



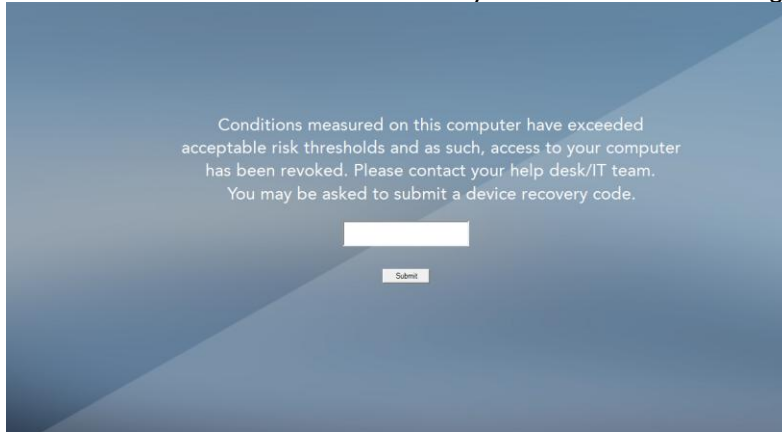
ScreenLock Response

When the computer status is set to Quarantine

When the computer status is set to **Kill**

ScreenLock immediately prevents an unauthorized user—even one with valid login credentials—from accessing the computer and can be used regardless of the encryption method in place. It provides a particularly simple alternative for computers using BitLocker-only encryption because access can be restored without requiring the user to enter a 48-character BitLocker recovery key. To restore access, an administrator can select the computer from the Computer Listing and click **Restore from Quarantine**. ScreenLock will be removed the next time the computer checks in.

Alternatively, the administrator can provide the user with a **Recovery Code** by selecting **More Actions > Recovery Code**. The user can enter this code directly into the ScreenLock dialog to restore access.



To recover access, the administrator can select the computer from the computer listing and click “Restore from Quarantine”. The ScreenLock window will be dismissed after the computer checks in. Alternatively, the administrator can provide the user with the recovery code by selecting the computer and clicking “Recovery Code” from the “More Actions...” link.

Computer Listing:

Change Status Quarantine Restore from Quarantine More Actions...

Computer Name	OS	OS Build	Accts	Check In	Online	Updated	Risk	Status	Version	Modified	Encryption Risk	Encryption
BHWin1126H1	Windows 11 Pro	28000.2704	2	Connected	✓	✓	✓	Active	6.11.1	8-28-2026 at 4:13PM	✓	BitLocker

ABOUT BEACHHEAD | SUPPORT | CONTACT US | HELPDESK TICKET

- Restart Computer
- Check In
- Lock Device
- Send Message
- Uninstall
- Clear Isolation
- Restore OneDrive
- Show Location
- Compliance Report
- Recovery Code

The ScreenLock action will be added disabled to the RiskResponders® wherever there is a “Revoke access to EFS encrypted files” action. An administrator just needs to turn on the action for it to take effect.

Administrator MFA Reset

Administrators can now reset MFA for another administrator. Resetting MFA turns off MFA for the next login. If MFA is mandatory, the administrator will be required to set up MFA again after logging in. If MFA is optional or off, the administrator must manually turn MFA back on by clicking their name in the header or selecting their account from the administrator listing. To reset MFA, go to the administrator listing page, select the checkbox next to the administrator whose MFA should be reset, and select “Reset MFA”.

Administrator Listing:

Add New Delete Audit Log Password Policy Reset MFA

Account	Admin ID	Email	First Name	Last Name	Type	Last Login
consumer1	consumer1	consumer@consumer1.com	John	Doe	Full Rights	2-15-2018 at 1:51PM

BitLocker Management Update

The “Suspend BitLocker” menu item has been replaced with “Manage BitLocker”. After selecting a computer, click “Manage BitLocker” to open a pop-up where the administrator can choose one of three actions: “Decrypt and Encrypt BitLocker”, “Suspend BitLocker”, or “Decrypt BitLocker”.

Computer Listing:

Change Status

Quarantine

Restore from Quarantine

More Actions...

	Computer Name	OS	OS Build	Accts	Check In	Online	Updated	Risk	Status	Version	Modified	Encryption Risk	Encryption
☒	BHWin1126H1	Windows 11 Pro	28000.2704	2	Connected	✓	✓	✓	Active	6.11.1	8-28-2026 at 10:20AM	✓	BitLocker

Restart Computer

Check In

Lock Device

Send Message

Uninstall

Clear Isolation

Restore OneDrive

Show Location

Compliance Report

Recovery Code

Manage BitLocker

Clear PCR Warnings

[ABOUT BEACHHEAD](#) | [SUPPORT](#) | [CONTACT US](#) | [HELPDESK TICKET](#)

“Decrypt and Encrypt BitLocker” displays options that allow the administrator to change BitLocker encryption settings and apply them to one or more computers.

Manage BitLocker

☐ Decrypt and Encrypt BitLocker
 ☐ Suspend BitLocker
 ☐ Decrypt BitLocker

OK

Cancel

☒ Decrypt and Encrypt BitLocker

BitLocker Authentication Mode

You can use TPM Authentication only, TPM Authentication plus a user entered pin, or create a password to secure the OS drive (requires Windows 8 Pro or later using agent version 6.5 or later).

No change

BitLocker Encryption Settings:

Use defaults

These options match the settings available on the BitLocker tab for a computer. “Suspend BitLocker” displays options that allow the administrator to suspend protection temporarily or indefinitely. To suspend BitLocker, select “Temporarily suspend BitLocker protection”, choose the time frame for re-enabling protection, and click “OK”. To resume BitLocker protection, clear the “Temporarily suspend BitLocker protection” checkbox and click “OK”. These settings are also available on the BitLocker tab for a computer.

☒ Suspend BitLocker

☐ Temporarily suspend BitLocker protection

When checked, the client will suspend all of the BitLocker keys which is useful when you are doing hardware or system updates to the device.

Indefinitely

Selecting “Decrypt BitLocker” will begin the process of decrypting a BitLocker-protected drive.

BitLocker Tab/BitLocker Recovery Changes

The BitLocker tab UI has been modified to make management simpler.

BitLocker:

BHWin1126H1 (BHS_INTERNAL)

Recovery Keys

Recovery Key ID	Volume ID	Volume	Value	Last Updated
0a9d8c83-b6e0-48bd-be37-66...	515694883	C:	View	8-28-2026 at 3:31PM

If BitLocker is asking for a key that does not match any of the above recovery Key IDs, try the Secure Decommission key, or contact support.

Secure Decommission Keys

Volume ID	Value	Last Updated
515694883	View	8-28-2026 at 10:20AM

Volumes

Volume	Status	Type	Encryption Type	Encryption Flags	Volume ID	Last Updated
C:	Fully encrypted.	Unprotected	TPM	XTS-AES 128	515694883	8-28-2026 at ...

TPM Status

TPM Version	TPM Activated	TPM Enabled	TPM Owned	TPM Ownership Allowed	Preboot	Partition Style
2.0	Yes	Yes	Yes	Yes	UEFI	GPT

Recovery keys and Secure Decommission keys have been moved into separate tables. In the Volumes table, the primary key protector for the OS drive now shows only the protector type in the Type column.

The BitLocker Recovery listing has also been modified so that it will only list the Recovery Keys and Secure Decommission Keys.

Installers

Users

Computers

ComplianceEZ®

USB Storage

Mobile

Computers

RiskResponders®

Windows Security

Account Settings

BitLocker Recovery ▼

+

Status: Active ▼ x

BitLocker Key Listing:

Recovery Key ID	Value	Volume ID	Type	Computer Name	Status
00000000-0000-0000-0000-000000000000	View	515694883	Numeric password	BHWin1126H1	Active
0a9d8c83-b6e0-48bd-be37-668cc0cec3a8	View	515694883	Numeric password	BHWin1126H1	Active

ComplianceEZ® BHS Addressable Indicator & Last Modified

An indicator has been added to the ComplianceEZ® page to show whether a BHS-provided implementation satisfies or partially satisfies a control. A filled dot indicates that a BHS-provided implementation satisfies the control. A hollow dot indicates that no BHS-provided implementation is available for that control. The “Last Modified” column has been added to the table to track when changes were made to each control.

ComplianceEZ® Dashboard

Security Posture for HIPAA Technical Controls Controls (55)

☐ Show only tracked controls

Track	BHS Addressable	Last Modified	Control
> ☐	☐	2026-08-21 15:04	45 CFR 164.308(2)
✓ ☒	☒	2026-08-25 7:53	45 CFR 164.308(3)(i)

ComplianceEZ® Report Scheduling

Report scheduling for ComplianceEZ® has been added. To schedule reports, go to the ComplianceEZ® page, click “Output Report”, and select “Schedule Report”.

Security Posture for HIPAA Technical Controls Controls (55)

+

Search

Output Report ▼

☐ Show only tracked controls

Track	BHS Addressable	Last Modified	Control	Description
> ☐	☐	2026-08-21 15:04	45 CFR 164.308(2)	Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies
✓ ☒	☒	2026-08-25 7:53	45 CFR 164.308(3)(i)	Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic

Track

Platform

BHS CUSTOM

Implementation Details

Download PDF

Download Excel

Schedule Report

This opens a report creation pop-up where the administrator can select report options.

Schedule Report

Schedule to run

Run:

Run:

Recipient email(s)

Report Options

☒ Assessment Stats
☒ Assessment Summary
☒ Controls
☒ List only
☐ With Implementations
☐ Only Tracked

Manage Reports

OK

Cancel

Clicking “OK” schedules the report to run based on the selected options.

EFS Path Updates

New data locations have been added for EFS targeting, along with CAD file types and several other data types.

CAD File Types: .dwg, .iges, .igs, .sldasm, .sldprt, .step, .stp

Other File Types: .eml, .webp, .wmv

Install Alerts

The server now generates alerts when an install fails during the install web call. For example, an alert is generated if there are not enough licenses or if a computer with the same name already exists.

MFA Policy Application

The MFA policy can now be applied to all users, domain users, or local users. This policy is applied from the Authentication Policies section on the RiskResponders® page. By default, the MFA policy applies to all users.

Policy	Actions
☐ Multifactor authentication (MFA)	
Multifactor Authentication	☐ Off ☐ Optional ☒ Mandatory
Reset users' settings	☐
Allowed authentication types	Authenticator App (TOTP) or Hardware Token
Authentication is required every	24 hours
Message to display to prompt the user to setup multifactor authentication	Please set up 2FA for your machine according to the BH_INTERNAL account policy.
Apply Policy	All users ☐ All users ☐ Local users only ☐ Domain users only
Update	
☐ Password enforcement for non-domain computers	

MFA Setup Code

Administrators can require a setup code before allowing users to set up MFA. To configure an MFA setup code, navigate to the RiskResponders® page and expand the Authentication Policies section. In the Multifactor Authentication (MFA) settings, change Multifactor Authentication to Mandatory. Then select Yes for MFA Setup Code and enter a setup code.

Administrators are responsible for communicating the MFA setup code to users because it is required to set up MFA. If MFA is not set up, the computer cannot be used.

Policies related to end user logons

Policy	Actions
☐ Multifactor authentication (MFA)	
Multifactor Authentication	☐ Off ☐ Optional ☒ Mandatory
Reset users' settings	☐
Allowed authentication types	Authenticator App (TOTP) or Hardware Token
Authentication is required every	24 hours
Prompt on resume	☐ No ☒ Yes
Don't prompt if connected	☐ No ☒ Yes
Message to display to prompt the user to setup multifactor authentication	Please set up 2FA for your machine according to the BH_INTERNAL account policy.
Use MFA Setup Code	☐ No ☒ Yes
MFA Setup Code	123456
Apply Policy	All users
Cancel Update	
☐ Password enforcement for non-domain computers	

NOTE: This feature is currently PC-only. In a future release, it will be added to the Mac agent.

OS Version Reporting

The server now retrieves the latest Mac and PC OS versions and attempts to indicate whether each computer is up to date. On the computer listing page, OS version numbers appear in the OS Build column. If a computer is not running the latest OS version, the OS Build text is highlighted; clicking the highlighted text opens an information pop-up.

ComputersRiskResponders®Windows SecurityAccount Settings

Computer Name: BHWin1126H1 x

Computer Listing:

Computer Name	OS	OS Build
BHWin1126H1	Windows 11 Pro	28000.2704

OS	OS Build
Windows 11 Pro	28000.2704
Windows 10 Pro	19043.2006

OS update 19044.7548 is available as of 2021-11-16. Service is available for this update through 2027-1-12: Long-Term Servicing Channel (LTSC). More information is available here: <https://support.microsoft.com/help/5099539>

OK

Report Updates

Reports have been updated to include Location. The EFS Encryption Status check in the Compliance report has also been updated to verify that EFS is being used on the computer.

Simplified UI-Attach/Detach Changes

The attaching and detaching from accounts has changed. Instead of attaching to an account, an administrator will manage an account. On the account listing and in the header, an administrator will see “Manage Account”. Clicking “Manage Account” will allow the administrator to work on the account. Administrators can also choose not to show the confirmation message that appears by default when managing an account.

Search

Account Listing:Manage Account

Account	Parent	Description
---------	--------	-------------

Account:
BHS_INTERNAL

You are about to switch from account **ROOT** to **BHS_INTERNAL**. After switching, you will be working in the BHS_INTERNAL account. Any policies, settings, or administrative actions will apply to BHS_INTERNAL until you switch again.

☐ Don't show this message box again

OKCancel

Administrators are placed in Default view for the account, but they can switch to Advanced view by clicking “Advanced” in the header. Default view is equivalent to Customer view. Advanced view is equivalent to the previous MSP View or Support View.

Mobile

Administrators

If the administrator is in Advanced view, the link changes to “Default” to return to Default view. To manage another account, click “Manage Account”. To return to the administrator’s own account, click “Return to Admin Account” in the header, which is equivalent to Detach.