XenVault Plug-in

Contents

XenVault Plug-in

The XenVault plug-in provides protection for corporate data on user devices, particularly devices like laptop computers regardless of whether the device is a member of the corporate domain. The plug-in creates a password-protected area on the user device where data is encrypted and only corporate applications delivered through the Citrix Receiver and Microsoft Application Virtualization (App-V) have access. The XenVault plug-in enables you to lock, unlock, and delete the safe zone as necessary.

Product documentation is available for the following XenVault plug-in release:

- XenVault Plug-in 1.0

Quick Links

- About XenVault 1.0
- Protecting Corporate Data

XenVault Plug-in 1.0

The XenVault plug-in provides protection for corporate data on user devices, particularly devices like laptop computers regardless of whether the device is a member of the corporate domain. The plug-in creates a password-protected area on the user device where data is encrypted and only corporate applications delivered through the Citrix Receiver and Microsoft Application Virtualization (App-V) have access. The XenVault plug-in enables you to lock, unlock, and delete the area as necessary.

In This Section

XenVault Plug-in 1.0

The XenVault plug-in provides protection for corporate data on user devices, particularly devices like laptop computers regardless of whether the device is a member of the corporate domain. The plug-in creates a password-protected area on the user device where data is encrypted and only corporate applications delivered through the Citrix Receiver and Microsoft Application Virtualization (App-V) have access. The XenVault plug-in enables you to lock, unlock, and delete the area as necessary.

In This Section

About XenVault Plug-in 1.0

The XenVault plug-in provides protection for corporate data on user devices, particularly devices like laptop computers regardless of whether the device is a member of the corporate domain. The plug-in creates a password-protected area on the user device where data is encrypted and only accessible through corporate applications delivered through the Citrix Receiver and Microsoft Application Virtualization (App-V). The XenVault plug-in enables you to lock, unlock, and delete the library as necessary.

The plug-in features include:

- **Encrypted area on the user device**. When the XenVault plug-in is delivered to the user device, it creates an AES-256 level encrypted library in which corporate data is stored. The encrypted library, referred to as a safe zone, is connected to Drive X: if it is available. XenVault is FIPS 140 compliant.
- **Safe zone accessible only with trusted applications.** By default, only applications delivered through Citrix Receiver and App-V can access data stored in the safe zone.
- **Targeted lock or delete of safe zones.** Through the use of targeted rules in Citrix Merchandising Server, you can lock or delete the safe zone on a single user device or entire groups of user devices.
- **Automated lock of safe zones based on time off the corporate network.** Specify the maximum number of days a user device can use a safe zone before logging back on to the corporate network. If that number is exceeded, the safe zone automatically locks.
- **Self-service password reset.** You can enable users to reset their own safe zone passwords.

System Requirements

The following are required in order to configure and deploy XenVault Plug-in:

- Citrix Receiver 2.0 for Windows
- Citrix Merchandising Server 2.0

User devices require Microsoft Windows 7.

Known Issues

This section contains:

- Installation issues
- Other known issues

- Third-party issues

Installation Issues

- **Safe zone locks unexpectedly if special characters are included in auto-lock value**

  Values in the **Time off the network until auto-lock (days)** field of the XenVault plug-in **Configuration** page in Citrix Merchandising Server are misread if commas, periods, or other special characters are used. Citrix Merchandising Server ignores any digits to the right of the special character causing the safe zone to lock at an unexpected time. For example, a value of 1,321 days becomes 1 day. Similarly, 3.5 days becomes 3 days. Do not use commas, periods, or other special characters when setting this value. [#241800]

- **Installation Fails if Surrogate Character Pairs are Used in Merchandising Server Deployment**

  If surrogate character pairs are used in the **Name of Safe Zone** field of the Citrix XenVault plug-in **Configuration** page in Citrix Merchandising Server, installation will fail. Surrogate pairs, which are two 16-bit code units that combine to make a single character, should not be used in the **Name of Safe Zone** field. After installation, rename the safe zone to include surrogate pairs if necessary. [#239021]

Other Known Issues

- **Printing data in the safe zone leaves the data unprotected while in the printer spooler**

  When printing data stored in the safe zone, the data passes through a print spooler outside the safe zone. During the time the data is in the print spooler, it is not protected. [#242425]

Third-Party Issues

- **Confusing messages may appear when saving with Citrix Receiver-delivered Microsoft Word**

  When saving a document, Citrix Receiver-delivered Microsoft Word may deliver two confusing feedback messages. One message indicates the user cannot save to the safe zone and offers to save to the My Documents folder. By clicking **Yes**, the user actually saves to the safe zone. The second message may appear after successfully saving a document. The message asks the user to "Check the drive to make sure the door is closed and it contains the correct disk or CD." Clicking **OK** closes this message. [#243254]

- **Microsoft Outlook cannot open certain email attachments when the XenVault plug-in is running**

  Microsoft Outlook cannot open graphics files attached to email using the default Windows Photo Viewer. A message stating the picture cannot be opened appears. Reset the default program for popular graphic file types to another program, such as Microsoft Paint. [#245015]

  Microsoft Outlook cannot open HTML files attached to email in a new tab in an open instance of Windows Internet Explorer. No error message or indicator of a problem occurs. To open the HTML files, open the attachment in a new window. [#243047]

- **Overwriting an unprotected file outside the safe zone with a copy from the safe zone may result in loss of the unprotected copy**

  Attempting to overwrite an unprotected file with a copy from the safe zone using Windows Explorer may result in loss of the unprotected copy. This situation occurs if **Allow Windows Explorer to read from files inside Safe Zone** was not enabled in the XenVault plug-in delivery through Merchandising Server. If a recipient of this delivery tries to overwrite a file outside the safe zone with a copy from the safe zone, the process fails and the copy outside the safe zone is deleted. [# 245574]

Protecting Corporate Data with an Encrypted Safe Zone

The XenVault plug-in provides protection for corporate data on user devices, particularly mobile devices like laptop computers and non-corporate owned devices. The plug-in creates a password-protected area on the user device where data is encrypted and only applications delivered through the Citrix Receiver and Microsoft Application Virtualization (App-V) have access.

To deliver the XenVault plug-in

In the Merchandising Server, prepare a delivery for the XenVault plug-in. At the scheduled time, the plug-in is delivered to users automatically.

1. Ensure Citrix Receiver is installed on your users' devices. See Installing Receiver for Windows for details.
2. If necessary, download the XenVault plug-in and metadata to the Merchandising Server. See Preparing Updates for details.
3. Create a rule to specify XenVault plug-in recipients. See Creating Delivery Recipient Rules for details.
4. Create a delivery for XenVault plug-in. See Creating Deliveries for details.

   Note: Do not use the special characters \ / : * ? < > | in the Name of Safe Zone field. Microsoft Windows standards prohibit these. If used, Merchandising Server changes each to _ when the safe zone is created.

To set password policies

On the **Configuration** page in the Merchandising Server, while creating or editing delivery settings, define XenVault password policies.

1. Click **Allow client to save password locally** to allow users the option of saving their XenVault passwords on their devices. If a user enables this option, the safe zone is automatically unlocked when Citrix Receiver starts.
2. In the **Minimum characters to require in passwords (will always be at least 1)** field, type the minimum number of characters a XenVault password can contain. If the field is blank, six characters are required.
3. Click **Enforce complexity requirements on passwords** to ensure users' XenVault passwords comply with the following password complexity requirements.

   - The password meets the minimum number of characters set in Step 2.

- The password contains a combination of at least three of the following character types:
    - Uppercase letters
    - Lowercase letters
    - Numbers
    - Symbols
- The password does not include the related user name.

Protecting Data by Locking the Safe Zone

The XenVault plug-in enables you to lock the safe zone on targeted user devices. You can target one user device or a group of devices. Data Lock deletes the encryption key, or header, data from targeted users' devices.

You can also lock users' safe zone data if they have not signed on to the network over a specified number of days. You can include this automatic data locking command in your initial XenVault plug-in delivery or as an update at a later time.

To back up header data from a user device

Before locking the safe zone on a user device, back up the header data from the device to ensure it can be unlocked. The Back Up command can be included in the delivery initially setting up the safe zone or most subsequent deliveries.

Caution: Do not include the Back Up command in the same delivery as the Data Lock command. Doing so may lock the safe zone, but not back up the header data. As a result, the safe zone cannot be unlocked.

1. In the Merchandising Server, create a rule to ensure the Backup command is delivered only to the targeted user devices.
2. Create a new delivery, adding the XenVault plug-in.
3. On the **General** page, make the **Evaluation order** setting for this delivery higher than that used for the general delivery of the XenVault plug-in. If a user device is targeted by multiple deliveries at the same time, it will only receive the delivery with the highest evaluation order, such as 4 instead of 10.
4. On the **Configuration** page, select **Back up header for unlock**.
5. Fill in the **UNC path for data lock/unlock backup** field with the UNC path to a hidden corporate network file share where the users have read, write, and modify permission. The users' encryption keys will be backed up to this location, enabling you to unlock the safe zone at a later time. If you do not provide this path, you will not be able to unlock the safe zones.
6. On the **Rules** page, add the targeting rule you created in Step 1.
7. On the **Schedule** page, schedule the delivery.

Once the delivery is activated, the header data is backed up to the file share you identified in Step 5. You can confirm that the backup has occurred by looking at that file share. A folder for each user containing the following files dated after the delivery indicates a successful backup:

- [BACKUP_UNC]\[USERNAME]\[COMPUTERNAME].backup — password reset backup file

- [BACKUP_UNC]\[USERNAME]\[COMPUTERNAME].que — questions backup file
- [BACKUP_UNC]\[USERNAME]\[COMPUTERNAME].unlock — unlock backup file

To lock data on targeted user devices

Before locking a safe zone, back up the header data. You cannot unlock a safe zone without a backup copy of the header data.

1. In the Merchandising Server, create a rule to ensure the Data Lock command is delivered only to the targeted user devices.
2. Create a new delivery, adding the XenVault plug-in.
3. On the **General** page, make the **Evaluation order** setting for this delivery higher than that used for the general delivery of the XenVault plug-in. If a user device is targeted by multiple deliveries at the same time, it will only receive the delivery with the highest evaluation order, such as 4 instead of 10.
4. On the **Configuration** page, select **Lock client's Safe Zone**.
5. On the **Rules** page, add the targeting rule you created in Step 1.
6. On the **Schedule** page, schedule the delivery.

Once the delivery is activated, the safe zone is locked as follows:

- If Receiver on the targeted user device checks the Merchandising Server for updates upon network logon, the Data Lock command is received and the safe zone is locked. The drive associated with the safe zone, typically Drive X:, is not attached to the user device.
- If the drive with the safe zone is already attached to the user device, but is not in use when the delivery is received, the drive is detached and the safe zone is locked.
- If the drive with the safe zone is already attached to the user device and in use when the delivery is received, the user can continue working in the safe zone with any applications currently in use. No additional applications are given access to the safe zone, however. Once the user completes work in the safe zone, the safe zone is locked. The drive associated with the safe zone is then detached.

To lock data after a user device has been off-network for a specified number of days

Before issuing this delivery, back up the header data. You cannot unlock a safe zone without a backup copy of the header data.

1. In the Merchandising Server, create a rule to ensure the Automatic Lock command is delivered only to the targeted user devices.
2. Create a new delivery, adding the XenVault plug-in.

3. On the **General** page, make the **Evaluation order** setting for this delivery higher than that used for the general delivery of the XenVault plug-in. If a user device is targeted by multiple deliveries at the same time, it will only receive the delivery with the highest evaluation order, such as 4 instead of 10.

4. On the **Configuration** page in the Merchandising Server, select **Automatically lock the Safe Zone based on a client's time off of the corporate network**.

5. Type the number of days the user devices may be off-network before triggering automatic safe zone locking in **Time off the network until auto-lock (days)**. The number must be higher than the number of days in **Check for updates** on the **Create a Delivery** page. If **Check for updates** is blank, Merchandising Server uses one day.

   Important: Do not use special characters, such as commas or periods, in the **Time off the network until auto-lock (days)** field. Merchandising Server ignores any digits to the right of the special character. For example, 1,395 days becomes 1 day, while 4.5 days is 4 days.

6. If you want to allow your users to automatically unlock their safe zones the next time they connect to the network, select **On auto-lock, do not erase the user's key to the Safe Zone**.

7. On the **Rules** page, add the targeting rule you created in Step 1.

8. On the **Schedule** page, schedule the delivery.

Warnings that the safe zone is about to be locked are issued to affected users at the following milestones:

- Two days remaining.
- One day remaining.
- Twelve hours remaining.
- Two hours remaining
- Ten minutes remaining.

If Receiver is not in use when the warnings are issued, they will appear the next time the user logs on to Receiver. However, if the allotted time has elapsed, the safe zone locks immediately.

Note: Warnings are suppressed if the warning milestone is greater than 60% of the days entered into the **Time off the network until auto-lock (days)** field. For example, the two day warning is not sent when 3 has been typed in the field.

To unlock data

If you backed up the users' encrypted keys, you can unlock locked safe zones. Typically, you would unlock safe zones after receiving requests from users.

1. In the Merchandising Server, create a rule to ensure the Unlock command is delivered only to the targeted user devices.

2. Create a new delivery, adding the XenVault plug-in.

3. On the **General** page, make the **Evaluation order** setting for this delivery higher than that used for the general delivery of the XenVault plug-in. If a user device is targeted by multiple deliveries at the same time, it will only receive the delivery with the highest evaluation order, such as 4 instead of 10.

4. On the **Configuration** page, select **Unlock client's Safe Zone**.

5. Fill in the **UNC path for data lock/unlock backup** field.

6. On the **Rules** page, add the targeting rule you created in Step 1.

7. On the **Schedule** page, schedule the delivery.

8. Notify the users that the safe zone should be unlocked the next time they log onto the network.

When the users log on, the XenVault delivery is received, copying the users' encrypted key back to the user devices.

Deleting the Safe Zone

Deleting safe zones on user devices requires preparing targeted deliveries containing the Data Delete command. The user must logon at least once to receive this targeted delivery in order for it to be executed and the safe zone deleted.

To delete the safe zone on targeted user devices

1. In the Merchandising Server, create a rule to ensure the Data Delete command is delivered only to the targeted user devices.
2. Create a new delivery, adding the XenVault plug-in.
3. On the **Configuration** page, select **Delete client's Safe Zone**.
4. On the **Rules** page, add the targeting rule you created in Step 1.
5. On the **Schedule** page, schedule the delivery.

Once the delivery is activated, the safe zone is deleted as follows:

- If Receiver on the targeted user device checks the Merchandising Server for updates upon network logon, the Data Delete command is received and the safe zone and its contents are deleted. The drive associated with the safe zone, typically Drive X:, is not attached to the user device.
- If the drive with the safe zone is already attached to the user device, but is not in use when the delivery is received, the drive is detached and the safe zone and its contents are deleted.
- If the drive with the safe zone is already attached to the user device and in use when the delivery is received, the user can continue working in the safe zone with any applications currently in use. No additional applications are given access to the safe zone, however. Once the user completes work in the safe zone, the safe zone and its contents are deleted. The drive associated with the safe zone is then detached.

Allowing Users to Reset Their Passwords

You can allow users to reset their safe zone passwords from their devices. For this to occur, first back up the users' unique header data which includes their answers to the security questions. Issue this command when initially setting up the safe zone or at a later time.

Before locking the safe zone on a user device, back up the header data from the device to ensure it can be unlocked.

1. On the **Configuration** page in the Merchandising Server, select **Back up header for password reset**.

2. Select **Allow client to reset password**.

3. Fill in the **UNC path for data lock/unlock backup** field with the UNC path to a hidden corporate network file share where the users have read, write, and modify permission. The users' encryption keys will be backed up to this location.

The next time a user logs on to the corporate network after receiving this delivery, the user provides answers to three security questions. These answers provide a means of identity verification when the user does a password reset. Once a user provides initial answers to the security questions, a backup of the header data is created. You can confirm that the backup has occurred by looking at the file share you identified in Step 3. A folder for each user containing the following files dated after the delivery indicates a successful backup:

- [BACKUP_UNC]\[USERNAME]\[COMPUTERNAME].backup -- password reset backup file

- [BACKUP_UNC]\[USERNAME]\[COMPUTERNAME].que -- questions backup file

- [BACKUP_UNC]\[USERNAME]\[COMPUTERNAME].unlock -- unlock backup file