Self-service BitLocker recovery key tools enhance security and reduce costs

Microsoft Core Services Engineering & Operations (CSEO, formerly Microsoft IT) uses BitLocker—the Windows operating system disk encryption and data protection feature—for both hardware enforcement and data protection. If a security condition is detected, BitLocker locks the operating system drive and requires a unique BitLocker recovery key to unlock it. The feature helps protect not only data, but also personal information and access to corporate networks.

Outside of a theft scenario, there are a variety of reasons that a BitLocker recovery key might be needed. They include hardware issues, operating system upgrades, or failed BIOS updates. In all of these situations, you can’t use your computer without a BitLocker recovery key.

Previously, if our employees didn’t know their BitLocker recovery key, they would have to call Helpdesk. These calls typically lasted about an hour, resulted in lost productivity, and tied up the Helpdesk technician. The employee would have to authenticate themselves to Helpdesk and the Helpdesk technician would recover the key on the employee’s behalf.

Our employees needed to be able to access their own BitLocker recovery key without the hassle of calling Helpdesk. We used Microsoft BitLocker Administration and Monitoring (MBAM), which provides enterprise management capabilities for BitLocker, to create a self-service BitLocker recovery key portal. Figure 1 shows the portal.
Remote solution needed

Even with the portal in place, it was still challenging for some of our remote workers. For example, a field-based sales employee might stay at a hotel where they couldn’t use a VPN or Direct Access connection to reach the corporate network. Typically armed with just their laptop and their phone, productivity effectively ground to a halt. They had to use valuable time to call Helpdesk, verify their identity and credentials, and work with the Helpdesk technician to access the recovery key on their behalf.

Over time, BitLocker recovery key calls consumed a lot of Helpdesk tickets and resource bandwidth. In fact, BitLocker recovery key call requests became the second most common type of call! Helpdesk always had to be staffed and prepared to support our employees, globally. Also, to obtain a BitLocker recovery key for an employee, the Helpdesk representative would have access to the employee’s recovery key information. This created a security risk because someone other than the employee had access to their recovery key.

microsoft.com/itshowcase  October 2018
We wanted to lower the number of calls to Helpdesk, while also reducing security risks. The challenge was to extend the on-premises portal to our remote employees so that they could use the BitLocker recovery key portal without corporate network connectivity.

Creating a companion web app

We knew that the solution needed to extend the MBAM self-service portal to any device with Internet access, such as a phone. To do this, we used Azure Active Directory Application Proxy (Azure AD Application Proxy) to publish a token conversion web app.

Azure AD Application Proxy helps bridge the gap between apps that were designed for on-premises environments that companies might want to move to the cloud. It also lets companies continue to use apps that simply can’t move to the public cloud. Azure AD Application Proxy uses our existing recovery key portal in the cloud—without having to extensively rewrite code.

How it works

The web app allows our employees to authenticate from a phone or any other mobile device that can access the Internet. They simply navigate to a web address, and then easily access their BitLocker recovery key without having to call Helpdesk.

The web app follows a series of steps to generate a recovery key.

1. The web app redirects to Azure Active Directory for identity authentication.
2. After successful authentication, a token is generated.
3. Principal name and service principal name properties are extracted from the token and provided to the Application Proxy Connector.
4. The Application Proxy Connector, using Kerberos-constrained delegation, requests a Kerberos token on the employee’s behalf.
5. The Kerberos verification ticket is retrieved from Active Directory.
6. The verification ticket is sent back to the Application Proxy Connector, where it is verified.
7. A response is sent to the employee, through the Azure AD Application Proxy.

Figure 2 shows the process.

![Figure 2. The token conversion web app process](image)
Developing the solution quickly

Creating the web app companion to the portal was very straightforward. Because the BitLocker recovery key portal already existed, much of the work on the web app involved changes to existing Active Directory and Azure services, and making sure that the services could communicate with each other.

In just about a week, the web app owner was able to perform replication and testing tasks. After standard user acceptance testing was completed, minor server modifications were made. Overall, the solution was much simpler and required far fewer resources than those of older web publishing technologies.

We aggressively continue our digital transformation to the cloud. We want to code directly for the cloud, and we want our employees to authenticate directly to Azure AD. However, in this scenario, we had very specific needs. We wanted to support our remote personnel and their productivity while lowering Helpdesk costs at the same time. We were able to quickly create a solution with Azure AD Application Proxy and keep our remote employees productive and secure.

NOTE: Azure AD Application Proxy and its extensive publishing functionality is available in the Basic and Premium editions of Azure Active Directory.

Improving the user experience

It’s easy for our remote employees to use the web app from an Internet-enabled phone, tablet, or another mobile device. They simply use a browser to navigate from the web app to the recovery key portal. To help ensure security, they’re prompted for multi-factor authentication. If the employee happens to be using another app in Azure, such as the Office 365 portal, their existing token will be used for the portal, and they do not have to sign in again.

Using the web app, it takes about five minutes for the employee to generate their BitLocker recovery key. This compares to the hour it took when they had to call Helpdesk.

Benefits

Our BitLocker recovery key solutions—the portal and web app—provide substantial productivity, resource, and security benefits. The tools get our employees back to a productive state, faster. An hour-long call has been replaced with a simple five-minute, self-service procedure.

The portal and web app free our Helpdesk resources for other tasks. For example, BitLocker-related Helpdesk calls were reduced by 20 percent shortly after the portal was released.

The solutions enhance security in a variety of ways. They minimize the number of transactions that a BitLocker recovery key must pass through. With the portal and the web app, only the employee interacts with their confidential recovery data.

Also, because our portal and web app were created with MBAM, a BitLocker recovery key is only good for a single use. If the employee needs a recovery key, a new key is generated and never used again.

We used to recommend that employees keep an extra copy of their BitLocker recovery key, in the form of a printout or saved to a USB drive, for safekeeping. In addition to the obvious issue—employees must remember where they hid the key—compromising one of these copies is a real risk. With our MBAM portal and web app in place, there is no reason for employees to create extra copies of their BitLocker recovery key for safekeeping because the key will never be used again. In a native BitLocker scenario, a recovery key can be used more than once. The recovery key is valid until BitLocker is disabled and then re-encrypted.

Conclusion

BitLocker is an essential protection mechanism for Microsoft and is applied to all our corporate assets. Our BitLocker recovery key solutions, enabled with MBAM, have evolved to a secure, fast, and efficient self-service portal and
The solutions save our employees time and increase their productivity, allow more strategic deployment of Helpdesk resources, and enhance security.

For more information

Azure Active Directory documentation
Azure Active Directory editions
Application Proxy blog on TechNet
Ask the Directory Services Team
Microsoft Desktop Optimization Pack Information Experience

Microsoft IT Showcase
microsoft.com/itshowcase