GoldKey® Software

User's Manual

Revision 7.12

WideBand Corporation
www.goldkey.com

Table of Contents

GoldKey Installation and Quick Start

To download the GoldKey software, open a browser and go to the following website:

http://www.goldkey.com/downloads

The GoldKey software is currently supported on Windows XP, Vista, 7, and 8 in both 32 and 64-bit versions, as well as in Mac OS X v10.5 (OS X Leopard) or higher. To use a GoldKey, computers must have an available USB port.

While installing the GoldKey software, you will most likely find the defaults to be acceptable. After a successful installation, you should reboot your computer if prompted.

Initial Personalization

Before you can use a GoldKey, it must be personalized. All GoldKey tokens should be registered to the appropriate Master before they are personalized. Masters can only unlock data encrypted by tokens that have been registered to them.

Figure 1. Before you personalize your GoldKey token, you will be given an opportunity to register it to a master, or to the GoldKey ID service online.

You will be given the option to register your GoldKey token to a Master over the Internet. Doing this allows you to utilize many of the GoldKey Master Functions via GoldKeyID.com. If you do not have a Master or have not received your token as part of an organization, we recommend using GoldKeyID.com.

Note: *If you received your GoldKey as part of an organization, it may already be personalized. In this case, you will need to know the PIN, along with the answer to a personal question, in order to re-personalize the token. See the Personalizing Your GoldKey section for more information.*

Creating a Primary Secure Drive

To begin using GoldKey encryption to secure your data, you will need to create a Secure Drive. If you have not already created a Primary Secure Drive, you may do so by clicking on the Create Primary Drive button in the GoldKey software.

Be sure to make your Secure Drive large enough to hold the information you would like to encrypt (see Figure 2). This drive cannot be resized later on. However, you may create more Secure Drives.

One feature of the Primary Secure Drive is that it supports Secure Folders. When you encrypt a folder using the Folder Encryption tab (see Figure 7), or by checking a box beside a folder to move during creation (see Figure 2), you encrypt your data by moving it into your Secure Drive, and placing a link to it in its original location.

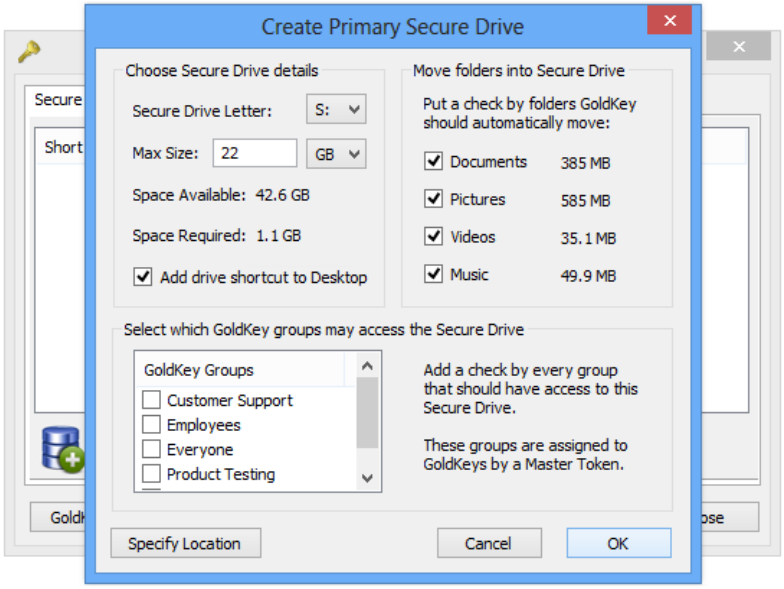


Figure 2. Creating a Primary Secure Drive

Any folders you encrypt in these ways will only be accessible while the Primary Secure Drive is unlocked.

Once you have created your Primary Secure Drive, you are ready to start using GoldKey encryption to secure your data – simply move data into your Secure Drive.

Note: *Using the Folder Encryption feature allows the encryption of data without having to reconfigure applications to look for their data in a new location.*

The GoldKey application can be accessed at any time from the Start Menu, in the GoldKey folder under All Programs. There will also be an icon in the system tray showing a golden key. Clicking on this icon will open the GoldKey application (see Figure 3).

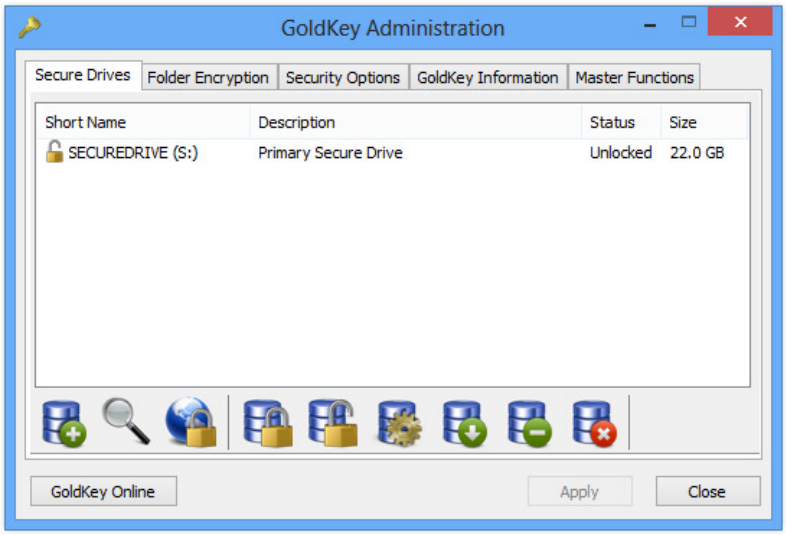


Figure 3. The GoldKey Application

Using the GoldKey Software in Windows

As you work your way through this manual, you will find references to buttons in the GoldKey toolbar. These buttons can be found as depicted in Figure 3. As you move your mouse over each button, you will be shown small hints regarding its functionality.

GoldKey Application toolbar buttons include:

Create a Secure Drive
Add a Secure Drive to your system. Please see the Creating GoldKey Secure Drives section for detailed information on this feature.

Search For Secure Drives
Using this feature, you can find Secure Drives anywhere. You may search through specific folders, your local disk or network mapped drives.

Lock All Secure Drives
This provides a quick, one-click method for locking all your Secure Drives.

Lock a Secure Drive
Lock the Secure Drive that is currently selected in the list above. You may also lock a Secure Drive by right clicking on the GoldKey icon in the system tray.

Unlock a Secure Drive
Unlock the Secure Drive that is currently selected in the list above.

Secure Drive Details
Access the details of the selected Secure Drive. See the Modifying a Secure Drive section for more information on this feature.

Open a Secure Drive in Explorer
Quickly access the data within a Secure Drive. This button unlocks the selected Secure Drive and opens it in Windows Explorer.

Remove a Secure Drive from the List
Remove the currently selected Secure Drive from the list. This does not delete the Secure Drive.

Delete a Secure Drive
This will permanently delete the selected Secure Drive. Make sure that you copy out any important data, as any data this drive contains will be lost.

Encrypting Data

There are a couple of different ways to encrypt data with a GoldKey. The first is to use a Secure Drive. The second is referred to as “right-click encryption,” and is covered in the section titled Right-Click Encryption.

Managing Secure Drives is done from the GoldKey application (see Figure 3). From there, you can create or delete drives, view information and statistics gathered per drive, and search for new drives.

Another way to create a Secure Drive is the new file method, which is especially useful for creating a Secure Drive in a specific location, such as on a network share.

As an example, open Windows Explorer to your Documents folder, right-click, select New, and click on GoldKey Secure Drive. This will create an un-configured Secure Drive file in the current directory.

Double-clicking on this file will then give you all the options necessary to configure the Secure Drive.

Creating GoldKey Secure Drives

The typical way to create a Secure Drive is to click on the Create a Secure Drive button on the GoldKey toolbar (refer to Figure 3). You will be shown the dialog in Figure 4.

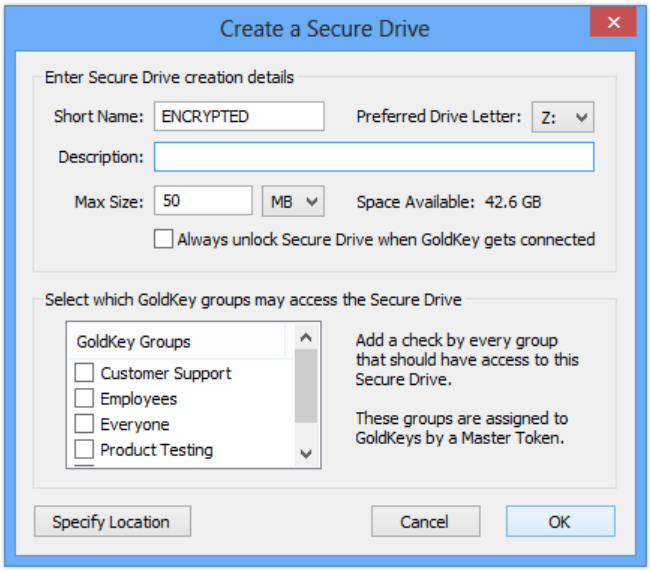


Figure 4. Create a Secure Drive

Secure Drive Creation Details

For each Secure Drive you create, you will be required to specify certain details. These include the short name, the preferred drive letter, and the size of the drive.

The short name assigned here will be the drive label that shows up in Windows Explorer.

The description is not required, but we recommend that you give descriptions for your Secure Drives. This will help you identify them later on, as the descriptions are displayed in the GoldKey software.

Note: *If the preferred drive letter is in use when this drive is unlocked, a drive letter that is available will be automatically selected.*

You may also specify a custom location for a Secure Drive. In this way, you can place Secure Drives on a different hard drive or a network file server.

Secure Drive Access

Up to thirty-two GoldKey groups may be given access to a particular Secure Drive at a time. In this way, you may have your data encrypted, but still allow multiple GoldKey tokens to access the data.

A Master assigns groups to GoldKey tokens. By default, GoldKey tokens that have not been registered to a Master are members of a single group called “Everyone”.

Note: *Data encrypted by a GoldKey will be accessible by the Master token that the GoldKey is registered to, regardless of which groups are selected.*

Modifying a Secure Drive

After a Secure Drive is created, certain settings may still be changed. These include the preferred drive letter, whether the volume should be unlocked at startup, the description, and group settings.

To change these settings, select the appropriate drive from the list shown in the Secure Drives tab, and click on the Drive Details button in the GoldKey toolbar. See Figure 5.

Note: *The description and group settings can only be modified while the Secure Drive is locked.*

Figure 5. Modifying a Secure Drive

To change what groups can access this Secure Drive, click on the Change Access button. You will be prompted for your PIN, and then you will see the list of groups you may allow to access this Secure Drive. You can grant access to as many as thirty-two groups.

To change which token owns a Secure Drive, plug in a GoldKey that can open the Secure Drive, and allow access to the Secure Drive by a group the new owner's token is a member of. Save these changes, insert the new token, and then use it to remove any unwanted groups.

Note: *When you change a Secure Drive's group settings, the GoldKey that is currently plugged in becomes the new owner of the Secure Drive.*

When you are finished making changes, click the OK button.

To change a Secure Drive's short name, unlock it and open Windows Explorer. Then, right-click on the drive and click on Properties. The drive label can then be changed at the top of the General tab (see Figure 6).

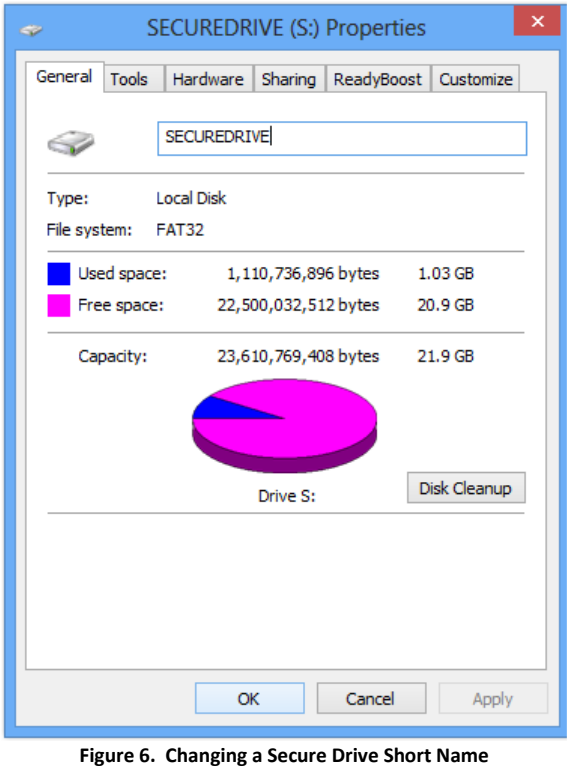


Figure 6. Changing a Secure Drive Short Name

Locking Secure Drives

To lock a Secure Drive, you may select it from the list in the GoldKey application, and click the Lock Drive button. Alternatively, you may right-click on the Secure Drive icon in the system tray (usually the right-hand side of the Start bar), and select the drive from the "Lock a Secure Drive" menu.

Secure Drive Discovery

If you would like to search for Secure Drive files within a given directory, or even through an entire hard drive, you may use the Find Drives button in the GoldKey toolbar. You will be asked to specify which directory to search for Secure Drive files in. All subdirectories will be included in the search.

Securing Folders

Using the GoldKey software, you can encrypt data without changing its apparent location. This feature requires that you have a Primary Secure Drive. See GoldKey Installation and Quick Start for information about creating the Primary Secure Drive.

To encrypt (or secure) a folder, go to the Folder Encryption tab in the GoldKey software, and click on the Add Folder button. Next, browse to the location of the folder you would like to secure, and click OK.

The folder will be moved into your Primary Secure Drive, and a link to its new location will be put in its place.

Warning: Before you attempt to secure a folder, make sure that none of its contents are in use.

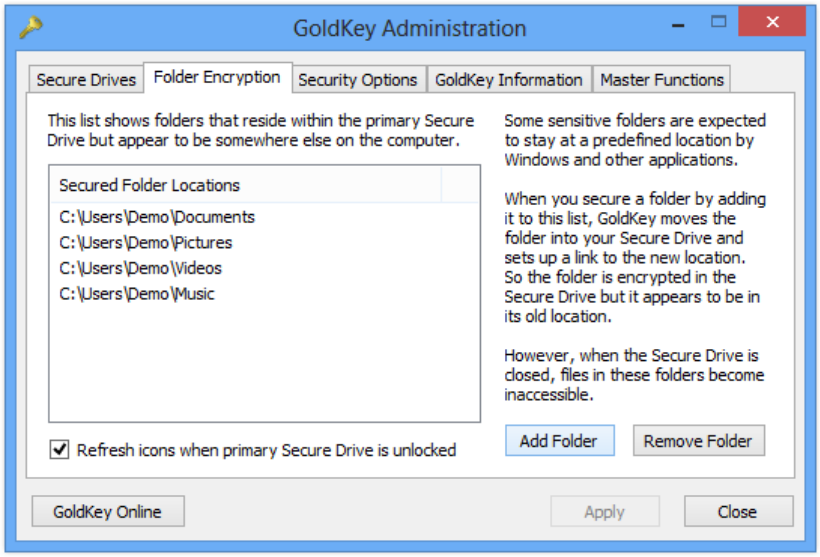


Figure 7. Securing a Folder

Note: *Only folders from your local hard drives may be secured in this manner.*

Right-Click Encryption

Another way to encrypt data using the GoldKey software is referred to as right-click encryption, and is used to encrypt a specific set of files or folders. The original data is either preserved or replaced, depending on your security settings. See the GoldKey Security Options section for more information.

To encrypt a small amount of data, or only specific files, etc., right-click on the file or folder to encrypt, and select Encrypt with GoldKey. You will be prompted for your GoldKey PIN, given the option to specify what groups may access the encrypted data, and then an encrypted version of the selected file or folder will be created in the same directory.

You are then able to securely email that encrypted version of your data to coworkers, with the assurance that only users with the correct GoldKey groups may access that data (controlled by the group settings selected).

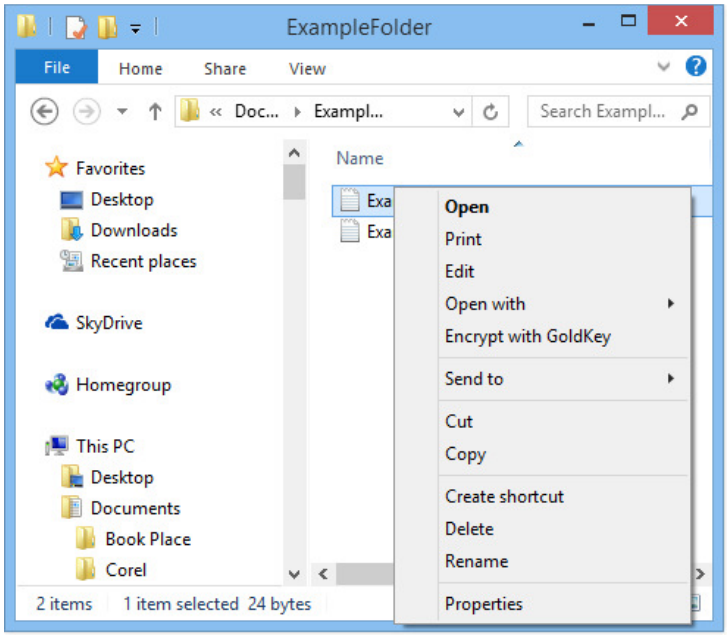


Figure 8. Right-Click Encryption

Right clicking on a Secure Drive file gives you several options that may speed things up a bit. You can:

- Lock a Secure Drive
- Unlock a Secure Drive
- Decrypt a Secure Drive's Contents

Note: *When you decrypt a Secure Drive's contents in this manner, all the encrypted data is copied into the directory containing the Secure Drive.*

Deleting Secure Drives

Before you delete a Secure Drive, unlock it and make sure you have copied out all of the data that you previously encrypted. All data within a Secure Drive will be lost when that drive is deleted.

To delete a Secure Drive, select the Secure Drive you want to delete from the list in the GoldKey application, and click on the Delete a Secure Drive button (see Figure 3). Remember, all of the data within that drive will be lost.

GoldKey Security Options

You are given the ability to configure much of the way that the GoldKey software behaves. You have several options concerning when you want your drives to lock, what happens when right-click encryption is used, and even some Windows tweaks to improve data privacy.

It is usually best to have your Secure Drives locked whenever you are not using them. However, problems can arise from Secure Drives locking while files within them are in use.

The GoldKey Security Options allow you to balance security and usability to fit your needs.

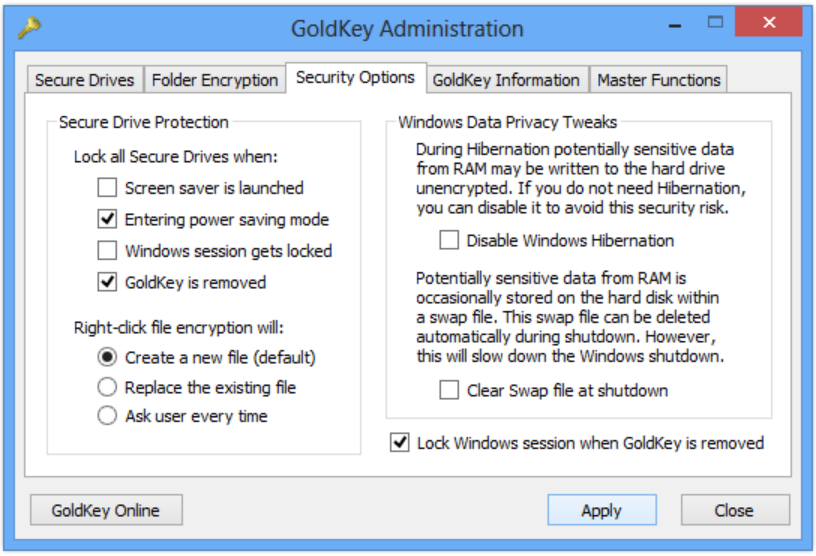


Figure 9. GoldKey Security Options

Personalizing Your GoldKey

You must personalize your GoldKey before it can be used. If you intend to use a Master, the GoldKey should not be personalized before it is registered. From the GoldKey Information tab, you can personalize your GoldKey, view groups and certificates, or open the GoldKey Management software. See the GoldKey Management section for more information.

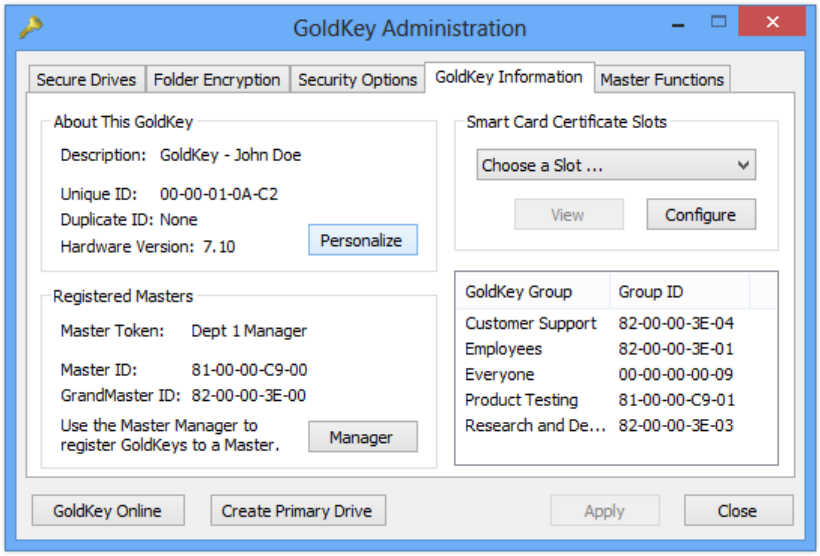


Figure 10. GoldKey Information Tab

To personalize your GoldKey, plug it into your computer and click on the Personalize button in the GoldKey Information tab (see Figure 10). To change personalization information, you will be required to enter the current PIN and the answer to a personal question.

Note: *If the Master has locked personalization for your GoldKey, only your PIN can be changed. In this case, no questions have been configured and you will only be required to enter your current PIN as verification.*

If you don't remember your PIN, or the answer to one of your personal questions, a Master token can be used to reset this information. See the Modifying a GoldKey section for more information.

Follow the steps below to complete the personalization process.

Step 1 – Set a PIN

First, you must specify a PIN for this GoldKey, which will be required for authentication with Secure Drives, or when your smart card certificates are used. The PIN must be at least four but not more than eight characters.

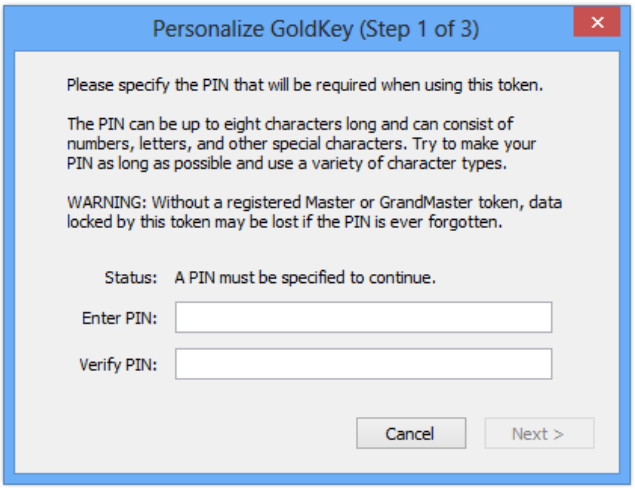


Figure 11. Personalizing a GoldKey – Enter the PIN

It is very important that you remember the PIN you assign to your GoldKey! A GoldKey PIN cannot be recovered, so forgetting the PIN might mean losing important data.

Note: *The use of Masters greatly reduces this risk. Even if a user is unable to remember his PIN, and cannot access encrypted data, the Master or GrandMaster he is registered to can unlock his Secure Drives or reset his personalization information. Registration must have been performed before the user began encrypting data.*

Step 2 – Select Personal Questions

The next step is to select one or more personal questions, and enter their answers. Only you should be able to answer the questions that you select. If you would like to use a question that does not appear in any of the pull-down lists, you may type your own into any of the question fields.

Note: *Only one of these questions will need to be answered to re-personalize the token.*

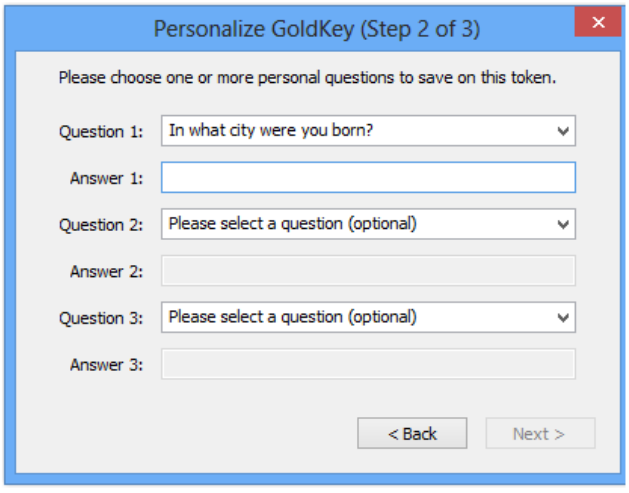


Figure 12. Personal Questions

Step 3 – Enter Basic User Information

You will be asked for the full name, phone number, and email address of the individual who will be using this token. This information will be used to help recover or identify this token if it is ever lost or stolen.

Master Functions

Masters can be used to manage GoldKey tokens, and lock down the GoldKey software. These functions can be accessed through the Master Functions tab. When the software is locked, it cannot be opened and none of its settings can be changed without a Master.

See the GoldKey Management section for more information.

GoldKey Secure Login

Windows Vista, 7 and 8 support GoldKey Secure Login, which allows you to lock down a computer account with GoldKey. Each GoldKey can lock an unlimited number of accounts, on any number of computers. GoldKey groups may also be used to lock an account.

Note: *Only one group at a time may have access to an account.*

Locking a Windows Account

To lock an account, log in as that user and press Control-Alt-Delete. Click on Change a password, and then on Other Credentials. Next, click on Enable GoldKey Login and insert the GoldKey you would like to use to lock the account.

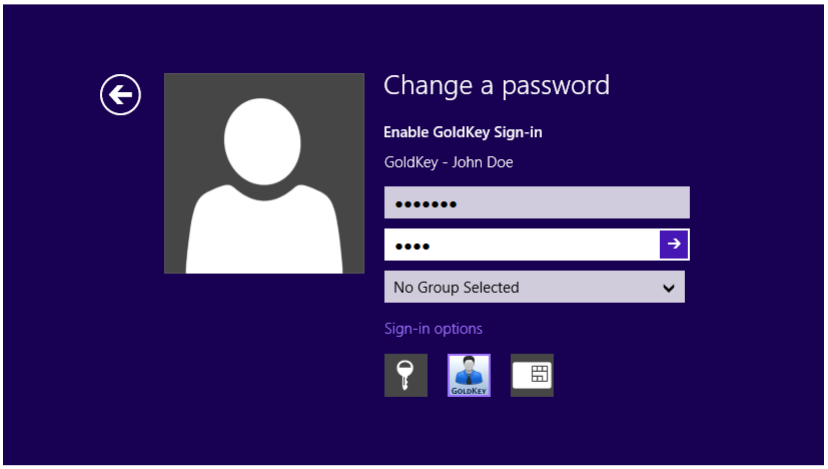


Figure 13. Locking a Windows Account

You will be required to enter the GoldKey PIN and the current Windows password in order to lock the account. If you would like to allow a group to access this account, select the group from the list provided. If you would like to enable automatic sign-in, so that you can open your Windows account without entering a PIN, select a group that is set to require no user verification. See Editing a Group under GoldKey Management for more information.

Note: *Regardless of group settings, the Master or GrandMaster your token is registered to will be able to log into or unlock the account.*

By selecting a group that requires no user verification, you can create the ability to sign in to your Windows account by inserting your GoldKey token into your computer.

Accessing a Locked Account

Figure 14. Selecting an Account

Windows 8

When accessing a Windows 8 account that has been locked by GoldKey, insert your token into the computer, then select the user you want to log in as. Finally, select the GoldKey method and enter your PIN.

Windows 7

When accessing an account that has been locked by GoldKey, you must insert your token before selecting the user to log in as. When you insert your GoldKey, you will be given a list of accounts your token is able to unlock.

Select the appropriate account and enter your PIN.

Accessing a Locked Account with No User Verification

When a Windows account has been GoldKey secured for access by a group that requires no user verification, you must simply insert your token to access the account.

Using the GoldKey Built-In Smart Card in Windows

The following list shows the Microsoft operating systems that are supported by the GoldKey software. For operating systems other than Windows 7, the GoldKey mini-driver or third-party PIV-capable middleware is required for smart card operation.

- Windows 8
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2
- Windows Vista SP1
- Windows XP SP2
- Windows Server 2003

In order to use your smart card, you will need to load certificates onto it. This requires the use of a Master token, the GoldKey mini-driver, or PIV middleware. See the Loading Certificates onto a GoldKey section for instructions.

Using the Smart Card for Active Directory Login

To log into Active Directory using a smart card, you will need to enroll for a certificate from the domain. The default Active Directory Certification Authority installation comes with two certificate templates that can be used for this purpose: Smartcard User and Smartcard Logon. We recommend that you use an enrollment agent to request certificates on behalf of your users.

Using the GoldKey mini-driver, you will be able to load certificates onto your tokens using utilities provided by Microsoft Windows, such as the Certificates snap-in for Microsoft Management Console and the command-line CertUtil.exe.

Note: *To load a certificate using the mini-driver, you must use the Microsoft Base Smart Card CSP.*

You will also be able to load certificates using the GoldKey software and the registered Master token. To use this method, you will need to export each certificate you enroll for as a PFX file. The process of loading a certificate onto a GoldKey from a PFX file using the GoldKey software is described in the section Loading Certificates onto a GoldKey.

Using the GoldKey Software in Mac OS X

Personalizing Your GoldKey

You must personalize your GoldKey before it can be used. If you intend to use a Master, this GoldKey should be registered to it before it is personalized.

To personalize your GoldKey, plug it into your computer and open the GoldKey Information window, available from the GoldKey menu. From here you may view important details about your GoldKey, personalize it, or access the Master functions.

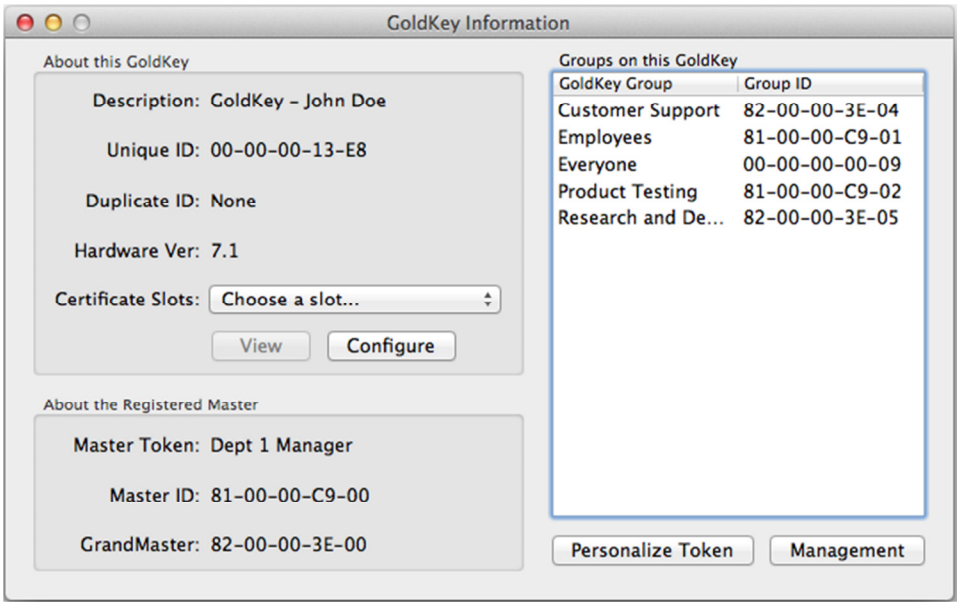


Figure 15. GoldKey Information

Next, click on the Personalize Token button. If this GoldKey has already been personalized, you will be required to enter the current PIN and the answer to a personal question before you will be allowed to continue. Follow the steps below to complete the personalization process.

Step 1 – Set a PIN

First, you must specify a PIN for the GoldKey, which will be required for GoldKey authentication.

It is very important that you remember the PIN you assign to your GoldKey! A GoldKey PIN cannot be recovered, so forgetting the PIN might mean losing important data.

Note: *The use of Masters greatly reduces this risk. Even if a user is unable to remember his PIN, and cannot access encrypted data, the Master or GrandMaster he has registered to can unlock his Secure Drives or reset his personalization information.*

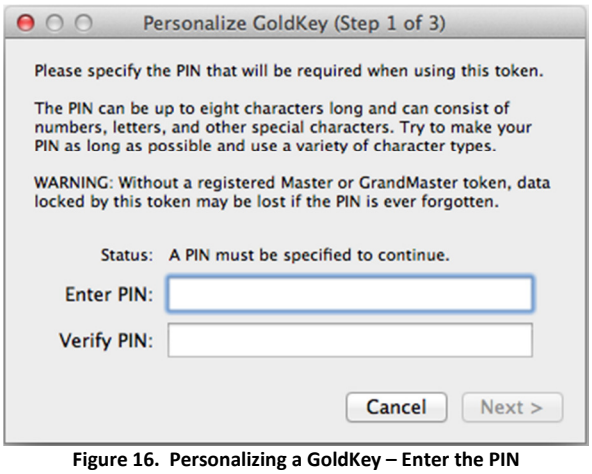


Figure 16. Personalizing a GoldKey – Enter the PIN

Step 2 – Select Questions and Enter Answers

The next step is to select one or more personal questions, and give the answers that will be required the next time your GoldKey is personalized. Select questions that only you can answer.

Note: *Only one of these questions will need to be answered to re-personalize the token.*

Step 3 – Enter Basic User Information

You will be asked for the full name, phone number, and email address of the individual who will be using this token. This information will be used to help recover or identify this token if it is ever lost or stolen.

GoldKey Security Options

These settings allow you to customize the behavior of the GoldKey software, including when you want your drives to lock and what happens when right-click encryption is used.

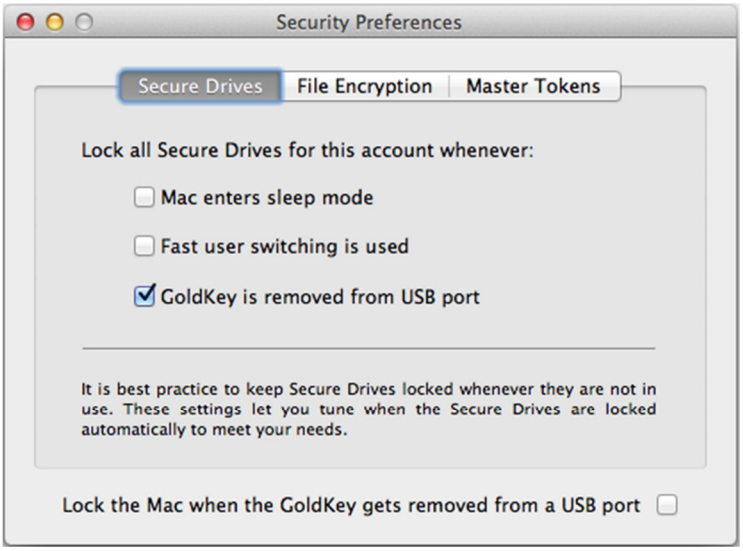


Figure 17. Secure Drives Options

Secure Drives Options

It is usually best to have your Secure Drives locked whenever you are not using them. However, problems can arise from Secure Drives locking while files within them are in use. These settings allow you to configure when your drives will be automatically locked.

File Encryption Options

When you encrypt a file, you may decide to keep the original file or to delete it. By default, the original data is left intact.

Using the File Encryption options, you may change the settings to automatically delete the original file, or to ask you which action you would like to take every time.

Master Options

This screen provides a way to lock down the GoldKey software so that a Master is required to make changes to your settings. You may also access the GoldKey Management Menu. See the GoldKey Management section for more information.

To lock down the software, insert a Master and check the box beside "Lock GoldKey security preferences with a Master Token." You will be required to enter the PIN for the Master.

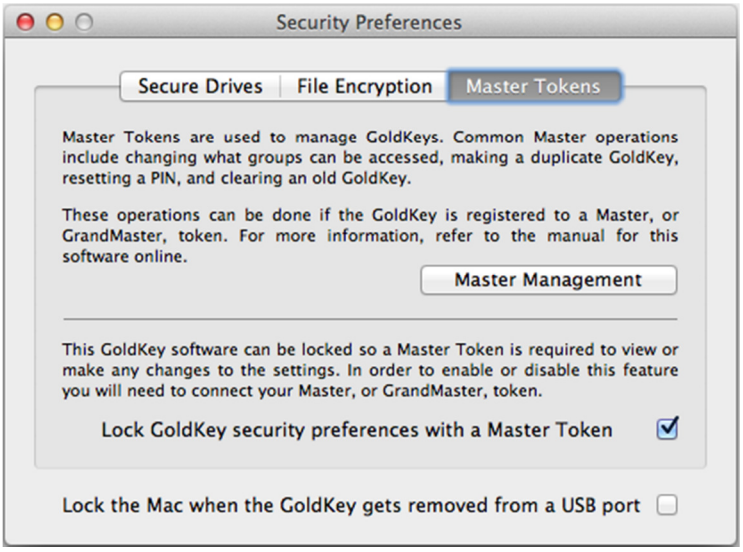


Figure 18. Locking Down the GoldKey Software

Note: *Right-click encryption may be used even after the software is locked down using a Master token.*

Managing Secure Drives

Managing Secure Drives is done from the Secure Drive List within the GoldKey program. From there, you can create and delete drives, view information and statistics gathered per drive, and search for drives.

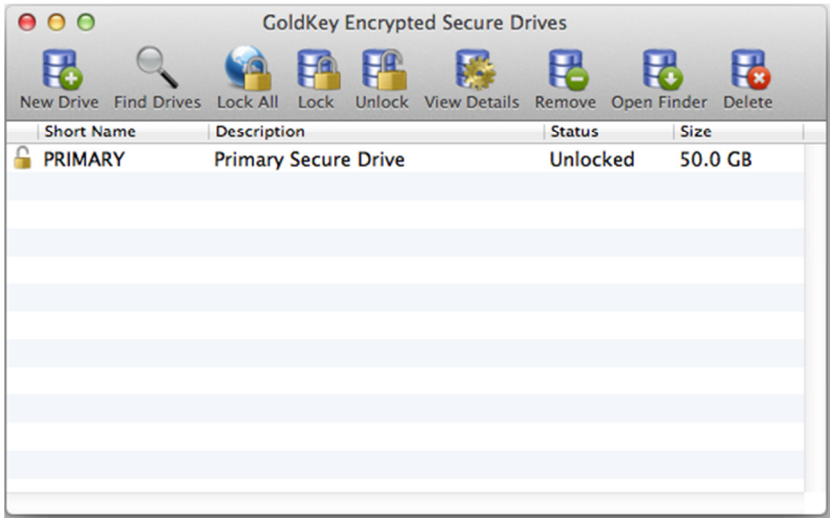


Figure 19. Secure Drive List

Creating GoldKey Secure Drives

When you unlock a Secure Drive, a removable drive icon appears on your Desktop and in Finder. When you copy data into this drive or save files here using an application, your data is secured using 256-bit AES encryption.

To create a Secure Drive, click on the Create Drive button in the Secure Drive List tab (refer to Figure 19). You will see the dialog shown in Figure 20. Follow the steps below to create a Secure Drive.

Step 1 – Choose a Name

You will be required to specify a name for each Secure Drive, which should be unique. You will see this name as the label of the drive that appears when you unlock this drive. This name cannot be longer than eleven characters.

Step 2 – Give a Description

You may give a description to each Secure Drive you create. You will see this description in the list of Secure Drives. This is intended to help you identify the Secure Drive.

Step 3 – Specify a Size

You will need to specify a size for your Secure Drive. Secure Drives cannot be resized, so be sure to create them large enough to hold all the data you would like them to contain.

Step 4 – Configure Options

Next, you may specify the different drive options. You may choose to have this drive unlock automatically whenever your GoldKey is connected, and you may specify a custom location for the encrypted file. Please see the Encrypted Files section for more information.

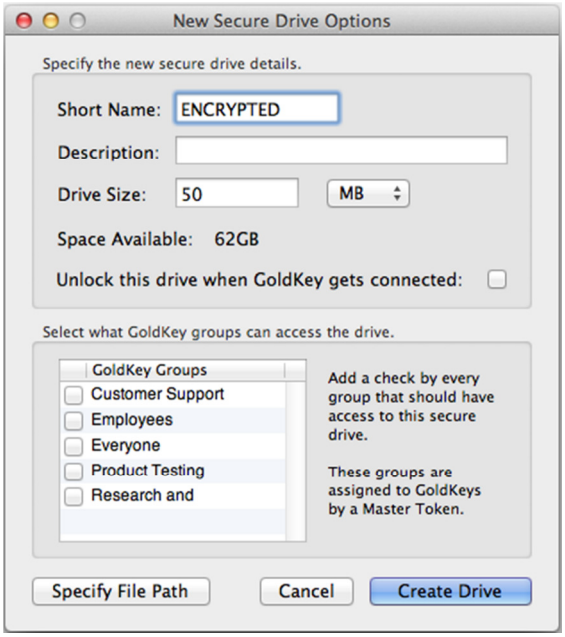


Figure 20. Create a Secure Drive

Step 5 – Set Group Privileges

Finally, you may allow up to thirty-two groups to access any particular drive. To allow access for a group, check the box beside the name of that group in the list shown in Figure 20.

Note: *The Master that the GoldKey is registered to (if any) will be able to access encrypted data regardless of the group settings.*

Modifying a Secure Drive

After a Secure Drive is created, you can only change certain settings. These include whether the drive should be unlocked automatically whenever a GoldKey is connected, whether to unlock the drive for read-only access, the description, and group access settings.

To change these settings, select the appropriate drive from the list shown in the Secure Drive List tab, and click on the View Details button.

To change this drive's access permissions, click on the Change Access button. You will then see the list of groups you may allow to access this Secure Drive. You can grant access to as many as thirty-two groups.

When you are finished making changes to this Secure Drive, click the Done button.

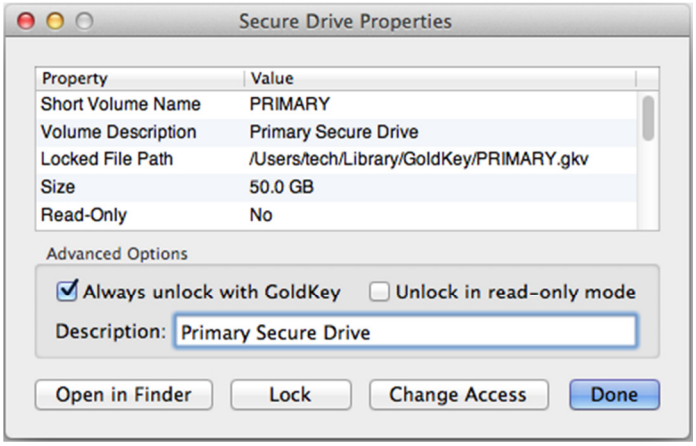


Figure 21. Modifying a Secure Drive

Locking Secure Drives

You may lock a Secure Drive simply by using any of the Mac "eject" techniques (dragging the unlocked drive over the Trash, etc.).

You may also lock Secure Drives from the Secure Drive List in the GoldKey application by clicking on the Lock All button, or by selecting the drive you would like to lock from the list provided and clicking on Lock.

Secure Drive Discovery

Note: *We suggest that you read the Encrypted Files section under Advanced Topics before attempting to use this feature.*

The GoldKey software can look in several places for Secure Drives to unlock. By default, it only searches the user's Library/GoldKey directory. New directories can be searched using the Find Drives button in the Secure Drive List (shown in Figure 19). This will open a dialog where you may select which folder you would like to search for Secure Drive files. Any subdirectories will be searched recursively.

Deleting Secure Drives

Before you delete a Secure Drive, unlock it and make sure you have copied out all of the data that you previously encrypted. All data within a Secure Drive will be lost when that drive is deleted.

To delete a Secure Drive, open the Secure Drive List in the GoldKey software, select the Secure Drive you would like to delete, and click on the Delete button (see Figure 26). Remember, all data within that drive will be lost.

Encrypting Data with a GoldKey

There are two ways to encrypt data with a GoldKey. The first is by creating a Secure Drive, as mentioned in the Creating a Secure Drive section, and copying your data into the new drive. The second method encrypts a single file or an entire directory.

Encrypting a File or Folder

Open Finder, control-click on the file or directory containing the data you would like to encrypt and select the Encrypt with GoldKey option.

Note: *If the Encrypt with GoldKey option is not available, you may need to enable it in System Preferences. From the GoldKey menu, select Services – Services Preferences. From this list, enable the Encrypt with GoldKey and Decrypt file contents options.*

You will be given an opportunity to select which GoldKey groups should have access to this encrypted data. Select the appropriate groups and click Continue.

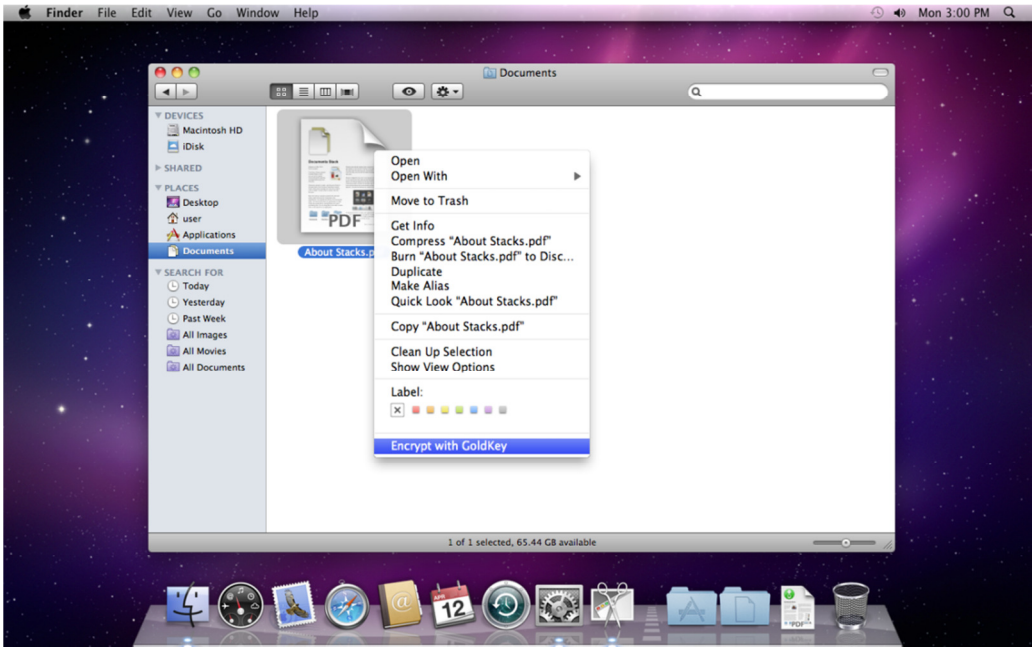


Figure 22. Encrypting a File or Folder with GoldKey

Accepting the default settings will create an encrypted version of the data, with no allowed group access. The original data may be preserved or destroyed, depending on the GoldKey Security Settings. See the File Encryption Options section for more information.

GoldKey Secure Login in Mac

Mac OS X versions 10.4 Tiger through 10.6 Snow Leopard can allow local user accounts to be secured by a smart card. Please refer to our online application note for detailed instructions:

http://www.goldkey.com/support/2011/03/locking-an-account-with-goldkey-in-mac/

Using Tokens with Built-In Flash

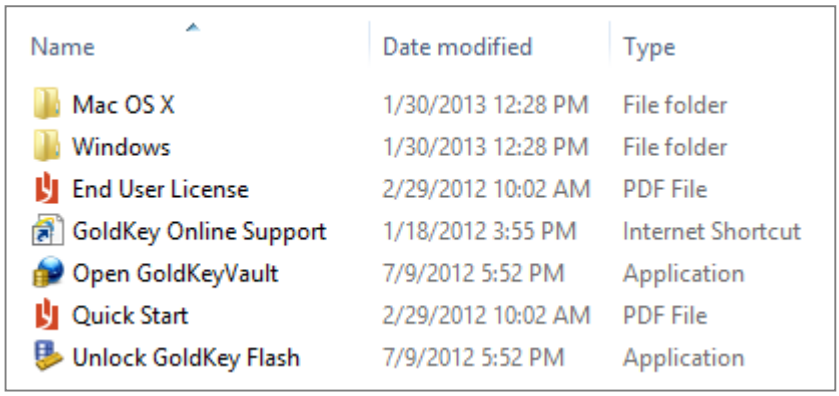
The GoldKey token with built-in flash has all of the security features of a GoldKey Token, with the addition of encrypted storage – enabling you to carry your data with you and keep it secure. Using this GoldKey token, you may access both the encrypted data stored on the token's built-in flash and GoldKey Vault Cloud Storage without installing the GoldKey software.

GoldKey tokens with flash are supported in Windows XP SP3, Vista, 7, and 8, as well as in Mac OS X v10.6 Snow Leopard or higher.

Unlocking the Built-In Flash

When you insert your token into a computer, the removable disk that appears is the startup disk, which contains the applications you will need to unlock your token's encrypted flash and access data you have stored in the cloud.

Once your token has been personalized, you can use the Unlock GoldKey Flash application to access your token's built-in encrypted flash. When you unlock the flash, the startup disk will disappear and will be replaced by the encrypted portion of the flash.



Note: *The Windows application can be found in the top level of the startup disk. The application for Mac OS X is in the Mac OS X folder.*

Using the Token's Built-In Flash

After you have unlocked the built-in flash, the GoldKey token is ready to be used, and will behave like a standard flash drive. However, all of the data copied onto the GoldKey token will be encrypted on the fly.

When you are finished using your GoldKey, please remember to safely remove it before unplugging it from your computer. This will help prevent data loss that occurs when the file system on the token's flash becomes corrupted. On Windows, you may eject the removable disk or use Microsoft's Safely Remove Hardware feature. In Mac OS X you may eject the removable disk.

GoldKey Management

A major concern when encrypting data within an organization is data loss, which can occur in a number of ways: forgotten passwords, employees being fired, etc. Another problem faced by companies around the world is data leakage – private data made available to the public by hackers or malicious users.

The goal, then, is to create a scenario where your data is secure, and the likelihood of data loss due to encryption is greatly reduced.

For this, the best approach is to create a management structure where any data encrypted by employees can be decrypted by their managers. The use of Masters and GrandMasters creates this management hierarchy.

Locked data may also need to be shared by coworkers. GoldKey groups provide that flexibility.

Deployment

How GoldKey tokens are deployed in an organization largely depends on the size and structure of the organization. In most cases, Masters would be assigned to the various managers, and the GrandMasters would be placed in a bank vault or other secure location. The typical management hierarchy is shown in Figure 23.

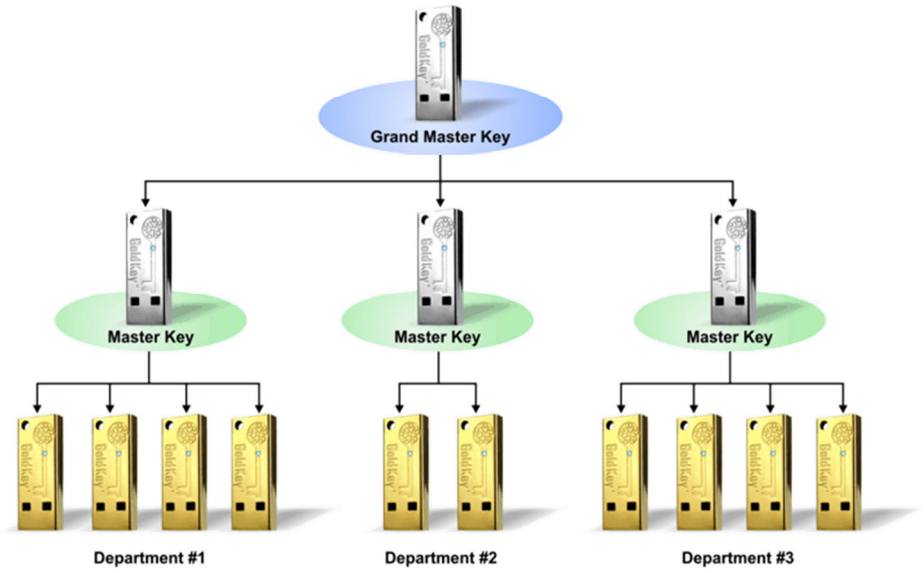


Figure 23. GoldKey Management Hierarchy

Basic groups for each department should be created on the GrandMaster. An example of this is creating an Accounting group on the GrandMaster, and writing it onto a Master. Then, additional groups may be created on the Master for more specific accounting-related rights.

Before You Start

You should avoid personalizing GoldKey tokens before they are registered to their Masters, and configuring Masters before they are registered to your GrandMaster. Before distributing any GoldKey tokens, configure your GrandMaster, register your Masters to it, and then register your GoldKeys to the appropriate Masters. This will ensure that all data locked by the GoldKeys will be accessible via the management tokens.

To use the GoldKey Management software, you need at least two available USB ports on the computer. You will need three USB ports if you are planning to duplicate tokens.

Note: *Most management functions can be done remotely using the GoldKeyVault software. Refer to the Managing GoldKey Tokens Remotely section for more information.*

Accessing the GoldKey Management Menu

To open the GoldKey Management software, insert a Master or GrandMaster and open the GoldKey application. If you are using Windows, click on the Master Management button in the Master Functions tab. Otherwise, open the GoldKey software and select Master Management from the Window menu.

Figure 24. The GoldKey Management Menu

Configuring a Master

If your organization has purchased a GrandMaster, you should register all of your Masters to it before programming any GoldKey tokens. The process used for clearing, registering, and duplicating Masters is the same as described below regarding GoldKey tokens, except that you must use a GrandMaster.

Note: *GrandMasters do not need to be registered, and cannot be duplicated after leaving the factory.*
For initial personalization of a Master, insert it into your computer and click on the Personalize button in the GoldKey Information tab. See the Personalizing Your GoldKey section for more information.

Adding a Group

To add a group to a Master or GrandMaster, open the GoldKey Management software by clicking the Master Management button in the Master Functions tab, and then click on the Create Groups button. You will be prompted for the Master PIN, and you will need to answer one of the personal questions. You will then see the dialog shown in Figure 25.

Click on the New Group button, type a name for the new group, and hit Enter.

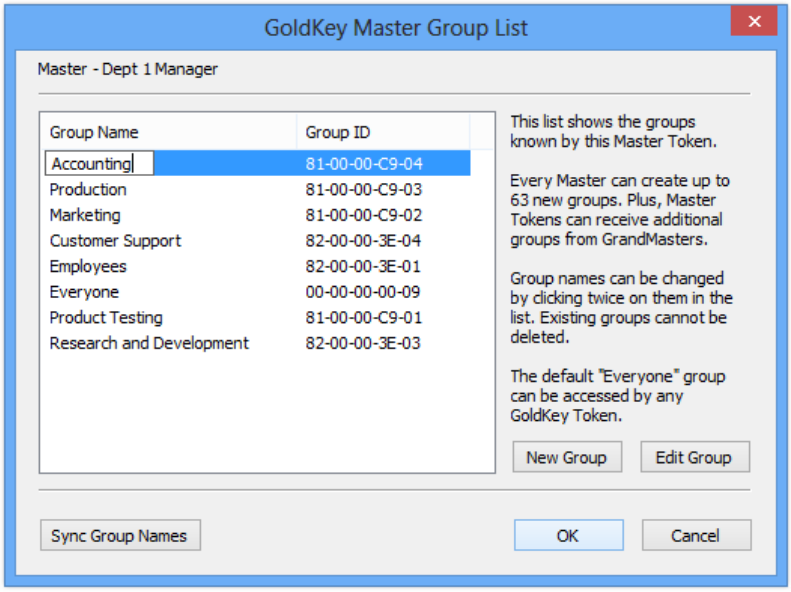


Figure 25. Adding a Group

Note: *If the Master you are adding groups to is in a set of duplicate tokens, add the groups to the original, and use the Sync Group Names feature to add them to any duplicates. Syncing group names will only work between duplicated tokens, or between Masters and GrandMasters.*

Most of the time, you will want to create your groups using the GrandMaster and write them to your Masters. You may do this during registration or at any time by selecting Modify GoldKeys from the GoldKey Management Menu. See the sections titled Modifying a GoldKey and Registering a GoldKey.

Editing a Group

To change a group's name or to change its verification requirement, select the group you want to edit, and then select Edit Group.

By default, verification with a GoldKey requires inserting the token into a computer and entering the PIN. However, not all access situations require the same rigorous process. To accommodate situations where it is appropriate, GoldKey groups can be set to allow token-only authentication.

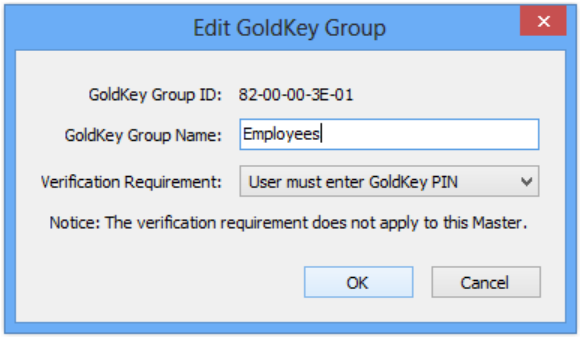


Figure 26. Editing a Group

An important aspect of this feature is that, because a GoldKey token can belong to more than one group, that token can be given access to data requiring both the token and the PIN for authentication *and* data that requires only the token.

Deleting a Group

Masters can remove groups from any GoldKey tokens that have been registered to them. GrandMasters can do the same for Masters. Please see the Modifying a GoldKey section for more information.

If you added a group to a Master or GrandMaster that you do not want, and have not yet clicked OK, use the Cancel button. This will discard any changes you have made. Alternatively, you can change the name of a group by clicking twice on its entry in the list, and typing a new name for the group.

Syncing Group Names

Group names can be synced whenever the group IDs is the same. The group IDs will be the same when using duplicate tokens, or when the groups originally came from a GrandMaster.

In this way, if you have changed group names on a Master, for example, and you want those changes reflected on the GrandMaster, you can click the Sync Group Names button, and the names of the groups that were changed on the Master will be updated on the GrandMaster. Group names can also be synced between Masters.

Figure 27. Syncing Group Names

Clearing a GoldKey

Clearing a GoldKey will make previously locked data inaccessible to that token. If the GoldKey has not already been registered to a Master, anything it has already encrypted will become inaccessible. Data that unregistered tokens have encrypted should be copied out of Secure Drives before the GoldKey is cleared.

Note: *Even after clearing a GoldKey, the registered Master will be able to access locked data, as will the members of any associated groups.*

To clear the token, select Clear GoldKey tokens from the GoldKey Management Menu, insert the token you would like to clear into the computer, and click the Apply button at the bottom of the dialog. You will be notified when this process is complete.

Figure 28. Clearing a GoldKey

Registering a GoldKey

Using a Master, you will be able to unlock any data that was encrypted by tokens that have been registered to it. If a token has already been personalized, it will need to be cleared before it can be registered to the Master. See the Clearing a GoldKey section for instructions.

When you register a GoldKey, you will need to choose which groups to place it in. Then, data can be locked for a specific group, and multiple users may have secure access to important information.

Once the appropriate data has been unlocked, select Register GoldKey tokens from the GoldKey Management Menu, and follow the steps below to register the token.

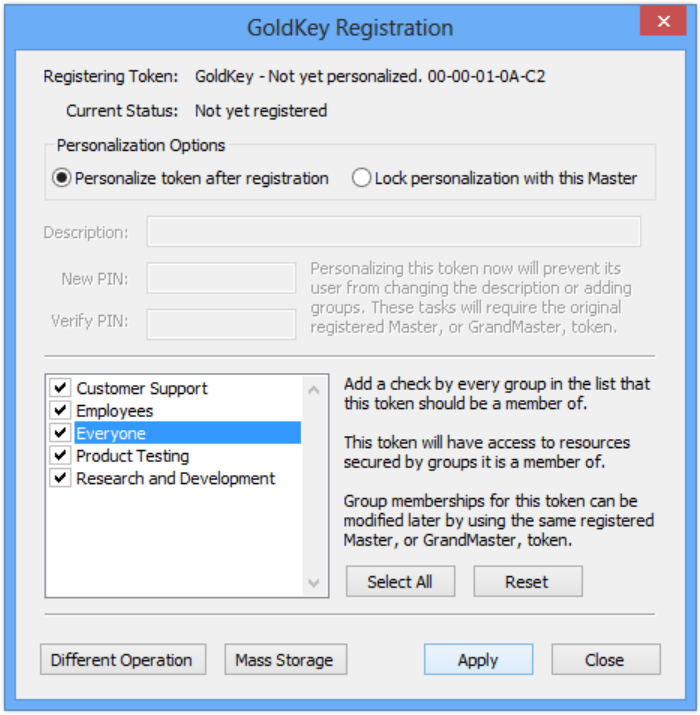


Figure 29. Registering a GoldKey

Step 1 – Connect a GoldKey

Both the Master and the GoldKey being registered must be plugged into the computer for the registration process. When the software detects a GoldKey, its description will be shown at the top of the dialog as depicted in Figure 29.

Step 2 – Personalizing the Token

You may personalize the GoldKey immediately, or allow the new user to personalize it later. To personalize the token, select "Lock personalization with this Master," and specify the token's description and PIN.

Note: *If you personalize this token now, the user will not be able to re-personalize it. They will be able to change their PIN, but they will not have personal questions or be able to change its description.*

Step 3 – Group Configuration

Select the groups you would like this GoldKey to be a member of. This token will have access to anything locked for any of the groups selected, and will also be able to create Secure Drives that can be accessed by any of them. You must have at least one group selected.

Step 4 – Mass Storage

If the token being registered is a GoldKey with built-in flash, you can select the Mass Storage button to customize the allocation of storage space on the token. By default a small, read-only startup partition is created, which is preloaded with the utilities required to unlock the encrypted flash. You can accept the default settings, customize the flash by changing the partition sizes, or configure either partition to be writable or read-only.

Click the Apply button at the bottom of the dialog when you are ready to personalize the token. The amount of time required to register the GoldKey will vary, depending on the number of groups you have assigned this token to. You will be notified when this process is complete.

Modifying a GoldKey

To modify a GoldKey, open the GoldKey Management software and click on the Modify GoldKey tokens button. Here you can change a token's personalization and group membership settings. You will be required to enter the Master token's PIN.

Note: *Any Master can add groups to a GoldKey, unless the token's personalization has been locked by a Master. However, only the Master that the GoldKey has been registered to, referred to as the registered Master, can remove groups or change the personalization without clearing the token.*

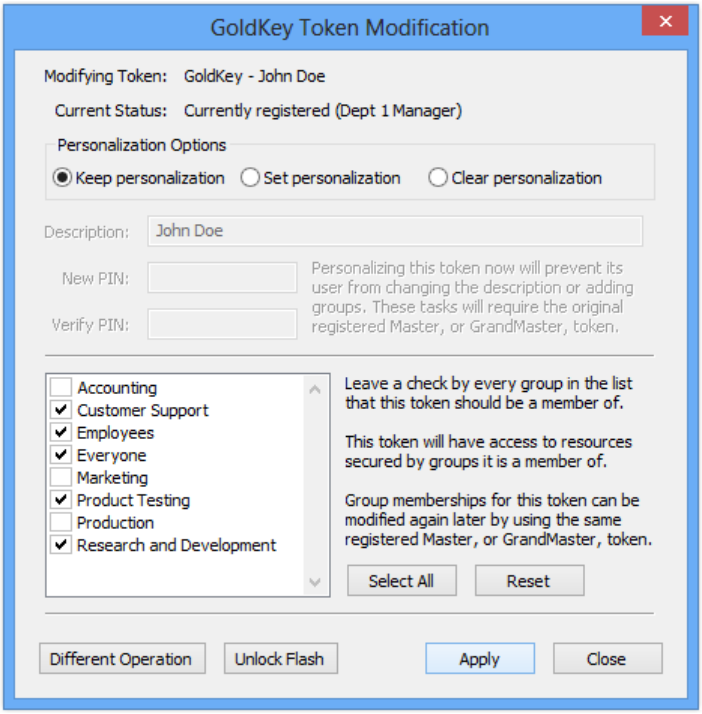


Figure 30. Modifying a GoldKey

If you set the personalization settings here, you will not be able to change the token's description using the Personalize button in the GoldKey software. The token will also not have personal questions, or be able to obtain groups from other Masters.

To reset a token so that you may personalize it again later, select "Clear personalization" and click Apply.

Note: *If the token being modified is a GoldKey with Flash, you can select the Unlock Flash button to access the token's encrypted flash partition.*

Loading Certificates onto a GoldKey

In each GoldKey there are four certificate slots that are accessible using the GoldKey software, each with a different general purpose. Each slot is given a name in the GoldKey software based on what the slot is generally used for. The GoldKey software currently supports loading certificates with 1024-bit or 2048-bit RSA keys.

To Load certificates onto a GoldKey, click on the Master Functions tab – Master Management button – Manage Smart Cards button. Then, select an available certificate slot, and use the Browse button to find the appropriate PFX file. Enter the file's password and click Import.

Note: *If you are loading a certificate for Active Directory login under Windows 7, you must use the first certificate slot.*

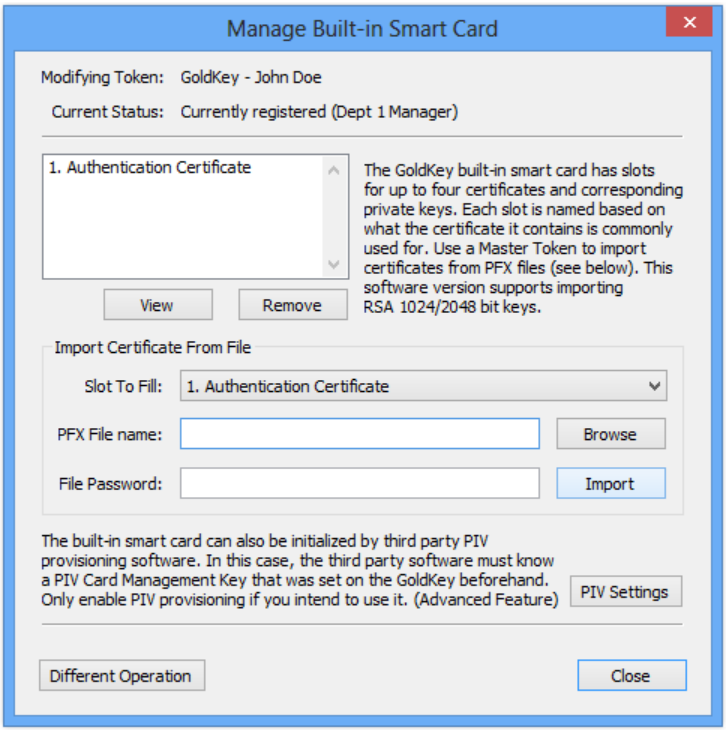


Figure 31. Managing the GoldKey Smart Card

Enabling PIV Provisioning

PIV provisioning allows a GoldKey PIN to be reset using the PIN Unblock Key, and for the token's PIV data to be completely cleared using the Card Management Key. Since this can all be done using a Master, some of these features are disabled on GoldKey tokens by default.

Note: *Tokens that have not had personalization locked by a Master, including unregistered tokens, have the default Card Management Key enabled.*

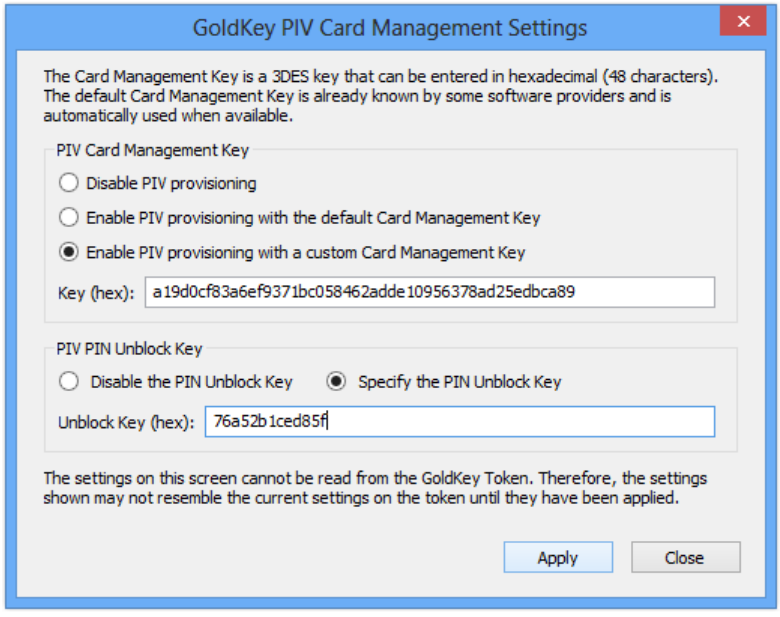


Figure 32. Configuring PIV Provisioning

If you would like to use PIV provisioning, open the GoldKey Management software and click on the Manage Smart Cards button. After you have entered the Master PIN, click on PIV Settings.

You will then be able to set the PIN Unblock Key and the Card Management Key. Both must be entered in hexadecimal format.

Duplicating a GoldKey

Once you have personalized your token, it can be duplicated. Any data encrypted using the original token will be accessible using a duplicate, and vice versa. However, groups obtained from Masters other than your registered Master will not be present on duplicate tokens; these must be obtained separately.

Note: *Certificates on the original GoldKey will not be present on the duplicate token.*

To duplicate a token, open the GoldKey Management software and click on the Duplicate GoldKeys button. Then, follow the steps given below.

Note: *If the original token is lost or stolen after having logged into GoldKeyVault using recent versions of the client software, you may create a duplicate using the GoldKeyVault software. Refer to the Managing GoldKeys Remotely section for more information.*

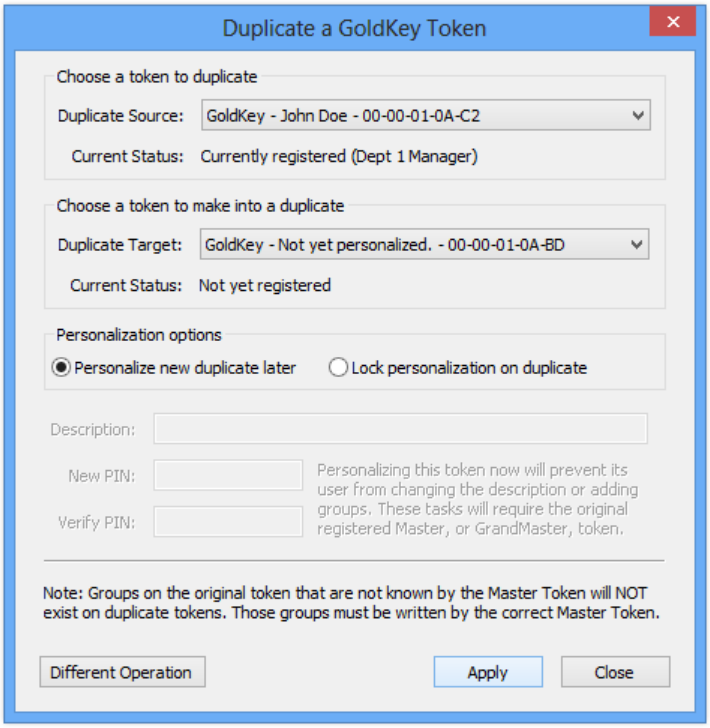


Figure 33. Duplicating a GoldKey

Step 1 – Connect the Token to Duplicate

Plug the token you would like to duplicate into the computer. This token must be registered to the Master you already have plugged in, and must also be personalized.

Step 2 – Connect the Duplicate Token

Next, insert the token you want to be a duplicate of the original. This token must not be personalized already.

Step 3 – Personalize the Duplicate Token (Optional)

If you would like the personalization data on the duplicate token to be locked by the Master, select the option Lock personalization on duplicate, and enter the personalization information.

Note: *Personalizing the GoldKey now will make the user unable to change the token's description, or set personal questions.*

Once you are ready, click the Apply button at the bottom of the dialog. You will be notified when the duplication process is complete.

GoldKeyVault

A GoldKeyVault is secure storage that utilizes GoldKey technology to provide the ability to share sensitive information that is encrypted both in transit and at rest.

All the data you store in your Vault is 256-bit AES encrypted before being sent over the Internet. Without having the right GoldKey and logging in through the GoldKeyVault Explorer, not even the names of your files are accessible to would-be intruders.

Masters may be used to manage Vaults and to allow groups to access shared data.

Claiming Your GoldKeyVault

When you purchase a GoldKey and a bundled Vault, you will be able to use your Vault as soon as you receive your GoldKey. However, the Vault's default label will begin with the ID of your GoldKey token. You may change this label using the GoldKeyVault Explorer.

You may also purchase a Vault for a GoldKey that you already possess. After obtaining such a Vault, change the label using the GoldKeyVault Explorer. Vault labels must be unique.

Using Your Vault

In the Start menu, under the GoldKey folder, you will find a program called GoldKeyVault. This is the GoldKeyVault Explorer, and must be used in order to access your Vaults. In the GoldKeyVault Explorer there are several buttons which are similar to those found in Finder or Windows Explorer, and have the same function. Some unique buttons are described below.

Change View
There are several different views that may be used within the GoldKeyVault Explorer. This button will toggle between them.

Properties
View or change information about a Vault, GoldKey group, or token, which is gathered and maintained by the GoldKeyVault server.

Import Files
Import files into your Vault. All data stored in your Vault is encrypted with AES-256 before being sent over the Internet.

Export Files
Export files from your Vault. Anything you export will be decrypted automatically before being saved onto your computer.

Remote Management
Start a remote management session to apply management changes remotely. User tokens must also be connected in order for changes to be applied.

Note: *Most functions are also accessible by right clicking on an item within the GoldKeyVault Explorer.*

Accessing Your Data

When you open the GoldKeyVault Explorer, you will be shown the list of Vaults that you own and GoldKey groups that you have access to. Vaults that you have access to, but do not own, will appear under the group you use to access them.

Note: *If you are using a Master or GrandMaster token, Vaults belonging to users registered to you will appear under the appropriate token.*

For instance, in the figure below, a user owns one Vault but has access to another through the Employees group. This second Vault will be shown after the user double-clicks on the icon for the Employees group.

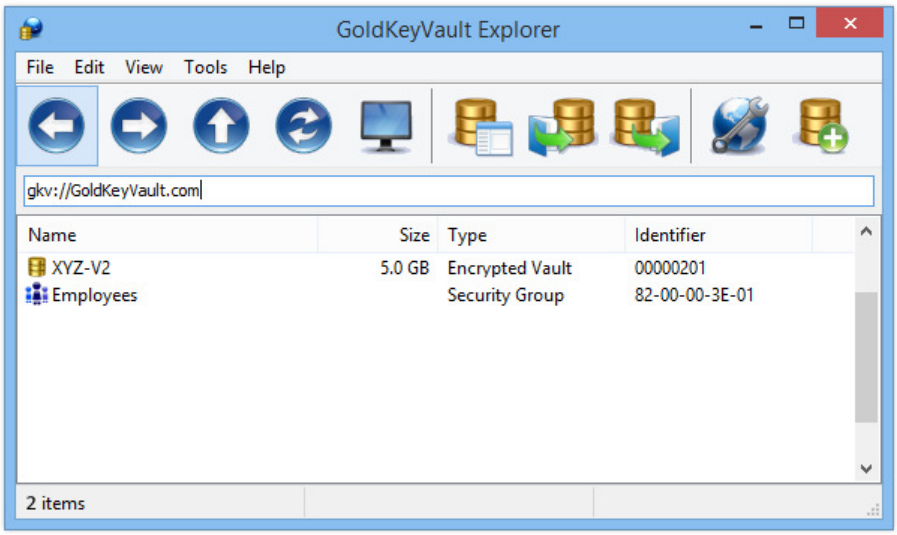


Figure 34. The GoldKeyVault Explorer

Storing, retrieving, and accessing data within a Vault is much like using Windows Explorer. You may use the normal copy and paste or drag and drop methods to copy data between your computer and your Vault, or use the Import and Export features of the GoldKeyVault Explorer. Other typical features are also provided, such as double-clicking to open a file, use of the Enter and Delete keys, etc.

When you open a file from your Vault, a temporary, read-only copy is downloaded to your computer. When you close the GoldKeyVault Explorer, these files are securely and completely erased from your computer. To change a file within your Vault, download a read-write copy, edit and save it, and upload the new version.

You may also create a link to your Vault on your Desktop to make accessing your data a little more convenient. To create a link on your Desktop, right-click on your Vault and select the "On the desktop" option in the Create link submenu.

Viewing Vault Properties

Along with usage statistics that are automatically kept by the GoldKeyVault server, each Vault may be given a label and a description. Any GoldKey with access to a Vault may view the Vault's properties, but only the owner or its Master can change the label or the description.

To view the properties of a Vault, open the GoldKeyVault Explorer, select the appropriate Vault and click on the Properties button. The General tab contains all the basic statistics, the label, and the description.

Note: *A token is given ownership rights if it owns the Vault directly, has a group that has been given "Owner" access, or, in the case of a Master token, a token registered to it has ownership rights.*

Managing Your Vault

GoldKeyVaults are managed using Master and GrandMaster tokens. If any GoldKey within an organization is lost or stolen, the Master can access encrypted data, revoke that token's privileges, and create a new token with access to the data. To manage access for a Vault, your token must have ownership rights.

Note: *As mentioned above, a token is given ownership rights if it owns the Vault directly, has a group that has been given "Owner" access, or, in the case of a Master token, a token registered to it has ownership rights.*

The first time you modify the permissions for a Vault, you will be asked if you would like to take ownership of that Vault. Once you have taken ownership of the Vault, it will no longer be available to the user it had belonged to. However, the original owner may be granted access through group privilege settings.

When the GoldKeyVault Explorer is opened with a Master, any GoldKey tokens that are registered to that Master and have logged into GoldKeyVault are displayed for management. Each token icon represents a GoldKey and any duplicates it may have. See Figure 36.

Securely Sharing Your Data

To give a group access to your Vault, open the GoldKeyVault Explorer, select the Vault, and click on the Properties button. Then, go to the Sharing tab. To change the privileges for a group, double-click on its entry in the list provided. As you continue to double-click on the entry, the value in the Access column will toggle through the four access levels that may be assigned to a group: None, Read-Only, Read/Write, and Owner. When the Access Column shows the rights you would like to grant to that group, click Apply.

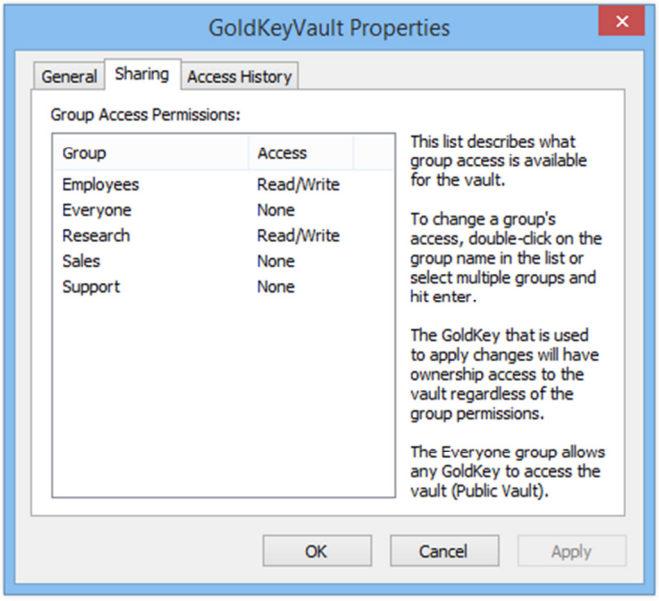


Figure 35. Setting Group Access

Any token that is part of a group that has been granted “Owner” access will be able to change the permission settings for that Vault.

There are four access levels that may be assigned to a group: None, Read-Only, Read/Write, and Owner. Any token that is part of a group that has been granted “Owner” access will be able to change the permission settings for that Vault.

Once you have allowed groups to access data within a Vault, group members are able to interchange emails containing links to data within the Vault, or place a similar link on their desktop.

To create a link in an email or on your desktop, right-click on a file or folder within a Vault and select the appropriate option in the “Create link” submenu.

Revoking Access

Using a Master, you are also able to block groups or specific GoldKey tokens that have been registered to your Master from accessing your data.

To block a GoldKey group or token, open the GoldKeyVault Explorer using a Master, right-click on the group or the token you wish to block, and select the “Block” option. You will see a red “X” appear beside the icon for that group or token. This is shown in Figure 36.

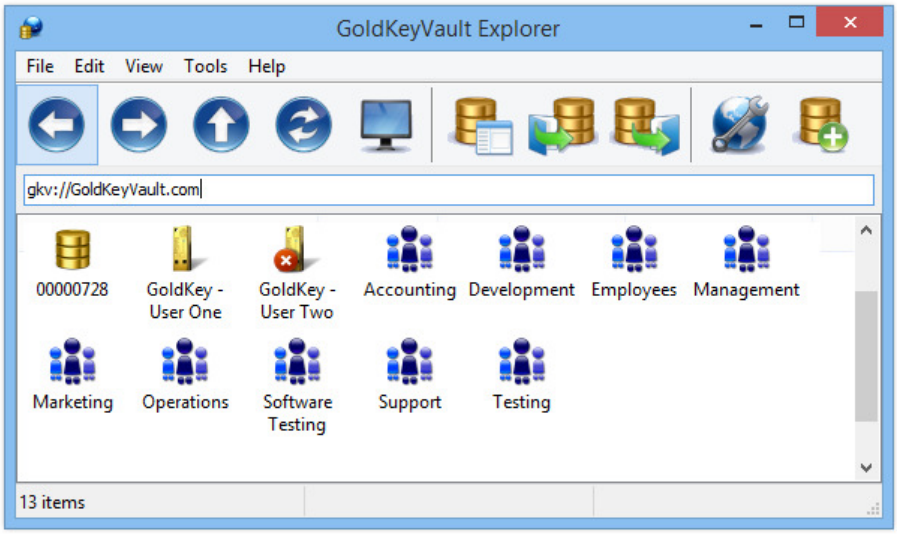


Figure 36. A Blocked GoldKey

Note: *Masters may be blocked using their registered GrandMaster. Users who are registered to a blocked Master will still have access to encrypted data.*

In some situations, such as when a GoldKey is lost or stolen, it is necessary to block a single token in a set of duplicates. If you block the token using the technique described above, none of those duplicates will be able to access your Vault.

To block a token that is part of a duplicate set, open the GoldKeyVault Explorer using a Master, right-click on the GoldKey icon that represents that set of duplicate tokens, and click Properties. Then navigate to the Duplicates tab and double-click on the ID of the token that was lost to toggle the Access value to “Blocked.” Then click Apply.

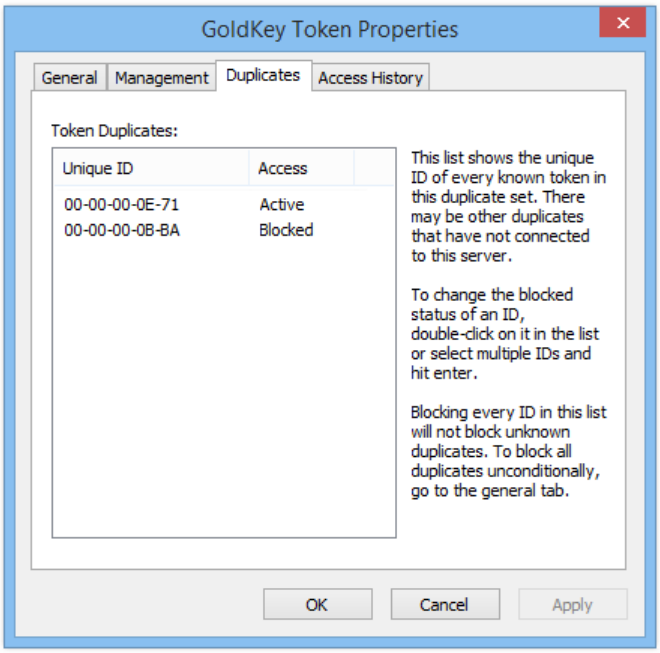


Figure 37. One Blocked Duplicate

Viewing Access Logs

The GoldKeyVault server logs each time a GoldKey, Master, or GrandMaster accesses a Vault, along with the access level they were given, the date and time, and the user's IP address. This information is available while using a Master or GrandMaster token.

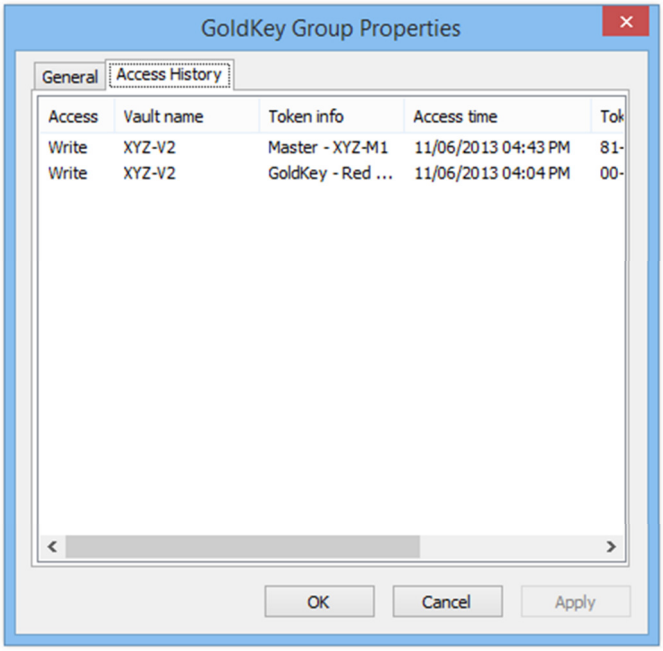


Figure 38. Viewing Vault Access Logs

To view access logs, open the GoldKeyVault Explorer, find and select the appropriate Vault, GoldKey group or token, and then click on the Properties button. From there, select the Access History tab.

In the Access History tab, you will see either a list of tokens that have accessed the selected Vault, or a list of Vaults that have been accessed using the selected group or token. Clicking on an entry in this list will show you the details for that session.

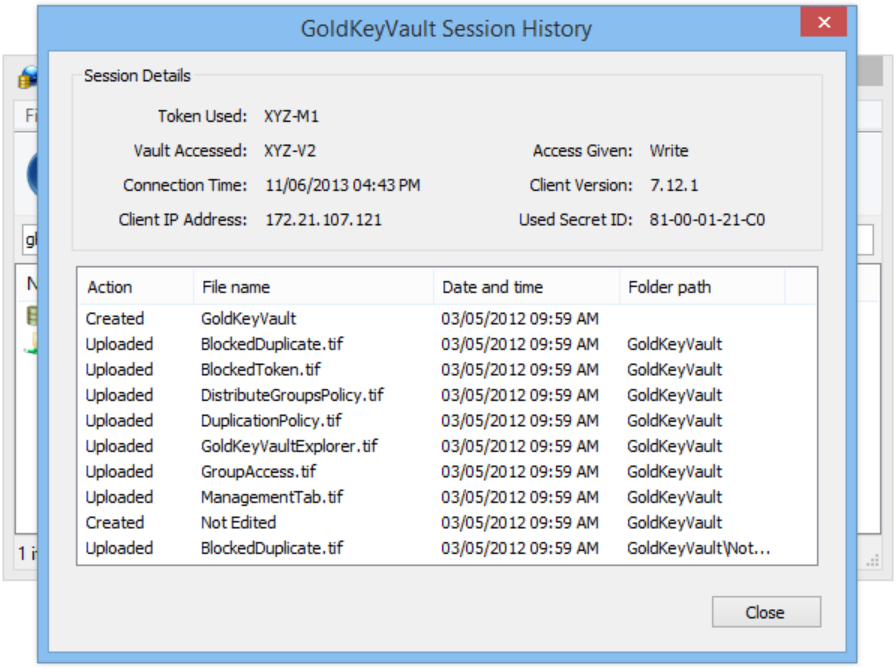


Figure 39. Vault Session History

Note: *The full action logging is only available to Master or GrandMaster tokens which have Owner access rights for the Vault being viewed.*

Managing GoldKey Remotely

Using the GoldKeyVault software, you are able to perform several GoldKey management operations remotely. For tokens that are registered to your Master, you can change or reset the personalization settings, or manage group membership. Through management policies, you can also register new tokens, duplicate registered tokens, or distribute groups to GoldKeys that are not registered to your Master.

Note: *Adding groups to a token that is not registered to your Master will only work if personalization for that token has not been locked by the registered Master.*

Remote management can be performed in two ways. The first is to modify a registered token through the Properties button, and the second is to create a management policy. Management policies must be used to register new tokens or add groups to tokens that are not registered to your Master.

After a management policy has been created, the user must sign in to GoldKeyVault during a remote management session. See the Applying Remote Management Settings section for more information.

Instructions that cover the process of creating a management policy are given in the section for the appropriate management function.

Registering a GoldKey

GoldKey tokens can be securely registered to your Master over the Internet. In order to accomplish this, you must create a management policy. To create a management policy, do the following:

1. Open the GoldKeyVault software with your Master token plugged in and select the "Management policy" option under New in the File menu.

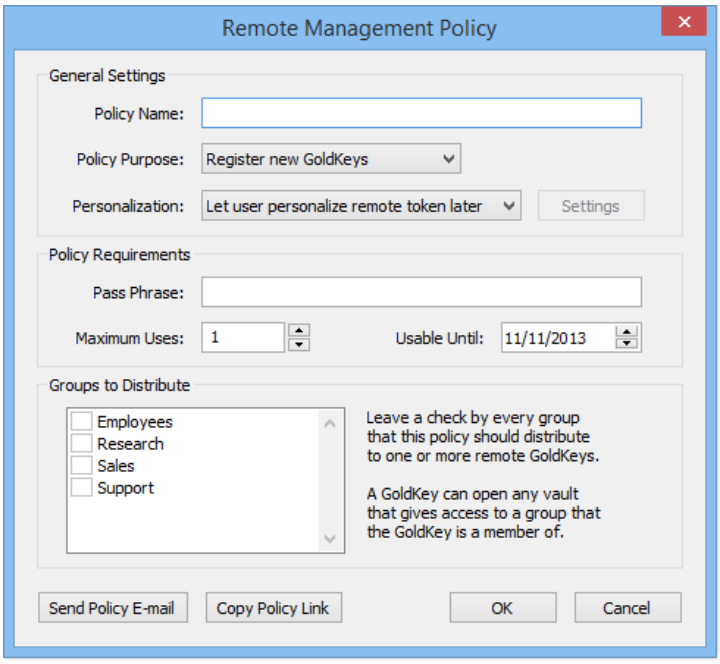


Figure 40. Creating a Registration Policy

2. Under General Settings, enter a name for this policy and select "Register new GoldKeys" as the Policy Purpose.
3. If you would like to lock the personalization settings on the duplicate token, change the Personalization drop-down box to "Lock token personalization right now," click on Settings, and enter the personalization information.
4. If you would like to require users to enter a pass phrase in order to apply this policy, enter the pass phrase in the appropriate field in the Policy Requirements section. You will also be able to set the maximum number of tokens that may use this policy to be registered, and to extend the amount of time this policy will be available. By default, the policy will be available until the end of the day.
5. The Groups to Distribute section gives you the ability to set which groups will be accessible to tokens that register using this policy.
6. When you are finished, click OK.
7. Now that this management policy has been created, you must send your users a link to the policy and start a remote management session, which must remain open while the users access the management policy. See the Applying Remote Management Settings section for more information.

Duplicating a GoldKey

GoldKey tokens can be securely duplicated over the Internet. This gives you the ability to create a duplicate GoldKey token even after the original has been lost or stolen. In order to accomplish this, the token you would like to duplicate must have already logged into GoldKeyVault using the latest software.
Note: *If you are creating a duplicate token because the original has been lost or stolen, make sure to block the original token. See the Revoking Access section for more information.*

To duplicate a token, do the following:

1. Open the GoldKeyVault software with your Master token plugged in.
2. Next, right-click on the token you would like to duplicate from the list provided, and select "New duplication policy."
3. Under General Settings, you will most likely find the defaults to be acceptable. If you would like to lock the personalization settings on the duplicate token, change the Personalization drop-down box to "Lock token personalization right now," click on Settings, and enter the personalization information.
4. If you would like to require users to enter a pass phrase in order to apply this policy, enter it in the appropriate field in the Policy Requirements section. You will also be able to set the number of duplicates that can be created using this policy, and extend the amount of time this policy is available for. By default, the policy will be available until the end of the day.
5. The Groups to Distribute section gives you the ability to set which groups the duplicate tokens will have access to. This defaults to all the groups on the original token that can be distributed by your Master.
6. When you are finished, click OK.
7. Now that this management policy has been created, you must send your users a link to the policy, and start a remote management session when they follow the link. See the Applying Remote Management Settings section for more information.

Now that this management policy has been created, you must send your users a link to the policy, and start a remote management session when they follow the link. See the Applying Remote Management Settings section for more information.

Managing Groups on GoldKey Tokens

There are two ways to add groups to a GoldKey token remotely. Which method you will want to use may depend on the number of tokens you would like to add groups to, and whether or not those tokens are registered to your Master.

Changing Group Membership for a Registered Token

You may remotely add or remove groups from any token that is registered to your Master. To begin, open the GoldKeyVault software with your Master plugged in. Then, select the token you would like to modify and click first on the Properties button, and then on the Management tab. See Figure 41.

From here, leave a check beside the groups that you would like the token to have access to, and click OK.

To apply the changes you have made to this token, you must start a remote management session and have the user sign into GoldKeyVault. See the Applying Remote Management Settings section for more information.

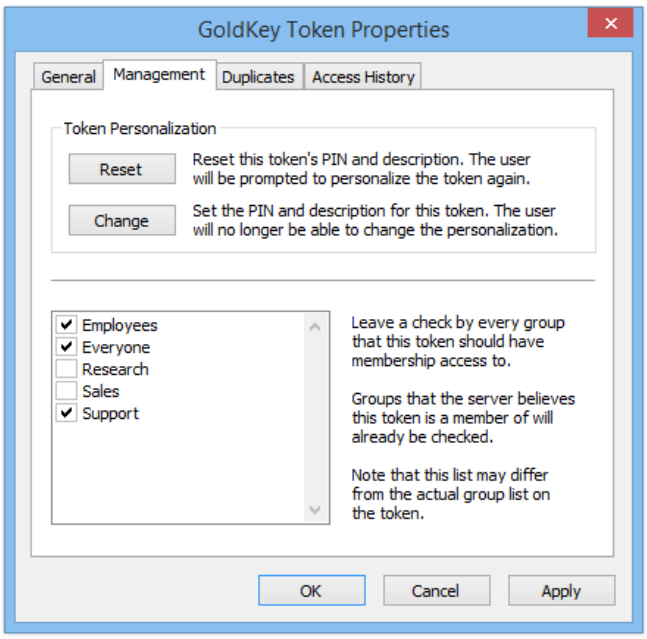


Figure 41. The Management Tab

Adding Groups through a Management Policy

If you are adding groups to a large number of tokens, or if you would like to add groups to tokens that are not registered to your Master, you may create a management policy to distribute the groups. To begin, open the GoldKeyVault software with your Master token plugged in. Then, select the "Management policy" option under New in the File menu.

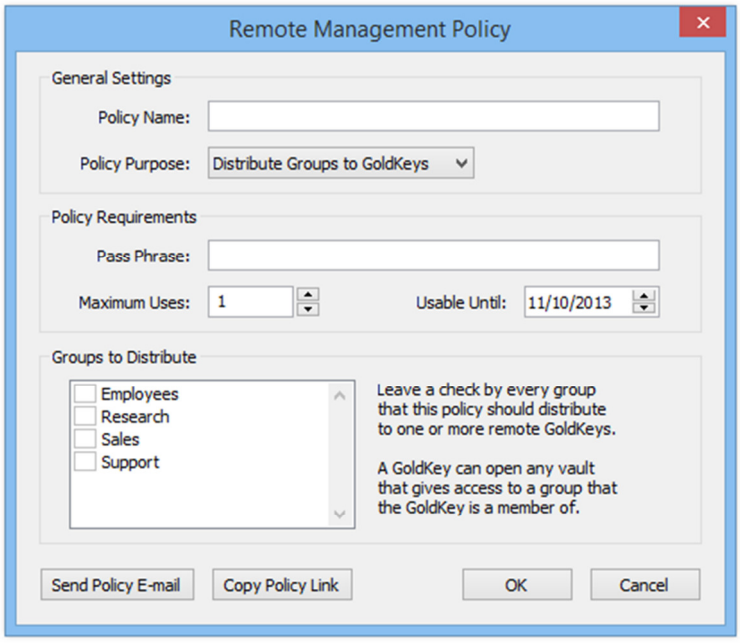


Figure 42. Creating a Policy to Distribute Groups

First, enter a name for this policy and select "Distribute Groups to GoldKeys" as the Policy Purpose. If you would like to require users to enter a pass phrase in order to apply this policy, enter it in the appropriate field in the

Policy Requirements section. Next, to limit the use of this management policy, select a maximum number of uses and an expiration date for it.

Finally, select the groups you would like to distribute and click OK.

Now that this management policy has been created, you must send your users a link to the policy, and start a remote management session when they follow the link. See the Applying Remote Management Settings section for more information.

Remote GoldKey Personalization

The GoldKeyVault software provides a secure way for you to remotely set or clear the personalization settings for any token that is registered to your Master and has logged into GoldKeyVault. This allows you to easily assist users at remote sites who have forgotten their PIN.

To begin, do the following:

1. Open the GoldKeyVault software with your Master token plugged in.
2. Then, select the token you would like to modify and click first on the Properties button, and then on the Management tab. Refer to Figure 41.
3. To clear the personalization settings on this token so that the user can re-personalize it later, click on the Reset button. If you would rather set the personalization settings for them, click on the Change button and enter the new settings.

Note: *Use of the Change button will lock the personalization settings on the token. The user will not be able to change the description, set personal questions, or obtain additional groups from other Master tokens.*

4. When you are finished changing these settings, click OK.
5. To apply the changes you have made to this token, you must start a remote management session and have the user sign into GoldKeyVault. See the Applying Remote Management Settings section for more information.

Applying Remote Management Settings

Whenever you would like to apply remote management changes you have made to your registered tokens or apply a management policy, you need to start a remote management session with your Master token.

If you are applying a management policy, users will need to know the policy ID and any pass phrase you have assigned to the policy. One very effective way to communicate the policy ID is to send them a link in an email. To send a link, you may right-click on the policy and select the “In an email” option in the Create link submenu. This will start an email containing a link to the policy using your default email client.

To begin a remote management session, open the GoldKeyVault software and click on the Remote Management button in the toolbar, or select the “Remote Management Session” option from the Tools menu. You will be prompted to enter the PIN for your Master token.

Once you have started the remote management session, you will be able to choose the criteria for approving remote management operations. You may require every operation to be approved manually, require use of management policies to be approved manually, or to automatically approve every management operation. By default, you will need to manually approve the use of management policies, but changes you have made to registered tokens will be applied automatically.

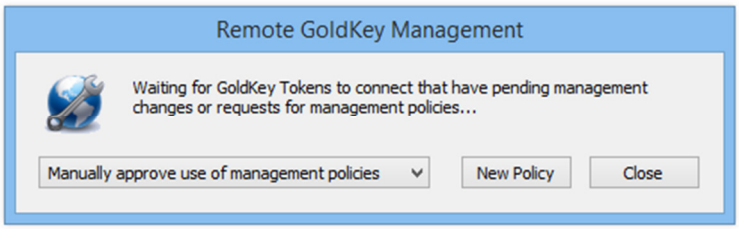


Figure 43. A Remote Management Session

When each client signs into GoldKeyVault using tokens that are registered to your Master, any pending management operations will be applied to those tokens. If you have opted to manually approve every operation, you will be asked if you would like to proceed before the changes are applied.

When a user follows a link to one of your management policies, they will be prompted to enter the pass phrase you set when you created that policy, if there is one. Once they have entered the pass phrase, you will be prompted to approve the operation unless you have selected to automatically approve management policy requests.

If you are distributing groups through a management policy, the user will also be required to enter their PIN and answer one of their personal questions. If the personalization for that token has been locked by their registered Master, they will not be able to continue.

GoldKey Soft-Tokens

As cyber-attacks have become more common, authenticating users based on a username and password is no longer sufficient. However, it has proven very difficult to provide multi-factor authentication in today's environment of mobile devices.

GoldKey Soft-Tokens allow you to use your mobile phone or other mobile device as a software authenticator in conjunction with a PIN to achieve two-factor authentication with online services, providing a secure alternative to traditional password-based systems. This unique approach solves the technical and convenience problems raised by requiring a hardware token for secure authentication.

Managing Soft-Tokens

Soft-Tokens are created and managed using the freely-available GoldKey ID service. To obtain a GoldKey ID, please visit the following website:

http://www.goldkeyid.com/

Creating a Soft-Token

Once you have created your account, you will be taken to your Dashboard where you will see a list of tokens currently associated with your account. To create a Soft-Token, click on Create Soft-Token.

We suggest that you specify the name of the computer you are creating the Soft-Token on as the name of the Soft-Token in GoldKey ID. Once you have entered the name of your computer, click on Continue and you will be prompted to create the Soft-Token on your computer.

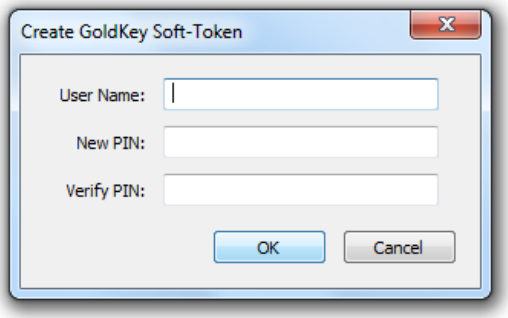


Figure 44. Creating a Soft-Token

Enter your user name and the PIN you would like to associate with the new Soft-Token, and click OK.

Changing a Soft-Token PIN

To change your Soft-Token's PIN, click the Change User button during Soft-Token sign-in, right-click on the Soft-Token you would like to change the PIN for, and click on Change PIN.

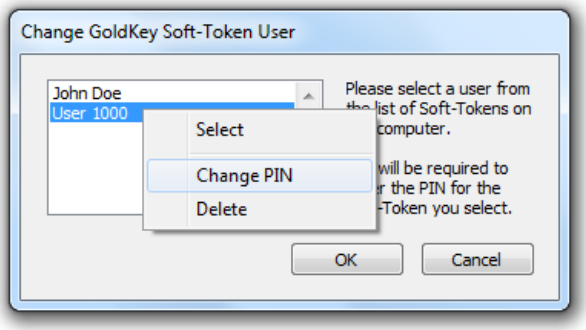


Figure 45. Changing a Soft-Token PIN

You will be required to enter the current Soft-Token PIN in order to set a new one. If you have forgotten the PIN you set for your Soft-Token, please see the Reset a Soft-Token PIN section.

Reset a Soft-Token PIN

If you have forgotten the PIN you set for your Soft-Token, you may reset it using the GoldKey ID website. Sign into GoldKey ID using your GoldKey or the alternative sign-in, select the Soft-Token you would like to reset from the list provided, and click on Reset PIN.

Enter your user name and set a new Soft-Token PIN. Then click OK.

Signing In Using a Soft-Token

After you have created a Soft-Token on your computer, a "Soft-Token Sign-In" option will be available when a website supporting Soft-Tokens asks you to authenticate with your GoldKey. Select this option and enter your Soft-Token PIN to sign in.

Figure 46. Soft-Token Sign-In

If multiple individuals use the computer or mobile device you are authenticating on, the Soft-Token that comes up by default may not be the one associated with your account. To change the Soft-Token being used to authenticate, click on the Change User button, select your Soft-Token, and click OK.

Advanced Topics

Encrypting Email with GoldKey

In this section, we will explain the process of protecting your email with GoldKey encryption, focusing on Mozilla Thunderbird, a popular email client. Following these instructions will only protect your email once the messages are stored on your computer.

To send encrypted emails, you may attach files that have been encrypted with a GoldKey, or set up digital signature and email encryption using your GoldKey token's built-in smart card. Refer to the Right-Click Encryption and Secure Email sections.

Note: *If you are using an IMAP account, your email is stored on your email server, not on your computer. These instructions are intended for POP accounts.*

Encrypting Mozilla Thunderbird Email

Open Thunderbird and select Account Settings from the Tools menu. From the list of accounts on the left, select the Server Settings option under the correct account.

At the bottom of this dialog, you will see a "Local directory" setting, indicating the path to the location on your hard drive where your mail is stored. Either write down the path shown here, or copy this text to your clipboard.

Close Thunderbird. Since Thunderbird has files open that we will need to move, you must close it before continuing.

Next, go to the Folder Encryption tab in the GoldKey software. Click on the Add Folder button, and paste the path to your mail in the field labeled "Folder." Click OK.

Your mail will then be moved into your Primary Secure Drive, and will only be accessible while that drive is unlocked.

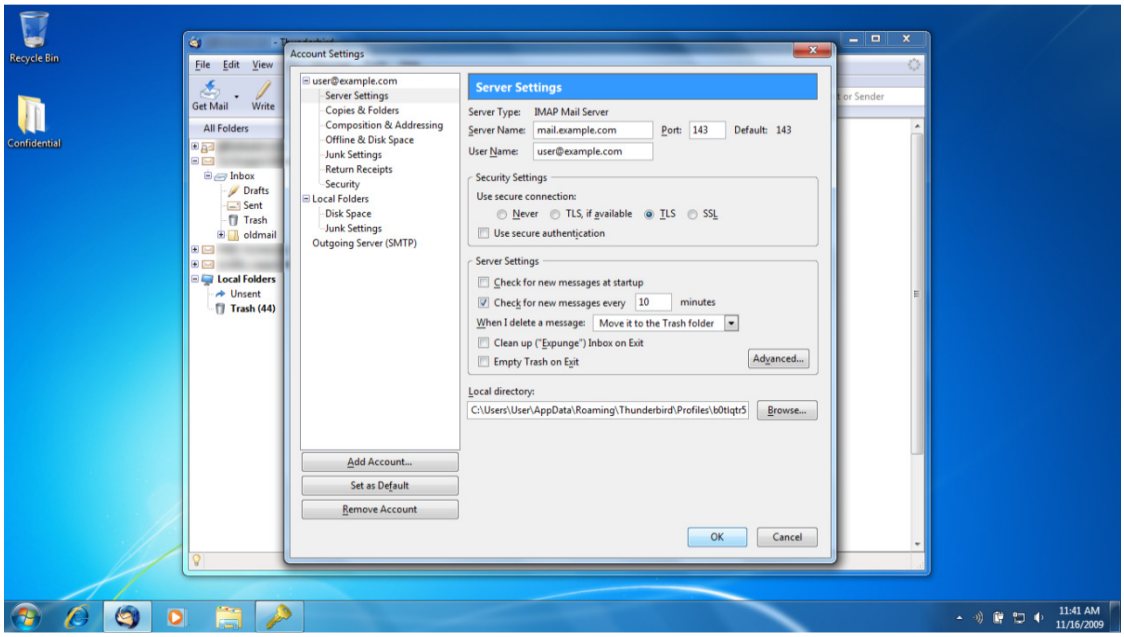


Figure 47. Mozilla Thunderbird Email Directory

Note: *If you plan to encrypt your email, we recommend that you plan your security options so that your Secure Drives do not lock while your email client is running.*

Encrypted Files

When you create a Secure Drive, a Secure Drive File is created with the size specified, and placed in a given directory ("AppData\Roaming\GoldKey" under the user's directory in Windows, and "~/Library/GoldKey" in Mac). This file actually contains an AES 256-bit encrypted version of the data, encrypted on-the-fly before being stored in the drive.

Note: *All Secure Drives stored within your directory are also protected by file permissions imposed by the operating system.*

There is another way to unlock Secure Drives, which was not covered earlier in this manual. This technique involves knowing the location of the file associated with the drive you would like to unlock. This technique is useful for accessing data stored on CDs, etc.

To unlock the drive, open Finder or Windows Explorer and browse to the location of the correct file. Once you have found the file, double-click on it. This will unlock the Secure Drive, and open it in a new window.

Unlocking a Windows Account

To disable GoldKey Login for an account, log into the account you would like to unlock and press Control-Alt-Delete. Click on Change a password, and then on Other Credentials if that button is available.

Select the Disable GoldKey Login option, and then enter your PIN and the new Windows password.

Figure 48. Secure Drive File

Uninstalling the GoldKey Software in Windows

1. Before uninstalling the GoldKey software do the following:
   a. Determine which data within the secure drives you want to keep and copy it out of all the Secure Drives you have created.
   b. Disable GoldKey Login for each secured account.
   See the Deleting Secure Drives and Unlocking a Windows Account sections for instructions.
2. For the Primary Secure Drive, first go to the Folder Encryption tab in the GoldKey software and, with the Primary Secure Drive unlocked, remove each folder in the list.
3. To uninstall the software, go to the Add/Remove Programs utility on your computer, select GoldKey, and click Uninstall/Change.

Note: *If you forget to unlock encrypted data, you can reinstall the GoldKey software. You will then be able to access your data and accounts again using the correct GoldKey tokens.*

Uninstalling the GoldKey Software in Mac OS X

Before uninstalling the GoldKey software, copy any data that you want to keep from all the Secure Drives you have created. These cannot be unlocked without the GoldKey software.

To uninstall the software, open Terminal, and run the following command:

```
/Applications/GoldKey.app/Contents/Resources/uninstall-goldkey.sh --all
```

Only an administrative account can uninstall the GoldKey software. During this process, you will be prompted for your password.

After the software has been successfully uninstalled, reboot your computer.

Note: *If you forget to unlock encrypted data, you can reinstall the GoldKey software. You will then be able to access your data with the correct GoldKey tokens.*

To uninstall the GoldKeyVault software, simply click and drag the GoldKeyVault Application to the Trash from the Applications folder.

Customer Support

If you have questions or comments, please feel free to contact GoldKey Customer Support. General product information can be obtained from our website.

Telephone: 888-663-2471
Email: techsupport@goldkey.com
Website: http://www.goldkey.com/

Acknowledgments and Disclosures

The GoldKey software installs the MacFUSE project. Downloads and documentation for MacFUSE are available at http://code.google.com/p/macfuse/.

Trademarks

Acrobat and Adobe are registered trademarks of Adobe Systems Incorporated.

Apple, Finder, Mac, Mac OS, and OS X are registered trademarks of Apple Computer, Inc.

GoldKey is a registered trademark of WideBand Corporation.

MacFUSE has been developed and copyrighted by Google Inc.

Active Directory, BitLocker, Microsoft, Outlook, Windows, Windows Server, and Windows Vista are registered trademarks of Microsoft Corporation.

Mozilla and Thunderbird are registered trademarks of the Mozilla Foundation.

DECLARATION OF CONFORMITY

According to 47 CFR Part 15

Responsible Party Name: **WideBand Corporation**
Address: 26900 E. Pink Hill Rd.
Independence, MO
64057, USA
Telephone: (816) 220-3000

Hereby declares that the product:

Name: **GoldKey Security Token**
GoldKey with Flash
GoldKey Master Token
GoldKey GrandMaster Token
Models: GK-011A, GKF8GB, GKF16GB, GKF32GB, GKF64GB, GKM1A, GKG1A

Complies with part 15 of the FCC Rules

Supplementary Information:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: (1) Reorient or relocate the receiving antenna. (2) Increase the separation between the equipment and receiver. (3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. (4) Consult the dealer or an experienced radio/TV technician for help**.**

FCC Warning: Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC rules.