u.trust LAN Crypt Cloud

EN

utimaco®

Imprint

Copyright 2023	Utimaco IS GmbH
	Germanusstr. 4 D-52080 Aachen Germany
	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
Phone	EMEA +49 800-627-3081
	APAC +81 800-919-1301
	https://support.hsm.utimaco.com/
Internet e-mail	support@utimaco.com

u.trust LAN Crypt Cloud is a powerful cloud-based application specifically designed for the administration of u.trust LAN Crypt instances within an organization. It is a flexible and efficient solution that provides administrators with a wide range of features to manage u.trust LAN Crypt instances.

This application can be used either as a complement to the existing on-premises administration of u.trust LAN Crypt instances or as a fully-fledged alternative to it. This means that companies have the option of either moving the administration of u.trust LAN Crypt completely to the cloud or using a hybrid solution that combines both on-premises and cloud administration.

Functionality of u.trust LAN Crypt

u.trust LAN Crypt enables the exchange of confidential data within authorization groups in small, medium and large organizations with transparent file encryption. u.trust LAN Crypt works without user interaction. It supports the role of a Security Officer (SO) who can restrict access rights to files encrypted with u.trust LAN Crypt. A Master Security Officer (MSO) has the right to manage u.trust LAN Crypt or to delegate permissions. This way a hierarchy of Security Officers can be set up to meet the security requirements in any company.

Encrypted files do not have to be assigned to individual users. Any user who has the required key can work with an encrypted file. This allows administrators to create logical user groups that can collectively access and work with encrypted files. This process can be compared to a kind of keychain used in everyday life. u.trust LAN Crypt provides users and user groups with a keychain whose individual keys can be used for different folders or files.

Every time a user moves a file to an encrypted folder, the file is encrypted on that user's computer. When another user from the same permission group reads the file from the folder, it is transferred in encrypted form. The file is decrypted only on the recipient's computer. The user can edit it there. Before the file is transferred back to the encrypted folder, it is encrypted again.

Unauthorized users may be able to access these encrypted files (only from workstations without u.trust LAN Crypt), but without the appropriate u.trust LAN Crypt authorization they will only see their encrypted contents.

---

u.trust LAN Crypt Cloud: Quickstart

After successful registration the entry into the workflow of u.trust LAN Crypt Cloud is divided into **three simple steps**:

Step 1: Define assets.

Assets are storage addresses that contain important data for an organization. With u.trust LAN Crypt Cloud, access rights for assets can be controlled and restricted to individuals or groups within the organization. However, before this is possible, storage addresses must be defined as such within u.trust LAN Crypt Cloud.

See Managing assets for detailed instructions on defining assets.

Step 2: Defining Identities

Identities in u.trust LAN Crypt Cloud represent individual users, groups and subgroups of your organization and thus enable a clear modeling of your company structure and an easy assignment of users to groups and subgroups. To achieve this, users must first be created and then the relevant people in your organization must be invited to create an u.trust LAN Crypt Cloud account to identify themselves. As an alternative to manually mapping your organization's structure, you can import existing structures from an Microsoft Entra ID.

See Managing assets for detailed instructions on defining identities and Microsoft Entra ID Synchronization for importing existing structures from a Microsoft Entra ID.

Step 3: Distribution of access permissions.

Once assets and identities have been created, access permissions can be assigned to users, groups, and subgroups. These permissions can be managed in the **Assets** and **Identities** tabs.

See Managing access permissions of groups, users and assets for detailed instructions on how to distribute access permissions.

---

u.trust LAN Crypt Cloud account management

Registration and login as administrator

The use of u.trust LAN Crypt Cloud requires the registration of an u.trust LAN Crypt Cloud account. After you have successfully completed the registration process, an email for account activation will be sent to the specified address. To activate the registered account, the activation link in the email must be accessed within the next 24 hours. If the registered account has not been activated within this period, it will be deleted. After the account activation, the given e-mail address and the chosen password will serve as login data.

Alternatively, you have the option to register and log in by using a Microsoft account.

Note

- Please note that too many consecutive failed login attempts will result in a waiting period between further attempts. This waiting time is maximum 15 minutes and serves as a protection against brute force attacks on your account.
- There is no permanent lock enforced by the system. However, a locked account cannot be used until the lock duration expires or the account password is reset.
- If the user is inactive for a longer period of time, a new login is required for security reasons.

Registration and login of users of an organization

The registration of a user of an organization can only be initiated by the administrator, but both parties are required to complete the registration process. When adding a member of the organization under the **Identities** tab, the user is assigned a unique email address and a login method.

Note

- If the Microsoft Entra ID login method is selected, it is important to ensure that the e-mail address provided matches the e-mail address of the Microsoft account of the user to be registered.

The user then receives an email to confirm their user account. After successful confirmation by setting an account password, the user's registration is complete. The user can now log in with the e-mail address used as the login name and their chosen password.

When logging in using Microsoft Entra ID, it is not necessary to create an additional password. After confirming the user account via the link in the confirmation email, the user can use their Microsoft account for future login processes.

Note

- The **circle icon with three dots** indicates the pending of the completed registration process. If the registration is completed successfully, the icon will disappear.

Requirements for creating a secure password.

A password chosen by the user must meet several requirements to ensure the security of the account:

Length: The password must be at least 8 characters long.

Capital letters: The password must contain at least one capital letter.

Lowercase letters: The password must contain at least one lowercase letter.

Digits: The password must contain at least one digit (0-9).

Special characters: The password must contain at least one special character, such as !, @, #, $, %.

History: Password history requires that the new password be different from the last three passwords used. This is to prevent users from reusing passwords that are too similar or have already been used.

Voidance of user name and email address: The password must not contain the user name or email address.

It is necessary to follow these requirements when creating a password to increase the security of the account and minimize potential points of attack.

Managing account data

To manage your account data, click on your account icon in the top right corner and click **Manage your u.trust LAN Crypt Cloud account**. Here you have several options to manage your u.trust LAN Crypt Cloud account:

Personal Info: Review and edit personal information. Here you can also set your preferred language and regional format.

Contact: Contact us directly using our form.

Subscriptions: Get detailed information about your subscription.

Clients: Here you will find an overview with links to the various LAN Crypt clients.

Export: Start the export process for encryption keys. These keys are required to be able to continue accessing encrypted assets even after the cloud account has been deactivated.

Dashboard: This takes you back to the dashboard overview.

Administration with u.trust LAN Crypt Cloud

Using the Dashboard

The dashboard provides a quick overview of the most important information you need to monitor the performance of your cloud platform. Here you can quickly and easily see at a glance which products have been installed and on which operating systems they are running.

In addition, our dashboard also provides information about the most recently accessed user profiles. You can see who has been active recently and who has not, to better understand how your users are using the applications. It also shows which devices users' profiles were accessed on, so you know exactly where and how your users are accessing each u.trust LAN Crypt product.

Managing assets

What are assets?

Assets are storage addresses that contain important data for an organization. With u.trust LAN Crypt Cloud you have the possibility to control and manage access to these storage addresses. You can own multiple assets and restrict access to them to individuals or groups within your organization. Access permissions are implemented by securely encrypting the data in the storage addresses, and matching keys are distributed only to authorized groups and individuals. It should be noted that access permissions to assets are inherited. This means that asset permissions are automatically inherited downwards and thus other assets located in subdirectories are always included when a new asset is defined.

Create and edit assets

To create an asset within the **Assets** tab, click on the blue action button next to **Add asset**. Now you need to assign the asset a name, a **storage address** and an **asset type**. Optionally, you can also directly assign groups that should have access to this asset. However, this can also be done afterwards. Finally, click **Save** and the asset creation is complete.

Properties and access permissions of an asset can be edited at any time. The exception here, however, is the **Asset type**, which remains unchangeable after the initial creation of the asset. To edit the properties of an asset, simply select the respective asset within the listing under the **Assets** tab. You can also delete created assets directly using the **trash icon** next to an asset entry.

Asset types

Shared

The use of **Shared** assets is recommended for storage addresses whose access rights are to be distributed to one or more groups. Here, all data within the specified storage address is encrypted in the background with an asset-specific key, which is distributed to the assigned groups and persons.

Public

The use of **Public** assets is recommended for storage addresses whose contents are to be excluded from all encryption. This causes all users of the organization to be able to freely access this content.

> **Note** In order to be able to use the functionality of a **Public** asset to its full extent, all users who have access to this storage address within the scope of a **Shared** asset or **Private** asset must be assigned to the respective **Public** asset. If this assignment does not take place, all data from unassigned users will be stored **encrypted** in the storage address of the **Public** asset.

Private

It is recommended to use Private assets when access needs to be restricted to individual persons. Within these assets, all data is encrypted using individual keys specific to the respective individuals, even if they belong to the same group.

Specifying storage addresses

Storage addresses in u.trust LAN Crypt Cloud define which data is to be encrypted. They represent encryption paths and define encryption rules for this.

Example:

Storage address: `C:\my_data\marketing\`

By specifying this storage address, all files within the `marketing` folder will be encrypted.

To avoid any malfunction, make sure the storage address always ends with a forward slash `/` (for UNIX systems like macOS and Linux) or a backslash `\` (for Windows).

Note

- Paths to compressed folders cannot be used as encryption paths.

Specifying storage addresses for SMB Shares

To ensure the correct encryption of your SMB shares, it is crucial that the paths specified in the encryption rules exactly match the paths of your mount points. If the paths do not match exactly, encryption will not be activated.

Example of a correct match:

Rule: `smb://newhost.newdomain.local/newpath/anotherpath/*.*`

Mount: `smb://newuser@newhost.newdomain.local/newpath`

Environment variables

u.trust LAN Crypt Cloud supports the use of the local environment variable `%USERNAME%` in path specifications. The environment variable `%USERNAME%` in path specifications is resolved by u.trust LAN Crypt Cloud by default.

Managing identities

What are identities?

Identities represent individual users, groups and subgroups in your organization within u.trust LAN Crypt Cloud. This enables the clear modeling of your internal company structure and subsequently the easy assignment of individual users to the respective groups and subgroups.

Create and invite users

To create and invite a user within the **Identities** tab, click **Users** in the list and then click the blue action button next to **New user**. Now you can give the new user a name, last name and description. It is also necessary to enter an e-mail address of the user, because the user will be invited via this e-mail address and it will be used later as login name. Optionally, the assignment to different groups can already be made when creating the user. However, this is also possible at any later time.

After the user has been created and invited, he will be asked to activate his account and to set a password for his user account via the specified e-mail address. If both of these steps are successfully completed, the user's registration is complete.

Once a user has been created and invited, he or she will appear in the list of all existing users. The **pencil icon** in the entry allows subsequent editing of user information and group assignments. The **circle symbol with three dots** signals the pending of the completed registration process. When the registration of the respective user is successfully completed, the icon disappears.

By clicking on the **arrow icon** in the respective user entries, more details about a user can be retrieved.

Creating and editing groups

To create a group within the **Identities** tab, first click on the parent group collection **Users and Groups** and then click on the blue action button next to **New group**. Now you can give the group a name and description. You can also customize the **Parent Group**, e.g. to subordinate the group to another group. You can also add further affiliations.

To create a subgroup, first click on the desired parent group and finally on the blue action button next to **New group**. Again, the name, description and **Parent Groups** of the subgroup can still be customized.

You can edit the name, description and **Parent Group** at any time afterwards by first selecting the group you want to edit within the list and then clicking on the **Pencil icon**.

Note

- If a subgroup is subordinate to several groups, changes to the subgroup or its subgroups are automatically updated in all corresponding places.

Managing access permissions of groups, users and assets

Access permissions for assets can be distributed in several ways:

One way to assign access permissions is to distribute them directly in the definition dialog for an asset. There, individual users and groups can be assigned to the respective asset. After asset creation, access permissions can also be managed in the asset overview in the **Assets** tab.

An alternative way to manage access permissions is to add them to the respective groups in the **Identities** tab. Each group or subgroup contains **Members** (users) and **Assets**. These can be assigned by expanding the group and clicking the respective blue action button next to **Add member** or **Assign asset**. This assignment will give all users in a group the specific access permissions over the assigned assets.

Note

- Asset permissions are inherited. This means that asset permissions are automatically inherited downwards and thus other assets located in subdirectories are always included when defining a new asset.

Settings

Synchronization

In the **Synchronization** section of the settings, the following configuration options are available:

Refresh interval: Sets the interval at which clients automatically connect to the server to retrieve policy updates.

Policy cache expiration: This setting defines how long received policies remain valid if no connection to the server can be established. Each successful policy refresh resets the set validity period to the full time period.

File encryption

In the **File encryption** section of the settings, the following configuration options are available:

User may decrypt: This setting determines whether the user is authorized to manually encrypt and decrypt files that are not subject any encryption policy.

Audit log

The **Auditlog** tab gives you access to a comprehensive log of your admin activities, which you can filter and search specifically. For example, you can filter by a specific time period, a specific activity type or an affected user by using the corresponding fields. Afterwards, you can confirm the set filters by pressing the blue action button with the **magnifying glass** icon.

Microsoft Entra ID Synchronization

In addition to adding users and groups manually, u.trust LAN Crypt Cloud can also synchronize user and group information from a Microsoft Entra ID. This is a quick and easy way to assign assets based on the organizational structure you already know. This is an outbound-only sync, where changes are only transferred from the Microsoft Entra ID to the application and not vice versa. This means that changes made in u.trust LAN Crypt Cloud are not synchronized back to the Microsoft Entra ID, but only changes within the Microsoft Entra ID are imported to u.trust LAN Crypt Cloud.

The Synchronization requires a few setup steps that are necessary to establish a connection between u.trust LAN Crypt Cloud and your Microsoft Entra ID. Once the connection is established, importing and synchronizing the latest user information can be done with one click within u.trust LAN Crypt Cloud.

Description of the setup process

Step 1: Registering u.trust LAN Crypt Cloud as an application with Microsoft Identity Platform

The first step of the setup process is to register u.trust LAN Crypt Cloud as an application with the Microsoft Identity Platform, because it performs identity and access management (IAM) only for registered applications. Registering u.trust LAN Crypt Cloud establishes a trust relationship between the application and the Microsoft Identity Platform. The trust is unidirectional: u.trust LAN Crypt Cloud trusts the Microsoft Identity Platform and not vice versa.

It is recommended to use a unique name for the application registration to clearly identify the application. It is important to select **Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)** when selecting **Supported account types** for application registration.

For information about registering an application with Microsoft Identity Platform, see Quick Start: Registering an Application with Microsoft Identity Platform.

Step 2: Grant API Permissions

In the next step API permissions have to be assigned to the registered application. These are necessary to allow u.trust LAN Crypt Cloud to authenticate itself without user interaction or consent.

To ensure full functionality of u.trust LAN Crypt Cloud six different permissions are required:

- **Directory.Read.All**
- **Group.Read.All**
- **GroupMember.Read.All**
- **Organization.Read.All**
- **User.Read**
- **User.Read.All**

Note

- When granting permissions for **Microsoft Graph**, you have two choices. It is important to select **Application permissions** since the synchronization operates in the background as a service.

Finally, after configuring API permissions, administrative approval must be granted to complete the configuration.

img/Permissions_EN.png

For information on granting API permissions to an application, see Quick Start: Configuring a Client Application to Access a Web API.

Step 3: Configuring the login information

u.trust LAN Crypt Cloud requires the configuration of credentials within the Registered Application with Microsoft Identity Platform to access the Microsoft Graph API. A secret client key allows the application to authenticate without requiring manual intervention from a user.

Create a new secret client key and select a desired validity period. A validity period of no more than 12 months is recommended.

Important: The generated **secret ID** will not be displayed after changing or closing the dialog. Since this is required for establishing a connection with u.trust LAN Crypt Cloud, it is recommended to keep it in another safe place.

For information on how to create a secret client key, see Quick Start: Registering an application with Microsoft Identity Platform.

Step 4: Connection setup with u.trust LAN Crypt Cloud

After all the Microsoft Entra ID Synchronization setup steps have been completed, the connection with u.trust LAN Crypt Cloud can be established.

To do this, log in to u.trust LAN Crypt Cloud and select the **Identity provider** dialog and then **Connections**. Create a new connection with the blue action button and now enter any **Connection Name**, the **Directory ID (Tenant)**, the **Application ID (Client)** and the previously generated **Client Secret** and click **Next**.

Now define the login method for your users and then click **Next** again. A summary of the Microsoft Entra ID synchronization is then displayed. Click on **Create** to complete the connection setup.

Note

- The **Directory ID (client)** and **Application ID (client)** can be viewed under **Overview** within the application at Microsoft Identity Platform.

Import and manage user and group information

User and group information from various Microsoft Entra IDs can be imported, updated, or deleted from u.trust LAN Crypt Cloud at any time. With this capability, administrators can quickly make changes to imported user and group information and ensure that the directory is always up to date.

Import user and group information.

To import new user and group information for the first time, log in to u.trust LAN Crypt Cloud and select the **Import** dialog under the **Identity Provider** item. Now you can select and import the desired persons and groups from all existing Microsoft Entra IDs. The import process is started and can be viewed under **Import Jobs** under the item **Identity Provider**. The imported users and groups can be assigned and managed under the item **Identities** in the groups created within the u.trust LAN Crypt Cloud.

Additional user and group information can also be imported at any time via the dialog **Import**.

Update and delete user and group information.

Under the **Identity Provider** item, existing user and group information can be updated and connections to Microsoft Entra IDs deleted in the **Connections** dialog. To do so, click on the corresponding icons in the entry of the respective Microsoft Entra ID connection.

Note

- When updating, only the previously imported user and group information is affected. No other user or group information will be imported.
- If one deletes the connection to a Microsoft Entra ID, all associated groups and users are automatically removed from the administered pool of identities.

Migration of password based keys

LAN Crypt 2Go and all mobile u.trust LAN Crypt applications support encryption with password-based keys. These keys are created and managed by the user. When created, password-based keys are stored locally in the user's key ring on the device itself. Keys are not synchronized with other devices and therefore must be added manually on each device on which they are needed.

When a user logs in with their **u.trust LAN Crypt Cloud account**, all newly created keys are linked to their account and uploaded to the **Cloud Management System**. This allows synchronization with all other devices where the user logs in with his u.trust LAN Crypt Cloud account.

When a user logs in for the first time within a u.trust LAN Crypt Cloud LAN Crypt application that supports encryption with password-based keys, a check is made to see if keys are stored in the user's local key ring. If the user has already created password based keys before, there are two options to proceed. The first option is to connect to the cloud - where all locally created keys will be uploaded to the cloud. Alternatively, the process can be aborted if it is not wanted that some or all of its keys are uploaded. In the latter case, it is possible to delete all keys from the key ring that are not to be uploaded to the cloud. After logging in again, all the desired keys are then linked to the account and uploaded to the cloud.

Exporting the keys

In order to be able to access encrypted data even after the use of u.trust LAN Crypt Cloud has ended, it is necessary to export the keys. To export all created keys, click on the profile icon and select **Manage your account** in the settings window. Then click on the **Export** tab to start the process. Once the export process is completed successfully, you will be able to download a file that contains all the keys.

Technical Support

Technical support for Utimaco products can be accessed as follows:

At support.Utimaco.com, maintenance contract customers can access additional information, such as knowledge items.

As a maintenance contract customer, send an email to technical support:

support@Utimaco.com

and specify the version number(s), operating system(s) and patch level of your Utimaco software and, if applicable, the exact wording of any error messages.

Legal notice

Last updated 27.03.2024.