timus SASE

Partner
Certification Handbook

Table of Contents

Partner Portal

Purpose:

The partner portal dashboard will provide visibility into customers' relevant information & all data pertaining to your partnership with Timus Networks.

MSPs will leverage the Timus Networks partner portal as their primary dashboard for day to day management of the Timus solution. Within the portal, you will be able to add, remove & manage all clients for both billing and technical management.

Link to - partner portal

Downloads and Installations

Agent Deployment

The Agent Deployment screen allows you to access the latest versions of Timus Connect Application for all supported platforms.

See More >

Timus Connect App for Microsoft Windows® User Guide

Timus Connect for Windows secures devices with an encrypted tunnel to your corporate network.

See More >

Timus Connect App for macOS® User Guide

The Timus Connect for macOS application allows your users to establish a secure, encrypted tunnel between their devices and your corporate network.

See More >

Timus Connect App for Android™ User Guide

The Timus Connect for Android application allows your users to securely connect to your corporate network by establishing an encrypted tunnel to the Timus platform.

See More >

Timus Connect for iOS: User Guide

The Timus Connect for iOS application allows your users to securely connect to your corporate network by establishing an encrypted tunnel to the Timus platform.

See More >

Timus Connect App Management

This article explains how to download and install versions of the Timus Connect App that are suitable for different operating systems.

See More >

Timus Connect App for Microsoft Windows Silent Deployment Script

Run locally without RMM by bypassing execution policy.

See More >

Timus Connect App for MacOS Silent Deployment Script

Bash Script - Mac
Give execute permission with:
chmod +x /path/to/script.sh

See More >

Certificate Install Script for Microsoft Windows

This script is designed to automate the installation of a digital certificate into the "Trusted Root Certification Authorities" store on a local machine.

See More >

Timus Connect App for iOS User Guide

This document is a guide explaining the use of Timus Connect for iOS application.
This application secures your connection by establishing an encrypted tunnel to the Timus Platform.

See More >

User Management

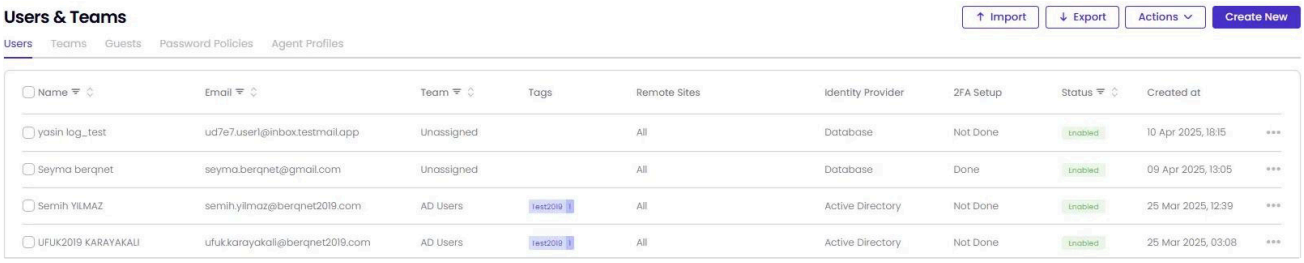
📍 To access this screen, go to Users & Teams → Users

Users:

The User Management screen provides complete visibility and control over all users in your organization. Whether you're onboarding new employees, enforcing security policies, or monitoring user activity, this screen helps you do it all—clearly, efficiently, and at scale.

1. The user list shows essential details for every user in your system:

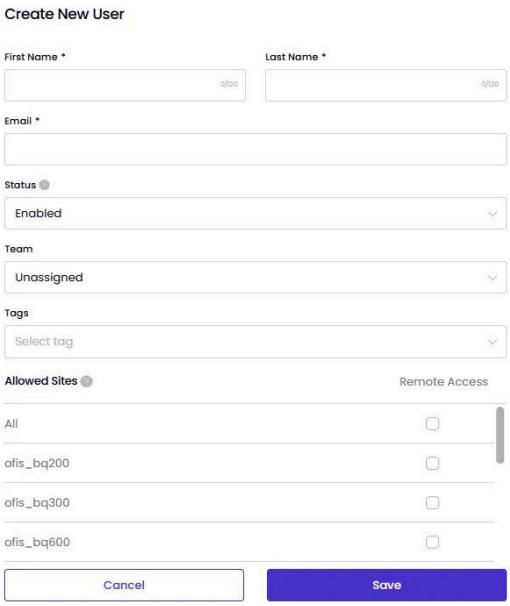
Column	Description
Username	Full name of the user
Email	User's email address
Team	eam membership; shows **Unassigned** if not assigned
Tags	Assigned static or dynamic tags
Remote Sites	Sites the user can access remotely
Identity Provider	Shows whether the user logs in via internal database or an external IdP
2FA Setup	Indicates whether two-factor authentication is configured
Status	Current status of the user
Created Date	Date when the user account was created



2. Create a New User

Click Create New to open the user creation form. You'll be asked to enter:

1. First Name (required)
2. Last Name (required)
3. Email Address (required)
4. Status (Enabled or Disabled)
5. Team (optional)
6. Tags (optional; supports static and dynamic)
7. Allowed Sites – Specify user accessible remote sites
   - Selecting All grants universal remote access.
   - If none are selected, remote access is blocked.



Click **Save** to create the user.

3. User Details

To view a user's activity and telemetry-based insights, click ••• and select Details.

Events

- Sign-ins, disconnections, and connection attempts
- Timestamp, device, network, and event type

Behavior Analysis

- Detected behaviors based on Sign-In Policy
- Helpful for spotting risk patterns or anomalies

Traffic

- Upload/download volume over time
- Adjustable via date picker

Productivity (if enabled)

If the user's Agent Profile has Productivity Tracker enabled:

- A time-based productivity graph
- Breakdown of time as Productive, Unproductive, or Neutral
- Table of app usage with durations and ratios

Want to see these insights?

Agent Profiles >

4. User Actions

From the ••• next to any user:

- View / Edit – Update user details
- Enable / Disable – Toggle account status
- Ban / Unban – Temporarily block login access
- Reset Password – Sends a reset email
- Drop Connection – Immediately disconnect the user. Does not prevent re-login unless the user is banned
- Reset 2FA – Clears two-factor setup
- Delete – Permanently deletes the account. Appears in reports as Deleted User (ID: {id})

5. Bulk Actions

You can select multiple users to apply actions in bulk:

- Edit Settings – Update team, tags, or site access
- Ban / Unban
- Reset Password
- Reset 2FA
- Drop Connection
- Delete Users

6. Import Users

Click Import to upload users via CSV (max 5MB)

Required Fields	Notes
First Name	Max 120 characters
Last Name	Max 120 characters
Email	Must be in valid format
Team	Optional – will auto-create if not found
Remote Sites	Optional – must match existing sites

You can **upload** up to **500 users** in a **single CSV.**

Separate multiple sites using commas: **HQ, Branch A, Branch B**

Imported users receive an automatic activation email.

7. Export Users

Click Export to download the current table view as a CSV file.

Applied filters and sorting are reflected in the export.

Productivity Tracker

📌 The feature must be activated in the **Agent Profiles** section to enable Productivity Tracker.

Purpose:

The **Productivity Tracker** is a core feature of Timus Manager that empowers organizations to monitor, analyze, and optimize workforce efficiency. This guide provides step-by-step instructions for managing and utilizing the Productivity Tracker, along with detailed insights into **Application Classification** and **Categorization**.

This feature allows you to monitor user activities on **Windows** and **macOS** systems through the **Timus Connect Application.** It categorizes application usage as **Productive, Unproductive**, or **Neutral** and provides actionable insights through intuitive reports.

Key Features:

- Automatic application **classification** using AI.
- **Customizable categorization** to align with organizational goals.
- Team-based application configuration for granular productivity analysis.
- Comprehensive reports for users, teams, and applications.

Enabling the Productivity Tracker

1. Navigate to **Users & Teams > Agent Profiles.**
2. Click on an existing **Agent Profile** or create a new one by selecting **Create New.**
3. Select the **Windows** or **macOS** tab.
4. Enable the toggle for Productivity tracker.

⚠️ Users assigned to this profile will automatically be monitored while signed into the **Timus Connect Application.**

Application Classification and Categorization

Applications are automatically classified into **Predefined Categories** and assigned a **Predefined Classification** by the system. You can:

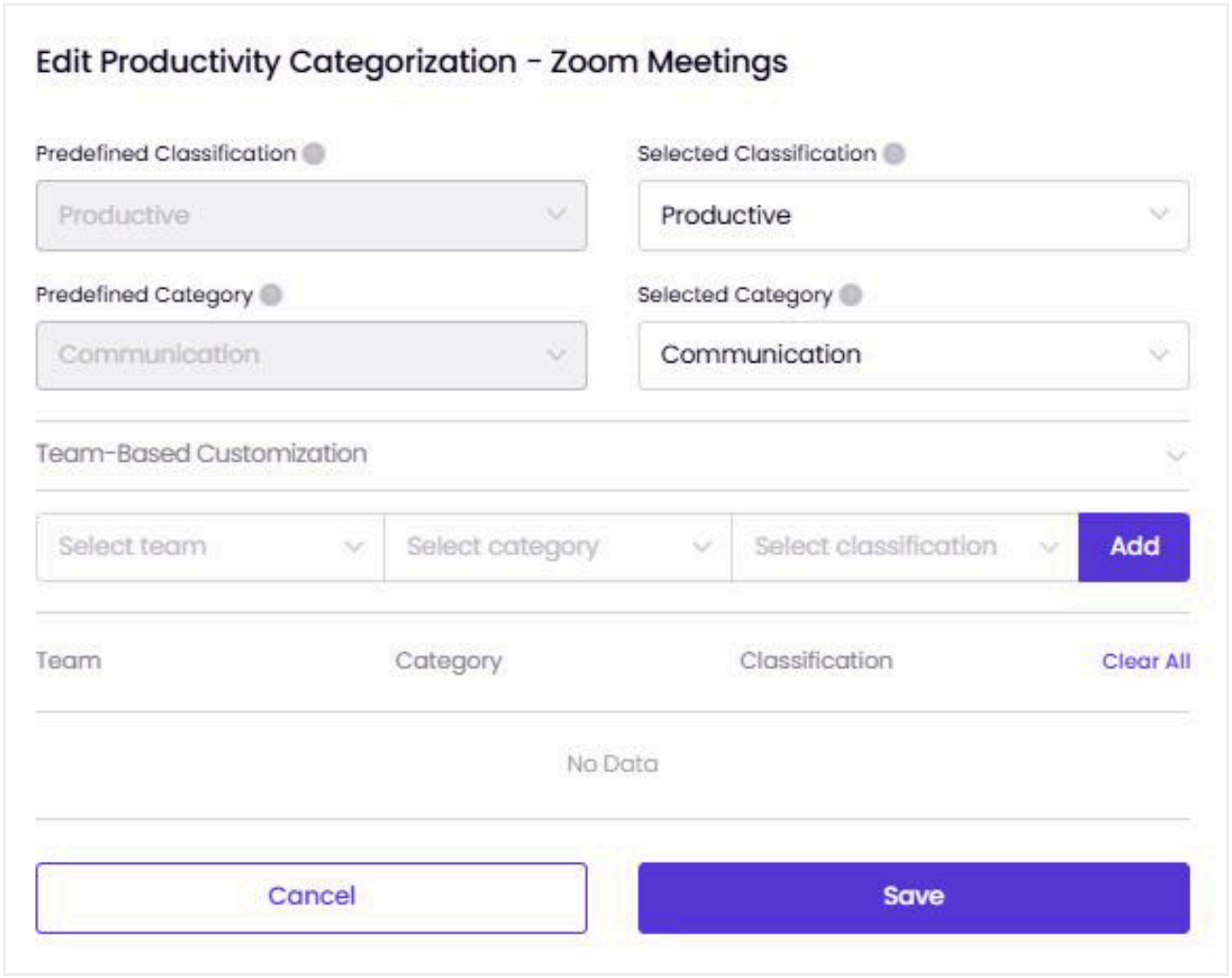
- Override predefined values by setting a **Selected Classification** or **Selected Category.**
- Customize configurations based on teams for more granular reporting.

Editing Application Details

1. Go to **Settings** > **Configurations** > **Productivity tab.**
2. Locate the application in the table and click **Edit**.
3. Update the following

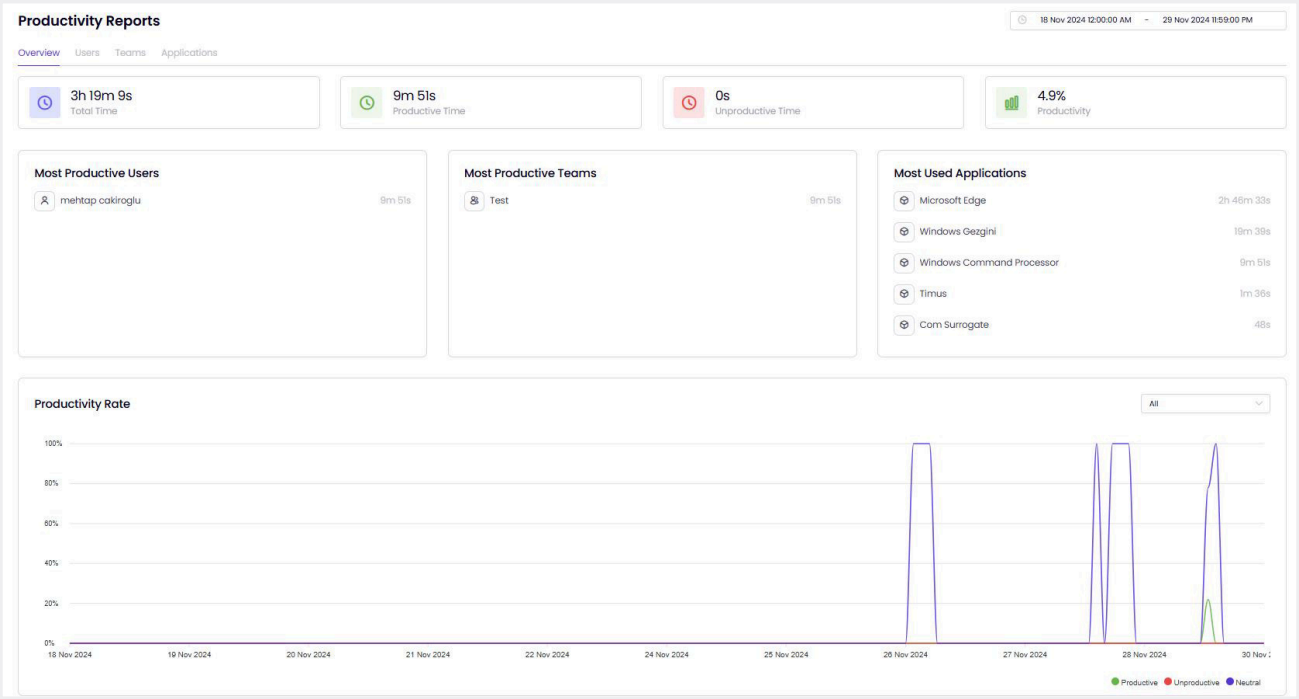
   - **Selected Classification:**
     -Choose between Productive, Neutral, or Unproductive.
   - **Selected Category:**
     - Reassign the application to an appropriate category.
   - **Team-Based Customization:**
     -Add team-specific configurations by selecting a team, category, and classification.

⚠ Changes will reflect in reports and productivity metrics across relevant users or teams.

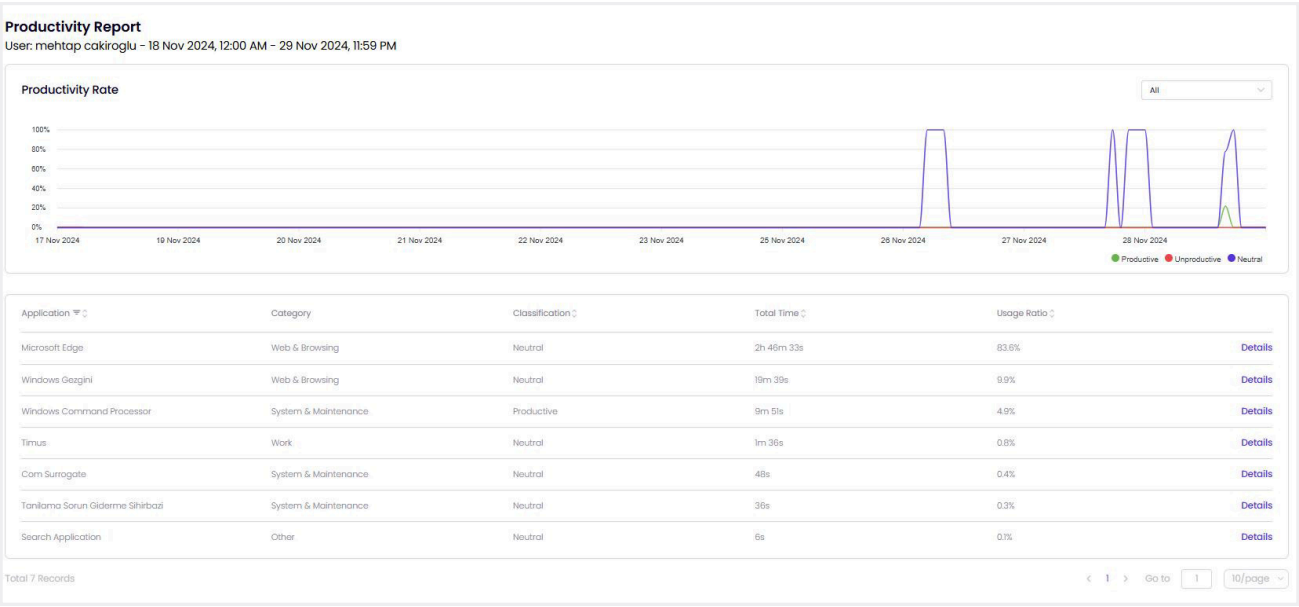


Accessing Productivity Reports

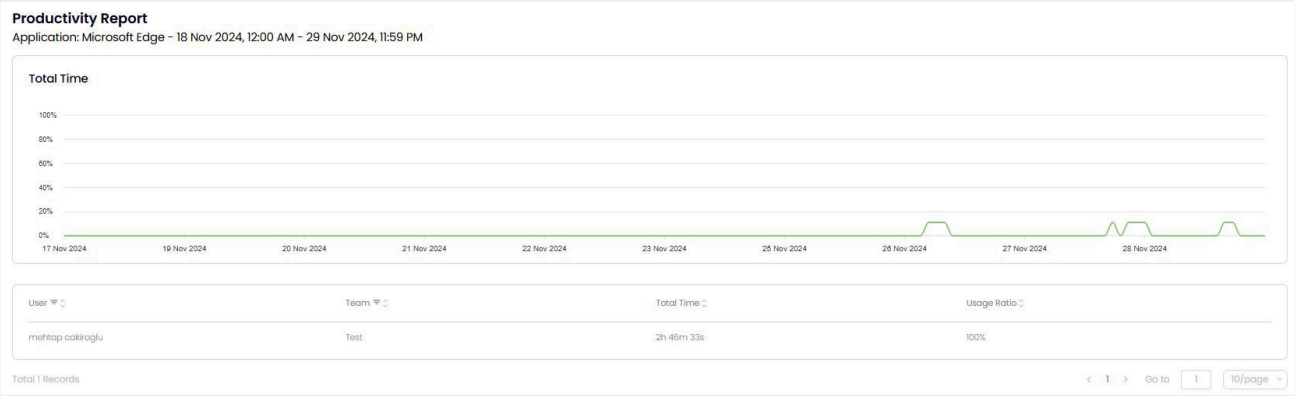
Productivity data can be reviewed in the **Insights > Productivity Reports** section. Reports are divided into the following tabs:



- **Overview:**
  -Displays total productivity metrics, top users, teams, and applications.
- **Users:**
  -Provides individual user activity and productivity rates.
  -View user reports, including active time, productivity breakdown, and application usage. Click **Details** for a deeper analysis.



- **Teams:**
  -Offers insights into team-level productivity trends.
  -Examine team-wide productivity, categorized by total productive and unproductive time.
- **Applications:**
  -Highlights application usage patterns and their impact on productivity.
  -Review application usage trends, categorized by predefined and selected values.



📌 Use the Export button to download reports in CSV format for further analysis.

Technical Considerations

1. **Windows Security Settings:**
   -Ensure **active-win-windows.exe** is whitelisted in Endpoint Protection Platforms (EPPs) to avoid interference.
2. **macOS Permissions:**
   -Grant **Full Disk Access, Accessibility,** and **Screen Recording** permissions to the Timus Connect Application for seamless tracking.

Administrators

Purpose:

Create new administrators, define their roles, assign these roles to the administrators, and establish new permissions/restrictions for existing roles.

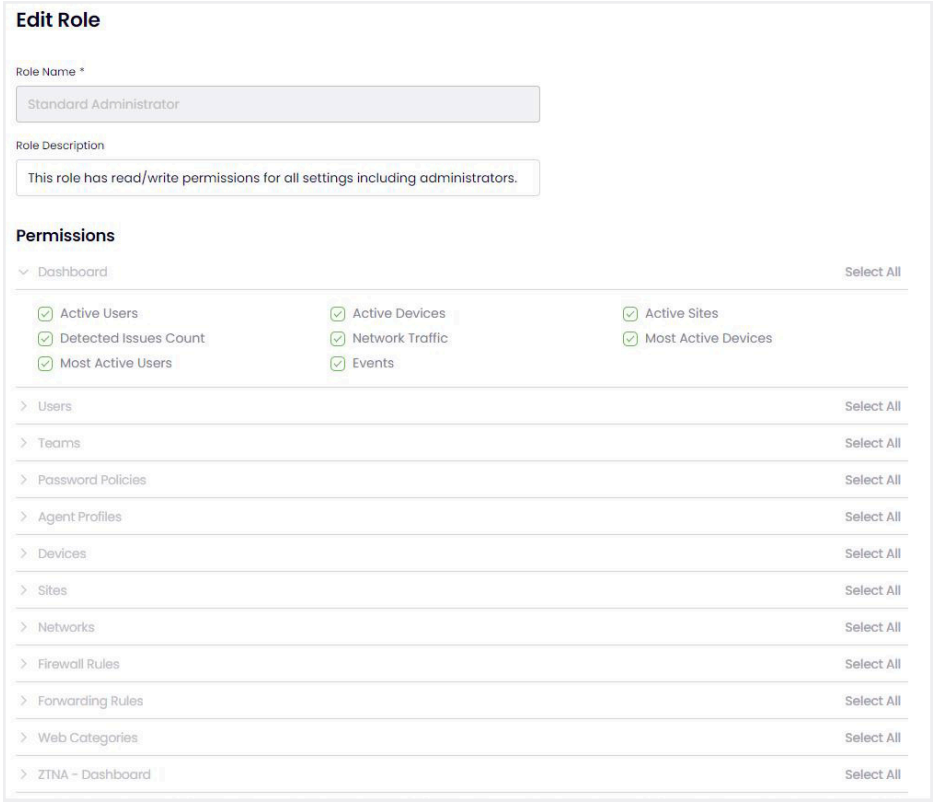
Roles and Permissions

Create a new role and configure the names and permissions of existing roles.

Follow these steps to create a new role:

1. Click the **Settings** tab.
2. Click **Administrators** then **Roles** and **Permissions**
3. Click on **Create Role** on the page that opens.
4. Enter a **Role Name** and a **Role Description.**
5. Choose from the Timus Manager **capabilities** for the role you are about to create.
6. Click **Confirm** at the end of the page.

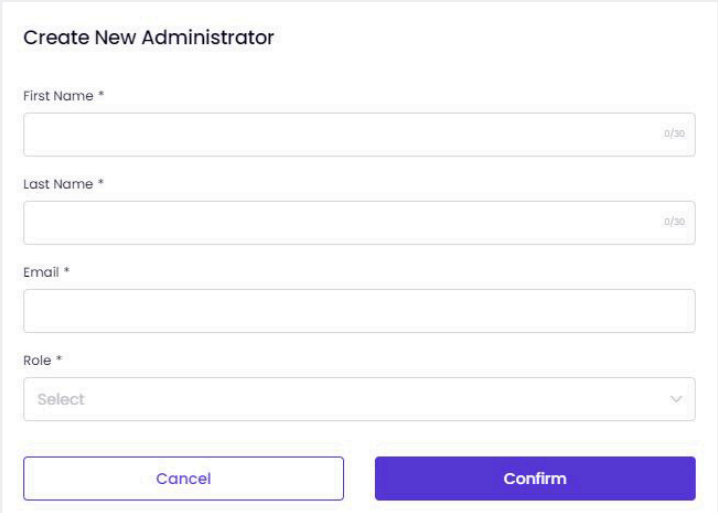
You can now view the role you created on the **Roles and Permissions page** and configure the role with **Edit** and **Delete** on the row where the role is located.



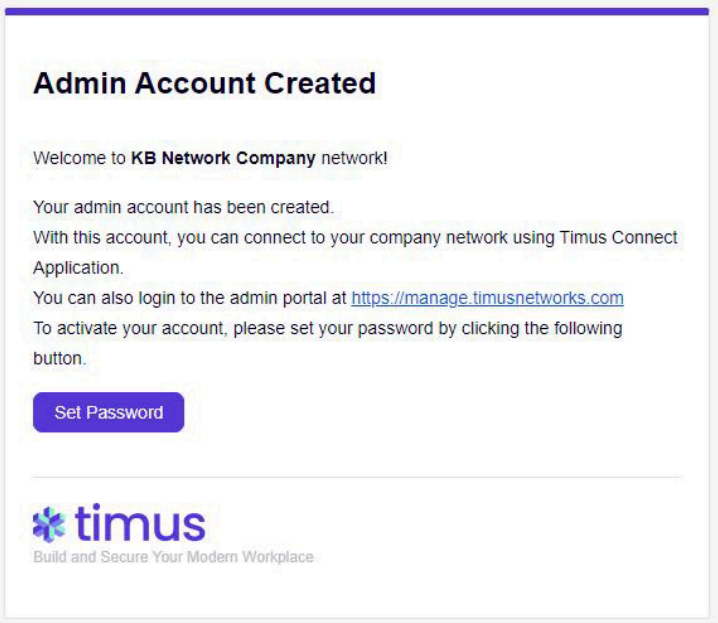
Use the **Create Administrator** button to create fully authorized **Administrators** for your company network.

Follow these steps to create a new role:

1. Click the **Create Administrator** button on the **Administrators** tab.
2. Enter the information requested from you.
3. Select **Role** for the administrator you are about to create.
4. Click **Confirm**.

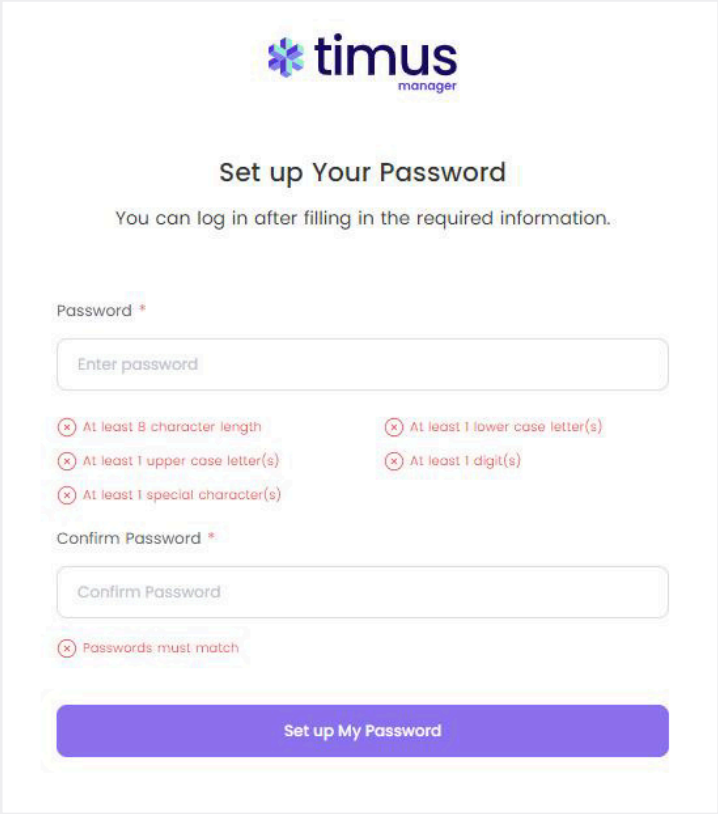


5. The created admin will be notified by email.

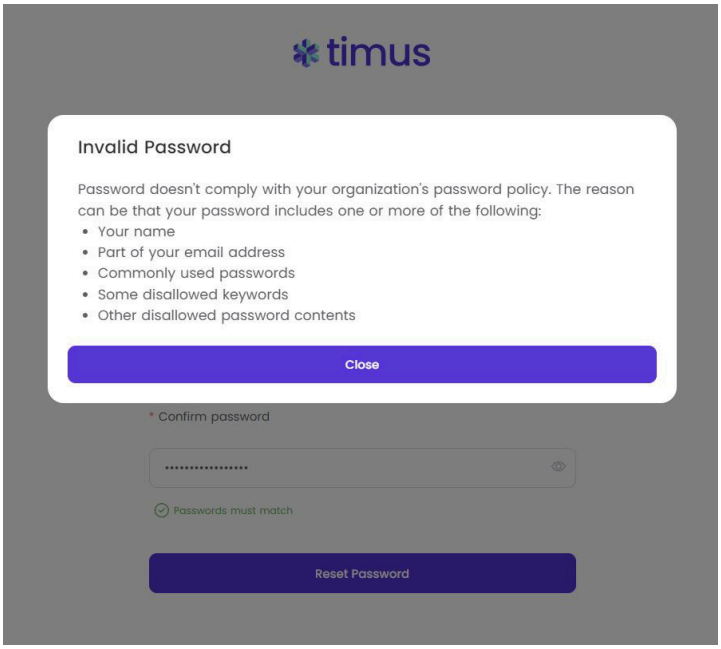


6. Once you click on Set Password, you will be forwarded to the page, which you can set your password.

7. On this page, you can set your password depending on Password Policies defined by the network admin.



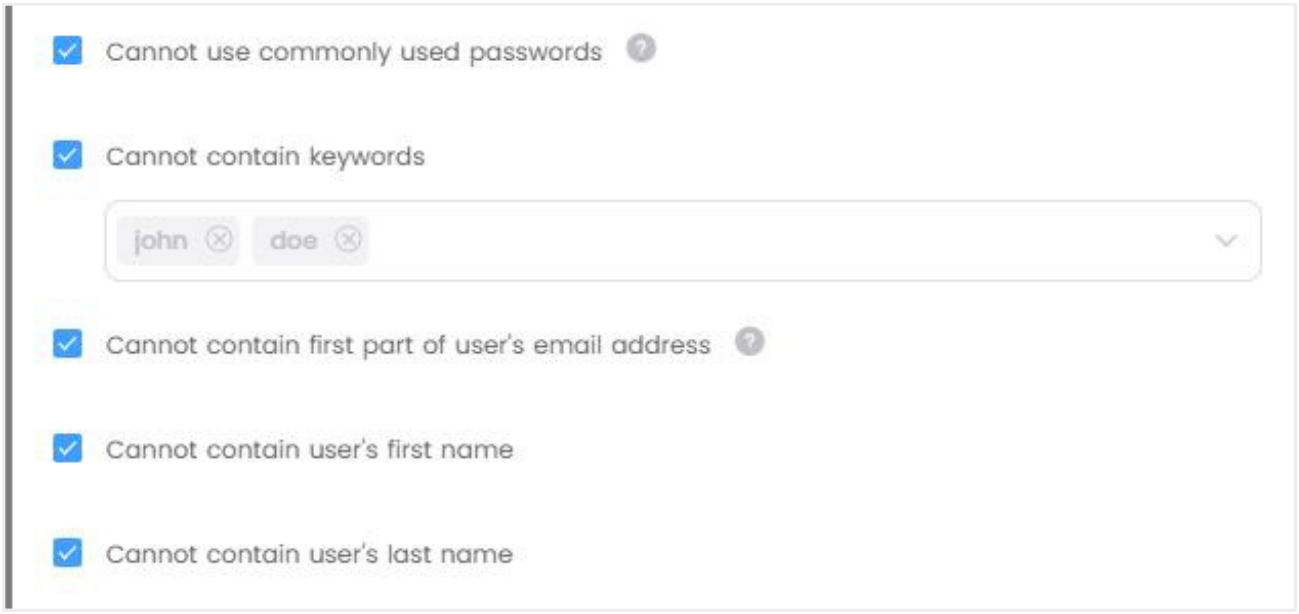
8. While setting or resetting your admin's password, you may see the pop-up as shown in the image below.



9. If you have seen the pop-up above while setting or resetting your admin's password, you need to check your password policies as shown in the image below. There 5 password policies, which can cause **Invalid Password** issue.

In this example, I have used "john" in my password. Therefore, I have seen Invalid Password pop-up on my screen.

You need to set your Password Policies, which totally depend on the network admins, for the users.



Audit Logs

View all changes made on your company network using Timus Manager.

On the **Audit Logs** tab,

1. You can **Search** the audit logs by using the search bar.
2. You can view the logs in a specific date range by selecting a **Date/ Time** range.
3. You can get detailed information about the old and new values of the modified components in your network.

Devices

Device Posture Checks

Device Posture Checks in Timus Manager let you enforce access policies based on the real-time security posture of user devices. This ensures that only healthy

See More >

Device Management (NEW)

The Devices screen provides full visibility into all endpoints connecting via Timus Connect. Whether users are on the internal network or working remotely,

See More >

Device Posture Checks

📍 To access this screen, go to **Zero Trust Security** → **Device Posture Checks** from the left-side menu

Purpose:

Device Posture Checks in **Timus Manager** let you enforce access policies based on the real-time security posture of user devices. This ensures that **only healthy, compliant, and trustworthy endpoints** are allowed to connect—regardless of whether the user has valid credentials.

As a core component of your **Zero Trust Security** architecture, posture checks shift access decisions from identity-based trust alone to **context-aware access,** incorporating endpoint risk into every session decision.

To use Device Posture Checks effectively, make sure your Endpoint Protection Platforms (EPPs) are properly integrated. Supported platforms include: Bitdefender, Heimdal, Microsoft Defender, and SentinelOne.

What Are Device Posture Checks?

Device Posture Checks allow you to define a set of required conditions a device must meet before access is granted. These conditions are evaluated using telemetry from the **Timus Connect agent** and **integrated EPPs.**

Examples of posture attributes include:

- Antivirus agent installed or signature updated
- Full disk encryption enabled
- Operating system version is within an allowed range
- No malware infections or unresolved detections reported by EPP
- Essential services and startup configurations are intact

Posture checks are continuously evaluated. If a device no longer meets the expected conditions, access can be dynamically revoked or downgraded using **User Sign-In Policies** and **Behaviors.**

Create a New Device Posture Check

Navigate to **Zero Trust Security → Device Posture Checks**. You'll see a list of existing posture checks. Click **Create New** to define a new one.

General Settings

Configure the high-level properties of the posture check:

- Antivirus agent installed or signature updated
- Full disk encryption enabled
- Operating system version is within an allowed range
- No malware infections or unresolved detections reported by EPP
- Essential services and startup configurations are intact

Posture checks are continuously evaluated. If a device no longer meets the expected conditions, access can be dynamically revoked or downgraded using **User Sign-In Policies** and **Behaviors.**

Field	Description
Title	Name of the posture check (required, max 30 characters)
Status	Enabled or Disabled
Description	Optional summary for internal reference (max 70 characters)
Assigned Operating System	Target OS for this posture check: Windows macOS Linux Windows Server iOS or Android

Each posture check is created per OS. After saving, you will proceed to define the logic using attributes.

Define Compliance Attributes

In the **Attributes** tab, you add one or more security conditions based on telemetry or EPP data.

Field	Description
Data Source	Where the data is coming from (Timus Connect or EPP)
Attribute	Security or system state to evaluate
Pass Value	Logical operator (e.g., is equal to is any of none of them)
Condition	Optional summary for internal reference (max 70 characters)

All attributes must be satisfied unless otherwise configured. For example, you can design posture checks that fail if any required value is missing (ideal for strict security teams).

Supported Data Sources by OS

Not all data sources are available on all operating systems:

OS	Timus Connect	Bitdefender	Heimdal	Microsoft Defender	SentinelOne
Windows	✅	✅	✅	✅	✅
macOS	✅	✅	✅	✅	✅
Windows Server	✅	✅	✅	✅	✅
Linux	❌	✅	✅	✅	✅
iOS	❌	✅	❌	✅	✅
Android	❌	✅	❌	✅	✅

Attribute Library (per Data Source)

Each data source exposes different posture elements:

🔷 Timus Connect

- Antivirus State
- Disk Encryption
- Firewall
- Operating System
- Running Processes
- Service State
- Startup Items
- Timus Connect Installed

🔷 Bitdefender

- Antivirus Agent Outdated
- Antivirus Agent Update Disabled
- Antivirus Agent Signature Outdated
- Antivirus Agent Signature Update Disabled
- Device Infected
- Malware Detected
- Disk Encryption
- Agent Installed
- Operating System
- Risk Score

🔷 Heimdal

- Detection Resolution
- Detection Status
- Vulnerable 3rd Party Software
- Probability of Infection
- Threat Severity
- Microsoft Update Severity
- Disk Encryption
- Operating System
- Risk Score

🔷 Microsoft Defender

- Antivirus Engine Mode
- Antivirus Engine Updated Mode
- Antivirus Platform Updated
- Antivirus Signature Updated
- Exposure Level
- Agent Installed
- Operating System
- Risk Score

🔷 SentinelOne

- Agent Installed
- Antivirus Agent Outdated
- Device Infected
- Disk Encryption
- Operating System

Monitoring & Reporting

Once deployed, each user device is evaluated at **sign-ins.** Failing devices are blocked or prompted with additional authentication steps depending on policies.

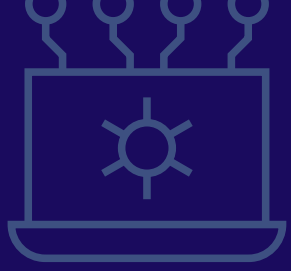
Logs and evaluation results are available under: **Insights → Device Posture Reports**

Go to Device Posture Reports

The device posture reports include:

- Summary of pass/fail rates
- Devices with repeated posture failures
- Top failing attributes
- Policy-level compliance trends

Integrations



SAML Integration for JumpCloud

This guide will walk you through the process of integrating JumpCloud with Timus using SAML 2.0 for secure Single Sign-On (SSO).

See More >

SAML 2.0 Integration

The SAML 2.0 Integration in Timus Manager allows you to configure secure, standards-based Single Sign-On (SSO) for users authenticating via identity providers such as Okta, JumpCloud, or Microsoft Entra ID.

See More >

Establishing an IPSec Tunnel Between Timus Networks and AWS

This article guides you through establishing a secure site-to-site IPSec tunnel connection between your Timus Network and an Amazon Web Services (AWS) Virtual Private Cloud (VPC).

See More >

Third-Party Integrations

The Settings → Integrations screen in Timus Manager provides a centralized interface to manage all available third-party integrations. These integrations extend Timus capabilities by synchronizing with identity providers.

See More >

Active Directory Integration

The Active Directory (AD) Integration in Timus Manager enables seamless synchronization of your on-premises AD users and groups with your cloud environment.

See More >

BitDefender Integration

The BitDefender Integration in Timus Manager allows you to retrieve real-time endpoint security data from your BitDefender GravityZone environment. This integration enhances your Device Posture Checks under Zero Trust Security.

See More >

Device Posture Check and EPP

This article explains the process of enabling EPP and Device Posture Check configurations on Timus Manager.

See More >

Google Sheets Integration

The Google Sheets Integration in Timus Manager allows you to automatically export user and device session data—such as sign-in and sign-out events—into a connected Google Sheet.

See More >

Google Workspace

The Google Workspace Integration in Timus Manager enables seamless synchronization of your Google Workspace users and groups into your cloud environment.

See More >

Heimdal Integration

The Heimdal Endpoint Protection Platform (EPP) integration allows Timus Manager to retrieve real-time security posture data from managed endpoints across your organization.

See More >

Microsoft Entra ID Integration

The Microsoft Entra ID Integration in Timus Manager allows you to synchronize users and groups from your Entra ID (formerly Azure Active Directory) environment into Timus.

See More >

Microsoft Defender Integration

The Microsoft Defender for Endpoint integration allows Timus Manager to collect real-time security telemetry from Defender-protected devices across your organization.

See More >

Okta Integration

The Okta Integration in Timus Manager allows you to synchronize users and groups from your Okta Directory.

See More >

Single Sign-On Integration with SAML Guide

SAML Integration for Microsoft Entra ID(Azure AD)
SAML Integration for Okta AD

See More >

SAML Integration for OKTA AD

This guide explains how to integrate Okta with Timus Manager using the SAML 2.0 protocol. Once configured, your users can securely sign in to Timus applications using their Okta accounts via Single Sign-On (SSO).

See More >

SAML Integration for Microsoft Entra ID (Azure AD)

Create a New Entra ID Application
Go to the Microsoft Entra Admin Center
Navigate to Microsoft Entra ID

See More >

SentinelOne Integration

The SentinelOne integration in Timus Manager allows you to retrieve real-time endpoint telemetry directly from your SentinelOne environment.

See More >

Slack Integration

The Slack Integration in Timus Manager allows you to receive real-time notifications about users, devices, security alerts, and other critical events directly in your Slack workspace.

See More >

Telegram Integration

The Telegram Integration in Timus Manager allows you to receive real-time alerts about users, devices, or system events directly in your personal Telegram account.

See More >

Zero Trust Security

View ZTNA Dashboard

This article explains how to access data on the ZTNA Dashboard and enhance productivity and security by leveraging all available information in zero trust scenarios.

See More >

Create Behavior

In Timus Manager, go to Zero Trust Security > Behaviors to add custom behaviors beyond ZTNA defaults for deeper risk assessments.

See More >

Manage Zero Trust Policies

Timus Zero Trust Policies provide user/behavior-based access control, replacing traditional IP-based methods and simplifying network access management.

See More >

Create an Administrator Sign-In Policy

This article shows administrator how to create Timus ZTNA's behavior-based administrator sign-in policies and apply them to your network.

See More >

Sites Networks

Cloud Gateways (NEW)

Cloud Gateway management has been completely reengineered in version 1.30.0—not just redesigned, but fundamentally rethought to align with real-world needs.

See More >

Tag Management

Purpose:

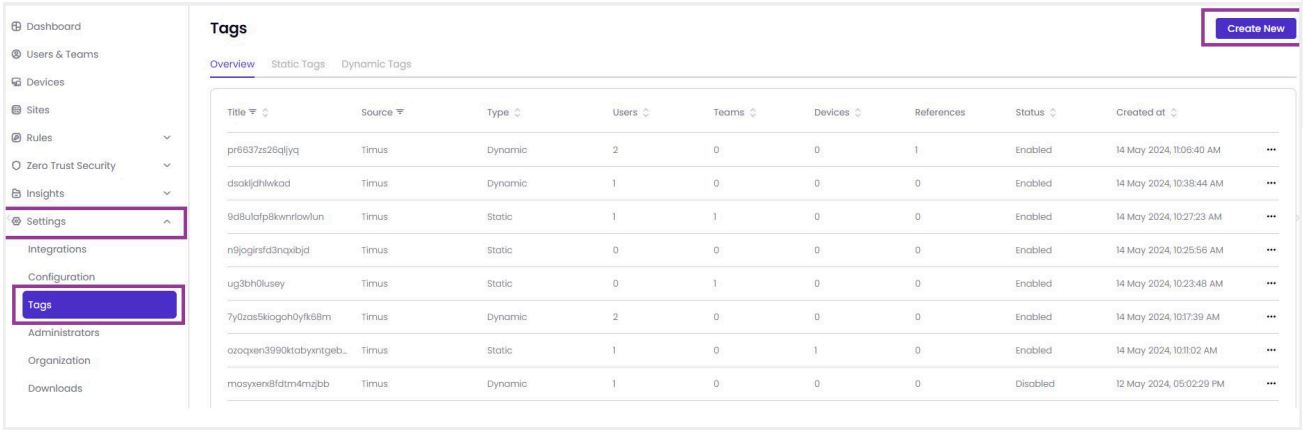
In this article, you will learn how to use and manage the Tag Management feature

To be able to go to the page Tag Management, you need to follow the **Timus Manager -> Settings -> Tags.**

Dynamic tags can be assigned to users and devices, and referenced in firewall rules, agent profiles, and sign-in policies. Their assignment is condition-based: tags remain applied as long as conditions are met and are removed when not. Administrators can edit tags anytime, including descriptions, objects, and references.

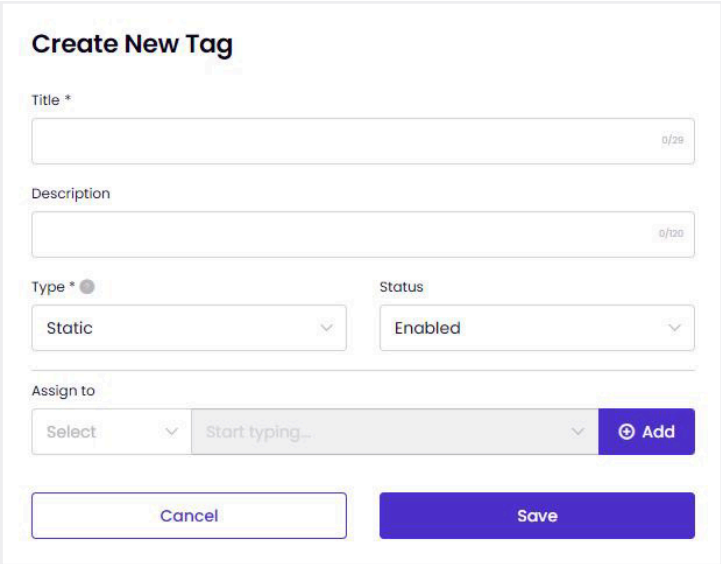
In ZTNA, dynamic tagging enables flexible, automated micro-segmentation. Tags automatically update firewall rules and policies, improving security and reducing manual work by dynamically adjusting access based on defined conditions.

You can click on Create New to create a new tag to manage or assign.



Column	Description
Source	This is where the tag is coming from.
Type	This is if it is a static tag or dynamic tag.
Users	This field will show how many users have been assigned to the Tag.
Teams	This field will show how many teams have been assigned to the Tag.
Devices	This field will show how many teams have been assigned to the Tag.
References	This field will show how many Firewall rules have been assigned to the Tag.

Once you click on **Create New**, you will be able to see the fields below and the Type is selected as **Static** by default. You can select either **Static** or **Dynamic**.



Static Tagging:

- **Title:** This field is required. You can name your Tag by using this field.
- **Description:** This field is not required.
- **Assign to:** You can select User, Team and Device here to assign the Tag, which you are creating.

Once you edit the **Static Tag(s),** you will be able to see where they have been used.

Dynamic Tagging:

You can assign either **Users** or **Devices.**

- Once you assign to **Users** and you select the **Type** as **User** under the **Condition**, you will be able to select the **Attribute** as **2FA Setup.** The **Operator** will be selected as "**is equal to**" and the Value will be selected as Done or Not Done. This data is fetched by the **Timus Manager** -> **Users & Teams** -> **Users.**
- Once you assign to **Users** and you select the **Type** as **Team** under the **Condition**, you will be able to select the **Attribute** as **Title**. The **Operator** will be selected as "**is equal to**" or "**is any of**" and the **Value** will be selected as the title(s) of the teams, which you have created. Plus, a quick reminder that some **Teams** are created automatically if there is an IdP like Microsoft Entra.
- Once you assign to **Users** and you select the **Type** as **Device** under the **Condition**, you will be able to select the **Attribute** as "**Timus Connect - Operating Systems**". The **Operator** will be selected as "**is equal to**" or "**is any of**" and the **Value** will be selected as **Windows, macOS, iOS or Android.**

- Once you assign to **Devices** and you select the **Type** as **Device Posture Check** under the **Condition**, you will be able to select the **Attribute** as follows:

BitDefender	Agent Outdated
BitDefender	Agent Product Update Disabled
BitDefender	Antivirus Agent Signature Update Disabled
BitDefender	Antivirus Agent Signature Outdated
BitDefender	Device Infected
BitDefender	Malware Detected
BitDefender	Disc Encryption
BitDefender	Risk Score
BitDefender	Agent Installed
BitDefender	Operating System
Microsoft Defender	Antivirus Engine Updated
Microsoft Defender	Antivirus Platform Updated
Microsoft Defender	Antivirus Signature Updated
Microsoft Defender	Risk Score
Microsoft Defender	Exposure Level
Microsoft Defender	Antivirus Mode
Microsoft Defender	Agent Installed
Microsoft Defender	Operating System
SentinelOne	Agent Outdated
SentinelOne	Device Infected
SentinelOne	Disc Encryption
SentinelOne	Agent Installed
SentinelOne	Operating System

The **Operator** will be selected as "**is equal to**" or "**is any of**" and the **Value** will be selected as **follows:**

- Other
- Active
- Passive
- Disabled
- EDRBlocked
- PassiveAudit

- Once you assign to **Devices** and you select the **Type** as **Team** under the **Condition**, you will be able to select the **Attribute** as **Title**. The **Operator** will be selected as "**is equal to**" or "**is any of**" and the **Value** will be selected as the title(s) of the teams, which you have created. Plus, a quick reminder that some **Teams** are created automatically if there is an IdP like Microsoft Entra.
- Once you assign to **Devices** and you select the **Type** as **Device** under the **Condition**, you will be able to select the **Attribute** as "**Timus Connect - Operating Systems**". The **Operator** will be selected as "**is equal to**" or "**is any of**" and the **Value** will be selected as **Windows, macOS, iOS** or **Android.**
- Conditional Tag Assignment: Unlike static tags which are manually assigned and remain constant, dynamic tags are assigned based on predefined conditions. Various attributes of the tagged entities are checked to assess whether these conditions are met. Examples of such attributes could be:
- Device attributes: Operating system type (Windows, macOS, etc.), Team and Device Posture Check attributes
- User attributes: 2FA Setup, Team, and Operating system type (Windows, macOS, etc.)
- Continuous Evaluation: Timus employs a continuous evaluation that constantly monitors the assets against the predefined conditions associated with dynamic tags. This ensures that the tags accurately reflect the current state of the assets.

Benefits of Dynamic Tagging:

- Automated Access Control: Dynamic tags automate access control decisions based on real-time asset conditions. This eliminates the need for manual configuration changes and reduces the risk of human error.
- Micro-segmentation: By dynamically assigning tags based on granular asset attributes, Timus facilitates micro-segmentation of the network. This allows for more precise control over user and device access to specific resources.
- Enhanced Security: The continuous evaluation and dynamic adjustment of access controls based on asset conditions strengthens the overall security posture of the network.

Conceptual usage scenarios:

1- Device attribute-based segmentation:

- Automated Access Control: Dynamic tags automate access control decisions based on real-time asset conditions. This eliminates the need for manual configuration changes and reduces the risk of human error.
- Micro-segmentation: By dynamically assigning tags based on granular asset attributes, Timus facilitates micro-segmentation of the network. This allows for more precise control over user and device access to specific resources.
- Enhanced Security: The continuous evaluation and dynamic adjustment of access controls based on asset conditions strengthens the overall security posture of the network.

2- User behavior-based segmentation:

- **Scenario**: An organization wants to segment its network based on user behavior to mitigate the risk of insider threats.
- **Implementation:** Dynamic tagging evaluates user behavior such as authentication patterns, access frequency, and file usage
- **Outcome:** By dynamically assigning tags based on user behavior, the organization can create micro-segments of users with similar behavior profiles. This enables the implementation of access controls and monitoring mechanisms tailored to the risk profile of each user segment.

3- Access privilege-based segmentation:

- **Scenario:** A healthcare provider needs to segment its network based on user access privileges to protect sensitive patient data.
- **Implementation:** Dynamic tagging evaluates user roles, permissions, and access levels within the organization's systems and applications.
- **Outcome:** By dynamically assigning tags based on access privileges, the organization can create micro-segments for different user roles (e.g. physicians, nurses, administrative staff). This enables the implementation of role-based access control (RBAC) and ensures that users only have access to the resources required for their role.

Example scenario:

Leveraging Device Posture Check Conditions:

- Scenario: An organization seeks to enforce security policies based on the risk status of devices seeking access to the network.
- Dynamic Tagging Implementation:
  - Criteria: Device attribute: “Bitdefender - Risk Score”
  - Condition: If the Risk score is "High
  - Tag Title: "Risky Device"
  - Outcome: Devices with a high-risk status are automatically tagged with the 'Risky Device' tag, triggering actions such as network quarantine or remediation. This action may include the application of predefined firewall rules that restrict the device's access to network resources to effectively mitigate potential threats.

Real-world use cases:

Healthcare Sector:

- Scenario: A hospital leverages dynamic tagging to segment its network based on user roles and patient data access requirements.
- Outcome: Granular access controls ensure that only authorized healthcare professionals can access patient records, mitigating the risk of data breaches and ensuring compliance with healthcare regulations.

Financial Services Industry:

- Scenario: A financial institution employs dynamic tagging to segment its network according to user privileges and transaction types.
- Outcome: By dynamically adjusting access privileges based on transaction risk levels, the organization fortifies its security posture and safeguards sensitive financial data from unauthorized access or fraudulent activities.

Educational Institutions:

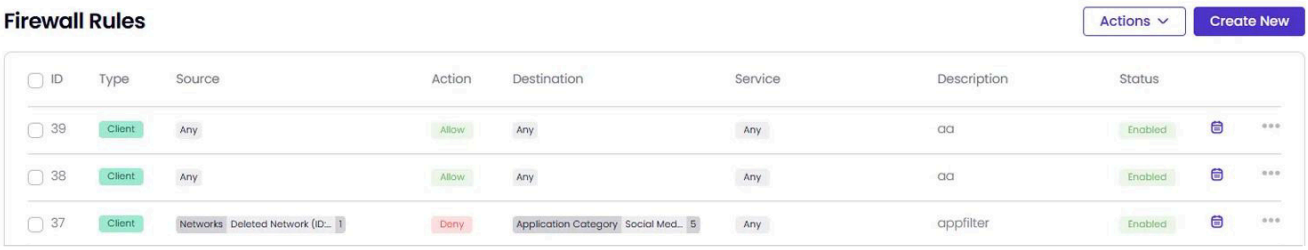
- Scenario: A university utilizes dynamic tagging to segment its network based on student, faculty, and administrative roles.
- Outcome: Micro-segmentation facilitated by dynamic tagging enables the university to enforce role-based access controls, ensuring that academic resources are accessed only by authorized users while minimizing the risk of data breaches or cyberattacks targeting sensitive research data.

Firewall Rules

📍 To access this screen, go to Rules → Firewall

Purpose:

Define how your organization handles network traffic by allowing or denying it based on source, destination, service, and schedule. Rules are evaluated **top-to-bottom;** the first match applies. Reorder by drag-and-drop.



1. Firewall Rules Table – Column Reference

Column	Description
ID	Unique identifier assigned to each rule
Type	Indicates whether the rule is created by your team **Client** or delivered by your partner as a security baseline **Global**
Source	Defines the traffic origin (e.g., IP, User, Device, Tag, or Interface)
Action	Choose to Allow or Deny traffic
Destination	Defines the target (e.g., IP, Application, Website Category)
Service	The type of traffic or protocol (e.g., HTTP, DNS, or a custom service)
Description	Short label explaining the rule's purpose
Status	Current status of the rule

2. Creating a Firewall Rule

Steps:

1. Go to Rules → Firewall.
2. Click **Create New.**
3. Complete the required fields:

Field	Description
Description	(Required) A meaningful name for identifying the rule
Action	(Required) Choose whether to Allow or Deny matching traffic
Status	(Required) Enable or disable the rule upon creation
Sources	Default is Any. You may specify multiple entries, including: Network, Site, IP, Location, User, Team, Device, Tag, or Interface (with Gateway 14.0.0)
Destinations	Default is Any. You may specify: Network, Interface (with Gateway 14.0.0), Site, IP, Location, Website Category, Application, Application Category, User, Team, Device, Tag, or Keywords
Services	Select from predefined or custom service definitions
Custom Source	(Optional) Define a specific port range if necessary
Clear Sessions	Forcefully end current sessions that match this rule's source, ensuring immediate enforcement
Enable Logging	Log matching traffic in Network Activity → Firewall
Schedule	Apply the rule only during specific hours or days (default: Everyday)

Once saved, the rule is added to the table and takes effect immediately—according to its position in the list.

💡 **Tip: Rule effect is instant once saved.**

3. Managing Rules

Rule Actions

Per Rule Actions (••• menu):

- View / Edit – Review or update the rule configuration
- Enable/Disable – Temporarily toggle the rule's active status
- Clear Sessions – Instantly drop all sessions affected by the rule
- Delete – Permanently remove the rule. Appears in records as Deleted Firewall Rule (ID: {id})

Bulk Actions

You can select multiple rules and use the Actions menu to:

1. Enable/Disable – Temporarily toggle the selected rules' active statuses
2. Clear Sessions – Instantly drop all sessions affected by the selected rules
3. Delete – Permanently remove the selected rules. Appear in records as Deleted Firewall Rule (ID: {id})

4. What's New – Global Policies

Global Policies

The Type column indicates whether a rule is created by you **Client** or pushed by your partner as part of a managed security baseline **Global** This enables consistent enforcement of critical protections across environments, while maintaining flexibility.

Type	What it means
Client	Fully editable rules created in your own portal
Global	Non-editable rules delivered by your security provider or partner

Why Global Policies?

Global rules are designed to help standardize and strengthen network security across all managed tenants—particularly useful for:

- MSP environments
- New customers needing out-of-the-box protections
- Preventing configuration gaps in high-risk areas

You can:

- Reorder **Global** rules to adjust their evaluation priority
- Enable or disable them as needed to fit your context

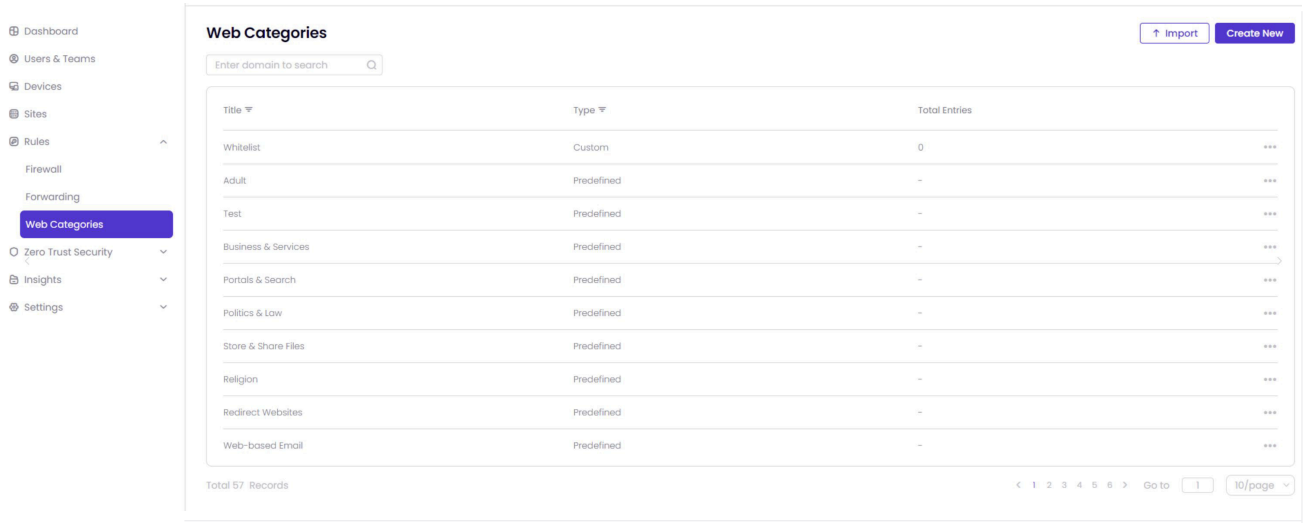
> They **do not override** your own rules—they simply provide a secure starting point.

Web Categories and Rules

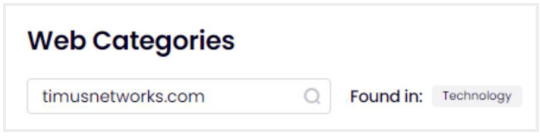
Purpose:

This article explains the process of creating firewall rules for a website or categories of websites. Furthermore, it explains you more details about the name of the categories and their descriptions in detail.

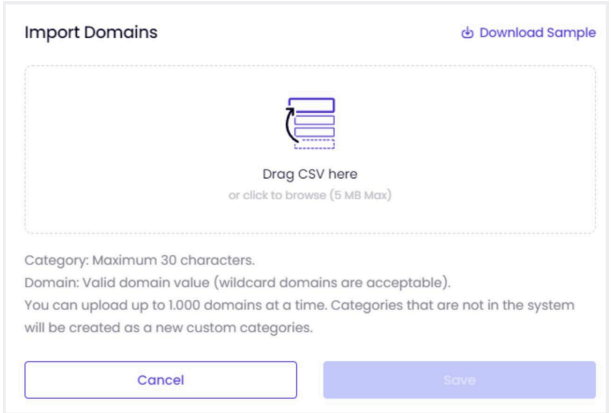
To be able to manage and use the Web Categories, you need to go to the page the **Timus Manager -> Rules -> Web Categories.**

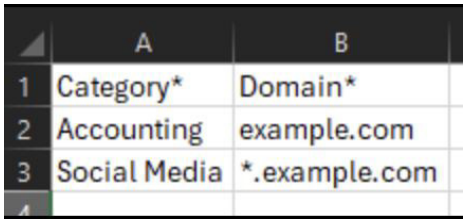


- If you want to look up the domain, you can use the search bar to enter a domain to search as shown in the image below.

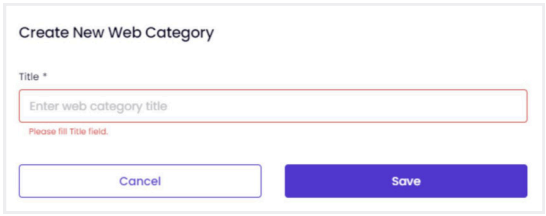


- We support **Import** functionality for the domain entries with a csv file, you can click on **Import** to be able to add the domains faster as shown in the image below. You can click on **Download Sample** and you can add your domains accordingly.



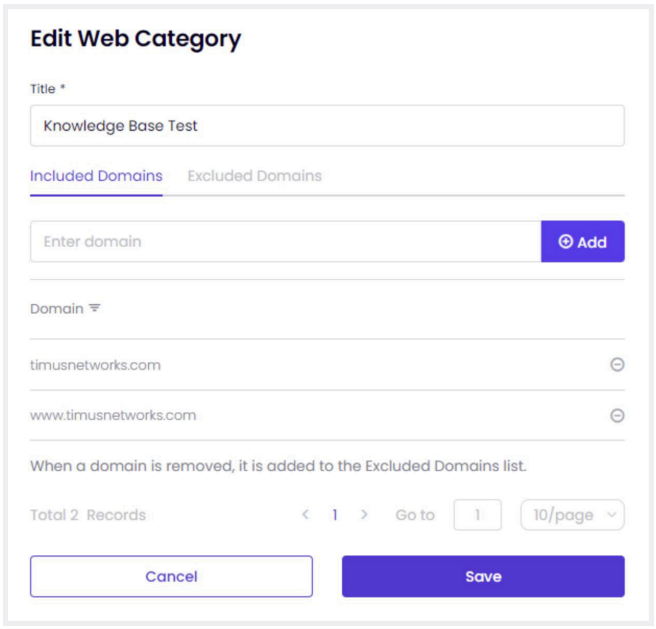


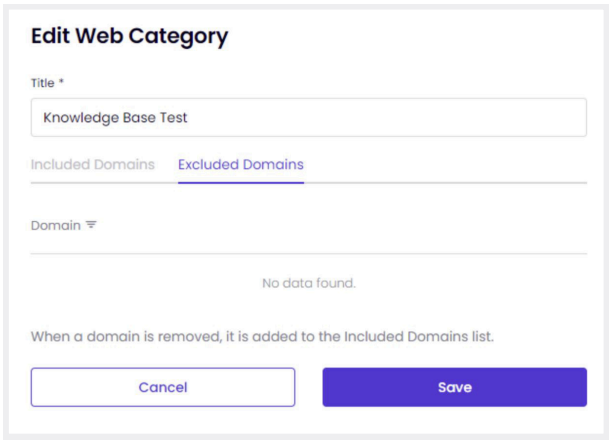
- You can either customize a web category by clicking on Create New or use the pre-defined categories as shown in the image below.



- As an example, here is a new created category called Knowledge Base and there are 2 domains www.timusnetworks.com and timusnetworks.com in it.

- You can either Include the domains or exclude the domains by editing the web category. Please note that you are not allowed to edit or delete the predefined web categories.





Adult

The "Adult" category includes web pages with sexual acts, explicit nudity, or sexual intent; frequent or serious profanity; child-oriented content with sexually themed sections; sex-related products or services without nudity; and tasteless or inappropriate material (e.g., animal cruelty, bathroom humor).

Alcohol

The "Alcohol" category covers web pages that promote, sell, or provide information on alcoholic beverages (beer, wine, liquor), including brands, events, production, distribution, consumption, and online or in-store purchase options.

Anonymizers

The "Anonymizers" category includes web pages offering proxies or tools that enable anonymous browsing, conceal user identity/location, bypass filters, and evade online restrictions.

Banking

The "Banking" category encompasses web pages operated by or dedicated to banks and credit unions, with a specific focus on online banking applications. This category excludes online brokerages, concentrating on financial institutions providing services related to traditional and digital banking, including account management, transactions, and financial services.

Business & Services

The "Business & Services" category covers a broad range of commercial and service-related content, including real estate, agriculture, construction, genetics, biotechnology, manufacturing, insurance, security (non-computer), retirement homes, inventory management, furniture, retail, and marketing/advertising services. It serves as a general category for businesses not fitting into more specific classifications.

Chat

The "Chat" category includes web pages and software for real-time communication, such as chat rooms, instant messaging, and buddy lists, enabling both group and one-on-one conversations in public or private settings.

Content Servers

The "Content Servers" category includes servers that host images and media files rather than full web pages, often used in CDNs to improve site performance, scalability, and faster content delivery.

Criminal Activities

The "Criminal Activities" category covers web pages promoting hate, discrimination, or extremist ideologies; illegal drugs and prescription misuse; child abuse; illegal acts such as burglary, murder, bomb-making, or fraud; tools for online crime or unauthorized access; marijuana-related content; pirated media and software; and sites aiding in cheating.

Culture & Arts

The "Culture & Arts" category includes web pages showcasing visual arts (paintings, sculptures, and more) and published writings such as novels, poems, biographies, and other literary works.

Dating

The "Dating" category includes web pages and platforms that promote relationships, offering profiles, matchmaking, communication tools, dating advice, and tips for building romantic or long-term partnerships.

Education

The "Education" category includes web pages for schools, universities, and educational institutions, as well as academic publications, research, curricula, online courses, and reference materials (e.g., encyclopedias, dictionaries, atlases, census data).

Entertainment

The "Entertainment" category includes web pages for humor (comics, jokes), music and media (streaming, downloads, bands), animated shows, movies, comics, celebrity news, and entertainment venues (clubs, theaters, festivals). It also covers TV/movie content such as reviews, showtimes, teasers, and discussions.

Environment

The "Environment" category encompasses web pages dedicated to fostering awareness and understanding of environmental issues. These pages provide information on various aspects of sustainability, including sustainable living practices and initiatives. Additionally, the category covers content related to ecology, delving into the study of ecosystems, biodiversity, and the interactions between organisms and their environments. Furthermore, these web pages offer insights into nature and the environment, sharing knowledge on topics like wildlife conservation, natural habitats, and environmental conservation efforts. By compiling information on environmental

Logs and Reports

Alerts

The Alerts screen offers a real-time overview of important security events across your environment.

See More >

Events

The Events screen provides a comprehensive audit trail of identity-based activities across your environment.

See More >

Automated Reports

The Automated Reports feature helps you track key metrics across your network by generating scheduled, customizable reports.

See More >

Device Posture Reports

The Insights → Device Posture Reports screen helps you monitor the effectiveness of your device posture enforcement policies.

See More >

Productivity Reports

The Insights → Productivity Reports screen provides a powerful lens into how time and digital tools are used across your organization.

See More >

Network Activity

The Network Activity screen provides a real-time view of all traffic events in your environment—both allowed and blocked.

See More >

User Traffic

The User Traffic screen offers a comprehensive view of user-related traffic across your network.

See More >

Teams Traffic

The Teams Traffic screen helps you analyze how traffic is distributed across teams in your organization.

See More >

Device Traffic

The Devices Traffic screen offers a device-level view of network traffic across your organization.

See More >

Application Traffic

The Applications screen gives you deep visibility into how applications are being used across your network.

See More >

View Traffic Logs

This article provides instructions on how to view traffic logs, an important step in troubleshooting agent and network-related issues.

See More >

Website Traffic

The Insights → Network Activity → Websites screen provides visibility into the most accessed websites across your organization.

See More >

View Blocked IP Addresses

To review blocked IP addresses in your Timus network, navigate to Timus Manager > Insights > Blocked IP Addresses.

See More >

View User Activity

View user activity from the Users & Teams page by clicking the ellipsis next to a user.

See More >

View Active Devices

This article explains how administrators can easily monitor active devices connected to the Timus network.

See More >

View IPsec Logs

This article provides instructions on how to view IPsec logs to troubleshoot IPsec site-to-site tunnels.

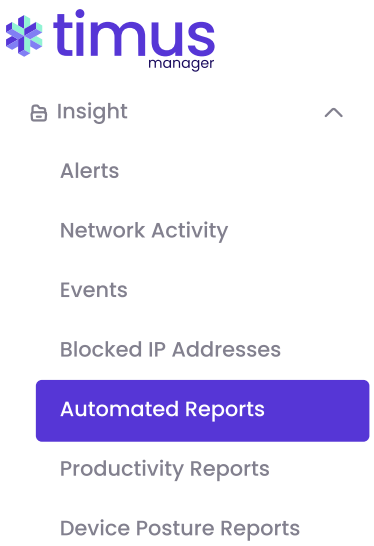
See More >

Automated Reports

📍 To access this screen, go to Insights → Automated Reportsz

The Automated Reports feature helps you track key metrics across your network by generating scheduled, customizable reports. Using templates and flexible scheduling options, you can automatically deliver reports that highlight user activity, bandwidth usage, threat patterns, and more—directly to the right recipients via email.

With Automated Reports, you don't need to build reports from scratch every time. You save time, reduce manual effort, and keep your team informed with clear, consistent insights—automatically.



1. Manage Report Templates

Templates define the structure and content of your reports. Before you can generate any reports, you need to set up at least one template.

- Go to **Insights → Automated Reports.**
- Click the **Manage Templates** in the top right corner.

Templates are organized into two types:

1. **Predefined Templates** – Ready-to-use templates provided by the system.
2. **Custom Templates** – Templates you create and configure based on your reporting needs.

Each template includes **widgets** which are visual or tabular components used to present data in the report.

2. Create a New Custom Template

To build a custom report layout:

1. In the **Manage Templates** screen, click **Create Custom Template.**
2. Enter a title and click **Create**.
3. On the template screen, click **Add Widget** to start adding data blocks.
4. Select the widgets you want to include and click **Add**.
5. Use drag-and-drop to arrange the widgets as desired.

To customize a widget:

1. Click **Configure**.
2. Choose a **Data Range Type:**
   - **Relative** (e.g., last 7 days)
   - **Fixed** (specific start and end dates)
3. Choose how data should be grouped: **Daily, Weekly, Monthly,** or **Yearly**
4. You can edit any template later by clicking the ••• → **Edit** option.

3. Create a New Report

After preparing your template, follow these steps to create a report:

1. Return to the **Automated Reports** screen.
2. Click **Create Report**, or use the ••• next to a template and select **Create Report.**
3. Enter a report title.
4. Choose the **Report Type:**
   - **On Demand** – Manually generated when needed.
   - **Scheduled** – Automatically generated and delivered on a schedule.
5. Select the **Template** you want to use.
6. In the **Recipients** section, add the email addresses of people who should receive the report.
7. Click **Save** to create the report.

To generate a report manually:

- Click the **Actions** button in the upper-right corner and select **Generate Report.**
- Click the link in the success message to view the report in your browser.

If you added recipients, the report will also be delivered to their email inboxes.

timus SASE

Timus Networks Study Guide

Thank you for learning with Timus Networks — your journey to certification starts here.

Need Help?

www.support.timusnetworks.com

support@timusnetworks.com

www.timusnetworks.com