TeamViewer Manual

Management Console

Rev 4-202205

Table of contents

1 About the TeamViewer Management Console

1.1 About the Management Console

The TeamViewer Management Console is a web-based management platform for intuitively managing your TeamViewer contacts and logging TeamViewer connections.

In addition, the TeamViewer Management Console provides extensive functions for managing several TeamViewer accounts and managing them through an administrative account (company profile).

The TeamViewer Management Console can be reached via the Internet using a web browser – as a result, it can be called up independently of the operating system. A local database or a Microsoft SQL server is not required.

Some functions of the TeamViewer Management Console, such as user management and connection report, are available only in conjunction with a TeamViewer license and a company profile. However, the basic functions for connection, account and computer & contact management are available to all users.

Note: You need a TeamViewer account in order to use the Management Console.

In the TeamViewer Management Console you can:

- Manage multiple TeamViewer accounts centrally at a company level with a powerful user management.
- Customize TeamViewer modules with your logo, colors and texts to fit your corporate identity.
- Configure setting policies for TeamViewer installed on your devices from one location.
- Manage customers' support requests, similar to a ticket system.
- Log TeamViewer connections for billing purposes or similar tasks.
- Monitor and track your devices to improve fault-free operation of your computers and devices.
- Open TeamViewer connections out of the web browser or completely within the browser.

- Manage your TeamViewer contacts and computers.
- Develop your own plug-ins, add-ons and scripts for integration into your own systems using the TeamViewer API or SDK.

Note: The scope of available features and functions in the Management Console depends on the license you use. Please visit our *product description page* for a detailed overview of licenses and features.

1.2 About the manual

This manual describes the most important functions for working with the TeamViewer Management Console. It is intended to help you to better understand the TeamViewer Management Console and its functionality and provide you with initial support.

The chapters describing TeamViewer Enterprise features (TeamViewer Tensor license required) are marked with the Tensor logo TeamViewer Tensor.

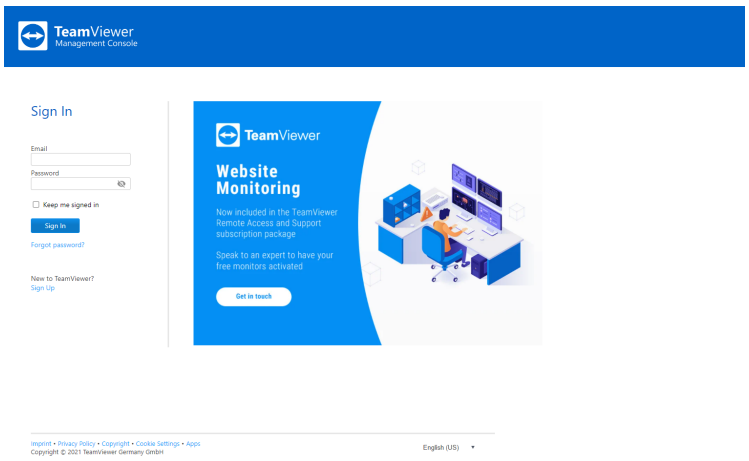
As described in section *Section 1 "About the TeamViewer Management Console", page 5*, some functions of the TeamViewer Management Console are available only in conjunction with a TeamViewer license. These functions are described starting with *Section 3 "Company profile", page 17*. If you do not have a TeamViewer license, it is not necessary to read chapter *Section 3 "Company profile", page 17*.

2 General

2.1 Start and Login

The TeamViewer Management Console is a web-based application. To call it up, open the page *www.login.teamviewer.com* in a web browser.

To be able to work with the TeamViewer Management Console, you have to log in on the left side using your TeamViewer account.



The login screen of the TeamViewer Management Console.

Note:

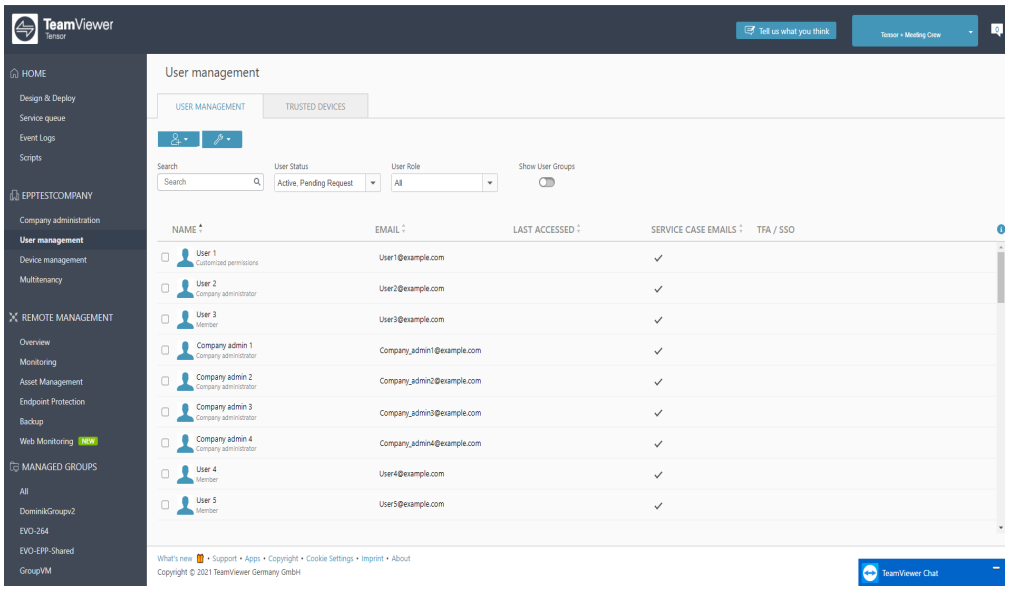
- If you do not yet have a TeamViewer account, you can create a new TeamViewer account by clicking on the Sign Up button.
- If you have never used your TeamViewer account on a device, with an app or within a browser, you have to authorize the account usage at the first login. You can find further information the TeamViewer Manual – Remote Control.

2.2 Graphical User Interface

After successfully logging into the TeamViewer Management Console with your TeamViewer account, the start screen is displayed.

The start screen is divided into three visually separated areas: menu bar (left), title bar (top) and content area. This allows an intuitive and quick operation.

The menu bar, the title bar, and the integrated chat are permanent elements and, as such, are always visible from any screen of the TeamViewer Management Console.



The start screen after login.

Menu bar

The menu bar is used for navigation through the TeamViewer Management Console.

In the menu bar, the groups of your Computers & Contacts list as well as the User management, Design & Deploy, the Service queue and Remote Management is displayed. Additional actions can be performed by moving the mouse over the menu items or a group or by selecting it.

If an entry is selected, the display in the content area of the screen is adapted.

Title bar

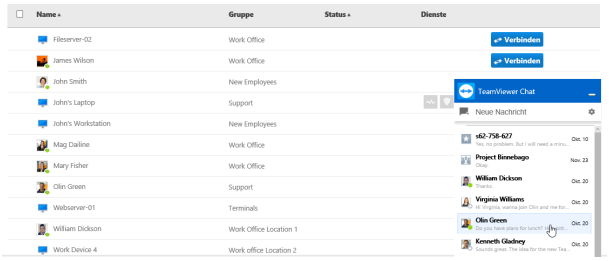
Various actions pertaining to your own TeamViewer account can be called up via the title bar.

Content area

The content area displays different pieces of information depending on the location on the screen.

Web-based TeamViewer Chat

With the integrated chat, it is possible to send text messages to computers and contacts of your Computers & Contacts list from within the TeamViewer Management Console.



TeamViewer chat within the TeamViewer Management Console.

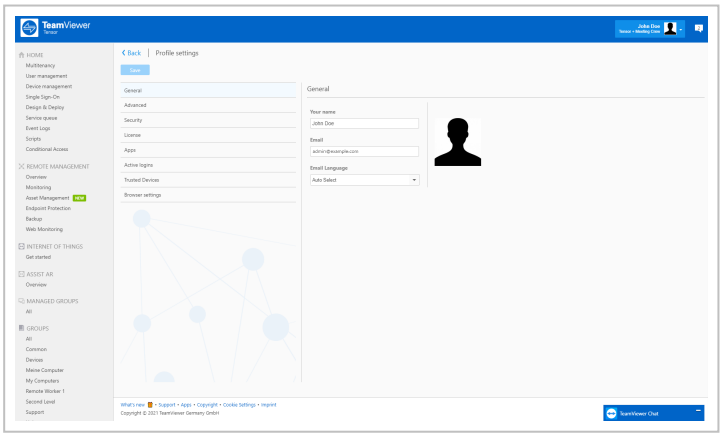
Hint: The TeamViewer Chat Widget provides the ability to integrate the TeamViewer chat in each of your web applications. Copy and paste the following code snippet into the code of the web application: `<script type="text/javascript" src="https://integratedchat.teamviewer.com/widget"></script>`.

2.3 My Account

The TeamViewer Management Console enables you to manage your TeamViewer account. Additional changes to your TeamViewer account can be made in the settings of the TeamViewer full version.

Note: If you joined a company profile (*section 3 , page 17*) with your TeamViewer account, the editing options of your account may be restricted (*section 5.2 , page 41*).

To edit your TeamViewer account, click on **Username | Edit profile on the title bar.**



Editing the profile.

General

In addition to the usual details such as display name, email and password, you can also add the following settings.

	Description
Two-factor authentication	Secure your TeamViewer account against unauthorized access with another factor in addition to email address and password. ➡ To do this, click the **Activate** link and follow the instructions in the dialog.
License	Assign your TeamViewer account a license. Thus you can establish licensed connections from any TeamViewer to which you log in with your TeamViewer account. ➡ To do this, click the **Change license** text link.
Remote Management	If you have acquired a Remote Management license, the number of monitored devices will be displayed.
Custom QuickSupport	Select an individual module from the dropdown list. Connection partners who connect for a session with a service case that is assigned to you, automatically participate in the session with this module.
Custom QuickJoin	Select a module from the dropdown list. Participants who participate in a meeting via a meeting link use this module.
Connection reporting	If you have joined a company profile or you administer this (*section 3 , page 17*), you can also specify here whether your connections should be logged and commented. • Log sessions for connection reporting: If enabled, all outgoing TeamViewer connections (except for meetings) of your account are logged in the TeamViewer Management Console. All logged connections are displayed in the connection report (*section 11 , page 87*). • Show comment window after each session: If enabled, a dialog is opened in the browser after exiting each outgoing TeamViewer connection (except for meetings). There you can record a comment about the connection (*section 11.1 , page 87*).
Email Language	Select the language for notification emails.
Email notifications	If you want to receive email notifications for newly created service cases, activate this option.
Product preview	If you want to get early preview access to new improvements and features within TeamViewer before they are released publicly, activate this option.

License

Depending on you license, this tab offers different options to manage you license – including activating you license.

Apps

Manage your own scripts and apps to which you have granted access in your own TeamViewer account or create your own scripts. If you have apps that have access to your TeamViewer account, you can revoke this access here.

To create a script that you can use with your TeamViewer account, you need a script token.

➡ For this, click the Create script token **button.**

Define the following properties for the token:

	Description
Name	Enter any name for the script token in the text field.
Description	Enter a description for the script token in the text field (e. g. the later function of the script that you program using the token).
Access level	Specifies the content to which the resulting script has general access. The access can be limited by the subsequent access rights. In this case, the script can access content within a TeamViewer account. If a script requires access to information from a company profile, create a script token in the properties of the company profile (*section 3.2 , page 18*).
Account management	Specify which account information the script may access. • **No access:** The script has no access to information in your TeamViewer account. • View without email: The script can call up all information in your TeamViewer account with the exception of your email address. • **View full profile: The script** can call up and display all information in your TeamViewer account. • **Edit full profile: The script** can display and edit all information in your TeamViewer account.

	Description
User management	Specify which information about the User management the script may access. • **No access:** The script has no access to information about your User management. • **View users: The** script can access and display user accounts of your User management. • **View, create and edit users: The script can** access and display user accounts of your User management, create new accounts and edit existing. • **View, create and edit users and admins: The script can access** and display user accounts of your User management, create new accounts and edit existing. This include administrator's user accounts.
Session management	Specify which functions for the management of service cases may be called up in the service queue. • **No access:** The script has no access to service cases in your service queue. • **Create, view own and edit own sessions: The script** can create service cases and display and edit service cases that are assigned to you. • **Create, view all and edit own sessions: The script can** create service cases, display all service cases and edit cases that are assigned to you. • **Create, view and edit all sessions: The script can** create service cases, display all service cases, and edit all.
Group management	Specify which functions may be called up for groups in your Computers & Contacts list. • **No access:** The script has no access to group information. • **View groups:** The script can display groups in your Computers & Contacts list. • **View, create, delete, edit and share groups: The** script can create and edit groups, as well as share individual groups with contacts from your Computers & Contacts list.

	Description
Connection reporting	Specify which functions may be called up for the management of connection reporting. • **No access:** The script has no access to connection reporting. • **View connection entries:** The script can display connection reports for your TeamViewer account. • **View and edit connection entries:** The script can display and edit connection reports for your TeamViewer account. • **View, edit and delete connection entries:** The script can display, edit, and delete connection reports for your TeamViewer account.
Meetings	Specify which information about your (scheduled) meetings the script may access. • **No access**: The script has no access to information about your (scheduled) meetings. • **View Meetings**: The script can access and display your scheduled meetings. • **View and create meetings**: The script can access and display your scheduled meetings, schedule new meetings or start spontaneous meetings. • **View, create, edit and delete meetings:** The script can access, display and edit your scheduled meetings, schedule new meetings, start spontaneous meetings or delete scheduled meetings.

	Description
Computers & Contacts	Specify which information about your Computers & Contacts list the script may access. • **No access:** The script has no access to information about your Computers & Contacts list. • **View entries:** The script can access your computers and contacts and their online status. • **View and add entries:** The script can display your computers and contacts and their online status, add computers and contacts to your Computer& Contacts list. • **View, add, edit and delete entries:** The script can display and edit your computers and contacts and their online status, add computers and contacts to your Computers & Contacts list or delete entries.
Chat	Specify which information about your chats the script may access. • **No access**: The script has no access to information about your chats. • **Read Messages**: The script can read your chats. • **Read and send Messages**: The script has reading permissions and may send chats.
TeamViewer policies	Specify which information about your TeamViewer policies the script may access. • **No access**: The script has no access to information about your policies. • **View TeamViewer policies**: The script can access and display your policies. • **View, add, edit and delete TeamViewer policies**: The script can display and edit your policy settings, add new policies or delete policies.
Manage SSO domains	Specify which information about your SSO domains the script may access. • **No access**: The script has no access to information about your SSO domains. • **View details about domains, add and remove email exclusions**: The script can view details about domains, add and remove email exclusions.

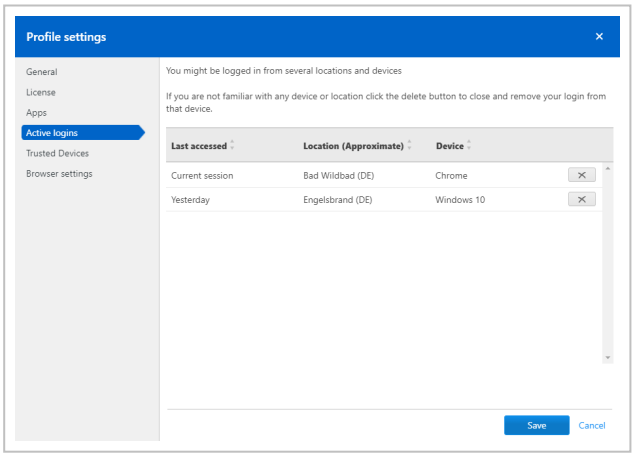
	Description
Event logging	Specify which information about Event logging the script may access. • **No access**: The script has no access to information about Event logging. • **Allow requesting all event logs**: The script can request all event logs.
Token (only available in the properties of the token)	The token is a unique character string with which the script requests access to your account via the API. Only give the token to people or scripts that you trust.

With a script token and the TeamViewer API you can program a script. For more information, visit the Integrations Website *integrate.teamviewer.com*.

Active logins

The TeamViewer Management Console provides the option of displaying all active logins of your TeamViewer account. If you should forget to sign out of your TeamViewer account at a computer-/device, you can do so by using this function.

With the ✕ icon next to an active account login, you can exit the active login.



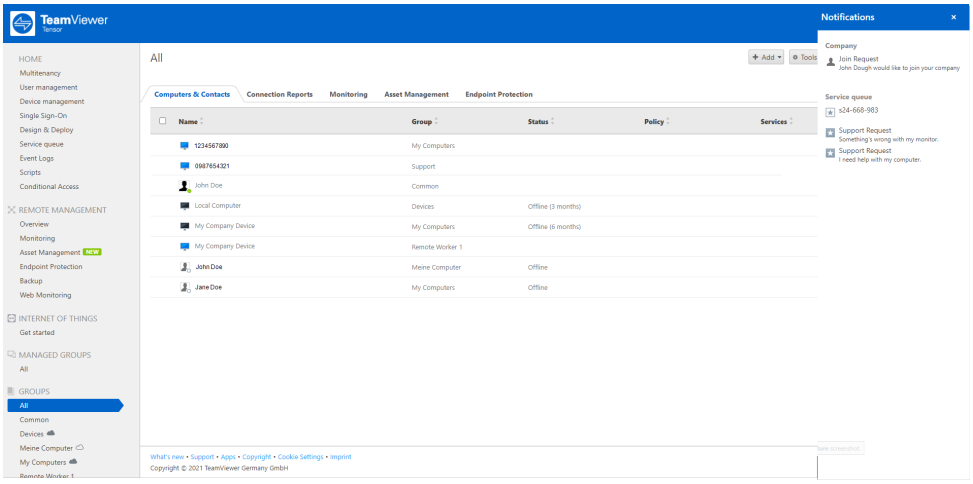
Showing active logins.

2.4 Notifications

All messages and news are collected and displayed within your Computers & Contacts list in the notifications. The notifications are linked to your TeamViewer account and in this way, these are available wherever you log in with your TeamViewer account.

Notifications are displayed for the following events:

- Newly created service cases
- Service cases that were assigned to you
- New contact requests for your Computers & Contacts list
- Alert messages for the integrated system health checks in TeamViewer
- Current Remote Management alert notifications
- A contact would like to share a group with you



The Notifications dialog in the TeamViewer Management Console.

Click the icon at the end of the line for each notification to open a context menu.

This contains all functions that you can also open within your Computers & Contacts list.

- For alerts, you can open the context menu of the computer that triggered the alert.
- For the service queue, you can open the context menu of the service cases.
- For contacts, you can process contact requests.
- For groups, you can process Share groups requests.

3 Company profile

With the TeamViewer Management Console, it is possible to centrally manage several TeamViewer accounts inside a company by one or several users. A company profile is required for this purpose. Users with an existing TeamViewer account can join a company profile, and it is possible to create new users who are automatically linked with the company profile.

All users who joined a company profile using their TeamViewer account are centrally managed by one or several users with administrative rights (administrators).

A company profile is required for **connection reporting, user management and connection commenting.**

Note: Creating a company profile in the TeamViewer Management Console requires a TeamViewer 8 Premium or Corporate license.

3.1 Creating a company profile

To illustrate the content of this section, an application case is used below to create a company profile:

***Example**: In a company, you are responsible for a team of employees who assist customers with their computer problems by using TeamViewer via remote control. You have a TeamViewer account in which you stored all the relevant computer IDs or TeamViewer contacts of the customers. In order to give your employees only the information and permissions relevant to the individual customers, it would be helpful if you could individually adapt the TeamViewer accounts of your employees. For this reason, you create a company profile. Afterwards, you can create new users or link existing TeamViewer accounts with this profile, thereby centrally managing all the TeamViewer accounts of your employees and adapting them to your requirements.*

- To create a company profile, click on **User Management in the sidebar.** In the text field in the content area, enter a Company name and confirm it by clicking the **Create & start trial** button.

You have now created a company profile and are the administrator of this profile.

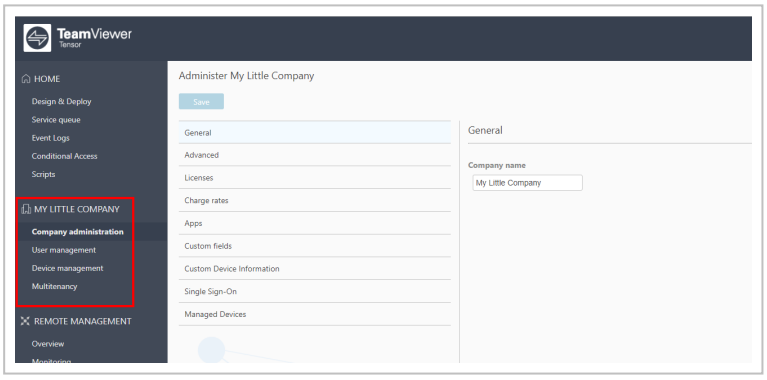
As administrator of a company profile, you have the following options:

- Edit a company profile (define charge rates, define individual text fields for the properties of a computer, manage licenses), *section 3.2 , page 18*.
- Manage users (create, edit, delete), *section 5 , page 31*.
- Allocate permissions to users, *section 5.2 , page 41*.
- Manage connections (create, edit, delete), *section 11.1 , page 87*.
- Export connection data (HTML, CSV), *section 11.1 , page 87*.
- Share groups from the Computers & Contacts list with users, *section 5.4 , page 45*.

3.2 Edit a Company Profile

Once you have created a company profile or you are the administrator of an existing company profile, you can define additional properties. You can complete the profile by adding TeamViewer licenses, creating charge rates and defining connection settings.

To edit the company profile, click **Company name – Company administration.**



Editing a company profile.

General

	Description
Company Name	The name of the company assigned by the administrator. It can be changed by an administrator.
Licenses	The overview of all licenses available for the company profile. If users join the company, whose account is linked with a license, this license is also available to the company. In the same way, additional TeamViewer licenses for the company can be added (see *section 3.4 , page 23*).

Charge rates

With the help of a charge rate, you can define how much a connection will cost. If a TeamViewer account, which joined your company profile, establishes a connection to a customer, the costs of the connection are calculated based on the predefined charge rate (see *section 11.1 , page 87*).

With the **Add new rate button, you can define several different charge rates for the billing of connections.**

The charge rates created can be assigned to groups from the Computers & Contacts list (see *section 11.1 , page 87*).

Advanced

	Description
Minimum connection duration	Specify the duration at which a connection should be logged in the TeamViewer Management Console. To do so, enter the minimum time in seconds which a connection has to last in order to be logged. All connections above this time limit will be logged.
Maximum connection break to merge (minutes)	If a brief interruption occurs during a session, you can combine several connections to one connection for billing purposes. Define up to which interruption duration connections should be combined.
Include breaks	If enabled, the duration of the interruption is taken into account when the connections are combined.
Customer satisfaction form	If activation is allowed, company members can activate the form in the custom QuickSupport module.
Custom QuickSupport	Select which custom QuickSupport module on the company level should be used. If no custom module is defined for groups and users, they inherit the selected module. If a customer connects to a session with service case that was created within the company profile, the selected module is executed at the customer.
Custom QuickJoin	Select which custom QuickJoin module on the company level should be used. If no custom module is defined for groups and users, they inherit the selected module. If a customer connects to a meeting that was created within the company profile, the selected module is executed at the customer.

	Description
Event Logging	If activated, the Event Logs category appears in the left side bar. This feature allows you to log all user activity, record remote sessions, and set user policies for complete auditability and visibility into who is doing what, when, and for how long.
Custom fields	Create user-defined custom fields. They are displayed in the properties of a computer where you can store corresponding values for these fields.

Apps

As administrator, manage a company profile, scripts, and apps, to which you have granted access to information of the company profile or create your own scripts. If you are using apps that have access to your company profile, you can revoke this access here.

To create a script that you can use with the company profile, you need a script token.

➡ For this, click the **Create script token** button.

Define the following properties for the token:

	Description
Name	Enter any name for the script token in the text field.
Description	Enter a description for the script token in the text field (e. g. the later function of the script that you program using the token).
Access level	Specifies the content to which the resulting script has general access. The access can be limited by the subsequent access rights. In this case, the script can access content within a TeamViewer account. If a script requires access to information from a company profile, create a script token in the properties of the company profile (see section , page).

	Description
User management	Specify which information about the User management the script may access. • No access: The script has no access to information about your User management. • View users: The script can access and display user accounts of your User management. • View, create and edit users: The script can access and display user accounts of your User management, create new accounts and edit existing. • View, create and edit users and admins: The script can access and display user accounts of your User management, create new accounts and edit existing. This include administrator's user accounts.
Session management	Specify which functions for the management of service cases may be called up in the service queue. • No access: The script has no access to service cases in your service queue. • Create, view own and edit own sessions: The script can create service cases and display and edit service cases that are assigned to you. • Create, view all and edit own sessions: The script can create service cases, display all service cases and edit cases that are assigned to you. • Create, view and edit all sessions: The script can create service cases, display all service cases, and edit all.
Group management	Specify which functions may be called up for groups in your Computers & Contacts list. • No access: The script has no access to group information. • View groups: The script can display groups in your Computers & Contacts list. • View, create, delete, edit and share groups: The script can create and edit groups, as well as share individual groups with contacts from your Computers & Contacts list.

	Description
Connection reporting	Specify which functions may be called up for the management of connection reporting. • No access: The script has no access to connection reporting. • View connection entries: The script can display connection reports for your TeamViewer account. • View and edit connection entries: The script can display and edit connection reports for your TeamViewer account. • View, edit and delete connection entries: The script can display, edit, and delete connection reports for your TeamViewer account.
Script Token (only available in the properties of the token)	The token is a unique character string with which the script requests access to your account via the API. Only give the token to people or scripts that you trust.

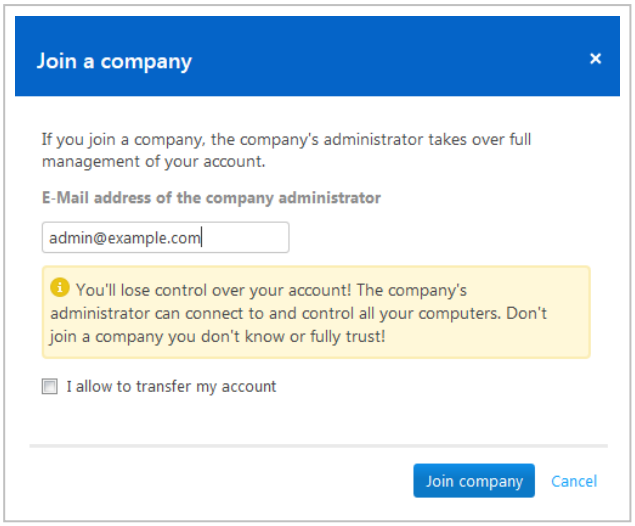
With a script token and the TeamViewer API you can program a script. For more information, visit the Integrations Website integrate.teamviewer.com.

3.3 Joining a company profile

Each TeamViewer account can join any company.

Caution: If you join a company with your TeamViewer account, you will loose control over your TeamViewer account! Do not join any company you do not know or do not completely trust! This process cannot be undone!

To join a company with a TeamViewer account, click on the **User Management** entry in the sidebar. Next, click on the link **Join an existing company now** in the content area and enter the email of a company administrator. Finally, confirm the process by clicking on the **Join company** button.



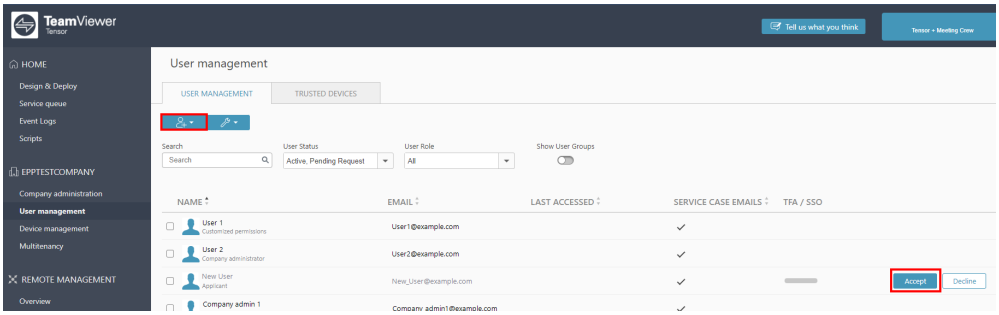
Joining a company.

Confirming users as an administrator

After a user has joined a company, the administrator of the company profile receives an e-mail and the user appears in the administrator's view of the user management (see chapter , page).

The administrator must confirm the user.

- As the administrator of the company profile, click on the **Accept** button in the User management to confirm the user.



Confirming new users.

3.4 Licensing

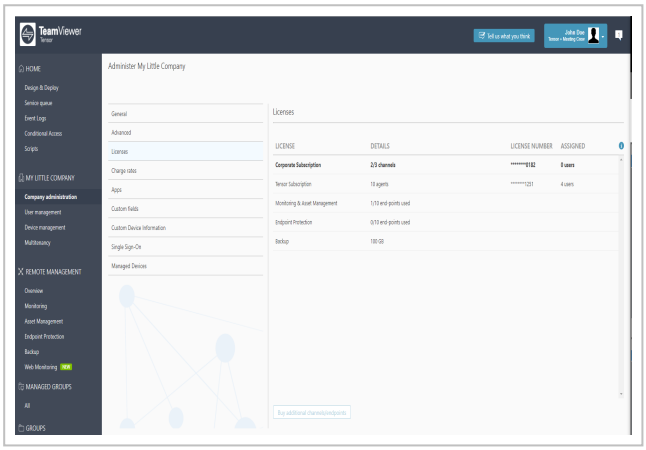
Note:

- Each company profile can have **one TeamViewer Core license** (=Premium or Corporate) activated and this license can be combined with other licenses of the TeamViewer product family (e.g. Pilot, Remote Management, IoT, etc.).
- You can not activate more than one core license on your company profile. As a company administrator, when you try to activate a new license (Premium or Corporate subscription)

to a company profile that already has a license, you will need to choose between keeping the existing license or replacing the existing license.

Administrators of the company profile can link TeamViewer licenses with a company profile by adding new licenses to the company.

If a license is linked with the TeamViewer account of the person who is creating a company profile, this license is automatically assigned to the company. As a result, it is available to all users of the company.

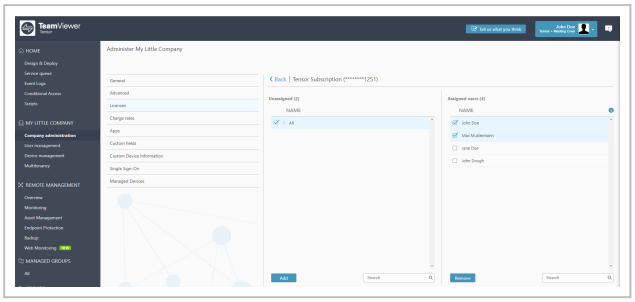


Managing licenses of a company profile.

Note: If no TeamViewer license is linked with the account creating a company profile, the use of the company profile in the TeamViewer Management Console is limited to a test period of 15 days.

Note: When a licensed user joins a licensed company (Premium or Corporate subscription) the user either needs to unlink the license linked to their account to be able to join, or they will not be joined to the company profile.

As administrator of a company, you can manage the licenses of all users in the **company profile.** You can assign users of your company additional licenses as needed via the User Management (see chapter , page).



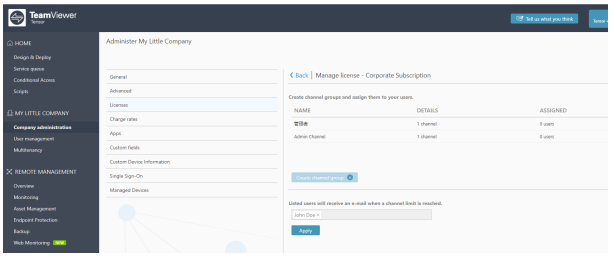
Assigning licenses to company users.

Note: If you joined a company profile, the administrator can view your license and, if needed, assign it to additional company users. This means: Each user who owns a TeamViewer license, loses the sole right to the use of this license upon joining a company. After joining, the administrators of the company profile have control over the license.

3.4.1 Channel groups

Use channel groups to assign the TeamViewer channels of your license to users from your company profile. There are various possibilities to use your company's TeamViewer channels:

- Bundle single TeamViewer channels (channel groups) and reserve them for use by assigned users.
- Reserve channels of your license for specific users
- Monitor how your license and the corresponding channels are used and by whom.
- Receive a notification, if the channel limit is reached and no connections can be established.



Manage TeamViewer channels of your company's licenses.

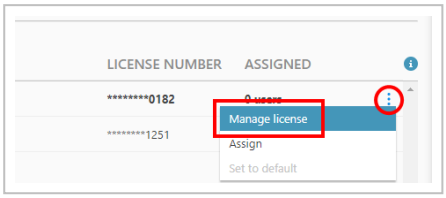
***Example**: You want to ensure that your IT support can always establish a connection. Do this by creating a channel group "IT support" and assign all support staff. They can use the selected number of channels at any time, regardless of the further use of your license.*

Create channel group

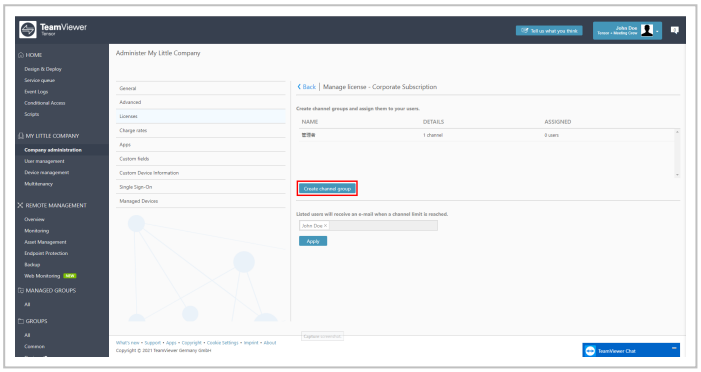
In a channel group, you can provide the assigned users with a number of channels limited by your license.

To create a channel group, follow the steps below:

1. In the company administration under **Licenses**, hover over the corresponding license and click the edit icon.
2. Select **Manage license**.



3. Click the button **Create channel group**.



4. Enter a name for the channel and select the number of channels you want to assign.
5. Click **Create**.

Create channel group

Options of a channel group

	Description
Name	Enter any name for the channel group in the text field.
Number of channels	Specify how many channels are available to the channel group.
Assigned users	Assign users to the group who are allowed to use the channels of the channel group.
Email notification	Select users who will receive an email notification as soon as the specified number of channels prevents further parallel connection (channel limit).

Delete channel group

To delete a channel group, follow these steps:

- In the company administration under General, click the icon followed by Delete at the desired channel group.

4 Multitenancy

Note: This feature requires a TeamViewer Tensor license. For more information, please visit our *TeamViewer Tensor website*.

With TeamViewer Multitenancy you can manage multiple companies from a single dashboard.

You can easily link existing companies to the parent company or main organization. The administrator of the parent company gets important information from all linked subsidiaries/companies such as license reports.

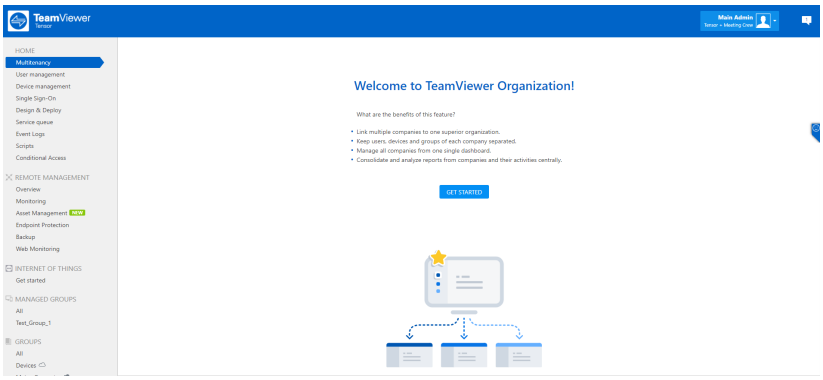
Note:

- The Multitenancy feature requires an activated Tensor license for your TeamViewer account. More information: *How to activate your license*
- The TeamViewer account needs a company Administrator role of a company. More information: *All about the TeamViewer company profile*

4.1 Create an Organization

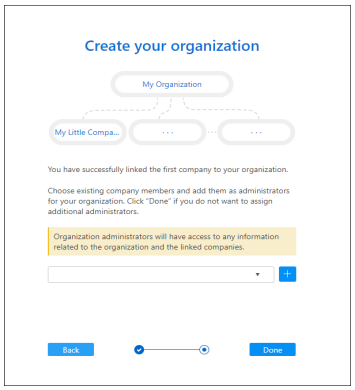
Before you can user the TeamViewer Multitenancy feature, you will need to create an organization.

1. Click the category **Multitenancy** in the left side pane.



Creating a TeamViewer Multitenancy organization.

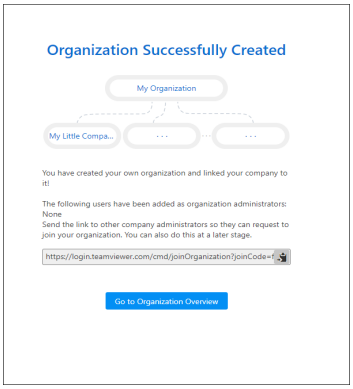
2. Click the **Get Started** button.
3. On the following page, enter the name for your organization and click **Next**.



Your company will be automatically assigned to the organization as the first company

4. Enter other company admins if necessary or finish the wizard by clicking **Done**.

Your have created your organization with your company attached to it.

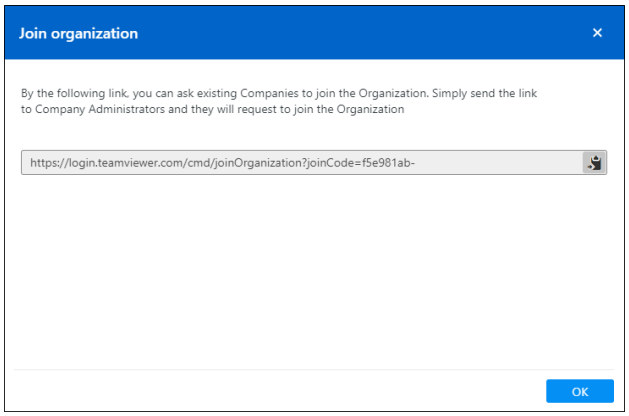


4.2 Invite Companies or Join an Organization

4.2.1 Invite companies to join your organization

1. Click the category **Multitenancy** in the left side pane.
2. Click the + button on the top left side of the page.

   The **Join Organization** dialog opens.



3. Copy the link and send it to other company administrators via email.

4.2.2 Join an organization

Make sure that a joining link has been sent to TeamViewer email accounts of the company administrators by the administrator of the organization.

1. Click the joining link.

   You can see the organization name and a description text field.

2. **Optional:**Enter your contact details (e.g., email address) in the text field so that organization administrators can contact you.

Note: Each company can only join one parent company/organization.

4.3 Add More Administrators to an Organization

4.3.1 Invite companies to join your organization

1. Log in into the Management Console as an administrator of the organization.
2. Click the button **Multitenancy Settings** in the Multitenancy overview page.
3. On the **Settings** page, open the **Multitenancy administration management** tab.
4. Add other users' email addresses who have company administrator roles in an existing company and click **Add** to confirm.
5. Click Save on the top left of the page.

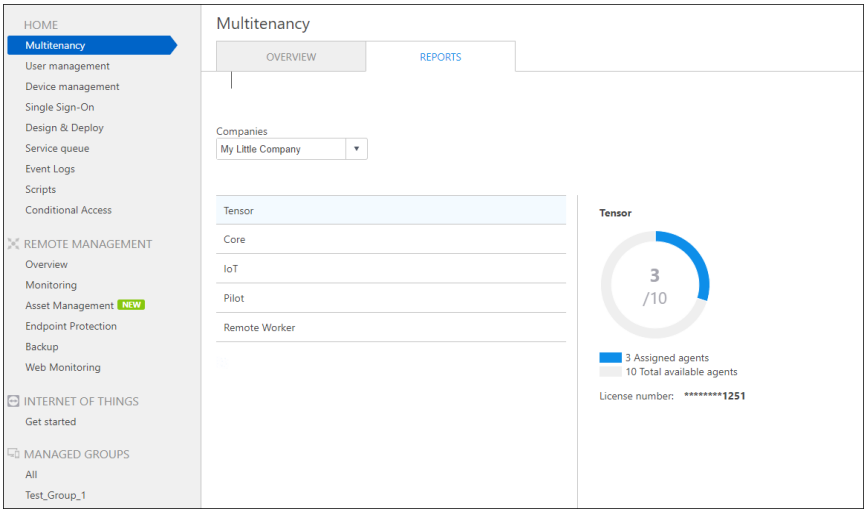
   Organization administrators that have been successfully added can access the parent organization via the Management Console.

Note: The added organization administrator needs an activated Tensor license or Remote Worker license in order have access to the organization.

4.3.2 Get license reports of the companies that joined the organization

Organization administrators can see an overview of the joined companies' licenses.

1. In the Multitenancy overview page, view the **Reports** tab.
2. Select the filters you need.
3. Review single license usages or a cumulative result of all license usages.



The Multitenancy reports view showing the usage of licenses.

5 User management

Note: The functions described in the following sections require a TeamViewer account with administrative permissions. How to get administrative permissions:

- Create a company (see *section 3.1 , page 17*) or
- An administrator of the company profile has granted you the permissions for this purpose (see *section 5.2 , page 41*).

The TeamViewer accounts that have joined your company profile can be centrally managed in the **User Management.** This is done by one or several user administrators.

> ***Example**: You are the administrator of a company profile. To avoid having to edit and manage the 200 users of your company profile by yourself, you can adjust the permissions of individual users so that they may manage other users as well as the company profile.*

The following functions are available in the user management:

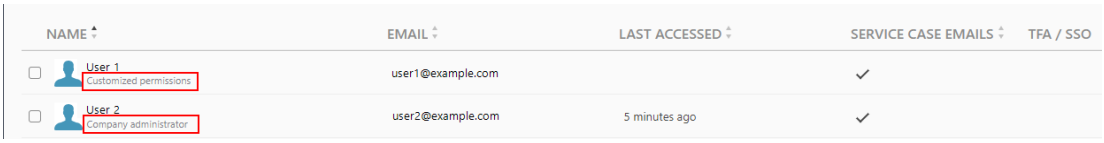
- Add user
- Add existing account
- Edit user
- Remove user
- Deactivate user
- Delete account
- Reset password
- Assign user-specific permissions
- Manage user-specific connections
- Share a group

5.1 Roles

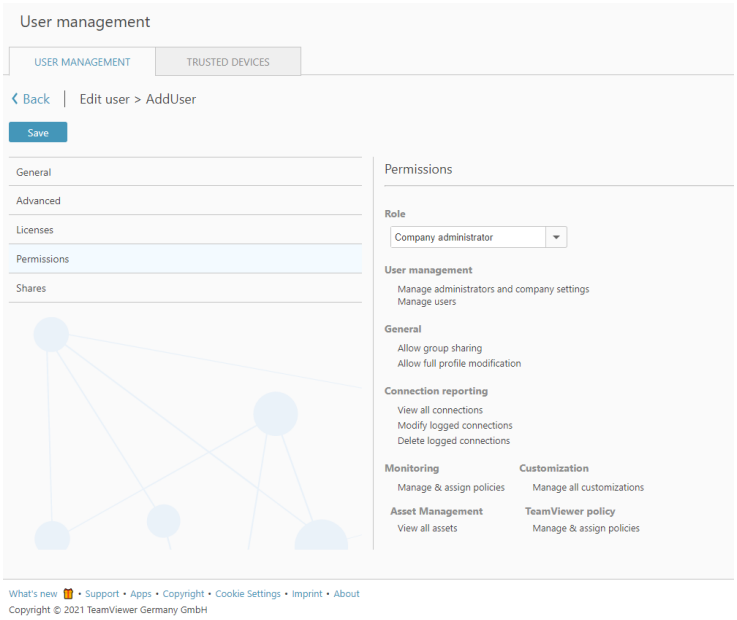
In the Management Console, administrators can easily assign a defined set of permissions to users without the need to choose and save all permissions for each user individually. This saves a lot of time when adding new users to the user management or when changing the permissions for existing users. The whole process of applying permissions to users becomes less error-prone because the

roles always have the same permissions set and administrators don't need to take care of assigning the correct individual permissions for each user.

You can view the user role in the user management overview under the user name.



Company administrator



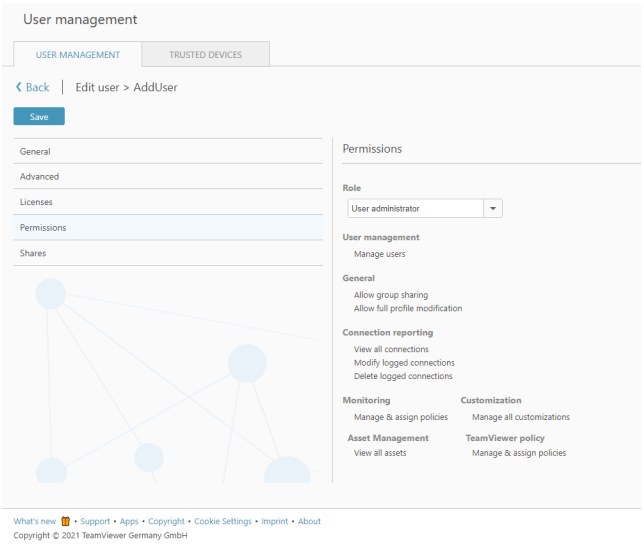
The company administrator's pre-defined permission set.

The company administrator role contains the following pre-defined permissions:

Permission	Description
Manage administrators and company settings	If enabled, the user can manage other users, administrators and the company profile. This also includes adding administrators, deleting users, editing a company profile.
Manage users	If enabled, the user becomes the administrator and can manage other users. This also includes creating users or editing users.
Allow group sharing	If enabled, the user can share groups from his list of Computers & Contacts with his contacts.

Permission	Description
Allow full profile modification	If enabled, the user himself can modify all of his properties in the TeamViewer settings under **Computers & Contacts.**
Connection reporting	**View all connections**: The user can see the connections of all the users of the company.
Modify logged connections	If enabled, the user can edit connections in the Connection report (see *section 11.1 , page 87*).
Delete logged connections	If enabled, the user can delete connections in the Connection Report (see *section 11.1 , page 87*).
Monitoring	Manage & assign policies: The user may create and edit policies for monitoring and assign computers or groups.
Asset Management	View all assets: The user can see all tracked computers.
Endpoint Protection	Manage & assign policies: The user may create and edit policies for Endpoint Protection and assign computers or groups.
Backup	Manage & assign policies: The user may create and edit Backup policies and assign computers or groups.
Customization	Manage all customizations: The user can create customized modules under Design & Deploy and manage all modules.
TeamViewer policy	Manage & assign policies: The user may create and edit policies.
Event Logs	None

User administrator



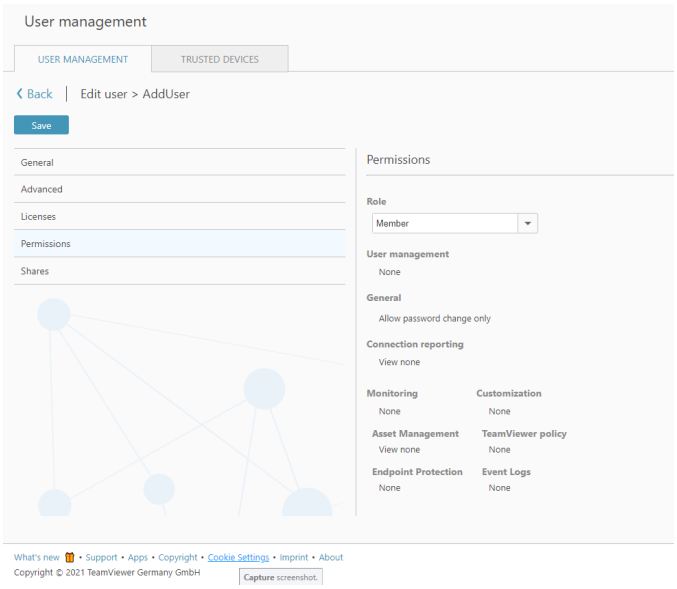
The user administrator's pre-defined permission set.

The user administrator role contains the following pre-defined permissions:

Permissions	Description
Manage users	If enabled, the user becomes the administrator and can manage other users. This also includes creating users or editing users.
Allow group sharing	If enabled, the user can share groups from his list of Computers & Contacts with his contacts.
Allow full profile modification	If enabled, the user himself can modify all of his properties in the TeamViewer settings under Computers & Contacts.
Connection reporting	View all connections: The user can see the connections of all the users of the company.
Modify logged connections	If enabled, the user can edit connections in the Connection report (see *section 11.1 , page 87*).
Delete logged connections	If enabled, the user can delete connections in the Connection Report (see *section 11.1 , page 87*).
Monitoring	Manage & assign policies: The user may create and edit policies for monitoring and assign computers or groups.

Permissions	Description
Asset Management	View all assets: The user can see all tracked computers.
Endpoint Protection	Manage & assign policies: The user may create and edit policies for Endpoint Protection and assign computers or groups.
Backup	Manage & assign policies: The user may create and edit Backup policies and assign computers or groups.
Customization	Manage all customizations: The user can create customized modules under Design & Deploy and manage all modules.
TeamViewer policy	Manage & assign policies: The user may create and edit policies.
Event Logs	None

User role



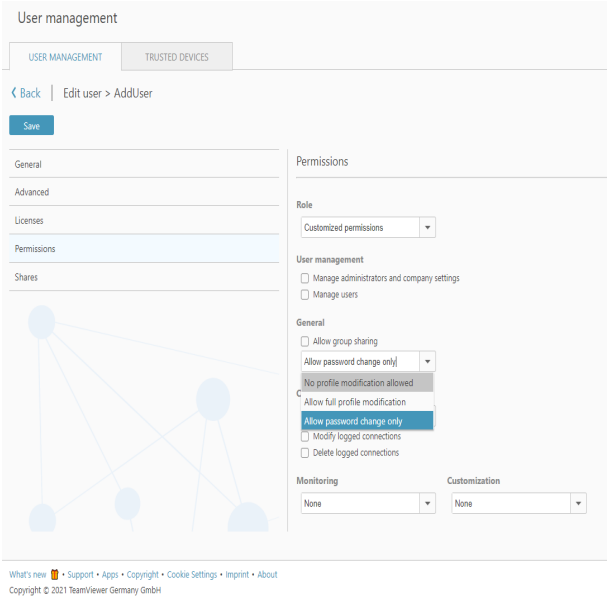
The user's pre-defined permission set.

The user role contains the following pre-defined permissions:

Permissions	Description
User management	None.

Permissions	Description
General	Allow password change only.
Connection reporting	View none: The user does not see any connections.
Monitoring	None: The user cannot use the Remote Management monitoring functions.
Asset Management	View none: The user cannot see any tracked computers.
Endpoint Protection	None: The user cannot use the Endpoint Protection functions.
Backup	None: The user cannot use the Backup functions.
TeamViewer policy	None: The user cannot use or set any policies.
Customization	None: The user cannot create and see any customized modules.
Event Logs	None: The user cannot view recorded events.

Customized permissions



The customization possibilities.

The customization mode offers the full variety of individual settings:

Permissions	Description
Manage administrators and company settings	If enabled, the user can manage other users, administrators and the company profile. This also includes adding administrators, deleting users, editing a company profile.
Manage users	If enabled, the user becomes the administrator and can manage other users. This also includes creating users or editing users.
Allow group sharing	If enabled, the user can share groups from his list of computers & contacts with his contacts.
No profile modification allowed	If enabled, the user cannot edit profiles.
Allow full profile modification	If enabled, the user himself can modify all of his properties in the TeamViewer settings under Computers & Contacts.
Allow password change only	If enabled, users can modify only their password.
Connection reporting	Select whether and which connections the user may view in the connection report. • **View all connections**: The user can see the connections of all the users of the company. • **View own connections**: The user can see only his connections. • **View none:** The user does not see any connections.
Modify logged connections	If enabled, the user can edit connections in the Connection report (see *section 11.1 , page 87*).
Delete logged connections	If enabled, the user can delete connections in the Connection Report (see *section 11.1 , page 87*).

Permissions	Description
Monitoring	Select whether and how the user may use the Remote Management monitoring functions. • Manage & assign policies: The user may create and edit policies for monitoring and assign computers or groups. • Assign policies: The user may assign monitoring policies to computers or groups. • View & acknowledge all alerts: The user can see and confirm alerts for monitoring. • View & acknowledge own alerts: The user can only see and confirm alerts from computers that are assigned to him. • None: The user cannot use the Remote Management monitoring functions.
Asset Management	Select whether and how the user may use the Remote Management asset Management. • View all assets: The user can see all tracked computers. • View assets: The user can see his own tracked computers. • View none: The user cannot see any tracked computers.
Endpoint Protection	Select whether and how the user may use the Remote Management Endpoint Protection functions • Manage & assign policies: The user may create and edit policies for Endpoint Protection and assign computers or groups. • Assign policies: The user may assign Endpoint Protection policies to computers or groups. • View & acknowledge all threats: The user can see and confirm threats detected on all protected devices. • View & acknowledge own threats: The user can see and confirm threats detected on own protected devices. • None: The user cannot use the Endpoint Protection functions.

Permissions	Description
Backup	Select whether and how the user may use the Remote Management Backup functions. • Manage & assign policies: The user may create and edit Backup policies and assign computers or groups. • Assign policies: The user may assign Backup policies to computers or groups. • View & acknowledge own alerts: The user can only see and confirm Backup alerts from computers that are assigned to him. • None: The user cannot use the Backup functions.
Customization	Select whether and how the user may use customized modules. • Manage all customizations: The user can create customized modules under Design & Deploy and manage all modules. • Manage own customizations: The user can create customized modules under Design & Deploy and manage his own modules. • None: The user cannot create and see any customized modules.
TeamViewer policy	None: The user cannot use or set any policies.
Event Logs	Select whether and how the user may view events that have been recorded during remote sessions and inside the Management Console by your company. • View: The user can view recorded events. • None: The user cannot view recorded events.

The permissions result in the following designations:

- User is everyone who joined a company profile with his TeamViewer account.
- User administrator is every member of a company who has the right to manage users.
- Company administrator is every member of a company who has the right to manage administrators and company settings.

5.1.1 Assigning a role to a user

Assign a role to a user following these steps:

1. Sign in to the TeamViewer *Management Console*.
2. In the user management, select the user you want to edit.

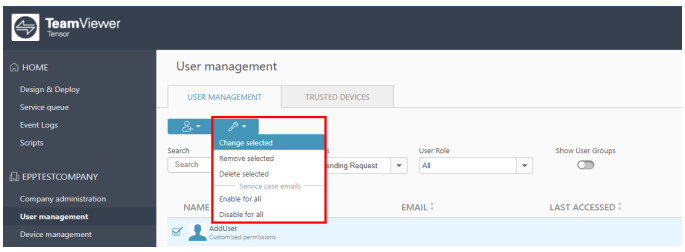
3. Click the ⋮ icon and select **Edit user**.
4. Click **Permissions**.
5. In the drop-down menu, select the role you want to apply to the user or configure a custom set of permissions.
6. Click **Save**.

   The role or the customized permissions are assigned to the user.

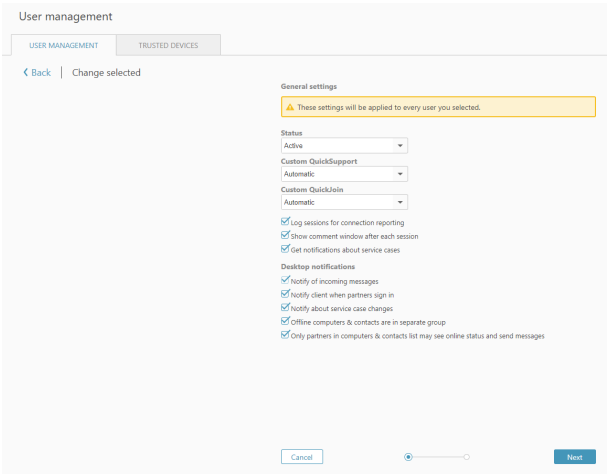
5.1.2 Assigning roles to users in bulk

In order to facilitate the role assignment for several users with the same role, you can selct the users and assign a role in one go.

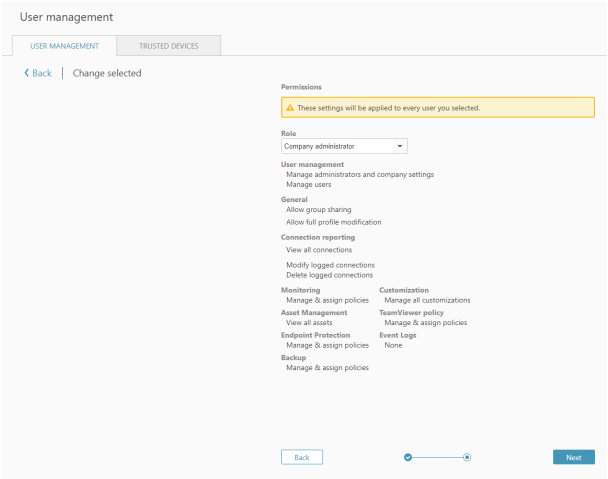
1. Sign in to the TeamViewer *Management Console*.
2. In the user management, select the users you want to edit by clicking the check box ☑.
3. Click the 🔧 button and select **Change selected**.



A configuration assistant opens.

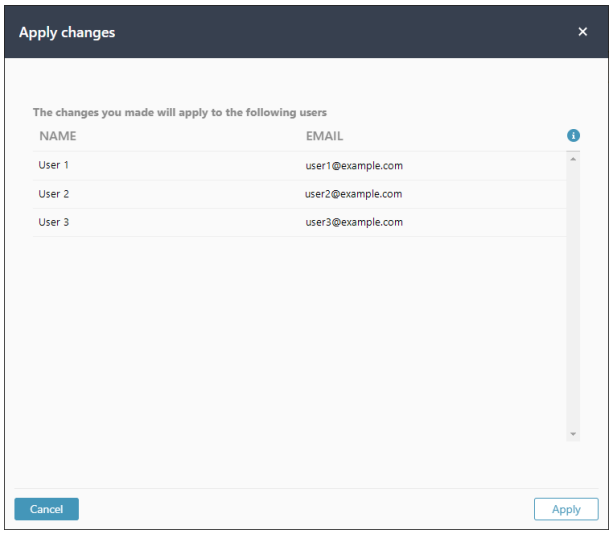


4. Enter your changes in the **General settings** tab and click **Next**.



5. Select the role you want to apply to the selected users or configure a customized set of permissions and click **Next**.

   A window with a summarized overview of all affected users opens.



Note: All selected users will receive the same set of permissions.

6. Click **Apply** to make your changes effective.

5.2 User Permissions

Users of the company profile can be assigned different permissions.

In addition to the regular permissions as a user, a TeamViewer account, which joined a company, can receive additional rights as **Connection administrator, Administrator or Company administrator.**

Permissions

The following permissions can be assigned in the properties of a user:

Rights	Description
Manage administrators and company settings	If enabled, the user can manage other users, administrators and the company profile. This also includes adding administrators, deleting users, editing a company profile.
Manage users	If enabled, the user becomes the administrator and can manage other users. This also includes creating users or editing users.
Allow group sharing	If enabled, the user can share groups from his list of computers & contacts with his contacts.
Allow full profile modification	If enabled, the user himself can modify all of his properties in the TeamViewer settings under **Computers & Contacts.**
Connection reporting	Select whether and which connections the user may view in the connection report. • **View none:** The user does not see any connections. • **View all connections**: The user can see the connections of all the users of the company. • **View own connections**: The user can see only his connections.
Modify logged connections	If enabled, the user can edit connections in the Connection report (see *section 11.1 , page 87*).
Delete logged connections	If enabled, the user can delete connections in the Connection Report (see *section 11.1 , page 87*).

Rights	Description
Monitoring	Select whether and how the user may use the Remote Management monitoring functions. • Manage & assign policies: The user may create and edit policies for monitoring and assign computers or groups. • Assign policies: The user may assign monitoring policies to computers or groups. • View & acknowledge all alerts: The user can see and confirm alerts for monitoring. • View & acknowledge own alerts: The user can only see and confirm alerts from computers that are assigned to him. • None: The user cannot use the Remote Management monitoring functions.
Asset Management	Select whether and how the user may use the Remote Management asset Management. • View all assets: The user can see all tracked computers. • View assets: The user can see his own tracked computers. • View none: The user cannot see any tracked computers.
Endpoint Protection	Select whether and how the user may use the Remote Management Endpoint Protection functions • Manage & assign policies: The user may create and edit policies for Endpoint Protection and assign computers or groups. • Assign policies: The user may assign Endpoint Protection policies to computers or groups. • View & acknowledge all threats: The user can see and confirm threats detected on all protected devices. • View & acknowledge own threats: The user can see and confirm threats detected on own protected devices. • None: The user cannot use the Endpoint Protection functions.

Rights	Description
Backup	Select whether and how the user may use the Remote Management Backup functions. • Manage & assign policies: The user may create and edit Backup policies and assign computers or groups. • Assign policies: The user may assign Backup policies to computers or groups. • View & acknowledge own alerts: The user can only see and confirm Backup alerts from computers that are assigned to him. • None: The user cannot use the Backup functions.
Customization	Select whether and how the user may use customized modules. • Manage all customizations: The user can create customized modules under Design & Deploy and manage all modules. • Manage own customizations: The user can create customized modules under Design & Deploy and manage his own modules. • None: The user cannot create and see any customized modules.
Event Logs	Select whether and how the user may view events that have been recorded during remote sessions and inside the Management Console by your company. • View: The user can view recorded events. • None: The user cannot view recorded events.

The permissions result in the following designations:

- User is everyone who joined a company profile with his TeamViewer account.
- Administrator is every member of a company who has the right to Manage users.
- Company administrator is every member of a company who has the right to Manage administrators and company settings.

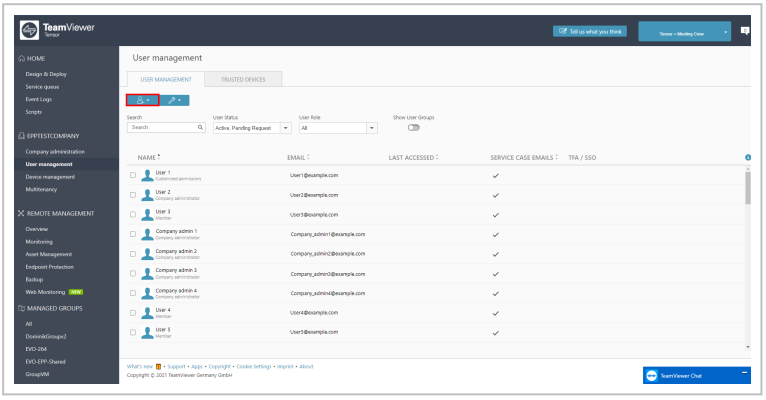
5.3 Adding users

In case not every employee of your company has a TeamViewer account, or new employees are entering the company, you can create and configure new TeamViewer accounts within a company profile.

5.3.1 Add a new user

1. Sign in to the TeamViewer *Management Console*.
2. In the **User management** tab click the button and select **Add user**.

   The properties described under *section 5.4, page 45* can be defined for new users.

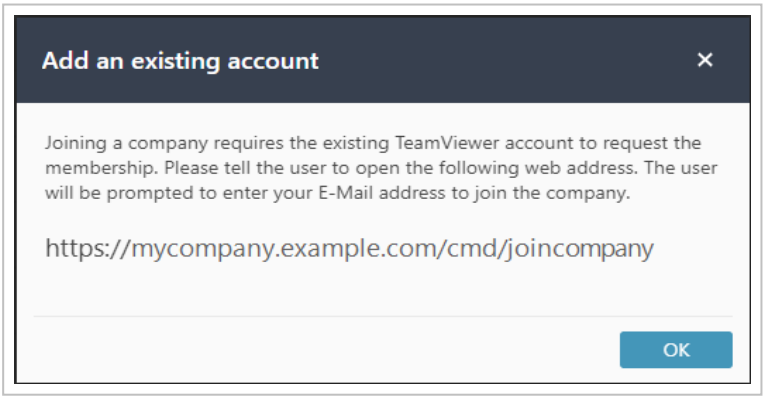


Adding a user.

3. Forward the login data you defined to your employees.

If all the employees of your company already have a TeamViewer account, you can ask them to join the company profile with their account in the TeamViewer Management Console.

1. Sign in to the TeamViewer *Management Console*.
2. In the **User management** tab click the button and select **Add existing account**.



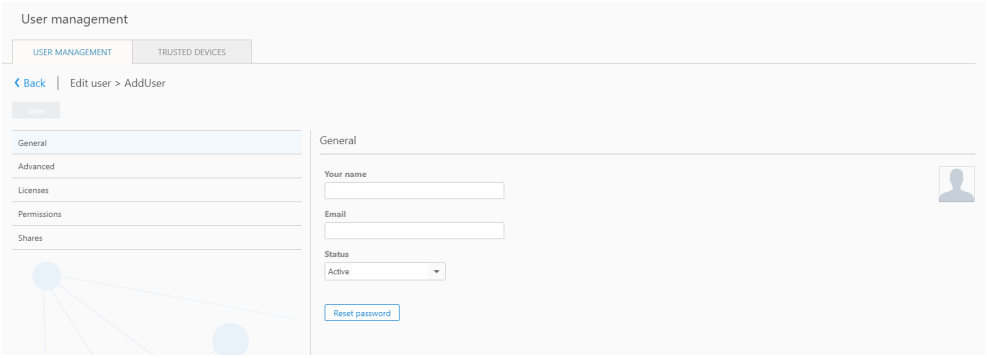
Adding a user with an existing TeamViewer account.

3. Copy the link in the dialog to your clipboard and send it to the user you want to add to your company by following the instructions.

5.4 Edit User

You can edit the properties of a user of your company:

1. In the user management, click the ⋮ icon.
2. Click **Edit user**.



The following properties can be defined for users:

General

	Description
	Click on the image to upload a profile picture for the user.
Your name	User name of the TeamViewer account.
Email	E-mail address of the TeamViewer account.
Reset password	Reset the password for the TeamViewer account.
Status	Select whether the user is active or inactive. If you select inactive, the user is deactivated and the account cannot be used. This is necessary, e.g. if a user leaves your company or you want to block the use of a user account for some other reason.
TeamViewer License	Select which license should be assigned to the user.
Meeting License	Select which license should be assigned to the user.
IoT Subscription	Shows the current status of your IoT Subscription.
Pilot Subscription	Shows the current status of your Pilot Subscription.

	Description
Custom QuickSupport	Select which custom QuickSupport module should be assigned to the user. If a customer connects to a session with service case that is assigned to the user, the selected module is executed at the customer.
Custom QuickJoin	Select which custom QuickJoin module the user should use. If the customer connects to a user's meeting, the selected module is executed at the customer.
Log sessions for connection reporting	If enabled, outgoing connections of the user are logged and displayed in the connection report.
Show comment window after each session	If enabled, the user can write a comment about this connection after the end of a connection.
Get notifications about service cases	If enabled, the user will be notified about service cases.
Notify client when partners sign in	If enabled, the user will be notified when partners sign in.

Permissions

Users can be assigned different rights. Depending on the permission, users have different options for the management of other users and connections.

For more information, see *section 5.2, page 41*.

Shares

Groups from the Computers & Contacts list can be shared with users (see *section 14.3 , page 106*).

- To do so, choose the group you want to share with a user from the Add group... drop down list, followed by clicking the Add button.

5.5 Remove a User

As a company administrator, you can remove users from your company profile. Removed users will be deleted from the user management, but can continue to use their TeamViewer account.

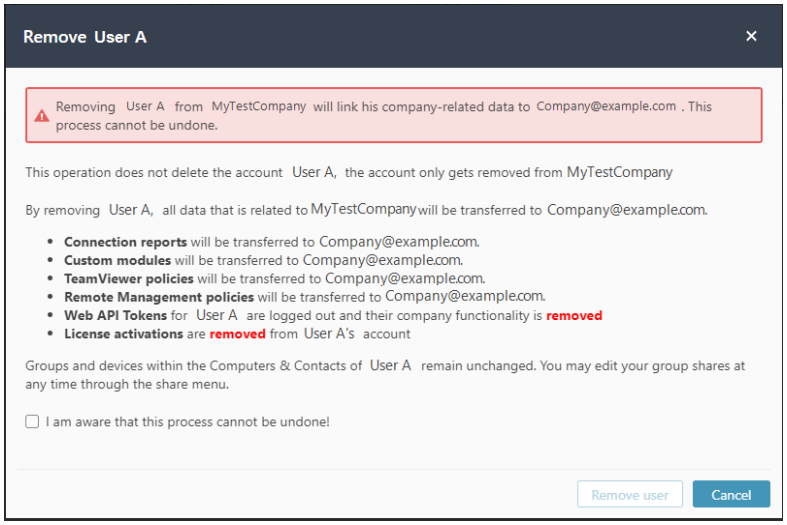
Removing a user means:

- Company-related data (e.g. connection protocols, custom modules and guidelines) will be transferred to the corporate administrator.
- The company's licenses will be revoked.
- Their shared groups will still be available for the company.

Note: Groups that have been shared with the user must be manually edited and withdrawn via the Share menu.

To remove a user, follow these steps:

1. Sign in to the TeamViewer *Management Console*.
2. Click the ⋮ icon.
3. Select **Remove user**.



4. Read and understand the warnings in the dialog carefully.
5. Click the check box and click **Remove user**.

5.6 Deactivate User

As a (Company) administrator, you can deactivate users in your company profile. Deactivated users will still be displayed in the user management, but can not use their TeamViewer account anymore.

> ***Example**: By deactivating users, you can for example map temporary absences. After the employee returns to your company, the account can be easily reactivated and the (company) administrator do not have to rebuild the previous account. In theory, the account can also be simply transferred to a new employee. Only the name and email address and the password need to be adjusted.*

The following restrictions apply for deactivated users:

- The user can not log into his TeamViewer account.
- The user can not use the company's licenses.
- *Service cases* can not be assigned to the user.
- The user can not access shared groups.
- The user can not connect to other users with his TeamViewer account, if only connections to users within the company profile are allowed.

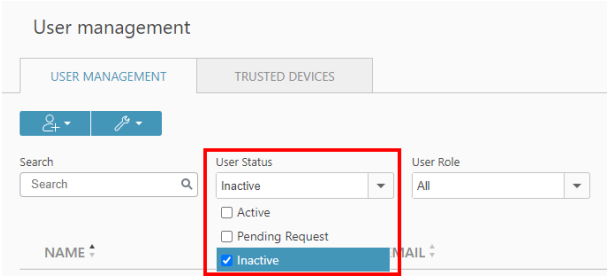
Note: Groups shared by the user can still be used.

To deactivate a user, follow these steps:

1. Sign in to the TeamViewer *Management Console*.
2. Click the ⋮ icon.
3. Select **Deactivate user**.

View deactivated users:

In the user management, click the **User Status** drop-down menu and select **Inactive**.

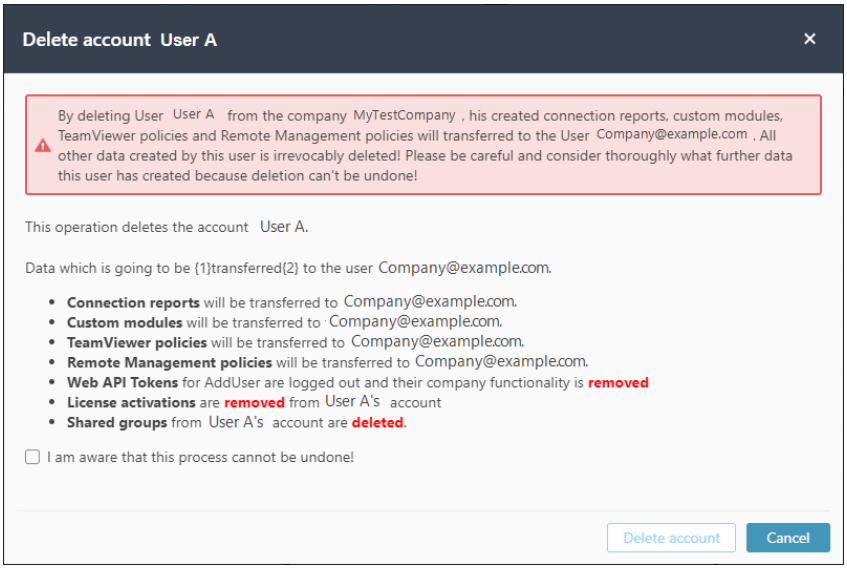


Note: Each inactive user can be reactivated by a (company) administrator.

5.7 Delete an account

Caution: Deleting an account should be carefully considered as most of the user's data will be lost.

After deletion the account is no longer available. Before deleting an account please read and understand the information provided in the warning dialog:



To delete an account, follow these steps:

1. Sign in to the TeamViewer *Management Console*.
2. Click the ⋮ icon.
3. Select **Delete account**.
4. Activate the check box **I am aware that this process cannot be undone!**
5. Click **Delete account**.

➡ The account is deleted and no longer available.

6 Single Sign-on

Note: This feature requires a TeamViewer Tensor license. For more information, please visit our *TeamViewer Tensor website*.

TeamViewer Tensor integrates with your single sign-on (SSO) identity providers, using SAML 2.0 and SCIM protocols, including Okta, Azure AD, OneLogin, Centrify, G Suite, and Active Directory Federation Services (ADFS).

6.1 General Information

TeamViewer Single Sign-On (SSO) aims to reduce the user management efforts for large companies by connecting TeamViewer with identity providers and user directories.

6.1.1 Prerequisites:

- TeamViewer version 13.2.1080 or newer.
- SAML 2.0 compatible identity provider (IdP)

Note: Currently we support the following identity providers:

- Centrify
- Okta
- Azure
- OneLogin
- ADFS
- G Suite.

These identity providers have been tested and detailed steps to set up one of these identity

providers can be found in this documents and other linked pages about SSO and the respective IdPs.

If you use a different identity provider, please use the technical information to set up your identity provider manually.

Hint: When adding a domain for Single Sign-On, it is recommended to add

- the owning account to the exclusion list. The reason for this is a fallback scenario that you keep the access to the domain configuration even if the identity provider is not working.

  Example: The TeamViewer Account "admin@example.com" adds domain „example.com“ for Single Sign-On. After adding the domain, the email address "admin@example.com" should be added to the exclusion list. This is required in order to make changes to the SSO configuration, even when Single Sign-On doesn't work due to misconfiguration.

- additional owners to the SSO domain, since the SSO ownership is not inherited within your company.

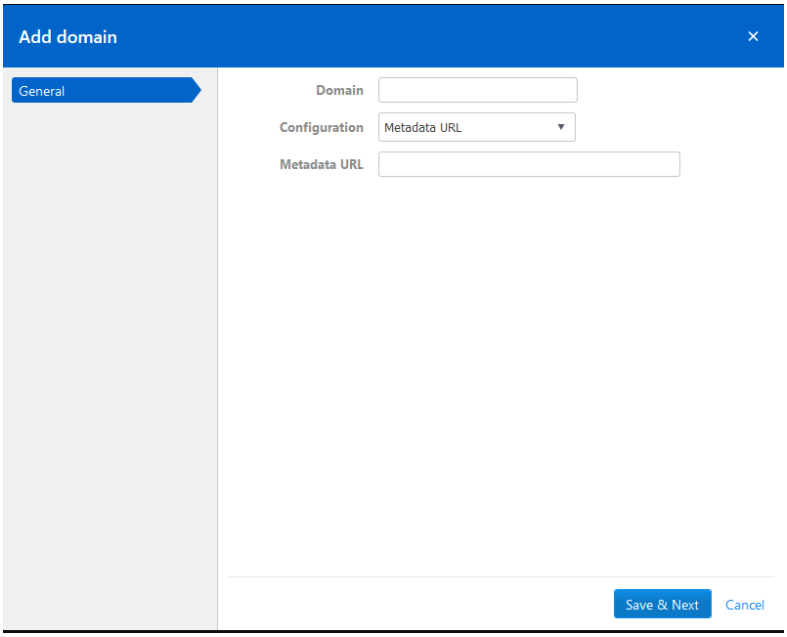
  Example: After the TeamViewer Account "admin@example.com" adds domain „example.com“ for Single Sign-On, he adds multiple company administrators (e.g. "admin2@example.com") as domain owners, so that they can also manage the domain and its SSO settings.

Single Sign-On (SSO) is activated on a domain level for all TeamViewer accounts using an email address with this domain. Once activated, all users that sign into a corresponding TeamViewer account are redirected to the identity provider that has been configured for the domain. This step is required independent of which identity provider is used.

For security reasons and to prevent abuse, it is required to verify the domain ownership before the feature is activated.

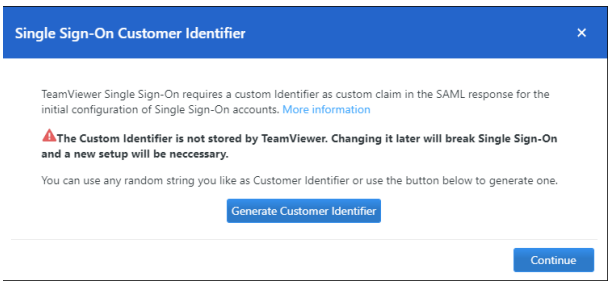
6.1.2 Add a New Domain

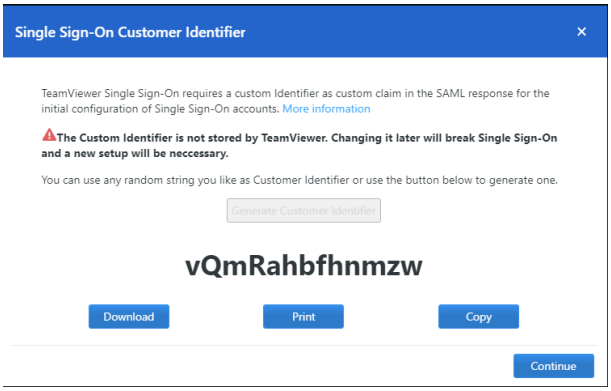
1. To activate SSO, log in to the Management Console and select the Single **Sign-On** menu entry.
2. Click on **Add domain** and enter the domain you want to activate SSO for.
3. You also need to provide you identity provider’s metadata. There are three options available to do so:
   - **via URL:** enter your identity provider metadata URL into the corresponding field
   - **via XML:** select and upload your metadata XML
   - **Manual configuration:** manually enter all necessary information. Please note that the public key must be a Base64 encoded string.



6.1.3 Create Custom Identifier

After the domain has been added, the custom identifier can be generated. This custom identifier is not stored by TeamViewer, but is used for the initial configuration of SSO. It must not be changed at any point in time, since this will break Single Sign-On and a new setup will be necessary. Any random string can be used as customer identifier. This string is later required for the configuration of the identity provider.

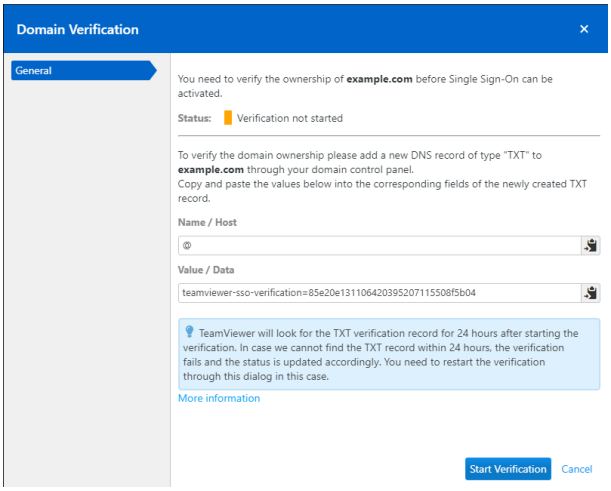




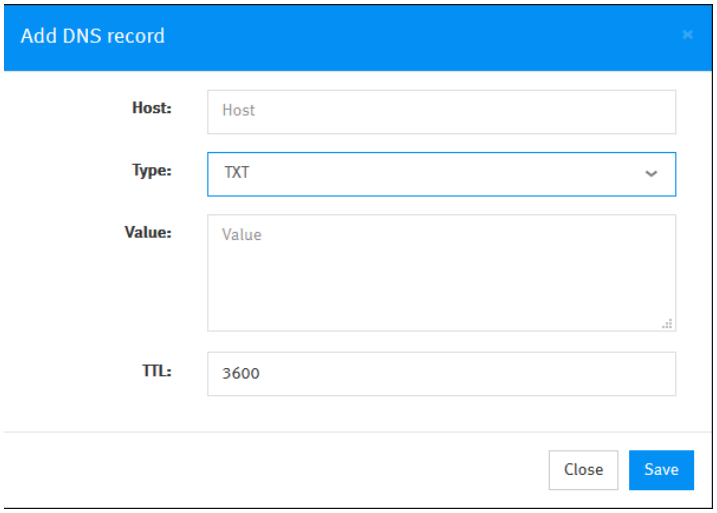
6.1.4 Verify Domain Ownership

After a domain has been added successfully, you need to verify the domain ownership. Single Sign-On will not be activated before the domain verification is completed.To verify the domain, please create a new TXT record for your domain with the values shown on the verification page.

Note: The verification process can take several hours because of the DNS system.



The dialog to add a TXT record might look similar to:



Note:

- Depending on your domain management system, the description of the input fields may vary. After creating the new TXT record, start the verification process by clicking the **Start Verification** button.
- The verification process can take several hours because of the DNS system.
- TeamViewer will look for the TXT verification record for 24 hours after starting the verification. In case we cannot find the TXT record within 24 hours, the verification fails and the status is updated accordingly. You need to restart the verification through this dialog in this case.

6.1.5 TeamViewer Client Configuration

TeamViewer is compatible to Single Sign-On starting from version 13.2.1080.

Previous versions do not support Single Sign-On and can not redirect users to your identity provider during the login. The client configuration is optional, but allows to change the used browser for the SSO login of the IdP.

The TeamViewer client will use an embedded browser for the identity provider authentication by default. If you would prefer to use the default browser of the operating system, you can change this behavior via the following registry key:

HKEY_CURRENT_USER\Software\TeamViewer\SsoUseEmbeddedBrowser = 0 (DWORD)

Note: You need to restart the TeamViewer client after creating or changing the registry.

SP Metadata URL	https://sso.teamviewer.com/saml/metadata.xml
Entity ID	https://sso.teamviewer.com/saml/metadata
Audience	https://sso.teamviewer.com/saml/metadata
Assertion Customer Service URL	https://sso.teamviewer.com/saml/acs
Assertion Consumer Service URL	https://sso.teamviewer.com/saml/acs
Assertion Consumer Service Bindings	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirec
SAML Request Signature Algorithm	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 TeamViewer supports SHA-256 as signature algorithm. We require the SAML assertion to be signed, while signing the SAML response is optional but recommended.
NameID	Unspecified

SAML Service Provider Metadata:

6.1.6 More Information and Online Resources

- **SP Metadata URL**: *https://sso.teamviewer.com/saml/metadata.xml*
- **Entity ID**: *https://sso.teamviewer.com/saml/metadata*
- **Audience**: *https://sso.teamviewer.com/saml/metadata*
- **Assertion Customer Service URL**: *https://sso.teamviewer.com/saml/acs*
- **Assertion Consumer Service URL**: *https://sso.teamviewer.com/saml/acs*
- **Assertion Consumer Service Bindings**:
  - urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
  - urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirec
- **SAML Request Signature Algorithm**: *http://www.w3.org/2001/04/xmldsig-more#rsa-sha256*

  TeamViewer supports SHA-256 as signature algorithm. We require the SAML assertion to be signed, while signing the SAML response is optional but recommended.
- **NameID**: Unspecified
- **Required SAML Response Claims**: *http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier*

  This should be mapped to a unique user identifier within the scope of the identity provider(and therefore within the scope of the corresponding company).

  For example, this can be the Active Directory Object GUID for ADFS or the email address for Okta: *http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress*

  This attribute should be mapped to the email address of the user that wants to sign-in. The email address needs to be the same as configured for the TeamViewer account. The mapping/comparison is done in a case-in-sensitive way.
- *http://sso.teamviewer.com/saml/claims/customeridentifier*

  This attribute should return a customer-specific identifier. The attribute must be named “customeridentifier.”

TeamViewer requires a customer identifier as custom claim in the SAML response for the initial configuration of Single Sign-On accounts.

- **The customer identifier is not stored by TeamViewer. Changing it later will break Single Sign-On and a new setup will be necessary.**: Any random string can be used as customer identifier.
- **Signature & Encryption Certificate (Public Key)**: The public key of the certificate that is used to sign SAML requests and for the encryption of SAML responses can be obtained by executing the following PowerShell command:

```
"-----BEGIN PUBLIC KEY-----`n" + `
((Select-Xml `
-Content ((Invoke-WebRequest `
https://sso.teamviewer.com/saml/metadata.xml).Content) `
-xpath "//*[local-name()='X509Certificate']").Node[0].'#text') + `
"`n-----END PUBLIC KEY-----" `
| Out-File -FilePath "sso.teamviewer.com - saml.cer" -Encoding ascii
```

The command downloads the metadata, extracts the public key and writes it to a file.

7 Customize & deploy

In the TeamViewer Management Console you have the opportunity to customize some TeamViewer modules according to your wishes. This option is available for the QuickSupport, QuickJoin and Host modules.

Customized modules distinguish themselves through the following characteristics:

- They can be customized with logo, colors and personalized texts to your needs
- They are linked to your TeamViewer account
- They are stored in the TeamViewer Management Console
- They can be customized at any time
- They are always available via a link (with the latest adaptations)
- They are always available in the latest TeamViewer version
- They can be created in an unlimited number
- They can be called up via customized links
- They can be customized individually for customers and your company
- They affect the appearance of the waiting room for meetings, go.teamviewer.com and get.teamviewer.com

In addition to using the standard modules, you can create one or more customized modules. This way, additional functions are available to you (e. g. the adaptation of the design with company logo and individual colors and the automatic integration of your partner into Computers & Contacts or automatic participation in a defined meeting).

➡ To create customized modules, click Design & Deploy in the menu bar.

7.1 Creating a customized QuickSupport module

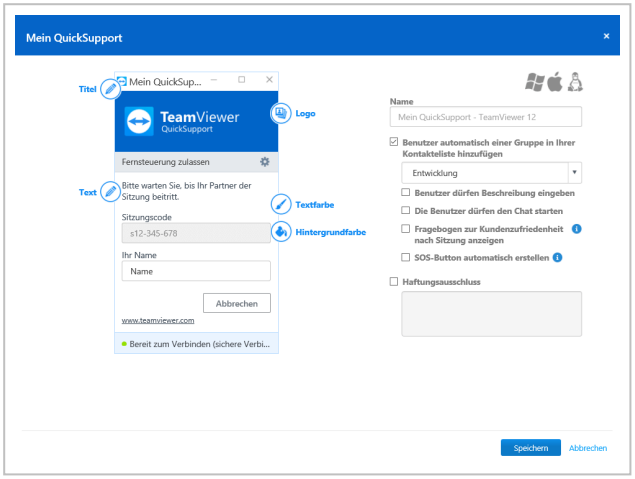
➡ To create a customized QuickSupport module, click the Add QuickSupport button.

Note: All the data transmitted on this website is encrypted for your security (SSL protocol).

Note: Unrestricted use of the customized TeamViewer QuickSupport module requires a TeamViewer license. Otherwise, the connection is automatically aborted after five minutes.

7.1.1 Individual QuickSupport preferences

The following can be configured:



Define custom settings for your QuickSupport module.

Visual customization

	Description
Title	Lets you edit the window title.
Text	Lets you edit the welcome text in the main window.
Logo	Select your own logo, which will be displayed in the top part of the main window.
Font color	Lets you edit the font color. Click in the left field to display a color palette and select a color.
Background color	Lets you edit the background color. Click in the left field to display a color palette and select a color.
Permanent link	Serves to call up the module. Provide this link to your customers. You can also define the link yourself. ➡ To do this, click the Edit button (only available after creating the module).

Behavior of the module

	Description
Name	Serves to identify the modules in the overview of your customized modules.
Automatically add users to a group in your Contacts list	If the box is checked, each QuickSupport module user will automatically appear in your Computers & Contacts as soon as the QuickSupport module is started. Select a group to which the service cases created by the QuickSupport module should be added.
Allow user to enter a description	If the box is checked, users of the customized QuickSupport can enter a problem description for their service case before a session has been started.
Allow user to initialize chat	If the box is checked, users of the customized QuickSupport can send you chat messages before a supporter assigned to the service case connects to them.
Show customer satisfaction form after session	If the box is checked, a feedback form will appear at the end of a remote control session automatically. With the feedback form users of this module will have the opportunity to rate and comment your support. **Note**: In order to allow other company members to activate the customer satisfaction form in the custom QuickSupport module, please enable the option **Allow activation** under **Company administration > Advanced > Customer satisfaction form**.
Automatically create SOS Button	If the box is checked, a shortcut to the module is created on the user's desktop after a connection to this module. Users can start a service case by
Use temporary password clicking on the shortcut.	If the option button is selected, a new random temporary password for establishing a connection will be generated every time the QuickSupport module is started.

	Description
Use a predefined password	As an alternative to a temporary password, you can assign a permanent password to the QuickSupport module. However, this excludes the functions underneath the **Use random password** option.
Password strength	Lets you select the complexity of the temporary password.
Disclaimer	Here you can enter an optional disclaimer to be displayed before TeamViewer QuickSupport starts. It is displayed before the start of TeamViewer QuickSupport. Your users must accept it in order to run TeamViewer QuickSupport.

7.2 Creating a customized QuickJoin module

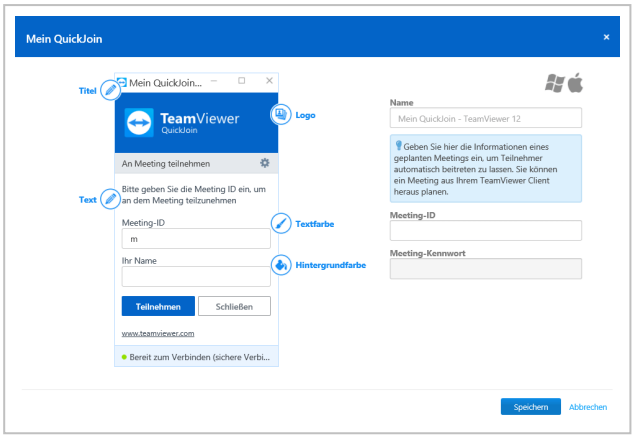
To create a customized QuickJoin module, click the Add QuickJoin button.

Note:

- The QuickJoin functionality may encounter compatibility problems when early versions of TeamViewer 15 (or older) are used for a connection with current TeamViewer Meeting versions. In order to avoid compatibility issues, we recommend to use our latest TeamViewer Meeting version. You may *download it on our website*.
- All the data transmitted on this website is encrypted for your security (SSL protocol).
- Unrestricted use of the customized TeamViewer QuickJoin module requires a TeamViewer license. Otherwise, the connection is automatically aborted after five minutes.

7.2.1 Individual QuickJoin Preferences

The following setting options are available:



Define custom settings for your QuickJoin module.

Visual customization

	Description
Title	Lets you edit the window title.
Text	Lets you edit the welcome text in the main window.
Logo	Select your own logo, which will be displayed in the top part of the main window.
Font color	Lets you edit the font color. Click in the left field to display a color palette and select a color.
Background color	Lets you edit the background color. Click in the left field to display a color palette and select a color.
Permanent link	Serves to call up the module. Provide this link to your customers. You can also define the link yourself. To do this, click the Edit button (only **available** after creating the module).

Behavior of the module

	Description
Name	Serves to identify the modules in the overview of your customized modules.
Meeting ID	Enter the Meeting ID of a scheduled meeting in the text field. At the start of the module, the user is directly connected with this meeting.
Password	Enter the password for the Meeting ID in the text field as an option.

7.3 Creating a custom Host module

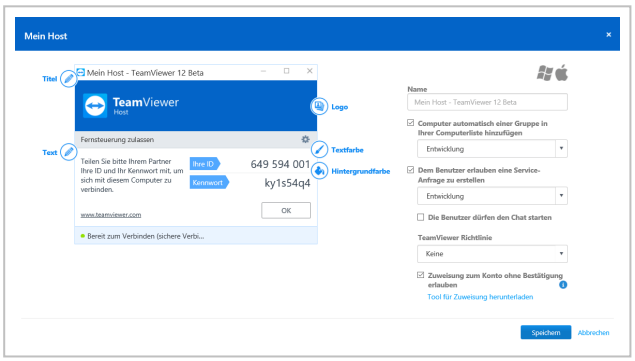
To create a customized Host module, click the Add Host > Host button.

Note: All the data transmitted on this website is encrypted for your security (SSL protocol).

Note: Unrestricted use of the customized TeamViewer Host module requires a TeamViewer license. Otherwise, the connection is automatically aborted after five minutes.

7.3.1 Custom TeamViewer Host settings

The following setting options are available:



Define custom settings for your TeamViewer Host module.

Visual customization

	Description
Title	Lets you edit the window title.
Text	Lets you edit the welcome text in the main window.
Logo	Select your own logo, which will be displayed in the top part of the main window.
Font color	Lets you edit the font color. Click in the left field to display a color palette and select a color.
Background color	Lets you edit the background color. Click in the left field to display a color palette and select a color.
Permanent link	Serves to call up the module. Provide this link to your customers. You can also define the link yourself. To do this, click the Edit button (only **available** after creating the module).

Behavior of the module

	Description
Name	Serves to identify the modules in the overview of your customized modules.
Add computers to Computers & Contacts automatically	If the box is checked, every computer on which the TeamViewer Host module is installed will be automatically added to your Computers & Contacts. Select a group name for these computers in your Computers & Contacts list.
Allow users to create a service case	If the box is checked, users of the TeamViewer Host module can start a service case for spontaneous support. Select a group name for these computers in your Computers & Contacts list.
Allow user to initialize chat	If the box is checked, users of the TeamViewer Host module can start a chat with you before a connection was established.
TeamViewer policy	Assign a policy to the TeamViewer Host module. The TeamViewer Host module is bound to the settings defined within the policy. More information *section 8 "Policies for TeamViewer Settings", page 66*..
Allow account assignment without confirmation	If the box is checked, it is possible to assign the Host module to your TeamViewer account remotely without any conformation needed on the client device.

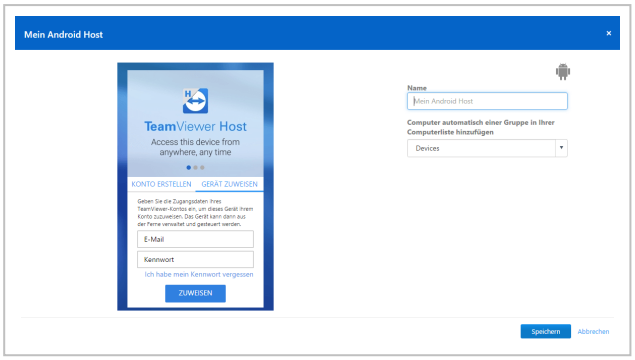
7.4 Deploy Android-Host module

To deploy an Android Host module to your Android devices, click the Add Host | Android Host button.

Note: This feature is included with the TeamViewer Corporate license version 11 (or later).

7.4.1 Custom Android Host settings

The following setting options are available:



Define custom settings for your Android Host module.

	Description
Name	Serves to identify the modules in the overview of your customized modules.
Automatically add computers to a group in your Computers list	If the box is checked, every device on which the TeamViewer Host module is installed will be automatically added to the selected group within your Computers & Contacts list. Select a group for these devices from your Computers & Contacts list.

8 Policies for TeamViewer Settings

Use the TeamViewer Management Console to configure TeamViewer settings for all your devices. Define setting policies and assign them to your devices. The settings of the installed TeamViewer full version are automatically be adjusted according to the policies.

The central administration of TeamViewer settings provides the following benefits:

- Configure all your TeamViewer installations from one place.
- Manage access rights with a general whitelist.
- Prevent users from changing the settings you have configured.
- Suggest useful settings and enforce safety-critical settings.
- Use your Active Directory or the TeamViewer Management Console to distribute the setting policies.
- After changing the settings, the export of the settings and rollout via MSI is obsolete.

Create any number of policies that define individual options for TeamViewer settings. Use different settings for the devices of your employees than your server, for example.

➡ To do so, open the **Policies** under **Design & Deploy**. Then click Add policy.

8.1 Add a New Policy

Define options for TeamViewer full version within the Add a new policy dialog.

➡ To do so, select an option from the drop-down list. Then, click Add.

Note: Remove options from the policy via Edit | Delete.

Hint: If you select the Enforce option, this option can not be changed on the device. Otherwise, the user is able to define the settings on the device itself.

The following options can be defined for TeamViewer setting policies:

Options	Description
Enable black screen on remote computer if partner input is deactivated	If activated, the screen on the remote computer is automatically deactivated as soon as the partner's input is deactivated.
Check for new version	From the drop-down list, select the interval at which you'd like TeamViewer to automatically search for an update. The following intervals are available: • Weekly • Monthly • Never
Log outgoing connections	If activated, TeamViewer writes information regarding all outgoing connections to a log file.
Automatic disconnect of inactive sessions	Select a time period after which an outgoing remote control session is automatically terminated if there is no interaction in the defined period.
Disable TeamViewer shutdown	If activated, TeamViewer cannot be shut down. This is useful, for example, if you, as the administrator, wish to guarantee the continuous availability of a computer.
Remove wallpaper	If activated, the wallpaper on the remote computer is hidden during the TeamViewer session. This optimizes the connection speed, since less data has to be transmitted.
Auto start screen sharing	If enabled, your screen is presented as soon as the first participant connects with your meeting.
Blocklist and allowlist	**Note**: You will still be able to set up outgoing TeamViewer sessions with partners on the blacklist.
Play computer sounds and music	If activated, the remote computer sound is transmitted to the local computer.
Share computer sounds and music	If activated, sound from the presenter's computer is transmitted to the participants.

Options	Description
Only users with Windows administrator rights can access TeamViewer options	If activated, TeamViewer options can only be changed by Windows user accounts with administrative rights.
Deactivate Drag & Drop Interaction	If enabled, the drag & drop functionality is deactivated in TeamViewer. In this case, files can no longer be transferred via drag & drop.
Remove own wallpaper	If enabled, the wallpaper of your own computer is hidden during a meeting.
Random password after each session	From the drop-down list, select whether or when you'd like TeamViewer to generate a new temporary password for incoming sessions. The following options are available: • **Keep current: The new password will not be generated until TeamViewer is restarted.** • **Generate new: TeamViewer generates a new password after each completed session.** • **Deactivate: A password is generated only once.** • **Show confirmation: TeamViewer asks you after each session whether you'd like to generate a new password.**
Incoming LAN connections	The following options are available: • Deactivated: Allows no LAN connections. • Accept: Accepts incoming LAN connections via Port 5938.
Log incoming connections	If activated, TeamViewer writes information about all incoming connections to a log file (Connections_incoming.txt).
Remote control invitation	In the text box, type an invitation message. The invitation text is used if a partner is invited to a remote control session from the device.
Meeting invitation	In the text box, type an invitation message. The invitation text is used if you send meeting invitations from the device.
Prevent removing account assignment	If activated, the account assignment for the device can not be removed.

Options	Description
Enable logging	If activated, TeamViewer writes all events and errors to a log file.
Auto record remote control sessions	If activated, every TeamViewer session will be automatically recorded.
Close to tray menu	If activated, TeamViewer will minimize to the tray menu after the program is closed (info area of the task bar). TeamViewer can subsequently be shut down by right-clicking the icon in the system tray.
Enable integrated system health checks	If enabled, the computer can be monitored and its assets traced via the integrated system health checks and Remote Management.
Password for Instant Meeting	In the text field, enter a password for the meetings you started. If you want to allow others to join the meeting only via Meeting ID, you can leave this field empty.
Temporarily save connection passwords	If activated, passwords will be stored per the default settings to allow immediate reconnection. After TeamViewer is shut down, the passwords are no longer saved.
Password strength	Here you can select how strong (complex) the random temporary password generated each time TeamViewer is started should be. • **Standard (4 digits)**The password consists of 4 digits. • **Secure (6 characters): The password consists of 6 alphanumeric characters.** • Secure (8 characters): The password consists of 8 alphanumeric characters. • **Very secure (10 characters): The password consists of 10 alphanumeric characters (including special characters).** • Disabled (no random password): No random password is generated.
Automatically minimize local TeamViewer Panel	If activated, the local TeamViewer Panel (if unnecessary) will automatically minimize to the screen edge after 10 seconds.
Show your partner's cursor	If activated, your partner's mouse movements will be graphically displayed on your desktop. You can also activate this option in the Remote Control window during a TeamViewer session.

Options	Description
Record meetings	If activated, all the meetings are recorded automatically.
Accept messages from trusted accounts	If activated, only chat messages from accounts that you have connected to before are accepted or shown.
Open new connections in tabs	If enabled, the remote control sessions and the remote computers' monitors will then be displayed in one (1) Remote Control window. If this option has not been enabled, these will then appear in separate windows.
Install new versions automatically	In the drop-down list, select whether or not TeamViewer should automatically install new versions. The following options are available: • **All updates (includes new major versions): updates will always be installed, even updates to newer major versions.** • Updates within this major version: Only updates within the current installed major version will be installed. • Security updates within this major version: Only updates within the current installed major version necessary to improve security will be installed. • No automatic updates: Updates will never be installed automatically.
Hide online status for this TeamViewer ID	If activated, your TeamViewer ID (computer) will not appear online on any Computers & Contacts list.
Quality	Here you can choose between • Auto select: Optimizes the display quality and transmission speed based on the available bandwidth. • Optimize quality: Optimizes the display quality, at the expense of transmission speed. • Optimize speed: Optimizes the connection speed. The display quality is also reduced to the optimum level for remote control. • Custom settings: Optimizes the display quality and transmission speed based on your custom settings.

Options	Description
QuickConnect button	If activated, the QuickConnect button is displayed in every windows' / applications' title bar.
Clipboard synchronization	If activated, any text copied to the clipboard will be available to the partner.
Send key combinations	If activated, key combinations (e.g. ALT+TAB) are transferred by default to the remote computer and not executed locally.
Start TeamViewer with Windows	If you did not configure TeamViewer to start with Windows during the installation process, you can do it here. Check the corresponding box. TeamViewer will then start automatically alongside Windows. That way, it will already be running even before you log into Windows.
Participant interaction	You can select from: • **Full interaction: All meeting participants can join the meeting and all the functions, such as VoIP, Chat or File box, are available.** • **Minimal interaction (presentation mode): Only you as the presenter can use the meeting functions.** All other participants can only observe. However the meeting functions can be enabled for all participants by demand. • Custom settings: Click the Configure... button to perform your own interaction settings.
Conference call	Define your own conference call data.
Use UDP (recommended)	If activated, TeamViewer will attempt to set up a fast UDP connection. You should only disable this feature if your connection is interrupted on a regular basis.
Report connections to this device	If activated, connections to this device will be reported and can be viewed in the TeamViewer Management Console. More information *section 11.2 "Device reports", page 93*.
Prevent removing account assignment	If activated, the account assignment for the device can not be removed. This is only possible if TeamViewer is uninstalled.

Options	Description
Record your partner's videos and VoIP (requires partner's permission)	If activated, participants can decide whether they would like their webcam video and VoIP to be recorded by a meeting recording session. If deactivated, only the screen and your own webcam video and VoIP will be recorded.
Record partner's video and VoIP (required partner's confirmation)	If activated, the connection partner can decide whether or not their webcam video and VoIP may be recorded. If deactivated, only the screen and your own webcam video and VoIP will be recorded.
Full access if a partner connects from the Windows login screen	If activated, partners who connect from the Windows login screen will automatically have full access to your computer.
Wake-on-LAN	Here you can configure the settings for TeamViewer Wake-on-LAN. By configuring these settings, you can remotely operate this computer even if it is switched off by waking it up before you establish a connection. Detailed instructions for configuration of TeamViewer Wake-on-LAN are available in the TeamViewer Manual – Wake-on-LAN.
Windows login	From this dropdown list, you can select whether to allow remote TeamViewer to connect to your computer with Windows login information instead of the random password. • Not allowed: Default setting. Authentication may only take place using the random or personal password. • Allowed for administrators only: Any partner who wants to connect to your computer needs the login information for a Windows administrator on your computer for authentication purposes. • **Allowed for all users: Any partner who wants to connect to your computer needs the login information for one of the Windows accounts on your computer.** **Note**: Make sure that all Windows logins are secured using strong passwords.

Options	Description
Access Control (outgoing connections)	Set what type of access you'll be granted on your partner's computer: • Full access • Confirm all • View and Show • Custom settings • Deny outgoing remote control sessions You can find further information in the *TeamViewer Manual - Remote Control.*
Access Control (incoming connections)	Set what type of access your partner will have to your computer: • Full access • Confirm all • View and Show • Custom settings • Deny incoming remote control sessions You can find further information in the *TeamViewer Manual - Remote Control.*
Access Control (meetings)	Set which rights you want you and the meeting participants to receive by default: • Full access • View and Show • Custom settings • Deny meetings You can find further information in the *TeamViewer Manual - Meeting.*

Note: Options that affect local settings, the TeamViewer account or security-related settings can not be defined in the TeamViewer Management Console.

Note: Options that are not defined in the policy keep the value of the locally defined settings.

8.2 Assign a Policy

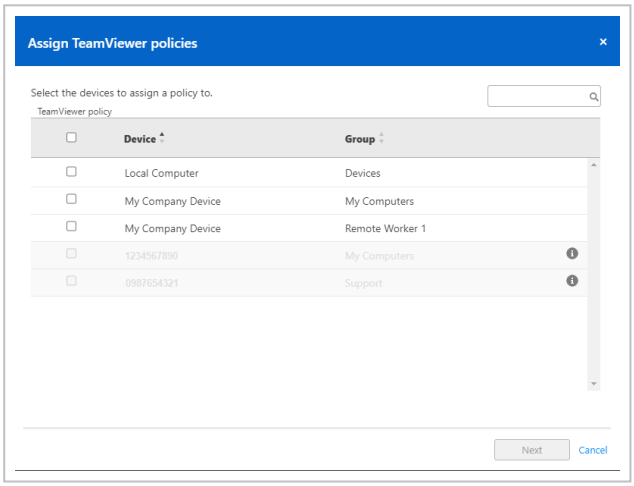
Assign configured TeamViewer setting policies to your devices. The defined settings are applied to the device. Changes of options within a policy are updated automatically on the device as soon as TeamViewer is launched.

To define the settings of a device using a setting policy, it must be ensured that the device is yours.

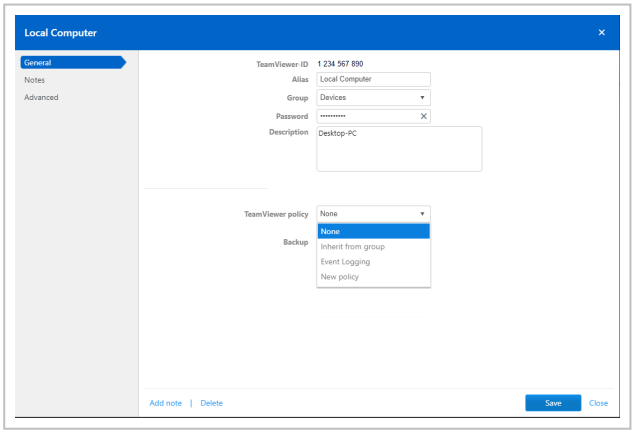
To do so, the device must be assigned to your TeamViewer account. This way, the settings of a TeamViewer installation can not be changed unauthorized.

To assign a TeamViewer setting policy to a device, choose one of the following methods:

- Click the **Assign Teamviewer policies** button + Assign TeamViewer policies on the top right under **Design & Deploy**. Follow the instructions in the dialog box:



- Open the properties of a group and choose a policy under **TeamViewer policy**:



The policy will be inherited for all devices of the group.

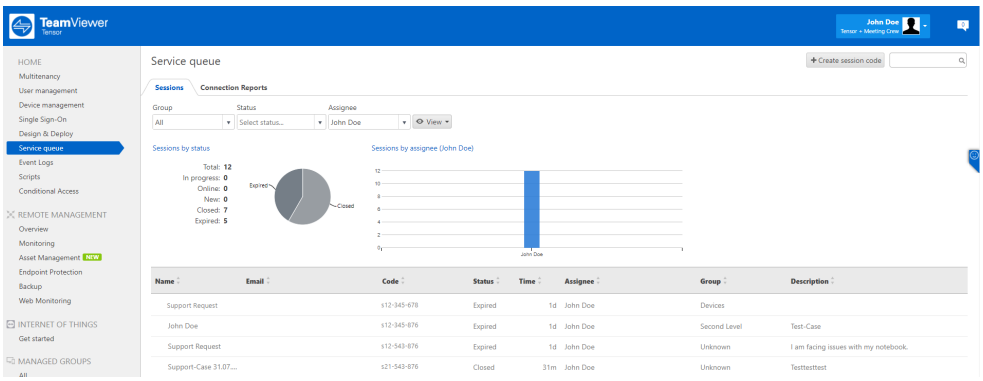
- Open the properties of a device and choose a policy under General | TeamViewer policy.

9 Service queue

With the service queue, you organize the spontaneous customer support on the team. Customer cases are collected in the service queue and depicted using a service case. Each service case represents the inquiry of a customer who needs help. After they are created, individual service cases can be worked on individually by colleagues from your team.

The typical application case of the service queue is depicted as follows:

> ***Example**: You are an employee in technical support of a company or a service provider for IT support. Your customer reports to you because he has a problem with his computer and he needs technical help. In the TeamViewer Management Console, you create a service case for this customer case and store the name of the customer, his email address, and a brief description of the problem that occurred. Then you can decide who from your team should work on the customer case by assigning the service case to a colleague. The colleague sends an invitation email to the customer. The customer connects to a TeamViewer session and your colleague can solve the problem with various TeamViewer functions such as remote control, file transfer or chat.*



The service queue with an overview of all service cases and the assignees.

For a clearer depiction, the following designation is specified:

- Customer: The person who makes the inquiry because he needs technical support.

9.1 Service Case

The service case represents a customer case within the service queue and is represented by a clear, unique session code. For more information about the properties of a service case, please see *section 9.2, page 78*.

9.1.1 Managing Service Cases

All service cases that you create or that are assigned to you are displayed and organized on the TeamViewer Management Console under Service queue | Sessions.

Within the view, the displayed service cases can be restricted even further. For this purpose, you can filter the service cases above the displayed table by Group, Status and Assignee. If you click an entry in the header of the table, you can sort the requests by column. You can select which columns are displayed in the table and enable or disable the graphical representation of service requests via the View menu.

The following possibilities are available to you for the management of a service case:

Assign

By default, service cases that you create are assigned to you. If during the creation of a service case you do not specify an assignee, it is possible to do this in the overview after the fact.

Assign the service case to yourself. You are then the assignee and you work on the case.

Assign
Use the link to specify a contact from your Computers & Contacts list as assignee and assign the service case to him/her.

Connecting

If a service case is assigned to you as assignee, you can establish a remote session with the icon.

Start a remote session. No connection partner is online. Wait until the customer also connects to the session.

Participate in the session with service case. The customer has started the connection and already connected to the session.

Edit

Edit a service case after the fact by clicking on the name of the service case on the list of sessions. Alternatively, click  at the end of a case select **Edit**.

Edit all information in the properties of the service case. There you will also find the link to participate in the TeamViewer session and the session code for the case.

- Code: Identifies a service case uniquely and serves to establish a TeamViewer session (e. g. `s12-345-678`).
- Link: Serves to participate in a TeamViewer session with service case (e. g. `https://-get.teamviewer.com/s12345678`).

Close session

If you have created a session or you have write rights for the group in which the case is located, it may be necessary to close the session. Close a session, e. g. if an assignee has finished with it and the customer's problem is solved.

- To do this, click ⚙ ▾ at the end of a case and select **Close session**.

9.1.2 Status of a Service Case

The status of a service case is displayed in the list of sessions in the Status column. A service case can have the following statuses:

- New: Service case was created. Neither the assignee nor the customer has connected to the session.
- Pending: One of the connection partners has connected to the session.
- In progress: Both connection partners have connected to a remote session. This is the case if the assignee starts the session and the customer connects to it or if the customer starts the connection and the assignee requests a remote session.
- Closed: The session was closed by the assignee or the creator of the case (see above).
- Expired: The case was not closed within 24 hours.

Depending on the status, the icon of the service case appears different.

	Description
☆	The service case is assigned to you. Wait until the connection partner connects to the session.
☆	The service case is assigned to another assignee. He can work on the case. The assignee waits until the connection partner connects to the session.
☆	The service case is assigned to another assignee. He can work on the case. The connection partners has connected to the session.
★	The service case is assigned to you and the connection partner has connected to the session. Work on the case.

9.2 Creating a case

Generally, you create service cases if a customer needs help. Via the case on your Computers & Contacts list, you can then connect to your customer without entering TeamViewer ID and password or call up other functions on the Computers & Contacts list.

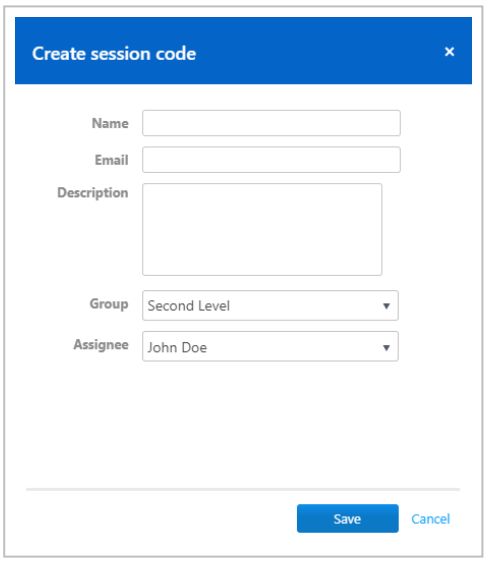
Service cases are connected with the Computers & Contacts list and are created in a group. In order to structure cases, you can create them in different groups for a better overview.

> ***Example**: You are the producer of several software products, then you create service cases for product A in a group "Product A" and service cases for product B in a group "Product B," and so forth.*

You must share the groups with the colleagues who work on the service cases.

> ***Example**: Colleague A is supporter for product A, therefore you share the group "Product A" with him so that you can specify your colleague A as assignee for these cases.*

Depending on the problem, create an individual service case by clicking the Create service case button on the list of sessions.



Define the properties of a service case on the Create service case dialog.

On the dialog, you define the properties of the case. A service case includes the following information:

- Name: Name of the customer making the inquiry.
- Email: Email address of the customer for the case.
- Description: Description of the problem of the customer case.
- Group: Group on your Computers & Contacts list in which the service case is created.
- Assignee: Contact from your Computers & Contacts list who works on the service case.

Then click the Save button. The service case appears in the overview and it can be worked on.

9.3 Assigning a case

By default, service cases that you create are assigned to you. However, you can also assign service cases to other assignees. This way you can coordinate customer cases and service cases, assign contacts from your Computers & Contacts list. You must share the groups in which the service cases are located with the contacts.

> ***Example**: Colleague A is supporter for product A, therefore you share the group "Product A" with him so that you can specify your colleague A as assignee for these cases.*

In order to assign the service case to a contact, you have various possibilities:

- When creating a service case, select another assignee than yourself.
- Click in the overview on the Assign link (only available if the service case has not yet been assigned to anyone).
- Select the Assign option when clicking on the  icon next to a service case.

Note: Contacts from your Computers & Contacts list with write rights for the group in which the service cases are located can also assign assignees.

9.4 Working on cases

If a service case is assigned to you, you can work on it and contact the customer in order to solve the problem.

> ***Example**: You are colleague A and supporter for product A. A colleague has shared the "Product A" group with you and assigned you the service case of a customer who has problems with product A.*

Depending on the problem, the TeamViewer Management Console and the TeamViewer full version offer you various possibilities for solving the problem.

- Establish a remote session to the customer in order to solve problems directly on the customer's computer.
  - To do this, click the  or  button.

The following possibilities are only available in the TeamViewer full version. Read the TeamViewer Manual – Remote Control.

- Start a meeting in order to explain facts to your connection partner, for example.
  - To do this, click the Presentation (confirmation prompt) button.
- Chat with the connection partner in order to investigate the case or solve smaller problems quickly.
  - To do this, click the  icon.

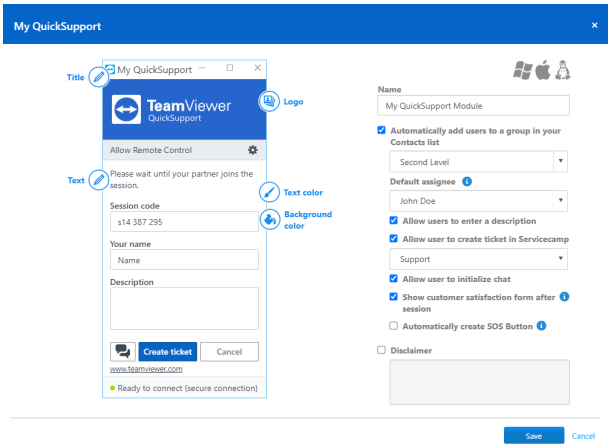
- Send files to the connection partner, e. g. manuals or pre-prepared instructions for frequently asked questions.
  To do this, click the icon.

- Copy e. g. log files from your connection partner's computer in order to be able to specify problems.
  To do this, click the icon.

9.5 Inquiry via custom QuickSupport module

You can configure custom QuickSupport modules so that they create a support case as soon as they are executed.

- You do not have to create service cases yourself
- Customers can describe their problem themselves directly in the module
- You only have to assign the cases to one assignee



Create a custom QuickSupport module with service case and problem description.

Hint: If you activate the Show customer satisfaction form after session feature for custom QuickSupport modules, users can rate sessions that connected to the custom module.

10 Auditability/Event Logs

Note: This feature requires a TeamViewer Tensor license. For more information, please visit our *TeamViewer Tensor website*.

Log all user activity, record remote sessions, and set user policies for complete auditability and visibility into who is doing what, when, and for how long. With TeamViewer Tensor™, you can ensure your enterprise stays compliant with security protocols and internal requirements, while detecting security risks before they impact your business.

10.1 General Information

10.1.1 Prerequisites:

- TeamViewer Client version 13.2 or higher
- You have a TeamViewer company account in order to access the Management Console where you can activate the feature for your company
- You/your company own(s) a TeamViewer Tensor license

Note: All event data is logged for 1 year on TeamViewer servers (located in Frankfurt). This retention period can't be changed. After 1 year all data will be automatically and completely deleted.

Collected Data

Event data during remote control sessions is only collected from users who are authenticated as a member of the company that has enabled event logging.

Examples of a remote control session with two users:

User 1 (initiator of the RC session)	User 2	Whose event data is collected?
Company member (authenticated)	Company member (authenticated)	User 1 and user 2

User 1 (initiator of the RC session)	User 2	Whose event data is collected?
Company member (authenticated)	Company member (not authenticated)	User 1
Company member (authenticated)	Foreign user (authenticated)	User 1
Company member (authenticated)	Foreign user (not authenticated)	User 1
Company member (authenticated)	Quick support user	User 1
Foreign user (authenticated)	Company member (not authenticated)	No data collected

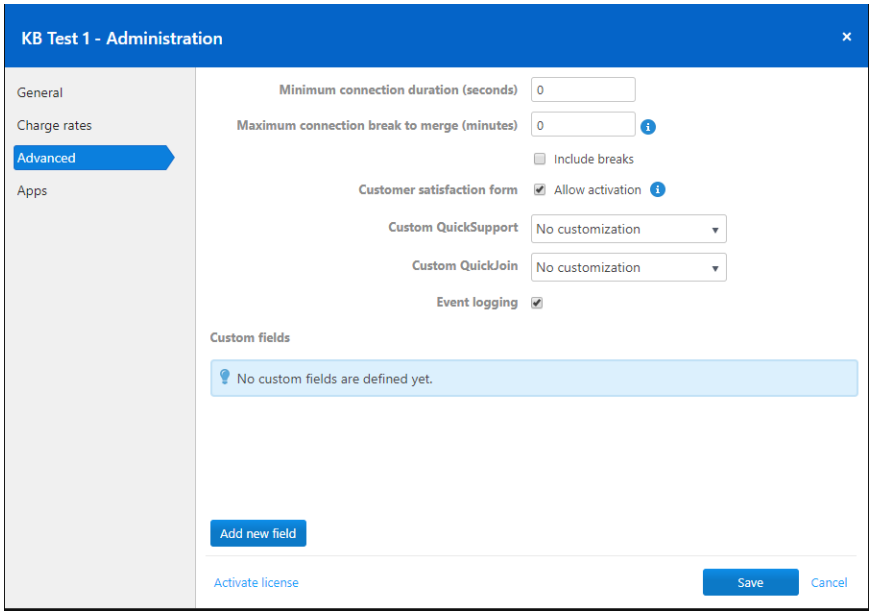
10.2 Activate Event Logs

By default, event logging is not activated for your company as you should get general consent within your company about collection and usage of the data.

Note: Activating event logging can only be done as a company admin.

- In the Management Console, click on your **user profile**.
- Navigate to **Maintain [your company]** > **Advanced** > **Event logging**.
- Click the checkbox **Event logging**.

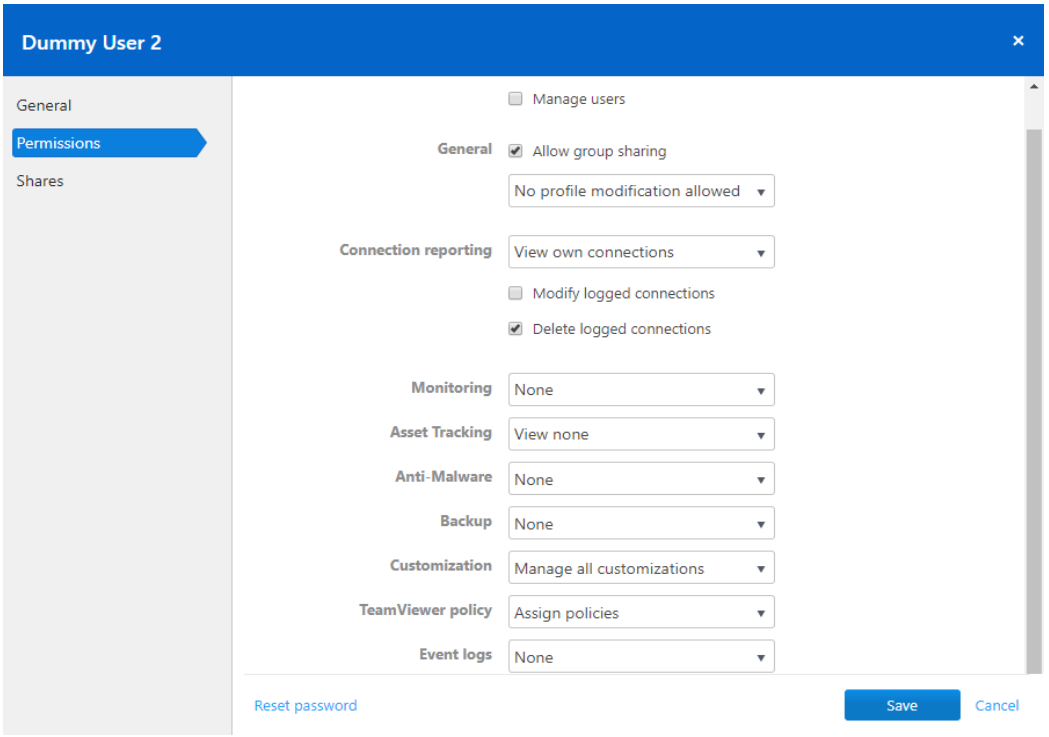
➡ Now certain activities of all users that belong to your company will be logged.



10.3 Access Event Logs for Auditing

Note:

- In order to have access to the event logs, you need to have access to the Event Log dialog in the Management Console. Your company administrator can grant you access to this page.
- Granting access to event logs only works with the 4-eye-principle. You need another company administrator granting you access.

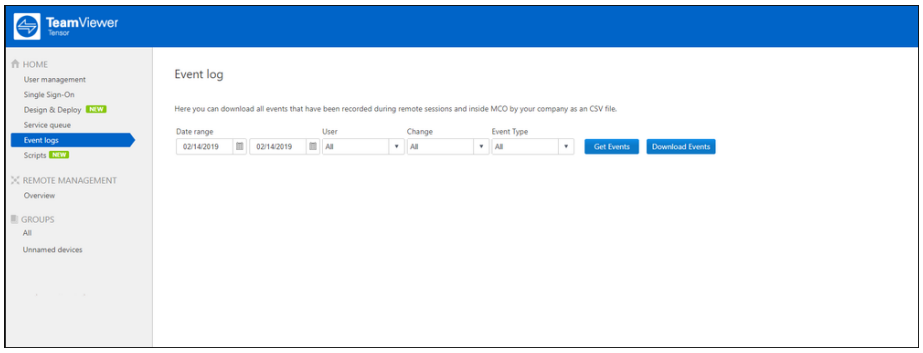


10.4 Watch and Filter Event Logs

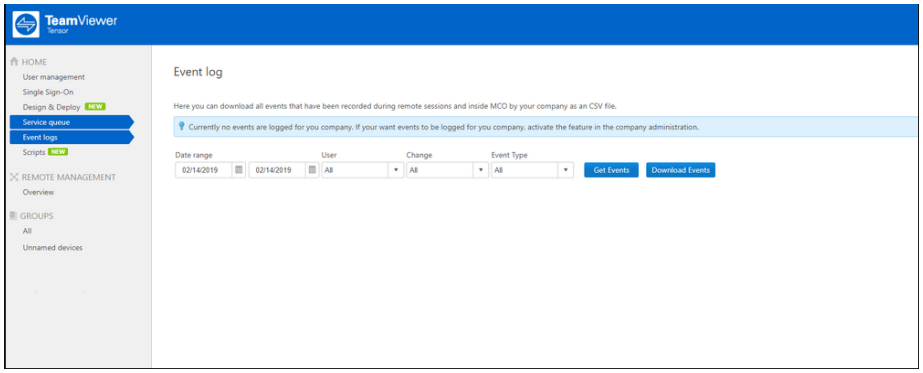
Note: You need to have access to the event logs of your company.

- In the Management Console, click **Event Logs** in the left navigation panel.

If event logging is active for your company you will see the following screen:



If event logging is deactivated for your company you will see the following screen:

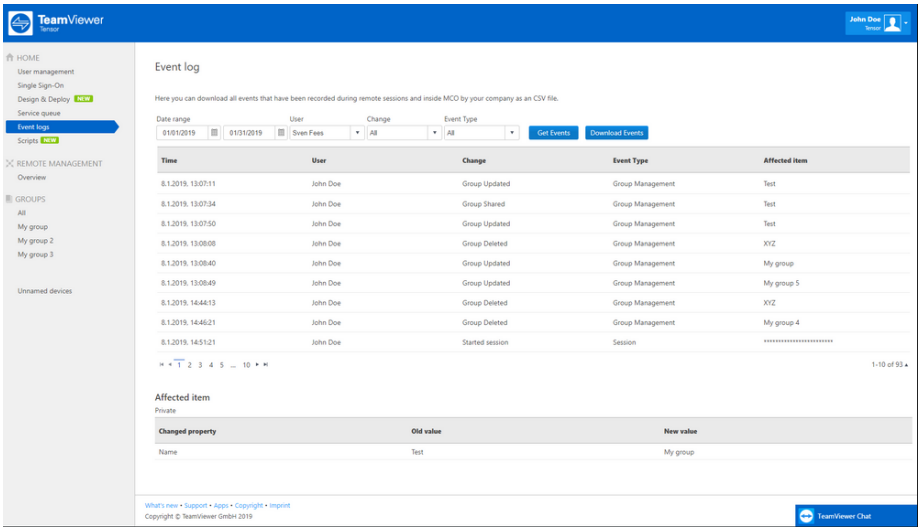


- Start to search for specific events by using the given filter possibilities:
  - **Date range**: Use this filter to search for events within a specific date range.

> **Note**: **The maximum date range is one month!** If you want to search for events throughout multiple months, you need to execute multiple searches.

  - **User**: Use this filter to search for events executed by a specific person.
  - **Change**: Use this filter to search for a certain change done by any user.
  - **Event type**: Use this filter to search for multiple events grouped under a certain category. It will help you, for example, to search for all changes done by any user in the User Management.
- After you selected your filters, click on **Get Events**.

➡ You will now see a filtered list of events.



Now you can click on single events to see more details for each event.

10.5 Download Event Logs

> **Note**: You need to have access to the event logs of your company.

- In the Management Console, click **Event Logs** in the left navigation panel.
- Apply your filters and click **Download Events**.

➡ You will receive a CSV file containing the filtered events.

- In order to have a good overview of all the downloaded events, we recommend to import the CSV file into Excel.

CSV Columns

The CSV file contains multiple columns that provide details about the recorded event:

Event	Description
Date	The date when the event was logged. The date logged in this column reflects the server date.
Time	The time when the event was logged.
Datetime (ISO8601)	The date, time and timezone in ISO8601 format of the logged event.
Author	The person that executed the event. The author is displayed by the user name or if that is not existing by the TeamViewer ID.
Change	This is the event the author performed (in a short and readable format).
Event type	A category each event belongs to. It will help to group for certain event types, e.g. when you are only interested in changes that have been done to user properties all over the company.
Affected item	The object on which the change was made.
Property	The detailed property that was changed on the affected item, e.g. the user name of a user object.
Old value	This column is only filled when an object was changed or deleted, but not when it was created. In case an object was changed the old, changed value is listed in order for you to see how the value was changed. If an object gets deleted, the old value shows the value the object had before deletion.
New value	This column shows the (new) value of the changed property.

10.6 Event log REST API

The event log can also be retrieved via the REST API. You will find more information about how to use the API in our *official API documentation.*

11 Connection reports

With the TeamViewer Management Console, it is possible to log and manage all outgoing TeamViewer connections (except for meetings) of the users of a company profile. Whether Windows or Mac, browser-based or from a smart phone, all connections can automatically be logged.

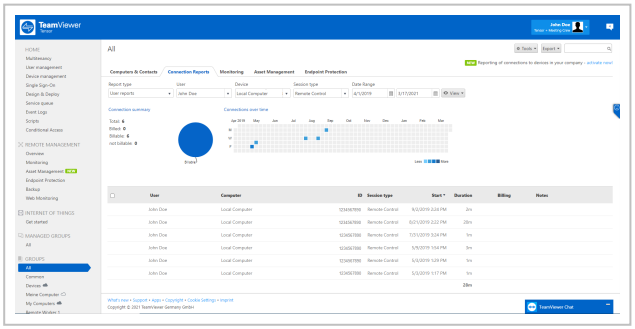
The connection report can also be used as the basis for billing or for authoring comments about TeamViewer connections.

Connection reports are distinguished by User reports and Device reports. The user reports contain information about outgoing connections of users within you company profile. The device reports contain information incoming connections to devices that are assigned to your company profile. You can choose between these reports under Report type.

11.1 User reports

With user reports, it is possible to log all outgoing connections of the users of a company profile within the TeamViewer Management Console. This makes it easier, for example, to prepare bills for chargeable support times for customers and provides a precise summary of previous sessions.

Connections are logged only if this function is enabled in the TeamViewer account of the users (enabled by default) and if they are logged into TeamViewer with their account.



A user report.

11.1.1 Show connections

The connection data are displayed on the **Connection report tab sorted by group.**

To call them up, select the desired group on the menu bar. To view user connection reports, select User reports in the Report type drop-down.

Within the view, the displayed connections can be restricted even further. For this purpose, you can filter the connections above the displayed table by User, Device and Date range. If you click an entry in the header of the table, you can sort the requests by column.

The following information can be displayed for every connection using the View menu:

Columns

- **User**: Name of the user who initiated the connection.
- **Computer**: Computer name of the remote computer.
- **Session type**: The type of the remote session.
- **Group**: Group within your Computers & Contacts list to which the remote computer was added.
- **Start**: Start time of the connection.
- **End**: End time of the connection.
- **Duration**: Duration of the connection in minutes.
- **Fee**: Incurring costs for the connection based on the defined charge rates.
- **Bill**: Indicates whether the connection will be billed or not.
- **Notes**: Comments that were added to the session.

Group by

Under View | Group by, you can group the connections by user or computer. For grouped connections, the overall duration and the bill are displayed.

Other

Under View | Other, can enable or disable the graphical representation of the number of logged connections.

11.1.2 Managing Connections

The TeamViewer Management Console provides extensive functions for managing the logged connections.

These functions can be called up via the buttons **Export** Export and **Tools** Tools in the connection report.

Export

	Description
Print list	Creates an *.html document with all the displayed connections.
csv export	Creates a *.csv file with all the displayed connections. Download this file to your computer to open your connections, e. g. in Microsoft Excel.

Tools

	Description
Billable	All selected connections are included in the calculation of the connection costs. If deactivated, the selected connections are excluded in the calculation of the connection costs.
Billed	All selected connections are marked as already billed.
Merge selected	All selected connections are combined. You can select whether breaks will be included or excluded. The icon is displayed at the beginning of the line.
Unmerge selected	All selected combined connections are separated again and displayed as individual connections.
Delete selected	All selected connections are deleted.

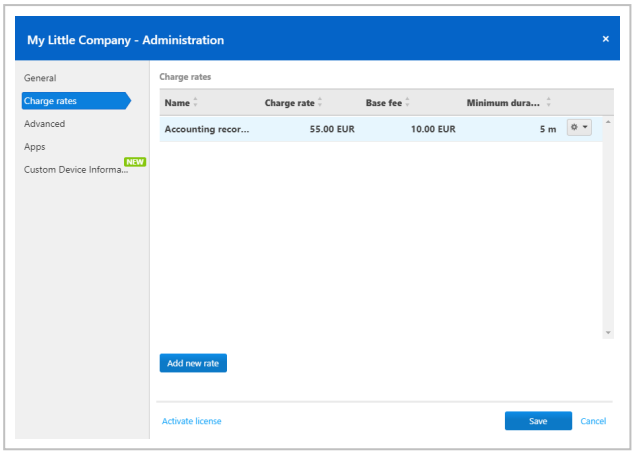
Note: To select several connections, click the check box in front of the according connection entries.

To edit individual connections directly, or to call up some of the functions described above, click on the icon at the end of the line while moving the mouse over a connection.

11.1.3 Billing connection costs

Within your company profile, you can perform calculations for connection costs of outgoing connections of all users of the company profile.

The costs of a connection are calculated based on a charge rate. Any number of charge rates can be stored for a company profile.



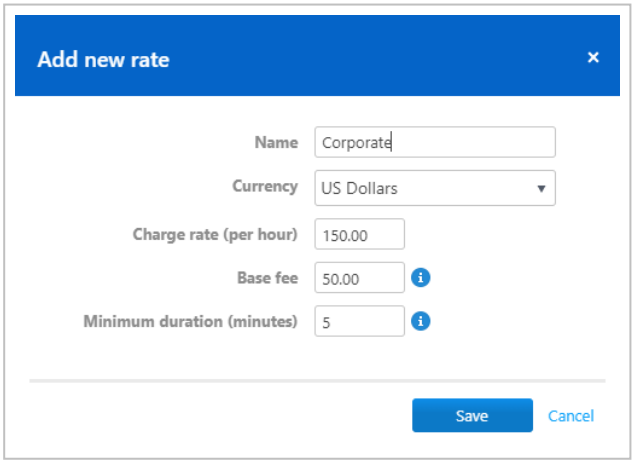
Overview of all charge rates in the company profile.

Creating charge rates

The charge rates are stored in the company administration by an administrator of the company profile.

The following values can be defined for a charge rate:

- **Name: Name of the charge rate.**
- **Rate: Calculated costs per hour.**
- Currency: Currency of the charge rate.
- Base fee: One-time fixed costs per connection (independent of the rate).
- **Minimum duration: Duration of a connection (in minutes) in which the base fee is being billed.** At the end of this time, the defined rate is used for any further calculation.



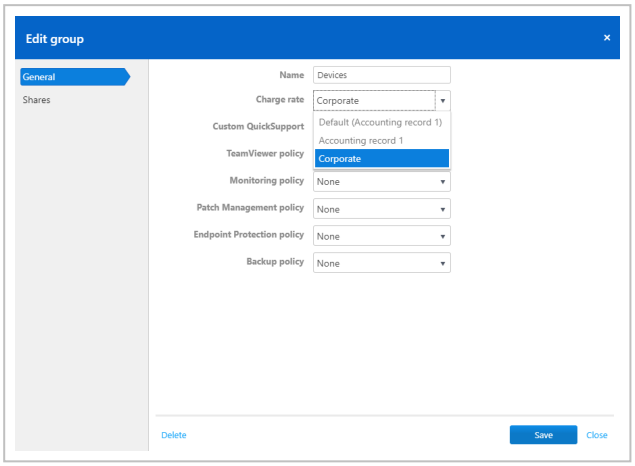
Adding a new charge rate.

Using charge rates

The billing of TeamViewer connections is done for each group. For this purpose, charge rates created can be assigned to the groups from the list of computers & contacts.

This makes it possible, e.g. to assess different connection costs for different customers.

To assign a charge rate to a group, select a group on the menu bar and click on the icon in front of the group name. You can select a charge rate from the Charge rate drop-down list.



Assigning a charge rate.

11.1.4 Comments

As administrator of a company profile, you can define for users whether they should write a comment about this connection after the end of a logged TeamViewer connection.

This requires that the options Log sessions for connection reporting and Show comment window after each session are enabled in the properties of the respective TeamViewer account (see *section 5.4 , page 45*).

Note: Note: For the connections of the users to be logged, the users have to be logged into TeamViewer with their TeamViewer account.

Creating a comment

If the requirements described above are met, a new window is opened after the end of a TeamViewer connection. The user can add a comment about the session in this window.

Editing comments

Comments for TeamViewer connections can subsequently be edited with the corresponding permission.

To do so, move the mouse over the desired connection in the connection report and click on the icon, followed by Edit comment.

11.1.5 Customer satisfaction form

As administrator of a company profile, you can define for users of a TeamViewer QuickSupport module, whether they should be prompted with a customer satisfaction form after the end of a logged TeamViewer connection.

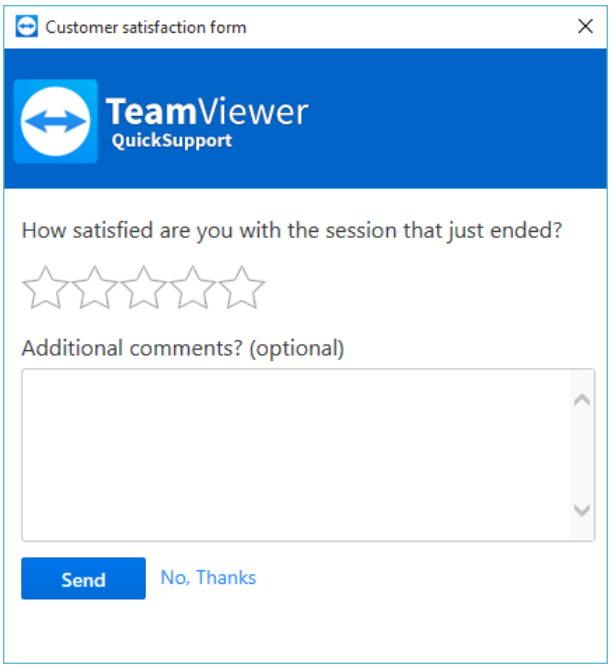
The user at the remote computer will then have the opportunity to evaluate or comment a finished remote control session.

This requires that the option Show customer satisfaction form after session is enabled in the properties of the respective TeamViewer QuickSupport module (see *section 7.1 , page 58*).

Note: In order to allow other company members to activate the customer satisfaction form in the custom QuickSupport module, please enable the option **Allow activation** under **Company administration > Advanced > Customer satisfaction form**.

Rate and comment remote control sessions

If the requirements described above are met, a new window is opened after the end of a TeamViewer connection. The user can complete a customer satisfaction form in this window.



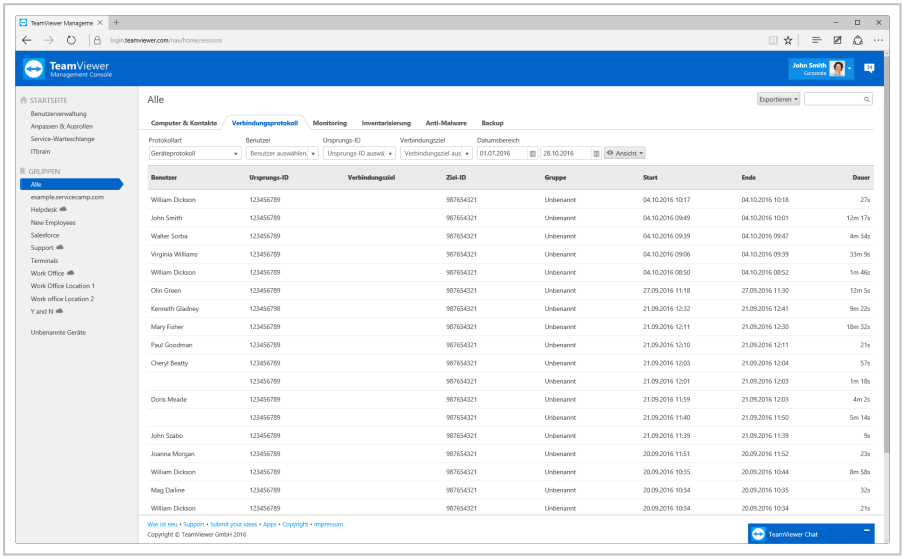
Customer satisfaction form after session end

Note: The customer satisfaction form will only be displayed after sessions that lasted at least 30 seconds.

11.2 Device reports

With device reports, it is possible to log all incoming connections to devices that are assigned to your company profile within the TeamViewer Management Console. This allows you, for example, to understand user has been connected to one of your servers when and how long.

Device reports are part of the TeamViewer setting policies. Connections are only logged, if this function is configured within the policy and the policy is assigned to the device.



A device report.

11.2.1 Set up device report

Device reports must be activated within a TeamViewer settings policy. If this option is configured for a policy, this affects every device which has assigned the specific policy.

To define the settings of a device using a setting policy, it must be ensured that the device is yours. To do so, the device must be assigned to your TeamViewer account. You can find further information in the TeamViewer Manual – Remote Control.

Note: Device reports are only available for devices and can not be set up for specific contacts.

To configure a policy for device reporting, follow these steps:

- Open the Policies tab under Design & Deploy. Select an existing policy or click Add policy. Select an existing policy or click Add policy.
- Choose the Report connections to this device option within the drop-down list. Then, click Add.

For more information on TeamViewer setting policies please refer to *section 8, page 66*.

Note: The Report connections to this device option is enforced by default. This is mandatory.

Hint: If devices do not inherit policies from the group they are located in, make sure to assign the policy to the respective devices as well.
More information *section 8.2 "Assign a Policy", page 74*..

11.2.2 Show connections

The connection data are displayed on the **Connection report tab sorted by group.**

To call them up, select the desired group on the menu bar. To view device connection reports, select Device reports in the Report type drop-down.

Within the view, the displayed connections can be restricted even further. For this purpose, you can filter the connections above the displayed table by User, Origin ID, Target computer, and Date range. If you click an entry in the header of the table, you can sort the requests by column.

The following information can be displayed f**or ever**y connection using the View menu:

Columns

- **User: Name of the user who initiated the connection.**
- Origin ID: Device ID of the user who initiated the connection.
- Target computer: Computer name of the computer the connection was established to.
- Target ID: Device ID of the computer the connection was established to.
- **Group:** Group within your Computers & Contacts list to which the remote computer was added.
- **Start: Start time of the connection.**
- **End:** End time of the connection.
- **Duration: Duration of the connection in minutes.**

Group by

Under View | Group by, you can group the connections by user, Origin ID, or Target computer. For grouped connections, the overall duration and the bill are displayed.

Export

	Description
Print list	It creates an *.html document with all the displayed connections.
csv export	It creates a *.csv file with all the displayed connections. Download this file to your computer to open your connections, e. g. in Microsoft Excel.

12 Scripts

12.1 Script execution with a single click

This function allows you to run prepared scripts during a remote control session with a single mouse click. Benefit from the advantages of this function:

- Upload your batch, PowerShell or Shell scripts encrypted for repetitive tasks to a secure storage in the Management Console.
- During a remote control session, you can select the saved scripts from the menu and run them with a single click.
- Save time by reducing processing time – so you can focus on important tasks and resolve other support issues.
- Automation reduces the likelihood of user errors.

12.1.1 Requirements

Before you can use the script execution with a single click, some requirements must be fulfilled.

Requirements for the scripts

- The following script types are currently supported:
  - **For Windows:** Batch (.bat, .cmd) and PowerShell (.ps1)
  - **For macOS:** Shell (.sh)
  - **For Linux:** Bash (.sh)
- The maximum file size of a script is 100 KB.
- The scripts you want to run on the remote device must be suitable for the operating system of the remote device.
- The scripts are ready to use and are stored either locally on your computer or on your network drives.

Requirements for your TeamViewer installation

Make sure that the requirements listed below are met so that you can run your scripts during a remote control session:

- You need a valid license for TeamViewer 14 (or higher) and you need to install this version (for Linux version 14.2 or higher).
- TeamViewer version 14 must be installed on the remote device to which you have connected.
- You must be logged in to the TeamViewer client with your licensed account. Otherwise your scripts will not be displayed during the session.
- **For Windows**: The TeamViewer client must be installed on the remote side (it must not have been started with **Run only**). Otherwise, the UAC query will not be visible on the remote client when running scripts that require administrator rights.
- An HTTP connection from the remote device to the cloud storage must be possible.

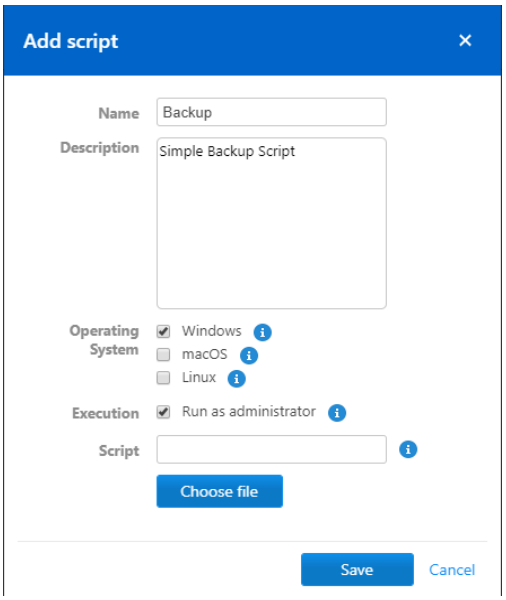
Note: There is no compatibility between TeamViewer versions 14.0/14.1 and 14.2! Make sure that either TeamViewer 14.0/14.1 or 14.2 is installed on both sides. The connection from a version 14.0/14.1 to a version 14.2 or vice versa does not work.

12.1.2 Uploading Scripts to the Management Console

To upload your scripts to the Management Console, follow these steps:

1. Log in to the Management Console with your TeamViewer account credentials.
2. Click **Scripts** in the left navigation area.
3. Click **Add Script**.

   The **Add Script** dialog box opens.

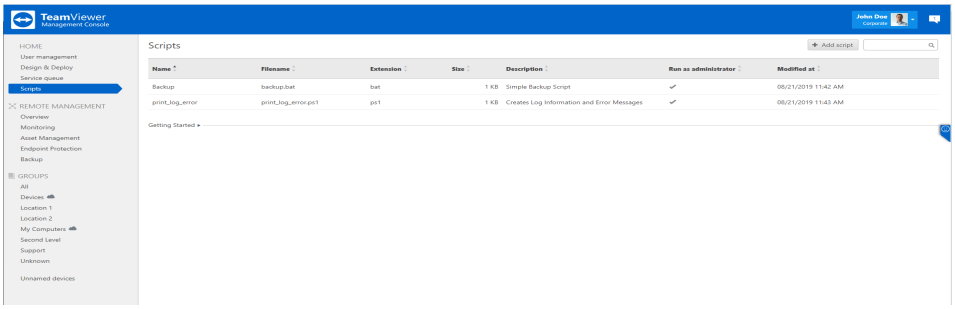


The Add Script dialog box.

4. Enter the required information for the script:
   - **Name (optional)**: If you do not enter a name, the file name of the script is used by default without the file extension.
   - **Description (optional)**: Enter a short and meaningful description of the script's function here.
   - **Operating system**: By selecting the operating system, only scripts that can run on the remote computer and its operating system will be displayed in the menu during your session.
   - **Run**: Enable this option if your script contains commands that require administrator rights.
5. Click **Select File** to select the script.

   The **Open** dialog box will be displayed.
6. Select the script and click **Open**.
7. Click **Save**.

The script is available to run during a remote control session.



In the Scripts overview, you can see all your uploaded scripts.

12.1.3 Running scripts during a remote control session

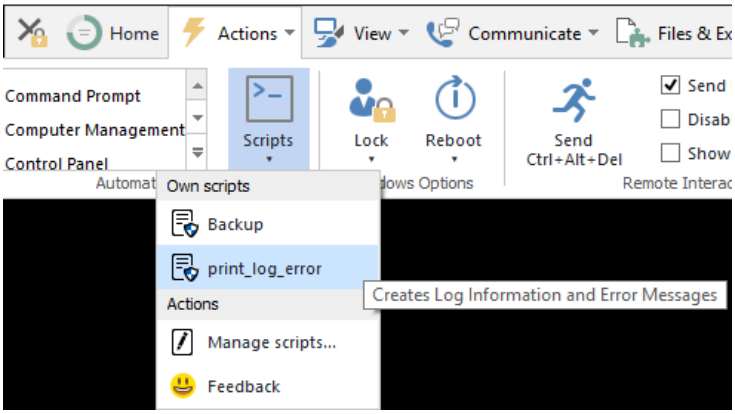
When you start your script, you will only be asked once for permission before it is executed (if the logged in user already has administrator rights). If the logged-in user does not have administrator rights, you will be asked for the administrator's credentials, regardless of how often or when such commands are used within your script (e.g. for longer-lasting tasks).

Note:
- Currently, you can only run the scripts as an administrator on an installed TeamViewer. For Windows, the Run Only (single use) and QuickSupport options are not available because the UAC query cannot be displayed on the client side.
- Administrative mode scripts are not yet supported for Linux.

To run your scripts during a remote control session, follow these steps:

1. Click **Actions**, and then click **Scripts** in the **Automation** area.
2. In the **Custom Scripts** area of the selection dialog box, click the script you want to run.

➡ The script will be executed.



Running a script during a remote control session.

13 Conditional Access

Note: This feature requires a TeamViewer Tensor license. For more information, please visit our *TeamViewer Tensor website*.

With TeamViewer Tensor Conditional Access, enterprise IT and security managers can maintain company-wide oversight of TeamViewer access and usage from a single location.

- Centralized rules management within the Management Console
- Assign permissions for remote session, file transfer, and meeting connections
- Configure rules at the account, group, or device level
- Cloud-based solution that provides greater flexibility than an on-premise approach
- Dedicated infrastructure is managed and serviced by TeamViewer
- Supports Windows and macOS

Overall, you gain full control over remote connections within your corporate environment. This TeamViewer Tensor functionality helps you tighten up your security by allowing access and connections to only authorized users or devices, consequently preventing data leaks, risky behavior, and minimizing risks.

13.1 Client Configuration

Note: Conditional Access is a security feature and therefore no connection is allowed initially as soon as the rule verification is activated!

Note: This article applies to all TeamViewer customers with a TeamViewer Enterprise/Tensor license and Conditional Access AddOn or Tensor Pro or Unlimited licenses.

13.1.1 Prerequisites:

- Activated license with the Conditional Access add-on
- TeamViewer Client version 15.5 or higher

- Created a TeamViewer company (possible via Management Console)
- Knowledge of the DNS/IP address of the dedicated router

Configure the client:

The client has to be configured to contact the dedicated routers because we are going to block the access to the usual TeamViewer routers in the firewall with the next step.

Windows

The configuration of the registry can be done running the following command or adding the registry keys through an import.

- **32-bit Version:**
  reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TeamViewer" /v "ConditionalAccessServers" /t REG_MULTI_SZ /d YOUR_ROUTER1.teamviewer.com\0YOUR_ROUTER2.teamviewer.com /f
- **64-bit Version:**
  reg.exe ADD "HKEY_LOCAL_MACHINE\SOFTWARE\TeamViewer" /v "ConditionalAccessServers" /t REG_MULTI_SZ /d YOUR_ROUTER1.teamviewer.com\0YOUR_ROUTER2.teamviewer.com /f

  ➡ After restarting the TeamViewer service, the client will not connect to the usual TeamViewer routers but to one of the dedicated routers instead.

Note: The MSI rollout with TeamViewer Settings is not possible with Azure and MS Intune!

macOS

To set the dedicated routers you have to execute one of the following commands while TeamViewer is not running, depending on whether TeamViewer starts with the system or not.

```
# start with system
sudo defaults write /Library/Preferences/com.teamviewer.teamviewer.preferences.plist ConditionalAccessServers -array YOUR_ROUTER1.teamviewer.com YOUR_ROUTER2.teamviewer.com
# not starting with system
defaults write ~/Library/Preferences/com.teamviewer.teamviewer.preferences.Machine.plist ConditionalAccessServers -array YOUR_ROUTER1.teamviewer.com YOUR_ROUTER2.teamviewer.com
```

Linux

To set the dedicated routers you need to change the global.conf file and add the following entry:

```
[strng] ConditionalAccessServers = "YOUR_ROUTER1.teamviewer.com" "YOUR_ROUTER2.teamviewer.com"
```

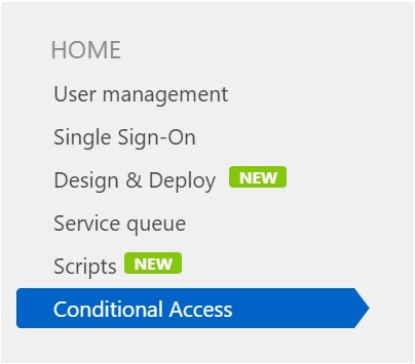
Configure the Firewall:

- Adjust your Firewall to block the following DNS-Entries:
  - master*.teamviewer.com
  - router*.teamviewer.com

As soon as this configuration is active, clients that didn't get the information to connect to the dedicated router will not be able to go online anymore. This is relevant for blocking unauthorized TeamViewer clients.

13.2 Add Rules

Note: Conditional Access is working with rule engine in the back end. You can manage the rules centrally in the Management Console. When you have purchased and activated your license then you will see an additional section in the navigation.



- Click **Conditional Access** to see an overview of all rules.

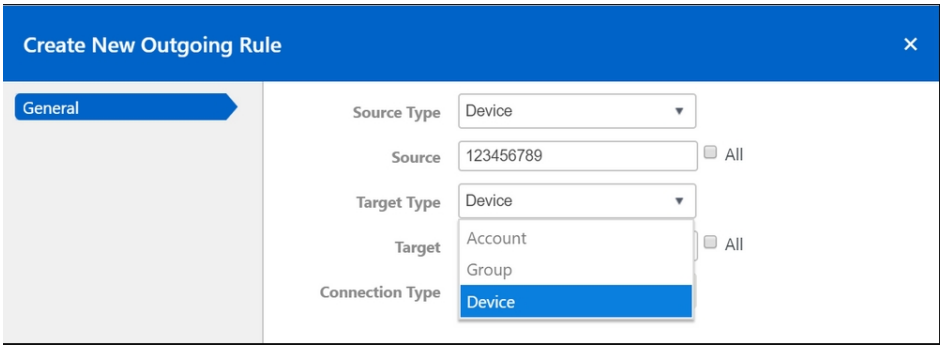
Note: Conditional Access starts from blocking everything initially, which also makes the management of the rules easier as there is no possibility for contradictory rules.

- Click **Add Rule**.

A new dialog pops up.

You have the possibility to add rules for devices, accounts and groups for both source and target. There is auto completion available for all devices and accounts that are in your Computers and Contacts list. Additionally, all accounts from your company are also considered in the auto completion. You are still able to add devices that are not in your Computers & Contacts list by entering the TeamViewer ID.

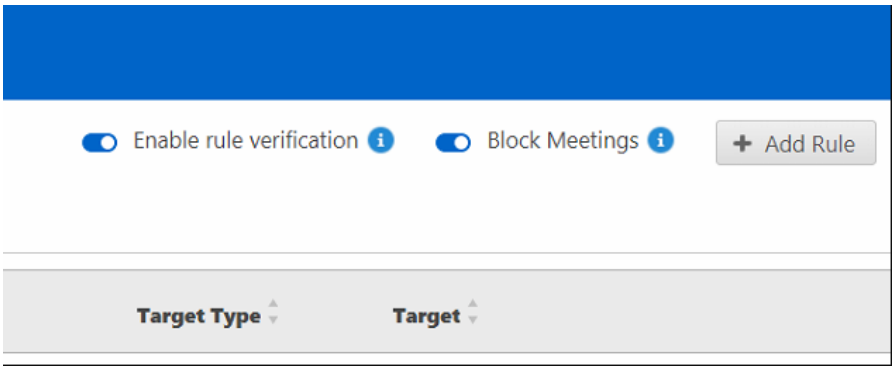
Note: With respect to groups, you can only add them if you are the owner of the group, which is a security measure.



There is also a field for the Connection Type, which is currently fixed to Remote Control.

13.3 Enable Rule Verification

Note: To make it easier to set up Conditional Access, we added a general on/off switch for the rule verification. This option can be used to ensure a smooth implementation of Conditional Access in your company. You can leave it deactivated until you have added all the rules that are necessary.



When the rule verification is turned off, the rules will not be enforced and therefore all connections that are initiated from or targeted to a client that is connected to the dedicated router are allowed.

Note: You can enforce the rules you have defined for TeamViewer Meetings as well.

14 Groups (Computers & Contacts)

In the TeamViewer Management Console, you can manage the groups, computers and contacts of your list of computers & contacts in a clear and central way and start remote control sessions.

All the groups of your list of computers & contacts are shown on the menu bar under **Groups.** Upon selecting a group, the computers and contacts from this group are shown in the content area.

14.1 Adding Groups, Computers or Contacts

The TeamViewer Management Console allows creating new groups, computers and contacts and adding them to your list of computers & contacts.

14.1.1 Add a Group

To share a group, choose one of the methods:

- Move the mouse over the **GROUPS**category title and click the icon.
- Select an existing group name for these computers in your Computers & Contacts list. Select an existing group in the Computers & Contacts view. Then click + Add and select **Add group**.

14.1.2 Add a Computer

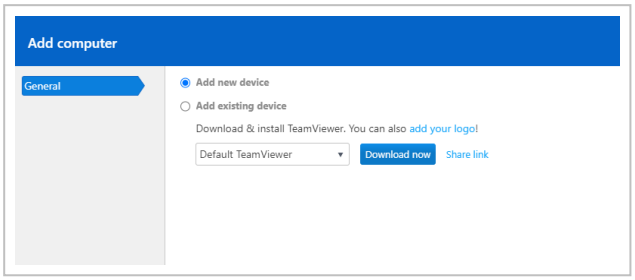
To add a computer, select one of the following methods:

- Select the group to which the computer should be added. Click + Add and select **Add computer**.
- Move the mouse over the group to which the computer should be added and click . Sselect **Add computer**.

Add a new device

Computers & Contacts > Add > Add computer > Add new device

Select this option, if you want to add the device that you are using at the moment to your Computers & Contacts list and TeamViewer is not yet installed on the device. Depending on your selection, either the TeamViewer full version, TeamViewer Host or a *customized TeamViewer Host module* is installed on the device.

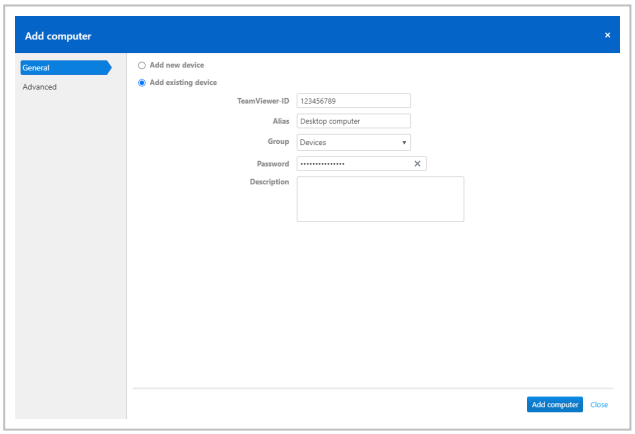


After installation, the device is available in the previously selected group. If you have a installed a customized TeamViewer Host module, the device appears in the group that was defined for the *Host module*.

Add existing device

> *Computers & Contacts > Add > Add computer > Add existing device*

Select this option, if you want to add any device to your Computers & Contacts list and TeamViewer is already installed on the device.



Enter the necessary data. Depending on the pre-selection, the group is already defined. If custom fields are available for the device, you can define them under Advanced.

14.1.3 Add a Contact

To add a contact, select one of the following methods:

- Select the group to which the contact should be added. Click + Add and select **Add contact**.
- Move the mouse over the group to which the computer should be added and click . Then select the Add contact option.

14.2 Edit Groups, Computers, or Contacts

14.2.1 Edit a Group

In the properties of a group, you can edit the following attributes:

- **Name**: Change the name of the group.
- **Charge rate**: Assign a charge rate to the group. Connections that are established to devices within the group are billed with this rate.
- **Custom QuickSupport**: Select a personalized module from the drop-down list. Connection partners, that connect to a session with a service case from within this group, automatically take part with the selected module.
- **TeamViewer policy**: Select a policy that defines the settings of the devices in this group.
- **Monitoring policy**: Choose a policy that is used by Remote Management to monitor computers within this group.
- **Patch Management policy**: Detect and patch outdated and therefore vulnerable software. Keep your IT systems up-to-date and safe by automatically evaluating, testing and applying OS and 3rd party application patches from a central location–completely remote, without establishing a VPN connection.
- **Endpoint Protection policy**: Endpoint Protection protects your computers 24/7 against threats such as viruses, trojans, rootkits, spyware and ransomware. You can start with the "Default Endpoint Protection Policy" or add a new policy.
- **Backup policy**: TeamViewer Backup can be deployed and activated remotely and your backed up files can be restored remotely from anywhere and at any time. You have the possibility to specify the files to be backed up. Choose your backup frequency and optimize performance with bandwidth throttling.
- **Shares**: Select the contacts from your Computers & Contacts list that you want to share the group with.
- **Delete**: Delete the group from your Computers & Contacts list.

➡ To do so, select the group you want to edit and click the icon. Then select the Edit option.

Note: To delete a group, this group may not contain any computer or contact.

14.2.2 Edit a Computer or Contact

You can perform the changes familiar from the TeamViewer full version (e.g. Alias, Group or Description) in the properties of the computer or contact. If activated, you can select a Remote Management Monitoring policy for devices within their properties (*section 15 , page 109*).

To edit a computer or contact, choose one of the following options:

- Move the mouse over the computer or contact and click on the icon, followed by Properties / Edit contact.
- Click on the name of a computer or contact and select the Properties / Edit contact option.

14.3 Share group

You have the option of sharing groups from your list of computers & contacts with individual contacts from your list. This allows making complete groups available to other contacts – quickly and easily.

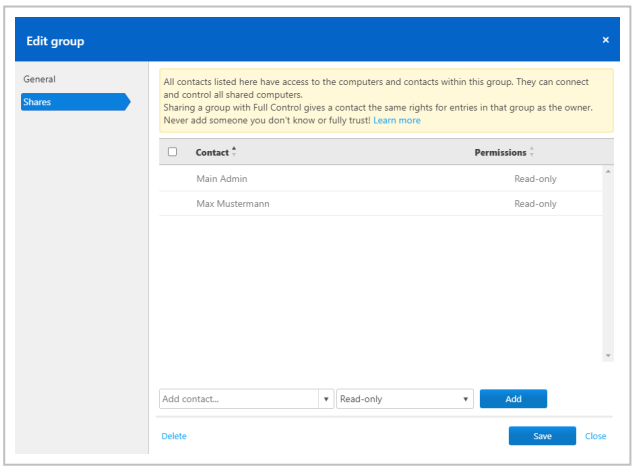
For shared groups, you can assign permissions to the users. As a result, groups can either be changed by specific users (Edit properties, Add contacts, etc.) or the groups are shown only in their list of computers & contacts and cannot be edited. Connections to computers or contacts from shared groups can always be created, regardless of the permissions.

Next to the group name of a group that you shared with contacts, the icon is displayed.

The icon is displayed next to the group name of a group that was shared with you.

To share a group, choose one of the methods:

- Open the properties of the group and click the Shares menu item. Here you can add the contacts with which you want to share the group, remove them from the list and assign permissions.
- Open the properties of the group and click the Shares menu item. You can then add the groups you want to share with the contact, remove shares from the list as well as assign permissions.



14.4 Connecting with a Computer or Contact

It is possible to establish a remote control session with a computer or a contact from the list of computers & contacts directly from within the TeamViewer Management Console.

To establish a connection to a computer or contact, select one of the methods:

- Move the mouse over an entry in the Computers & Contacts view and then click the Connect button.
- Click on the name of a computer or contact and select the Connect option.

If TeamViewer is installed on your computer, a connection is automatically established to your partner. If TeamViewer is not installed on your computer, a pop-up window appears and you can decide whether to install TeamViewer or to establish the connection from within the browser.

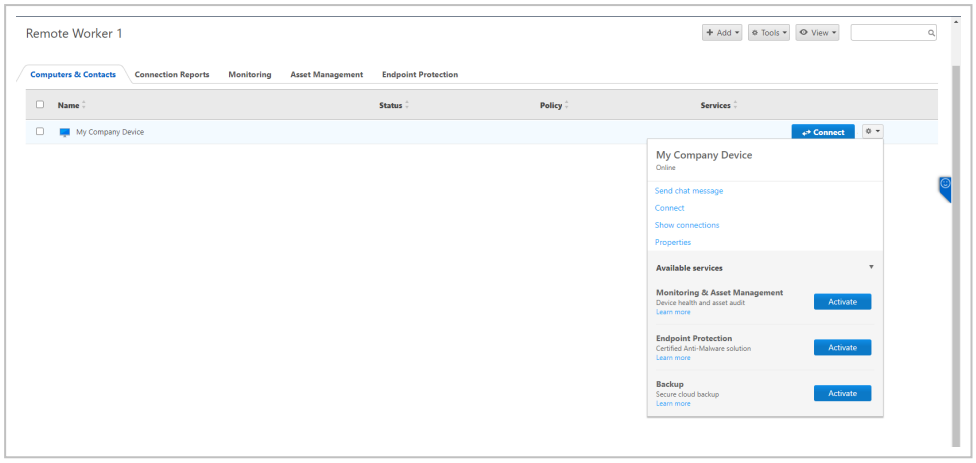
14.5 Calling up Functions for Computers or Contacts

You can call up additional functions for computers and contacts.

- To do so, move the mouse over an entry in the Computers & Contacts view and click on its name.

The following functions can be called up:

	Description
Send chat message	Opens a chat pop-up where you can send messages to the computer or contact from within your browser.
Connect	Establishes a connection with password entry.
Show connections	Displays the connections filtered by the Device in the Connection Report (see *section 11 , page 87*).
Properties	Opens the properties of the device or account.
Alerts (only computers)	Alert messages through Remote Management or the system checks in the TeamViewer full version (see *section 15 , page 109*).
Wake up (only computers)	Wakes the computer through Wake-on-LAN. More information can be found in the TeamViewer Manual for Wake-on-LAN.
Remote Management (only computers)	Activate Remote Management components like Monitoring & Asset Management, Endpoint Protection, or Backup for the device (see *section 15 , page 109*). If you do not have a Remote Management license yet, a trial period is started.



The available functions depend on whether a device or account is selected.

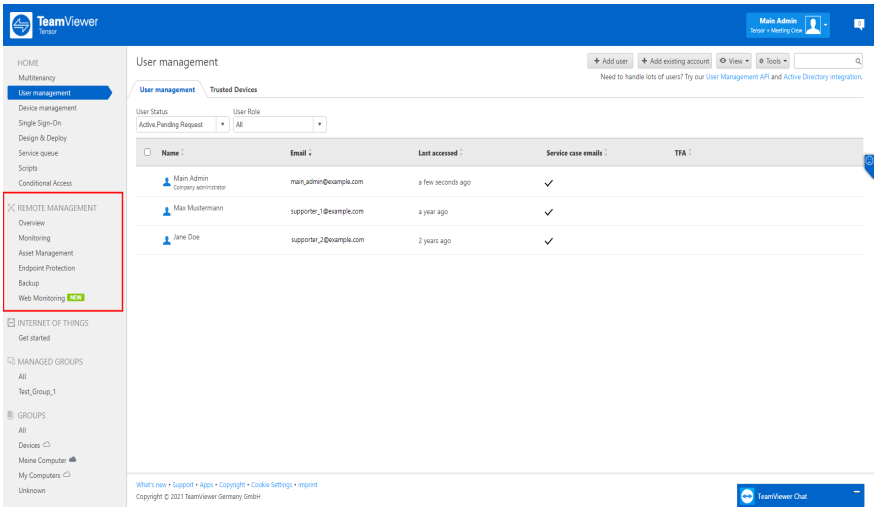
15 Remote Management

TeamViewer Remote Management is a professional and efficient IT management platform integrated into a secure remote desktop access tool, completely tailored to your company's needs. The platform is designed to protect and remotely monitor devices, to keep track of IT assets, and/or to store the data in a secure cloud backup. In order to achieve these goals, TeamViewer Remote Management offers the following services, available on the TeamViewer Management Console and on the TeamViewer client:

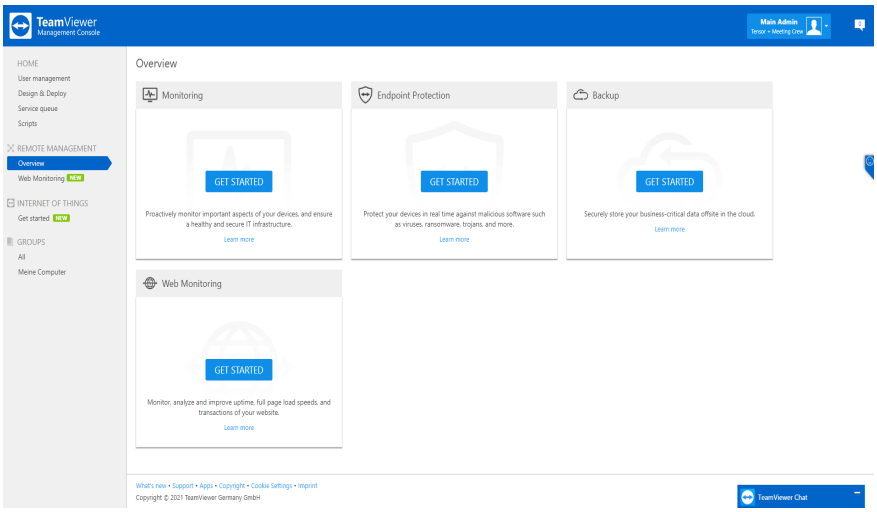
- TeamViewer Monitoring & Asset Management
- TeamViewer Endpoint Protection
- TeamViewer Backup
- TeamViewer Web Monitoring

Note: For each computer that you would like to monitor, a Remote Management end-point is required. The Remote Management license is linked to a TeamViewer account and can be used independently of your TeamViewer license.

Access Remote Management functionalities with the left navigation panel in the Management Console:



Activate Monitoring, Endpoint Protection, Backup, or Web Monitoring by clicking the corresponding "Get Started" button and following the instructions.



Computers that you are monitoring with Remote Management must fulfill the following requirements:

- The computer must be assigned to your TeamViewer account.
- Remote Management must be activated on the computer.

Use the tabs in the content area to call up all functions for Remote Management:

- **Overview:** Provides an overview of monitoring status, alert messages, and detected threats for monitored and protected computers. You also have the possibility to buy more endpoints and storage in our Shop.
- **Monitoring:** Add and manage endpoints and display alert messages for the monitored computers. Here you can also see the status of each alert and configure your monitoring policies. Alerts are also displayed on the context menu of each computer (with a click on the computer name).
- **Asset Management:** View and generate reports on all your devices' hardware, installed software and more, with only a few clicks.

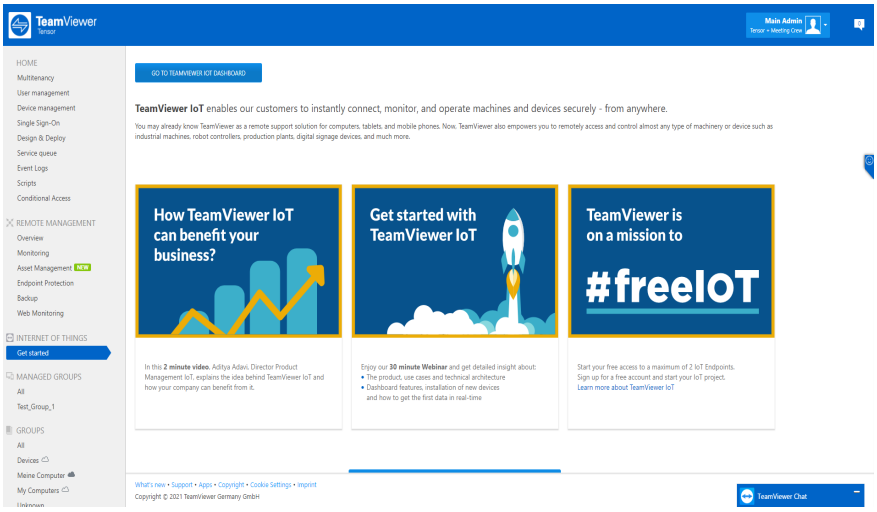
- **Endpoint Protection** protects your computers against threats such as viruses, ransomware, Trojans, rootkits and spyware. 24/7—no matter if on- or offline.
- **Backup:** TeamViewer Backup is your simple, hassle-free, and reliable solution to endpoint data protection. Deploy and activate TeamViewer Backup remotely within seconds. Your, or your customers', data will be stored in the cloud using the highest security standards.
- **Web Monitoring:** Continuously monitor your website's uptime, page load speeds, and important transactions such as your web shop or customer login—from more than 30 locations worldwide!

You can also call up some of the functions mentioned above using the groups in the Computers & Contacts list.

Online Resources

- For more information about TeamViewer Remote Management, please visit our *TeamViewer Remote Management Website*.
- You will find detailed feature explanations and how-tos for many use cases in our *TeamViewer Remote Management User Guide*.

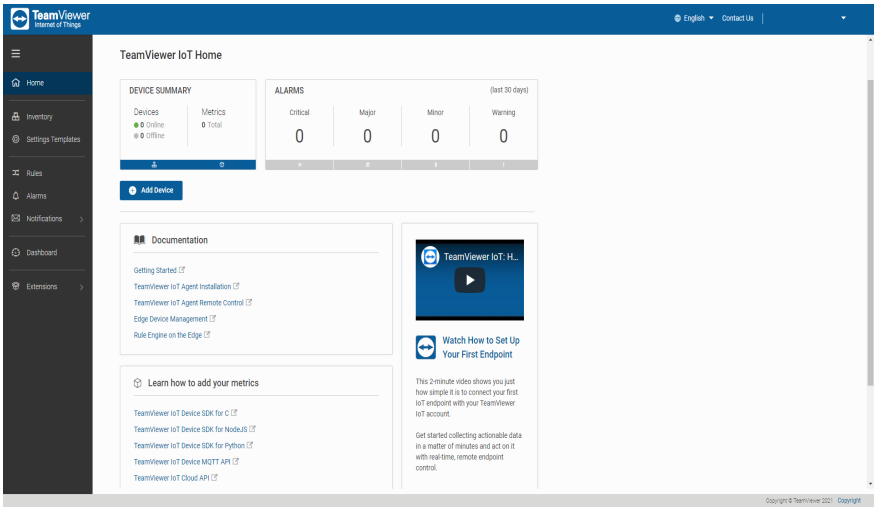
16 TeamViewer IoT



TeamViewer Internet of Things enables you to instantly connect, monitor, and operate machines and devices securely – from anywhere.

Get full visibility into all IoT devices with real-time status alerts and early insights, so you can react quickly to mitigate risks and proactively solve issues, before they impact your business:

- Combine remote control functionalities with monitoring capabilities
- Operate endpoints remotely for faster, more economical operations – at the enterprise scale
- Receive alerts based on monitored IoT Data, enabling you to react quickly to incidents
- Enables remote assistance and support to fix devices and machine issues as they occur
- Accelerate roll-out time for your IoT solution with out-of-the-box connectivity – no complicated IoT VPNs



TeamViewer IoT Dashboard overview

- For more information about TeamViewer Remote Management, please visit our *TeamViewer IoT Website*.
- You will find detailed feature explanations and how-tos for many use cases in our *TeamViewer IoT documentation*.