure a policy with the appropriate BitLocker To Go settings.

Specify the following:

- 1. General Settings
- 2. Setting: Encrypted drive recovery
  - Encryption recovery rule (certificate-based recovery)
  - Administrative password rule
- 3. Setting: Enforce encryption

A sample configuration explains all necessary steps.

Once you have completed, saved, and assigned the configuration to the DriveLock agents, a new **DriveLock BitLocker To Go** entry appears on the user's Start menu with submenus for restoring, encrypting, connecting, and changing the password of each USB storage device.

The next time a user connects a USB storage device to the DriveLock Agent, an unencrypted drive is immediately encrypted. DriveLock walks users through the encryption process. USB storage devices that have been encrypted before will be recognized in the corporate network, won't be re-encrypted and can be used immediately.

Note: Please note that all passwords (user or administrator) should follow the complexity rules (8 characters, upper case, lower case, number, special characters - e.g. DriveLock1\$)

# 3.1.1 General settings for BitLocker To Go

You can specify the following policy settings to configure how BitLocker To Go is used on DriveLock Agents:



- 1. User interface settings in the Global configuration node:
  - By specifying the **Taskbar notification area settings**, you can configure different types of user notifications. You can move the BitLocker To Go entry to any location here.

#### 2. BitLocker To Go settings in the BitLocker Management node:

- Minimum required password complexity for encrypted folders: Specify how complex the passwords must be. If you select Use password policy, make sure to define exact requirements.
- Password complexity policy: Specify the minimum requirements that users must meet when entering a
  - BitLocker To Go password.
- Settings in the Encryption user experience section:



All settings affect the display of BitLocker To Go in the Start menu, taskbar or Windows Explorer.

For more information, visit BitLocker To Go on the DriveLock Agent.

## 3.1.2 Recovering encrypted drives

To start with, you select the main certificate (or create a new one) that is essential for the recovery process. Then, you assign an administrative password that will be used to encrypt the USB storage devices.

## 3.1.2.1 Administrative password

Use a central administrative password for accessing encrypted removable storage devices.

Mote: Ensure that the administrative password is complex enough.

In addition to the central password, you can also create additional administrative password rules and prioritize them differently. By using different passwords, you can provide increased security.

To create a new administrative password rule, select **Encrypted drive recovery**, open the context menu, click New and then **Administrative password rule**.

You can also restrict the password rules for specific **users** or user groups, **computers** or **networks**. Enter the required information on the tabs in the dialog. See the Use cases for more information.

<ul> <li>BitLocker To Go - Centrally stored DriveLock policy</li> <li>Global configuration</li> <li>EDR</li> <li>Drives</li> </ul>	Priority     Description <sup>P</sup> Lowest      Administrative password <sup>P</sup> Lowest      Certificate-based recovery	Comment
Devices      Applications	1 Properties	? ×
<ul> <li>Applications</li> <li>Encryption</li> <li>Settings</li> <li>DriveLock Encryption 2-Go</li> <li>DriveLock File Protection</li> </ul>	General Options Computers Networks Users Description User 1	
<ul> <li>∂ DriveLock Disk Protection</li> <li>✓  BitLocker Management</li> <li>④ Hard disk encryption</li> </ul>	Password Confirmation	
<ul> <li>✓ ☐ BitLocker To Go</li> <li></li></ul>	Strength	Weak

# 3.1.2.2 Certificate-based recovery

Before creating an encrypted USB storage device, select a master certificate consisting of a public and private key pair. See chapter Encryption certificates for more information.

You can either create a new certificate or use an existing one. See chapter Create encryption certificates for more information.

You can create several Encryption recovery rules with various certificates, which can be restricted and prioritized differently depending on the information you enter on the Computers, Users, Networks tabs. This is useful if you want to allow different users to restore encrypted data.

Mote: Use the standard recovery certificate (lowest priority) as a minimum.

No other information is required in this dialog.

#### 3.1.3 Settings for enforced encryption

First, please create a default enforced encryption rule. If required, you can create additional rules for specific users, groups, computers or networks later. See the Use cases for more information.

When you create the first rule, you will find a description already entered on the **General** tab. Add a comment and your own text, which is displayed in the user selection dialog.

On the **Settings** tab you can use the default settings or select the following options:

- Use administrative password. Don't prompt user: If you enable this option, the storage device will be encrypted with the administrative password only. Users are not prompted to enter their own password during encryption.
- **Prompt user for encryption password**: This setting prompts the user for their own password.
- Attempt to mount using administrative password first: Initially, the user is not asked for their own password. The user will only be prompted for their own password if DriveLock cannot load the storage device automatically, for example, when the administrative password does not match.

Note: Note that this option only works if you have specified an administrative password in the Encrypted drive recovery section.



- **Encryption**: Select the appropriate encryption method. Please note the following:
  - The default option is AES (256 bit key length).
  - Select AES (128 bit key length) if compatibility with older systems is critical for you.
  - **AES-XTS (128 or 256 bit key length)** encryption methods are only available for Windows 10 1511 and higher. Drives encrypted with XTS AES cannot be accessed on older versions of Windows.

# 3.2 Sample configuration for BitLocker To Go encryption

To encrypt or unlock removable storage devices (USB storage devices) with BitLocker To Go, follow these instructions in the order given.

Mote: For more information on the individual steps, see the cross-references.

1. Create a policy (or open an existing one) that contains the settings related to BitLocker To Go.

Note: Verify that you have licensed BitLocker Management in this policy and that the option is selected in the Licensed Computers section.

2. Go to the **Encryption** node in the policy and click the **Settings** sub-node. At first you define the encryption method.

Note: If you do not select anything here, Encryption 2 Go is the default encryption method.

- 3. Select Available encryption methods.
- 4. In the dialog box, select **Set to value** and check the **Drive encryption on removable data drives (BitLocker To Go)** option. Save your settings and close the dialog.
- 5. Open the **Drives** node. Keep the default value **Not configured (locked)** in the **Removable drive locking** settings for **USB bus connected drives**.
- 6. Open the context menu from the **Drive whitelist rules** sub-node, see the figure below. Select **Drive rule...**.

Drives			
Settings			
Removable drive lo	cking		
🖞 Drive whitelist	New	>	Drive rule
🖓 File filter tem			brive rulem
Drive collectic	View	>	Drive collection rule
Ø Authorized m	New Window from Here		Network drives rule
Devices			WebDAV-based network drives rule
Network profiles	Export List		Drive size rule
Applications	B (1)		
Encryption	Properties		Encrypted media rule
] Authentication	Help		Base rule
Security awareness			Terminal services rule
<sup>2</sup> Systems management			Rule from template
Management console			Faller.
	<ul> <li>Drives</li> <li>Settings</li> <li>Removable drive lo</li> <li>Drive whitelist</li> <li>File filter temp</li> <li>Drive collectic</li> <li>Authorized m</li> <li>Devices</li> <li>Network profiles</li> <li>Applications</li> <li>Encryption</li> <li>Authentication</li> <li>Security awareness</li> <li>Systems management</li> <li>Management console</li> </ul>	<ul> <li>Drives</li> <li>Settings</li> <li>Removable drive locking</li> <li>Drive whitelist</li> <li>Prive whitelist</li> <li>Prive collectic</li> <li>Authorized m</li> <li>Devices</li> <li>New Window from Here</li> <li>Export List</li> <li>Properties</li> <li>Authentication</li> <li>Authentication</li> <li>Security awareness</li> <li>Systems management</li> <li>Management console</li> </ul>	<ul> <li>Drives</li> <li>Settings</li> <li>Removable drive locking</li> <li>Drive whitelist</li> <li>File filter temp</li> <li>Drive collectic</li> <li>Authorized m</li> <li>Devices</li> <li>Network profiles</li> <li>Applications</li> <li>Encryption</li> <li>Authentication</li> <li>Security awareness</li> <li>Systems management</li> <li>Management console</li> </ul>

- 7. Create a drive rule for the corresponding USB drive. To see how this works, click here.
- 8. Next, open the **Encryption** node again and then the **BitLocker Management**subnode. Here you go directly to **BitLocker To Go** and select the **Encrypted drive recovery** option.
- 9. Here we have already created two standard rules that cannot be deleted.
  - First, open the **Administrative password** rule. Specify a complex administrative password.
  - Second, open the rule for **certificate-based recovery**. You will need to specify a certificate, as this is required for recovery. Either create a new certificate or select an existing one. Save your settings and close the dialog.
- 10. Next, open the context menu of the **Enforce encryption** option, click **New**, and then click **Enforced encryption rule**.

In the following dialog, enter a description on the **General** tab (the first rule already has the description **Default settings for enforced encryption** in this text field). On the **Settings tab**, accept the default settings: **Prompt user for encryption pass-word** and select the option **Attempt to mount using administrative password**. This setting ensures that DriveLock can access the administrative password in the back-ground.

11. Last, assign your policy to all or to specific DriveLock Agents.

#### 3.2.1 Create drive whitelist rule

Please do the following:

 On the **General** tab, select the USB drive from the list of **Installed drives**. In the figure below, this is the USB drive **E:\** with the vendor ID **VendorCo**.



剩 22-BL-2Go - Centrally stored Drive	Vendor ID / Rule type Product ID / Condit Serial number	Status Rule type Comment	Unique identifier
> 🖑 Global configuration	Enter text here 🛛 Enter text here	Enter text h 🝸 Enter text h 🍸 Enter text here	Enter text h 🍸
> 🔆 EDR		thed with ex. Drive collectio	2716ee9e-5b34
✓	New drive exception Properties ? X	t locked Encryption Automatically generated rule - En	0000000.000
Settings		clocked Encryption Automatically generated rule - En	000000-000
Removable drive locking	Computers Networks Users Drive letters Awareness		
Drive whitelist rules	Messages Encryption Options Commands		
쓴 Whitelist template rule	General Permissions Filter / Shadow Time limits		
<ul> <li>File filter templates</li> </ul>	Vendor ID Vendor Co		
File type definitions			
File type groups	Product ID ProductCode		
Drive collections		Choose drive Properties	? ×
Authorized media		V	
> 🖾 Devices	Comment	Installed drives Device Scanner database	
✓ -			Connect
Settings	Carbol O	Californity installed devices / drives @rocal	Connoct
Continue / Sites	Symbol	Drive Bus type Vendor Product	Serial number
E Configuration profiles	Only allow selected serial numbers	C:\ SAS VMware VMware Virtual S	
>      Applications		D:\ SATA NECVMWar VMware SATA CD	
✓	Senal number Comment Add	E:\ USB VendorCo ProductCode S	96485711218
Settings	96485711218415 Remove		
✓ Image: View Provide Amplitude			
Settings	Edit		
Container password re			
Enforce encryption			
V 👸 DriveLock File Protection			
Estings			
Encrypted folder recov			
Enforce encryption	OK Cancel Apply		
DriveLock Disk Protection			
> MA DILLOCKER Management		Refreeh	
> III Authentication		Herear	
> Lag Security awareness			
> 7/ Systems management		0	Cancel
	1		

- On the **Permissions** tab, specify that you want to allow this USB drive.
   For more information on creating whitelist rules, please refer to the administration guide at DriveLock Online Help.
- 3. The **Encryption** tab has nothing selected by default.
  - Check the **Require drive to be encrypted** option. This will ensure that the connected and allowed USB drive is encrypted according to your settings.
  - Second, check the **Automatically encrypt unencrypted media** option to start encryption as soon as a user inserts an unencrypted USB drive and to open a wizard on the DriveLock Agent to guide the user through the encryption process.

Save your settings and close the dialog.

#### **3.3 BitLocker To Go recovery**

DriveLock BitLocker To Go provides a recovery procedure which helps users, who forgot or lost their password, to access their encrypted USB storage device.

The password may be reset even if the client computer is currently not on the corporate network.

This challenge-response procedure is very similar to the one used for temporary offline unlocking of locked drives or devices. DriveLock guides users through the recovery process. Administrators can easily generate the requested response code in the DriveLock Management Console.

## 3.3.1 Recovery procedure

Please do the following:

- 1. Open the **Operating** node in the DriveLock Management Console and select **Agent remote control**.
- 2. Select **BitLocker Management recovery** from the context menu and then select **Recovery of encrypted removable media...**.



- 3. In the meantime, the user at the client computer has launched the Recovery Wizard and viewed the **request code**. Ask the user to pass it on to you.
- 4. Enter the **request code** in the **Encrypted volume offline recovery** dialog, use copy&paste if you wish. The request code is needed to find the information stored on the DES for the encrypted USB storage device. The text field below shows when and by which user the USB storage device was last encrypted.
- 5. In the next dialog you will see the generated **response code**. Pass it on to the user.
- 6. Next, the user enters the **response code** on the client computer. In the following dialog the user will specify a new user password for the USB storage device.

# 3.3.2 Recovery in the DriveLock Operations Center (DOC)

You can also restore encrypted USB storage devices with request and response codes from the DriveLock Operations Center (DOC).

Please do the following:

- 1. Open the **DOC** (from the DriveLock Control Center or from a browser).
- 2. Select the Tasks section and choose BitLocker To Go recovery.
- By now, the user on the client computer has launched the Recovery Wizard and retrieved the **request code**.
   Ask the user to pass it on to you.
- 4. Enter the **request code** in your DOC screen.



= 🗙 Drive	Lock	🙁 Administrator@root (Administrator) 🤱 My account	🌐 en
Dashboard	Tasks		
	File Protection recovery Encryption 2-Go recovery	Recover data protected with BitLocker To Go	^
귽. SecAware	BilLocker To Go recovery	Please enter the recovery code as shown on the agent:	
Events		USWID-DUQTB-41BIA	
o-ÇEDR		Recovery data was found. Select the certificate you want to use to generate a response code. The certificate is not transferred over the internet!	
Tasks		Select a certificate DLBI2GoRecovery.ptx	
		Passverd for certificate	- 11
T MAIN.PERMIS		Generate response code	
		Please enter this response code on the agent: RBVQC5-7RUP7L-XPNBZD-N7LBOW-YWD3FZ-P3VBBH-C7ZABG-BD43VN	à

- 5. Select the appropriate **certificate** and the matching password.
- 6. Click Generate response code and share it with the user.
- 7. Next, the user enters the **response code** on the client computer. In the following dialog the user will specify a new user password for the USB storage device.

#### 3.4 DriveLock Agent

#### 3.4.1 BitLocker To Go on the DriveLock Agent

When the user plugs in an external USB storage device or external drive to the DriveLock Agent, the following options are available, depending on the policy settings:

#### 1. Unlocking an encrypted drive

To unlock a drive encrypted with BitLocker To Go, a password entry dialog appears immediately. This allows quick unlocking and access to the existing data.

File     Computer     View	Manage This PC Drive Tools		BitLocker (H:)
$\leftarrow \rightarrow \checkmark \uparrow \blacksquare$ > This PC			Enter password to unlock this drive.
📌 Quick access	Folders (7)		
This PC	3D Objects	Desktop	More options
Desktop	Documents	Downloads	
Documents  Downloads  Music	Music	Pictures	Unlock
Pictures     Videos	Videos		
Local Disk (C:)	<ul> <li>Devices and drives (6)</li> </ul>		
DLV (F:)	Local Disk (C:)	New Volume	(D:)
USB Drive (H:)	DVD Drive (E:)	DLV (F:)	01 5.70 00
DLV (F:)	USB Drive (G:)	202 MB free o	of 399 MB
👝 New Volume (D:)	• 14.1 GB free of 14.6 GB		~
13 items 1 item selected			

2. Various options in the context menu in Windows Explorer:



#### • Mount...

If you want to mount a drive encrypted with BitLocker To Go, clicking this menu item will open a wizard where you can select the appropriate drive letter and enter the password. This option can also be configured so that the password is set as the administrator password and then entered automatically.

#### • Change password...

To change the password of an encrypted drive, click this menu item. Again, a wizard will open where you can first enter your old password and then your new password.

#### Recover...

Use this menu command to restore the password. The recovery process of an encrypted drive takes place between the administrator and the user. For more information, please visit here.

#### Unmount

Use this menu command to unmount the drive, even without having administrator rights.

2	USB Drive (H:)	
	Open	
	Open in new window	
	Pin to Quick access	
	Change BitLocker password	
	Manage BitLocker	
	Open AutoPlay	
	🚼 Scan with Windows Defender	
	Give access to >	
	🔒 Unmount	
	🔒 Change password	

3. If specified, the different options for BitLocker To Go can also be selected from the taskbar, see the figure below:



#### 3.5 Use cases

Please see the use cases for the following DriveLock BitLocker To Go options:

- Administrative password
- Enforced encryption

#### 3.5.1 Administrative password rules

- a. You do not assign an administrative password and allow users to assign a password themselves:
  - During initial encryption, each user may choose their own password for encryption. An encrypted drive can only be automatically decrypted if you allow the user to save the password. On any other computer it must be entered when connecting.
- b. You assign an administrative password and allow users to assign a password themselves:
  - During initial encryption, each user may choose their own password for encryption.
  - The administrative password can be used to automatically decrypt data on corporate computers where the DriveLock Agent is running. The user does not have to enter a password.

# c. You assign an administrative password and choose encryption with administrative password:

- Users cannot assign their own password during initial encryption.
- The removable storage device can only be decrypted on corporate computers where the DriveLock Agent is running
- When connecting the encrypted removable storage device, the user does not need to enter a password
- Outside the company or on company computers without the DriveLock Agent, the data cannot be decrypted
- d. You create multiple administrator password rules, setting filters for users and/or computers and choosing encryption with administrative password:
  - Users cannot assign their own password during initial encryption.
  - The removable storage device can only be decrypted on corporate computers where the DriveLock Agent is running
  - When connecting the encrypted removable storage device, the user does not need to enter a password



- Outside the company or on company computers without the DriveLock Agent, the data cannot be decrypted
- Access is restricted to specific users or to specific computers (e.g. a department or a team):

You create an administrative password rule that is restricted to user group A. User A1 encrypts a USB stick (forced encryption with administrative password) with administrative password.

Result:

The USB stick can only be decrypted if a user from user group A is logged on to a company computer.

Examples:

- USB sticks encrypted in the Human Resources department can only be decrypted by the users of the Human Resources department
- USB sticks encrypted in the Research department can only be decrypted on computers in the Research department

Warning: Note the priority and the filters set on the Users, Computers and Networks tabs.

#### 3.5.2 Encryption rules

- a. For example, you could choose the user group you want your rule to apply to:
  - User group A may assign their own password
  - User group B may not assign their own password
- b. Or you could choose specific company computers you want your rule to apply to:
  - You do not add an administrative password for USB storage devices that are encrypted on the works council computers.
  - All USB storage devices that were encrypted on the computers in the development department may only be decrypted within the company.

# Index

	Α
assignment 41	
authentication type 22, 31	
	В
BitLocker license 9	
	с
certificate store 10, 35	
Copyright 100	
	D
data partition 23	
decryption 15, 18, 28	
	E
encryption 6, 10, 15, 24, 31, 34, 41-42	
encryption algorithm 16, 31	
encryption certificates 10-11, 31	
encryption method 16	
events 54	
	н
hard disks 6, 15, 22, 27, 31-32, 40	
hardware encryption 16	
	I
Index 98	
	Ρ
password options 24, 31	
pre-boot authentication 22, 31, 41, 44	

private key 12, 20

R

recovery 10-11, 20, 32, 34

recovery keys 35

S

system partition 23, 32, 35, 44





# 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.

