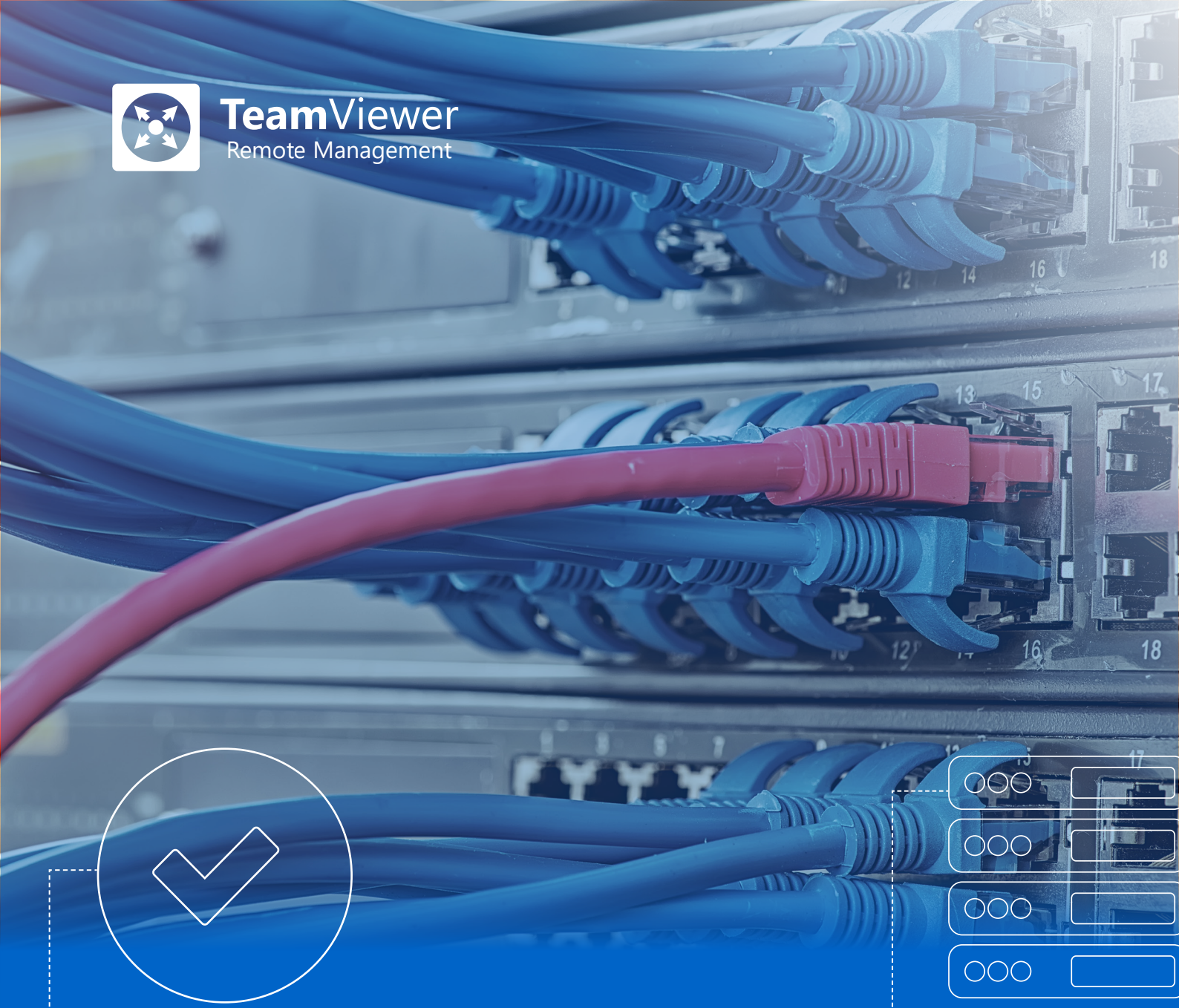


TeamViewer
Remote Management

TeamViewer Remote Management
Benutzerhandbuch

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

August 2020

Table of Contents

1. Allgemein

1.1 About the User Guide

Dieses Benutzerhandbuch beschreibt die Arbeit mit dem Fernverwaltungstool von TeamViewer. Sofern nicht anders angegeben, beziehen sich die beschriebenen Funktionalitäten immer auf die TeamViewer-Vollversion für Microsoft Windows. Mac OS, iPhone und iPad sind Warenzeichen von Apple Inc. Linux® ist ein eingetragenes Warenzeichen von Linus Torvalds in den USA und anderen Ländern. Android ist ein eingetragenes Warenzeichen von Google Inc. Windows und Microsoft sind eingetragene Warenzeichen der Microsoft Corporation in den USA und anderen Ländern. Der Einfachheit halber werden die Betriebssysteme Microsoft® Windows® XP, Microsoft® Windows® Vista, Microsoft® Windows® 7, Microsoft® Windows® 8 und Microsoft® Windows® 10 in diesem Handbuch einfach als "Windows" bezeichnet. Eine Liste aller unterstützten Betriebssysteme finden Sie auf unserer Website oder auf unserer Community Seite.

1.2 Über das Benutzerhandbuch

TeamViewer Remote Management ist eine professionelle und effiziente IT-Verwaltungsplattform, die in ein sicheres Tool für den Remote-Desktop-Zugriff integriert und vollständig auf die Bedürfnisse Ihres Unternehmens zugeschnitten ist. Die Plattform dient dem Schutz und der Fernüberwachung von Geräten, der Verfolgung von IT-Assets und/oder der Speicherung der Daten in einem sicheren Cloud-Backup. Um diese Ziele zu erreichen, bietet TeamViewer Remote Management die folgenden Dienste, die auf der TeamViewer Management Console und auf dem TeamViewer Client verfügbar sind:

TeamViewer Monitoring & Asset Management

TeamViewer Endpoint Protection

TeamViewer Backup

TeamViewer Web Monitoring

Mit TeamViewer Remote Management behalten Sie den Überblick über alle wichtigen Informationen und Funktionen Ihres Systems und Ihrer IT-Infrastruktur.

1. Mit **TeamViewer Monitoring & Asset Management** können Sie Ihre Geräte proaktiv überwachen und individuelle Prüfungen einrichten, um Benachrichtigungen z.B. über den Zustand der Festplatte, Antiviren-Software, Online-Status, RAM-Nutzung und laufende Prozesse auf einem Computer zu erhalten. Mit der integrierten Asset-Management-Funktion können Sie außerdem Ihre eingesetzten Geräte verfolgen und IT-Bestandsberichte für Ihr Netzwerk erstellen. Verwalten Sie alle Ihre Geräte bequem über die TeamViewer Management Console oder Ihren TeamViewer Client und erhalten Sie direkte E-Mail-Benachrichtigungen.

2. Mit **TeamViewer Endpoint Protection** können Sie Ihre Computer sauber und sicher halten. Endpoint Protection schützt Ihre Geräte rund um die Uhr vor Bedrohungen wie Viren, Trojanern, Rootkits und Spyware - egal ob on- oder offline. Endpoint Protection scannt Ihre Geräte in regelmäßigen Abständen, erkennt potenzielle Bedrohungen frühzeitig und schützt Ihre Geräte zuverlässig. Entdeckte Malware wird sofort beendet und kann später vollständig gelöscht werden. Mit der TeamViewer Management-Konsole können Sie alle Bedrohungen und Scans auf einen Blick verwalten - jederzeit und überall.

3. Mit **TeamViewer Backup** können Sie Ihre Daten unter höchsten Sicherheitsstandards in der Cloud speichern, und gesicherte Dateien können jederzeit und von überall aus der Ferne wiederhergestellt werden. Schützen Sie Ihre wichtigen Dateien, indem Sie das komplette Dateisystem, gängige Dateiformate oder bestimmte Dateien und Ordner regelmäßig sichern. Stellen Sie Dateien wieder her und vermeiden Sie so einen möglichen Datenverlust. Mit der TeamViewer Management-Konsole haben Sie jederzeit Zugriff auf jedes Backup von jedem Ihrer Geräte. Console, you have access to each backup of any of your devices at any time.

4. Mit **TeamViewer Web Monitoring** können Sie die Verfügbarkeit und Antwortzeiten Ihrer Website überprüfen. Unsere weltweit verteilten Server überprüfen Ihre Website regelmäßig und informieren Sie, wenn Ihre Seite nicht verfügbar ist oder die Antwortzeit zu lange dauert. Erhalten Sie Einblick in die Ladezeiten Ihrer Seite und sehen Sie sofort, welche Elemente auf Ihrer Website eine höhere Last verursachen, so dass Sie Ihre Endnutzererfahrung optimieren können. Sie können auch wichtige Transaktionen auf Ihrer Website skripten und regelmäßig automatisch ausführen lassen und werden benachrichtigt, wenn bei einer Transaktion nicht verstanden wird, ob Ihr Webshop reibungslos läuft oder Ihr Kunden-Login richtig funktioniert.

2. Anforderungen

Dies sind die Voraussetzungen, die erfüllt sein müssen, um alle Funktionen von TeamViewer Remote Management nutzen zu können.

> **Hinweis:** Sie können TeamViewer Remote Management auch 14 Tage lang kostenlos testen, ohne Lizenz und ohne Verpflichtung zum Abonnement.

2.1 Lizenzierung

TeamViewer Remote Management ist ein Add-on zum TeamViewer-Fernsteuerungsprodukt, aber es ist nicht im TeamViewer-Lizenzmodell enthalten. Dies bedeutet, dass:

1. Remote Management ist nicht Teil der TeamViewer Corporate, Premium oder Business Lizenz.
2. Remote Management kann auch ohne eine TeamViewer Corporate, Premium oder Business Lizenz verwendet werden.
3. Sie benötigen eine TeamViewer Remote Management-Lizenz, um alle Funktionen von Remote Management nutzen zu können.

TeamViewer Remote Management Services sind als Monats- oder Jahresabonnement erhältlich. Beim Lizenzmodell für die Fernverwaltung erwerben Sie für jeden Computer, auf dem Sie die Fernverwaltung nutzen möchten, einen sogenannten "Endpunkt". Die Backup-Lizenz zählt das Speichervolumen. Die Web-Monitoring-Lizenz basiert auf Paketen, die Variablen wie Art und Anzahl der Monitore, Prüffrequenz und die Anzahl der Standorte enthalten, von denen aus Sie Ihre Monitore ausführen möchten.

> **Hinweis:** Sie benötigen separate Endpunkte für die TeamViewer Remote Management Services: Überwachung & Asset Management und Endpunktschutz. Die verschiedenen Endpunkte können unabhängig voneinander verwendet werden.

Zum Beispiel

1. Wenn Sie fünf (5) Computer mit TeamViewer Endpoint Protection schützen möchten, benötigen Sie eine TeamViewer Endpoint Protection-Lizenz mit 5 Endpunkten.
2. Wenn Sie zehn (10) Computer mit TeamViewer Monitoring & Asset Management überwachen möchten, benötigen Sie eine TeamViewer Monitoring & Asset Management-Lizenz mit 10 Endpunkten.
3. Wenn Sie zwanzig (20) Computer mit TeamViewer Backup sichern möchten, benötigen Sie eine TeamViewer Backup-Lizenz mit dem erforderlichen Speichervolumen. TeamViewer Backup kann auf beliebig vielen Geräten installiert werden.

> **Hinweis:** Die Lizenzierung für den Backup-Dienst basiert auf dem verwendeten konsolidierten Speichervolumen. Daher kann der Dienst auf einer unbegrenzten Anzahl von Endpunkten genutzt werden.

4. Wenn Sie 20 Basismonitore und 10 erweiterte Monitore mit 5 bzw. 20 Minuten Kontrollhäufigkeit aus 3 von maximal 30 Standorten haben möchten, müssen Sie ein individuelles Paket kaufen. Wenn Sie jedoch nur 50 Basismonitore haben möchten, können Sie ein Basispaket erwerben

Weitere Informationen über das Lizenzmodell für das Remote Management finden Sie in unserem TeamViewer Remote Management Shop.

2.2 Lizenz Aktivierung

Sie benötigen eine TeamViewer Remote Management-Lizenz, um alle Funktionen der TeamViewer Remote Management Services nutzen zu können.

Nachdem Sie eine TeamViewer Remote Management-Lizenz erworben haben, erhalten Sie eine Bestätigungs-E-Mail. Klicken Sie auf den Aktivierungslink in der E-Mail, um die Lizenz für Ihr TeamViewer-Konto zu aktivieren.

Sobald Sie die Lizenz aktiviert haben, wird sie automatisch mit Ihrem TeamViewer-Konto verknüpft und ist sofort einsatzbereit.

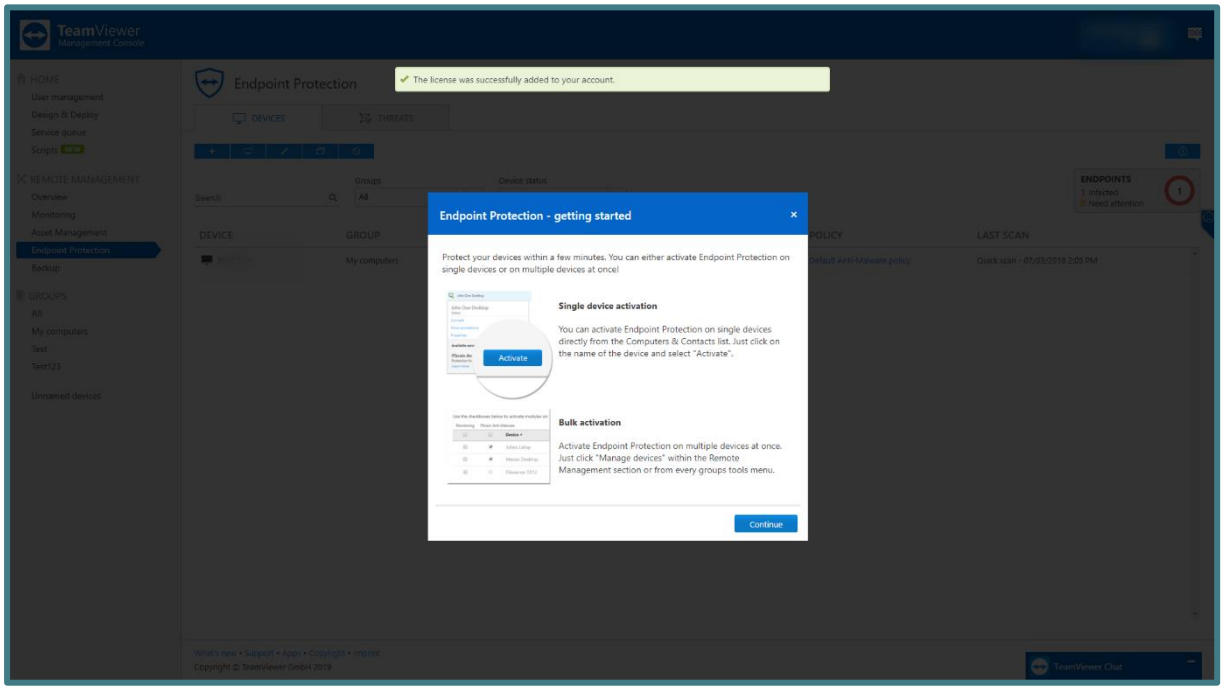


Bild: Aktivierung der Remote Management Lizenz.

Hinweis: Wenn Sie Ihr TeamViewer-Konto unter einem Firmenprofil einrichten, ist die TeamViewer Remote Management-Lizenz Teil des Firmenprofils und alle Benutzer mit der entsprechenden Berechtigung können die Remote Management-Dienste verwalten.

Hinweis: TeamViewer Remote Management Lizenzaktivierungen können nur in Ausnahmefällen rückgängig gemacht werden.

Hinweis: Pro Konto kann nur eine Lizenz für TeamViewer Web Monitoring aktiviert werden.

2.3 System Anforderungen

Zur Konfiguration und Verwaltung von TeamViewer Remote Management Services benötigen Sie die TeamViewer Management Console.

Die TeamViewer Management Console ist browserbasiert und daher unabhängig vom Betriebssystem.

Zum Aktivieren und Anzeigen von Alerts können Sie die TeamViewer Vollversion mit den folgenden Betriebssystemen verwenden:

1. Windows

Nur zum Anzeigen von Warnmeldungen können Sie die TeamViewer Remote Control App auf folgenden Plattformen installieren:

1. Android
2. iOS

2.3.1 TeamViewer Monitoring & Asset Management

Um die Überwachung nutzen zu können, muss auf den Geräten (Endpunkten), die Sie überwachen möchten, eines der folgenden Betriebssysteme laufen:

Windows

1. Windows 10 / 8.1 / 8 / 7 / Vista / XP SP3.
2. Windows Server 2012 R2 / 2012 / 2008 R2 / 2008 / 2003 R2 32 bit.
3. Der Anti-Virus Check ist für Serverbetriebssysteme nicht verfügbar
    - Das Windows-Sicherheitscenter (WSC) ist auf dem Windows-Service-Betriebssystem nicht aktiv. TeamViewer 11 full version of Host (or newer) must be installed.

macOS

1. macOS Sierra, High Sierra, Mojave, oder neuer.

2. TeamViewer 14 Vollversion oder Host (v14.2.2558 und neuer)
    a. TeamViewer muss mit dem Systemstart beginnen

Linux

1. Debian 9 oder neuer
2. GRML, Kali Linux, Purism, Pure OS, Tails, Ubuntu und andere .deb Distributionen.
3. TeamViewer 14 Vollversion oder Host (14.1.9025 und neuer).
    a. Das Konto muss vor der Aktivierung zugewiesen werden

Um Asset Management (einschließlich Patch Management) verwenden zu können, muss auf den Geräten (Endpunkten), die Sie überwachen möchten, eines der folgenden Betriebssysteme laufen:

- Funktioniert mit der neuesten Version von TeamViewer 14 (14.5.1691) und neuer.
- Nur mit diesen Windows-Betriebssystemen kompatibel
    - Windows 7 SP1/8.0/8.1/10
    - Windows Server 2008R2/2012/2019

2.3.2 TeamViewer Endpoint Protection

Um Endpoint Protection verwenden zu können, muss auf den Geräten (Endpunkten), die Sie schützen möchten, eines der folgenden Betriebssysteme ausgeführt werden:

1. Windows 10 / 8.1 / 8 / 7.
2. Windows Server 2012 R2 / 2012 / 2008 R2.
3. TeamViewer 11 Vollversion oder Host (oder neuer) muss installiert sein.

2.3.3 TeamViewer Backup

Um Backup zu verwenden, sollten Sie sicherstellen, dass eines der folgenden Betriebssysteme auf dem/den Gerät(en) läuft, das/die Sie mit TeamViewer Backup sichern möchten:

1. Windows 10 / 8.1 / 8 / 7 SP1 und später.
2. Windows Server 2012 R2 / 2012 / 2008 R2.
3. TeamViewer 11 Vollversion oder Host (oder neuer) muss installiert sein.

3. Erste Schritte

Mit der TeamViewer Management Console können Sie alle Dienste des Remote Management konfigurieren. Öffnen Sie dazu die TeamViewer Management-Konsole unter https://login.teamviewer.com und melden Sie sich mit Ihrem TeamViewer-Konto an. Alle weiteren Schritte zur Konfiguration von TeamViewer Remote Management werden im Folgenden beschrieben.

Hinweis: Abhängig von den Benutzerrechten können TeamViewer-Konten, die unter einem Firmenprofil eingerichtet wurden, auch die nachfolgend beschriebenen Funktionen nutzen.

3.1 Aktivierung

Alle Computer, auf denen Benutzer TeamViewer Remote Management verwenden möchten, werden als "Endpunkte" bezeichnet. Der TeamViewer Remote Management Service muss auf jedem Endpunkt aktiviert und konfiguriert werden. Die Lizenz kann per Massenaktivierung oder auf jedem Endpunkt separat aktiviert werden.

Nach der Aktivierung von Monitoring & Asset Management an den Endpunkten werden die folgenden Schritte automatisch durchgeführt:

1. Der **Monitoring** Service wird heruntergeladen und auf dem Gerät installiert.
2. Der **Asset Management** Dienst, der auch für Patch Management zuständig ist, wird heruntergeladen und auf dem Gerät installiert.
3. Die Standardrichtlinie für Überwachung und **Asset Management** wird dem Gerät zugewiesen.
4. **Asset Management**-Daten werden zum ersten Mal hochgeladen.
5. Die Informationen zu fehlenden **Patches** werden zum ersten Mal hochgeladen.

Nach der Aktivierung des Endpunktschutzes an den Endpunkten werden die folgenden Schritte automatisch durchgeführt:

1. Der **Endpoint Protection** Service wird heruntergeladen und auf dem Gerät installiert.
2. Die neuesten Virendefinitionen von **Endpoint Protection** werden heruntergeladen.
3. Die **Standardrichtlinie für Endpoint Protection** wird dem Gerät zugewiesen.
4. Ein Schnell-Scan wird gestartet.

Nach der Aktivierung von Backup auf den Endpunkten werden die folgenden Schritte automatisch durchgeführt:

1. Der **Backup** Dienst wird heruntergeladen und auf dem Gerät installiert.
2. Sie müssen eine Standard-Sicherungsrichtlinie mit Dateipfaden für die Sicherung definieren.

Nachdem Sie **Web Monitoring** aktiviert haben, können Sie damit beginnen, Ihre Monitore zu erstellen und zu konfigurieren.

Hinweis: Für die Transaktionsüberwachung müssen Sie auch das Browser-Plugin (Transaction Recorder) als Erweiterung herunterladen und hinzufügen - siehe: Transaction Recorder Plugin Installation

3.1.1 Aktivierung über die TeamViewer Vollversion

Einzel-Aktivierung

Sie können Fernverwaltungsdienste* für einzelne Geräte in Ihrer Computer- und Kontaktliste aktivieren. Zuerst wird das Gerät Ihrem TeamViewer-Konto zugeordnet und dann wird der Fernverwaltungsdienst konfiguriert.

* Wenn **Monitoring & Asset Management** direkt von einem Gerät aus aktiviert wird, wird **Patch Management** nicht aktiviert. Dies kann nur über die TeamViewer Management-Konsole aktiviert werden.

Um die zu tun:

1) Klicken Sie auf den Gerätenamen in Ihrer Computer- & Kontaktliste.
2) Wählen Sie Aktivieren für den jeweiligen Dienst.

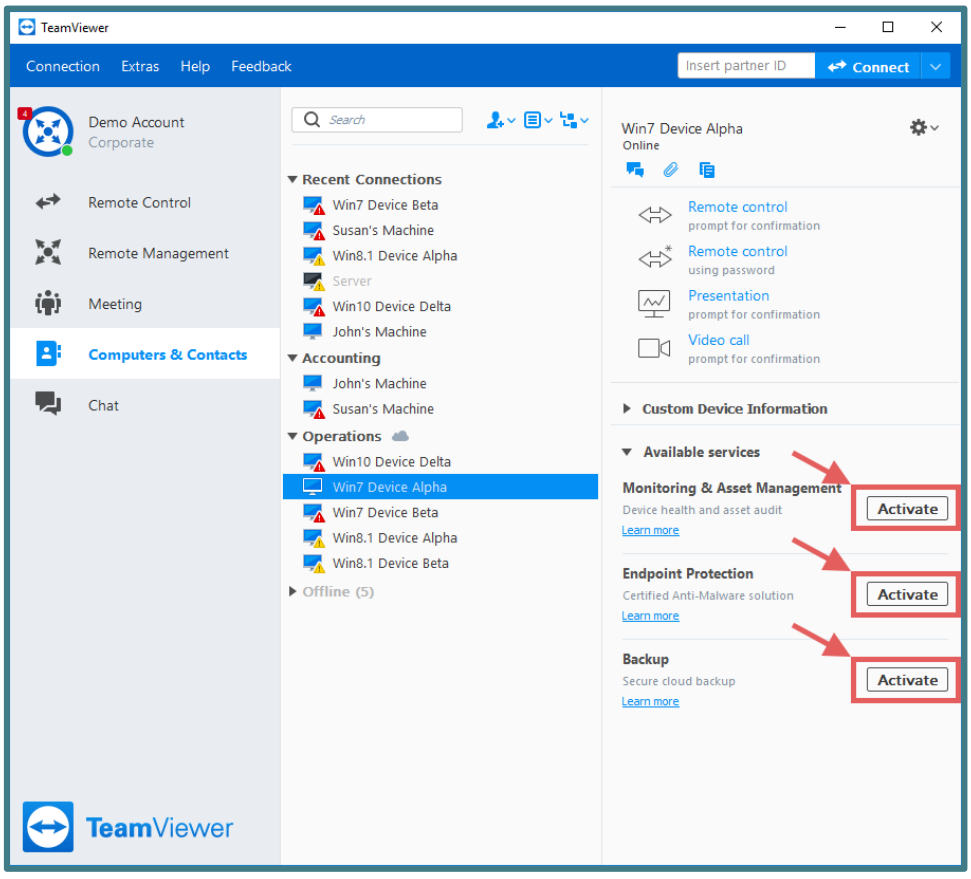


Bild: Aktivierung über die TeamViewer-Vollversion.

Wenn Sie das persönliche Passwort für das Gerät nicht in Ihrer Computer- und Kontaktliste gespeichert haben, geben Sie es im Dialogfeld ein.

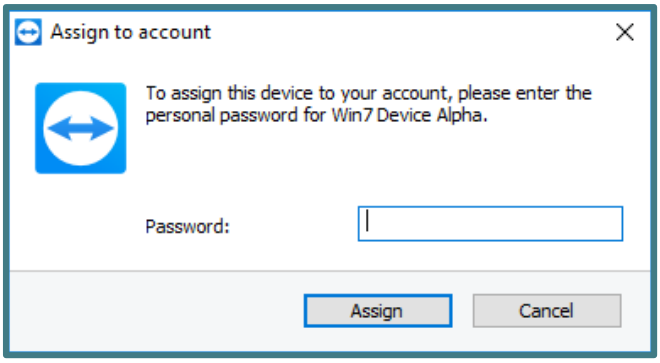


Bild: Geräte Kontozuweisung

Wenn Sie kein persönliches Kennwort für den Endpunkt festgelegt haben, können Sie den Endpunkt über die Einstellungen in der TeamViewer-Vollversion Ihrem Konto zuweisen.

Dazu müssen Sie lokal auf dem Rechner unter auf die Einstellungen zugreifen:

Extras → Optionen → Allgemein→ Account Zuweisung.

Remote Management Tab

Beginnend mit TeamViewer 14 und aufwärts haben wir einen neuen Reiter im TeamViewer-Client eingeführt.

Die Registerkarte Fernverwaltung zeigt den Status für alle aktiven Dienste an und enthält Schnelllinks zur Verwaltungskonsole.:

1. Schaltfläche für die Aktivierung eines weiteren Endpunkts

2. Einstellungsmenü

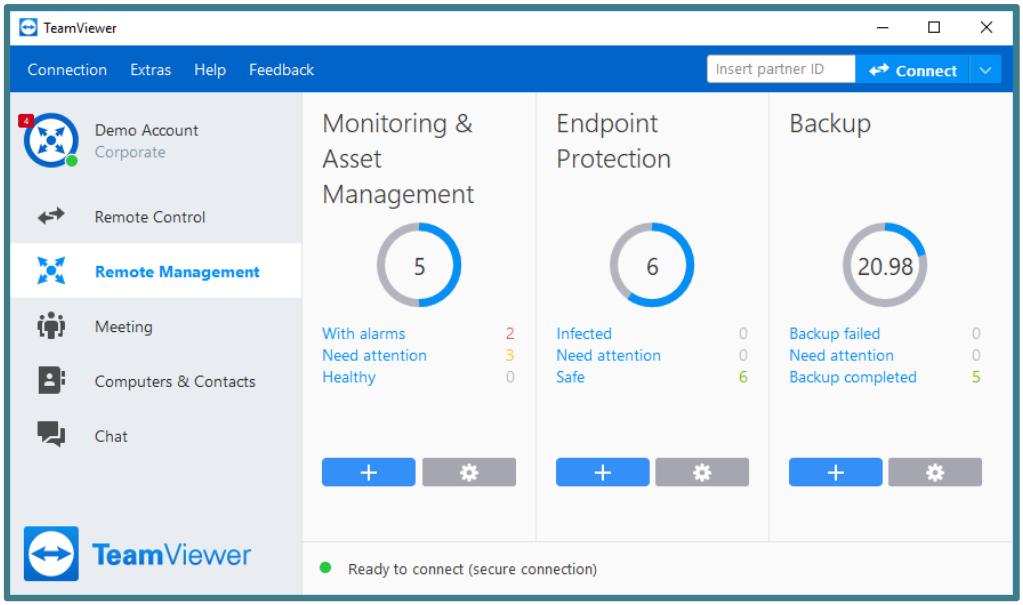


Bild: Registerkarte "Remote Management" im TeamViewer Client.

3.1.2 Aktivierung über die TeamViewer Management Console

Auf die TeamViewer Management-Konsole kann hier zugegriffen werden:
https://login.teamviewer.com

Einzelne Aktivierung

Sie können Fernverwaltungsdienste für einzelne Geräte in Ihrer Gruppenliste aktivieren. Um diese Funktion nutzen zu können, müssen Sie über eine aktive Lizenz verfügen..

1. Gehen Sie zu einer beliebigen Gruppe im linken Fensterbereich, wählen Sie das Gerät aus und klicken Sie auf das Symbol für die gewünschten Dienste auf der rechten Seite.
2. Klicken Sie auf aktivieren.
3. Nun wird das Gerät Ihrem TeamViewer-Konto zugewiesen, und dann wird der entsprechende Remote Management Dienst konfiguriert.

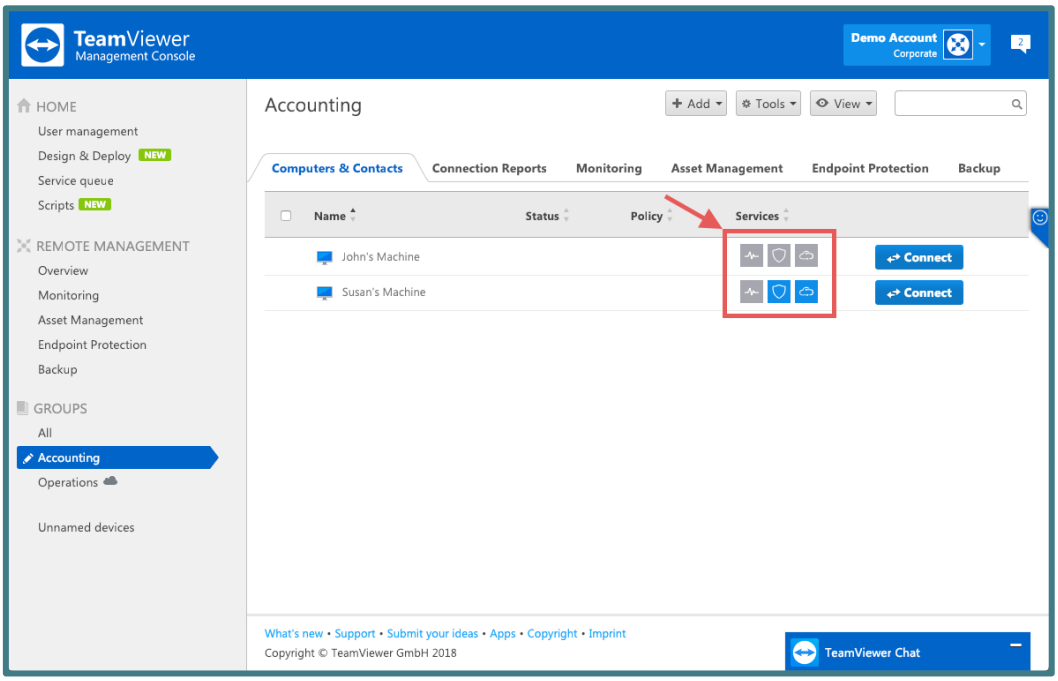


Bild: Einzelaktivierung via TeamViewer Management Console.

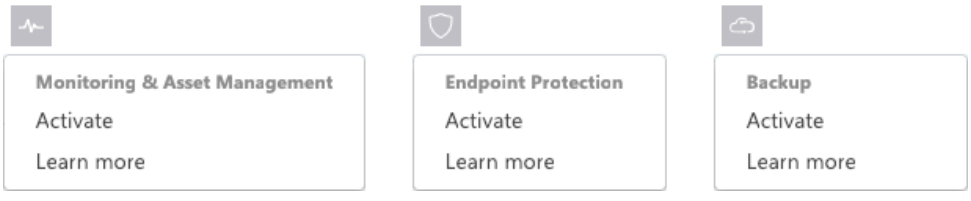


Bild: Activation icons.

Massenaktivierung

Die Massenaktivierung hilft Ihnen bei der Aktivierung von TeamViewer Remote Management Services auf mehreren Geräten und ordnet sie alle gemeinsam Ihrem TeamViewer-Account zu. Durch die Verwendung Ihrer persönlichen Kennwörter werden alle Endgeräte automatisch Ihrem Konto zugeordnet und der/die TeamViewer Remote Management Service(s) für die Endgeräte in einem Schritt aktiviert. Um diese Funktion nutzen zu können, müssen Sie über eine aktive Lizenz verfügen.

1. Aktivieren aus der Fernverwaltungsübersicht.
   a. Klicken Sie im linken Fensterbereich unter dem Abschnitt Remote Management auf die Registerkarte 'Übersicht'.
   b. Klicken Sie in der linken unteren Ecke der Service-Kachel auf die Schaltfläche '+'.
   c. Wählen Sie die Geräte aus der Liste aus und klicken Sie auf "Weiter".
   d. Wählen Sie die Standardrichtlinie, die für alle Geräte zugewiesen werden soll.
   e. Klicken Sie auf Aktivieren.

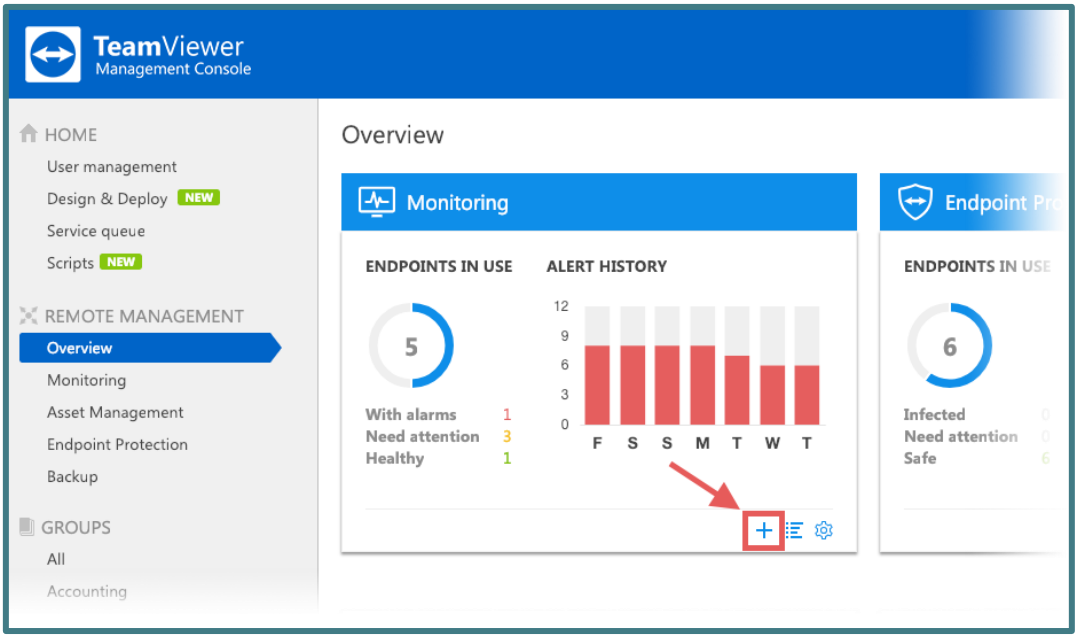


Bild: Massenaktivierung über TeamViewer MCO 1.

2. Aktivieren über die Registerkarte Service.
   a. Klicken Sie auf die Service-Registerkarte, für die Sie Endpunkte aktivieren möchten.
   b. Klicken Sie auf die Schaltfläche '+' in der linken oberen Ecke.
   c. Wählen Sie die Geräte aus der Liste aus und klicken Sie auf "Weiter".
   d. Wählen Sie die Standardrichtlinie, die für alle Geräte zugewiesen werden soll.
   e. Klicken Sie auf Aktivieren.

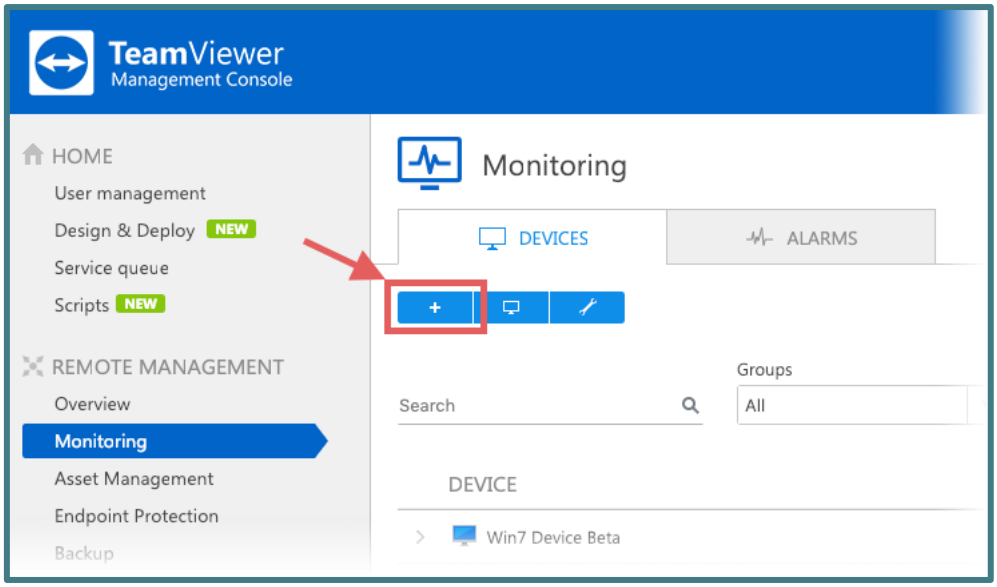


Bild: Massenaktivierung über TeamViewer MCO 2.

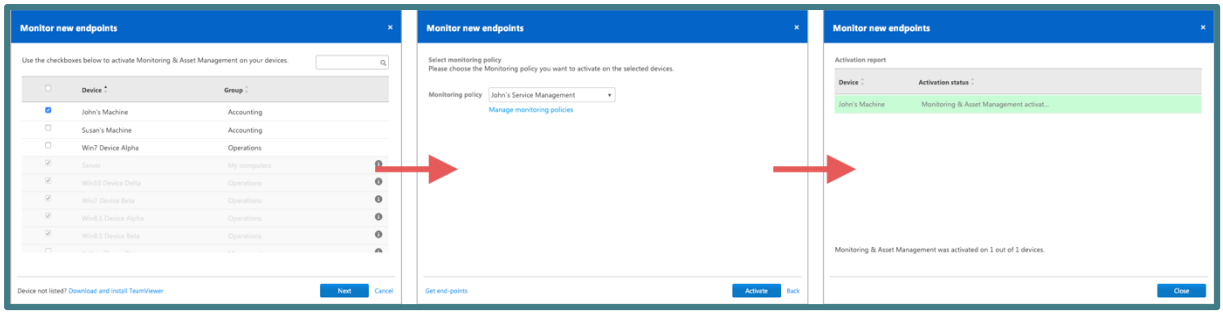


Bild: Massenaktivierung über TeamViewer MCO 3.

3.2 Richtlinien

Richtlinien werden als individuelle Einstellungen definiert, die nach ihrer Anwendung an die Endpunkte gesendet werden.

Sie enthalten alle notwendigen Informationen darüber, wie der Dienst:

1. Remotely manage the device.
2. Alert the user if something is not working properly.
3. Deploy missing patches.
4. Setup thresholds and parameters.
5. Send e-mail notifications.

Monitoring Richtlinien: Bestimmen Sie die Kriterien, auf die Ihre Geräte für die Berichterstattung eingestellt werden, wenn etwas nicht innerhalb der zugewiesenen Schwellenwerte oder Parameter läuft.

Asset Management Richtlinien: die Kriterien bestimmen, auf deren Grundlage fehlende Patches automatisch bereitgestellt werden.

Endpoint Protection Richtlinien: bestimmen, wann und in welchem Umfang Ihre Geräte gescannt und vor Malware geschützt werden.

Backup Richtlinien: bestimmen, wann und in welchem Umfang die Dateien auf Ihren Geräten gesichert werden.

3.2.1 Standardpolitik und Richtlinienoptionen

Für jeden Dienst wird eine Standardrichtlinie erstellt, wenn der erste Endpunkt aktiviert wird.

1. Die Standardrichtlinien werden auf jeden aktivierten Endpunkt angewendet, wenn bei der Aktivierung des Endpunkts keine andere Richtlinie angegeben wird.
2. Die Standardrichtlinien können jederzeit geändert werden.
3. Neu erstellte Richtlinien können als Standardrichtlinien zugewiesen werden.

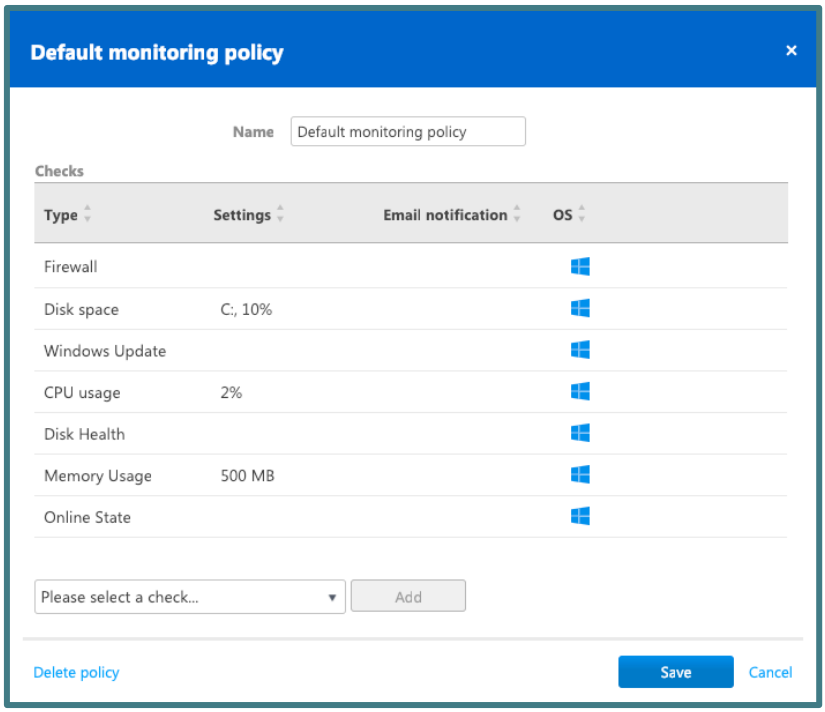


Bild: Monitoring Standardrichtlinie.

Alle Richtlinien finden Sie unter:

Remote Management → Service Namen Tab → Zahnrad Symbol→ Richtlinien verwalten

Im Fenster Policies können Sie:

1. Erstellen Sie eine Richtlinie.
2. Eine Richtlinie bearbeiten.
3. Eine Richtlinie duplizieren.

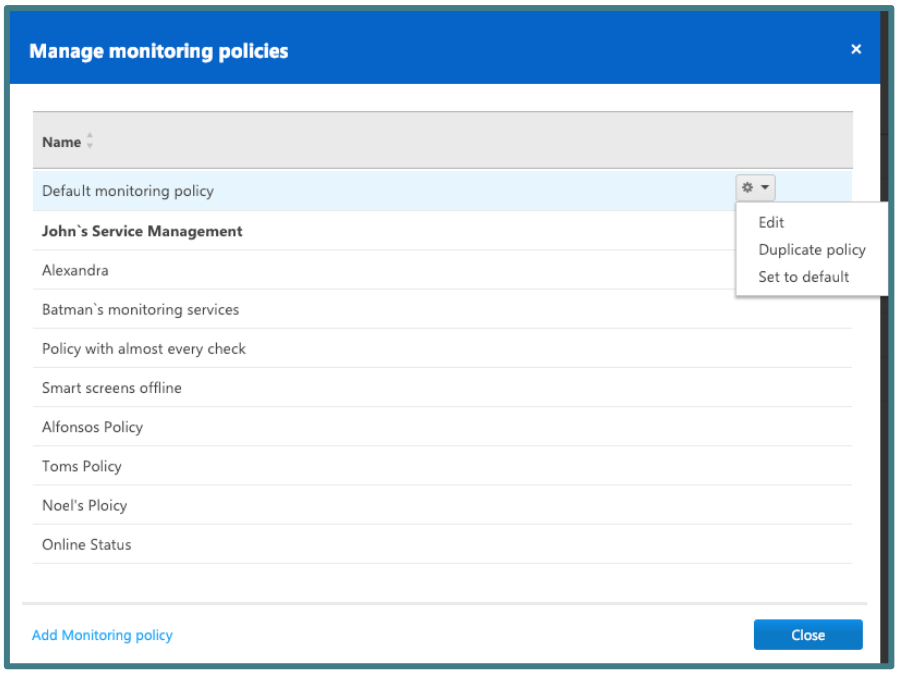


Bild: Verwalten Sie Ihre Monitoring Richtlinien.

3.2.2 Zuweisen einer Richtlinie

Einzelne Richtlinienzuweisung

Sie können jedem Gerät eine Richtlinie zuweisen, indem Sie auf die gewünschte Dienst-Registerkarte gehen und die Richtlinienspalte auf der rechten Seite der Geräteansicht auswählen. Klicken Sie zum Speichern auf das Häkchen.

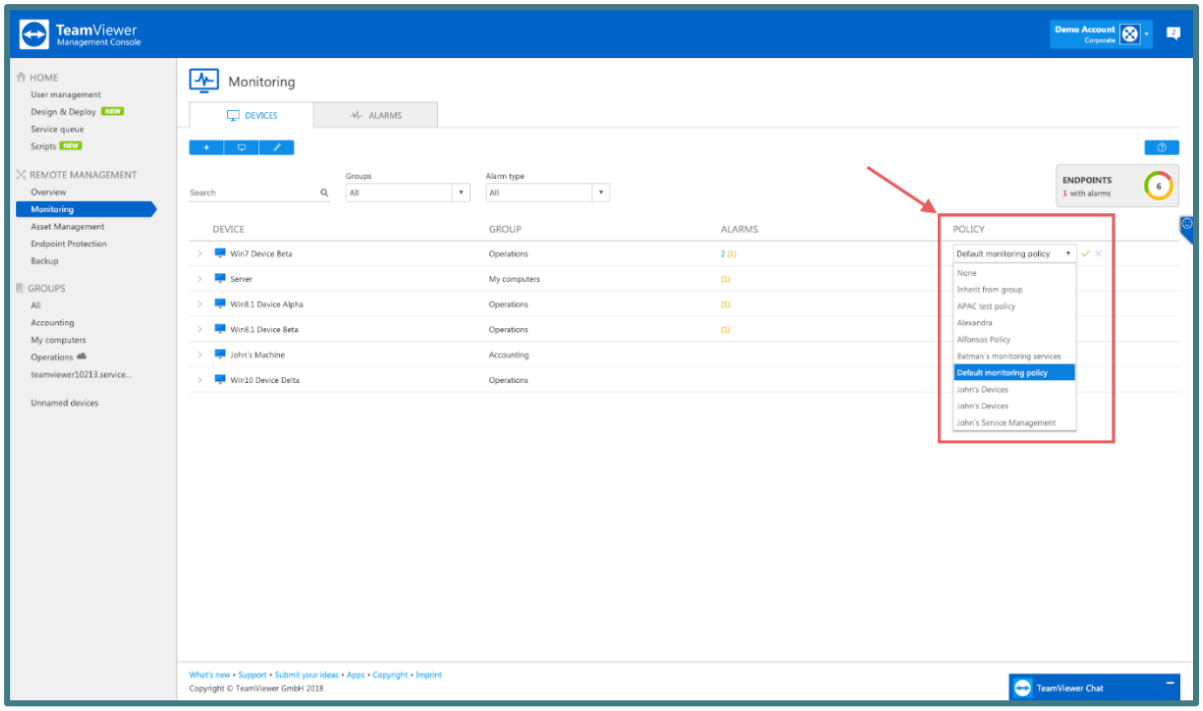


Bild: Einzelne Richtlinienzuweisung.

Zuweisung von Gruppenrichtlinien

Wenn Sie eine Richtlinie für eine ganze Gruppe von Computern haben möchten, wählen Sie "Von Gruppe vererben" in der Zeile "Richtlinie" für alle Computer in einer Gruppe (Sie können auch nach einzelnen Gruppen filtern). Klicken Sie zum Speichern auf das Häkchen..

1. Gehen Sie in den linken Bereich der gewünschten Gruppe.
2. Fahren Sie mit der Maus über die Gruppe.
3. Klicken Sie auf das Stiftsymbol und dann auf "Bearbeiten".
4. Wählen Sie die Richtlinie für den gewünschten Dienst und klicken Sie auf "Speichern".

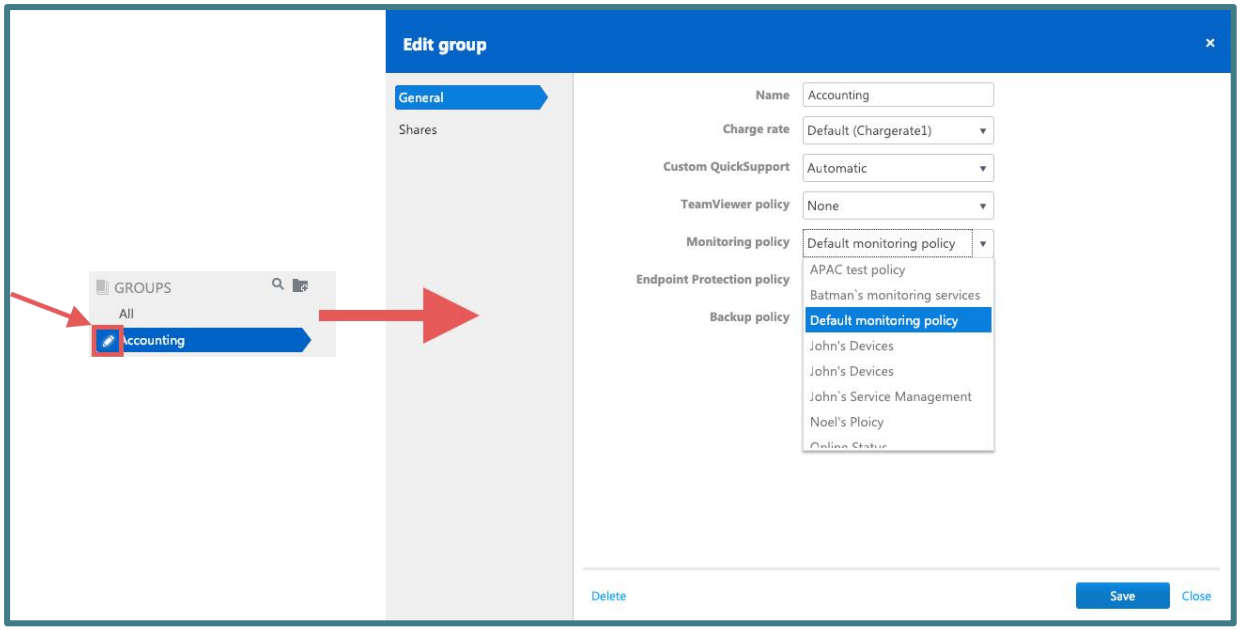


Bild: Zuweisung von Gruppenrichtlinien.

4. Monitoring & Asset Management

Um Ihre Geräte zu überwachen und Ihre IT-Assets zu verwalten, nutzen Sie den **Service TeamViewer Monitoring & Asset Management**.

Die Überwachungs-Richtlinien definieren das proaktive Verhalten der einzelnen Checks, die den Geräten zugeordnet sind.

Für die Für die **Lizenzaktivierung** siehe 2.2 Lizenz .

Die **Systemanforderungen** finden Sie unter 2.3 Systemanforderungen.

Für die Konfiguration von Richtlinien und deren Zuweisung zu einem Gerät siehe 3.2 .

Wenn alle definierten Bedingungen für eine Prüfung erfüllt sind, wird ein Alarm ausgelöst und als Alarmmeldung in der TeamViewer Management-Konsole und in der TeamViewer Vollversion angezeigt. Eine E-Mail-Benachrichtigung wird ebenfalls gesendet, falls in der Richtlinie konfiguriert. Eine Alarmmeldung zeigt an, dass auf einem der überwachten Geräte ein Problem aufgetreten ist.

4.1 Monitoring & Asset Management Aktivierung

Zur Aktivierung von Endpunkten siehe: 3.1 .

4.2 Monitoring Checks

Die Überwachungsprüfungen sind in 3 Kategorien eingeteilt, die Ihnen helfen, festzustellen, wie kritisch die Situation auf einem Gerät ist.

Windows Checks

Bild: Die drei Kategorien von Monitoring Checks.

1. **Systemzustand und Sicherheit**
    a. Online Zustasnd
        i. Dies ist eine proaktive Prüfung, die den Benutzer warnt, wenn das Gerät offline geht und wieder online geht.
        ii. Wenn die Prüfung auf ein Gerät angewendet wird, wird überwacht, ob das System über eine Internetverbindung verfügt. Wenn das Gerät für mehr als 1 Minute offline geht, wird ein Alarm ausgelöst.
        iii. Nachdem das Gerät offline gegangen ist, wird es die Zeitdauer in diesem Zustand verfolgen. Wenn das Gerät wieder online geht, wird zusätzlich eine Wiederherstellungsbenachrichtigung generiert und der Status der Überprüfung kehrt auf grün zurück.
        iv. Die Überprüfung kann mit einer Zeitverzögerung von 5 oder 10 Minuten angepasst werden. Wenn Sie eine Zeitverzögerung wählen, wird der Online-Zustand erst dann gemeldet, wenn das Gerät länger als den gewählten Zeitverzögerungswert offline ist.
    b. System Update
        i. Diese Prüfung warnt den Benutzer, wenn Windows Update deaktiviert ist.
        ii. Der Benutzer wird sehen, ob es verfügbare Updates gibt, die auf dem Gerät installiert werden können.
        iii. Eine Variante von "Windows Update ist ausgeschaltet" oder "Updates sind verfügbar" kann ausgewählt werden. Ein Alarm wird ausgelöst, wenn eine der Variablen erfüllt ist.
    c. Antivirus
        i. Diese Prüfung wird ausgelöst, wenn die installierte Sicherheitslösung, die in Windows-Sicherheit registriert ist, ausgeschaltet ist oder wenn die Updates der Malware-Definitionen mehr als 2 Tage lang nicht aktualisiert wurden.

    d. Firewall
        i. Ein Check, der generiert wird, wenn die Windows-Firewall oder die Firewall eines Drittanbieters deaktiviert ist.
    e. Netzwerkadapter-Traffic

i. Diese Prüfung warnt die Benutzer, wenn Probleme im Zusammenhang mit dem Netzwerkverkehr, wie z.B. Unterbrechung oder hohe Auslastung, auf dem Netzwerkadapter auftreten. Mit dieser Prüfung kann der Benutzer sowohl den eingehenden als auch den ausgehenden Datenverkehr überwachen.
    1. Art des Datenverkehrs: eingehender oder ausgehender Verkehr.
    2. Mindestwert des Datenverkehrs: Wenn es weniger Datenverkehr gibt, erhält der Benutzer eine Warnung. Es besteht die Möglichkeit, zwischen zwei Metriken zu wählen - KB/s oder MB/s.
    3. Maximaler Wert des Datenverkehrs: Wenn es mehr Datenverkehr gibt, erhalten die Benutzer eine Warnung. Es besteht die Möglichkeit, zwischen zwei Metriken zu wählen - KB/s oder MB/s.

ii. Mehrere Prüfungen können in einer Richtlinie hinzugefügt werden.

2. **Softwareausführungen**
    a. Windows-Dienst
        i. Diese Prüfung überwacht einen definierten Windows-Dienst und löst eine Warnung aus, wenn der eingestellte Dienst läuft oder nicht läuft.
        ii. Um diese Prüfung einzurichten, muss der genaue Dienstname im Konfigurationsmenü der Prüfung hinzugefügt werden.
        iii. Den genauen Dienstnamen finden Sie unter:
            Windows Dienste → Service Details.

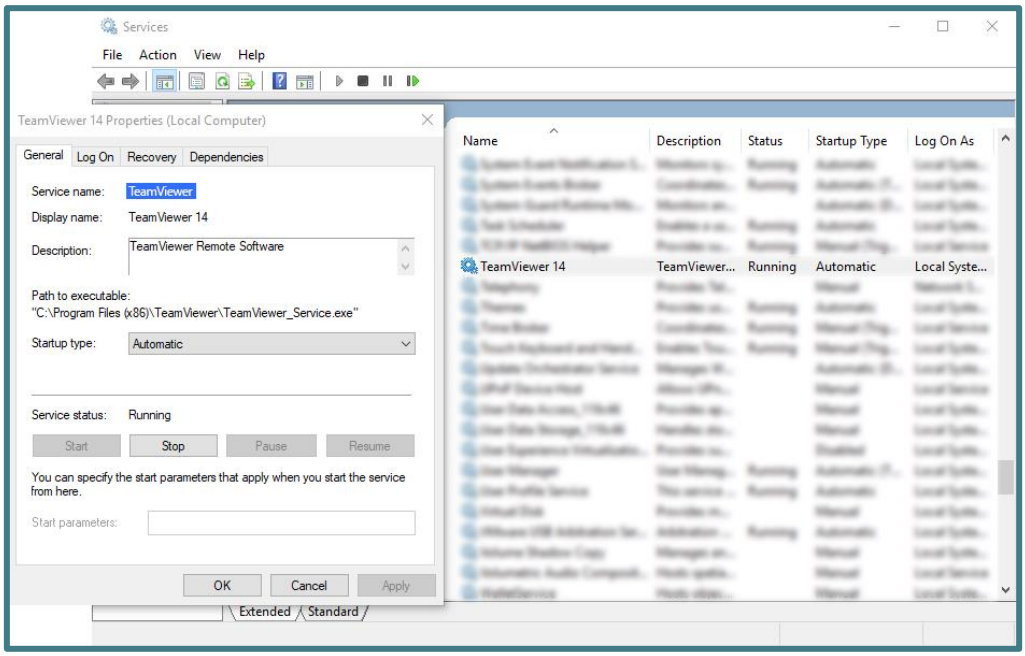


Bild: Software Operation check auf Lokaler Maschine.

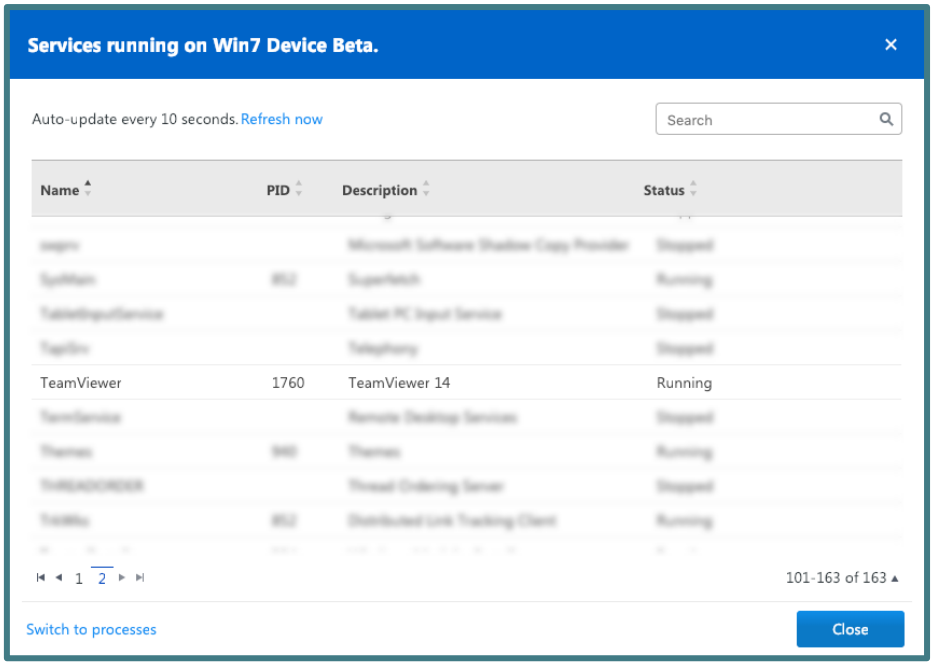


Bild: Software-Betriebsüberprüfung in der Verwaltungskonsole.

Hinweis: Laufende Dienste können durch Öffnen des Remote Task Managers eingesehen warden.

b. Prozess
   i. Diese Prüfung überwacht einen definierten Windows-Prozess und löst eine Warnung aus, ob der Prozess läuft oder nicht.
   ii. Um diese Prüfung einzurichten, muss der genaue Prozessname im Konfigurationsmenü der Prüfung hinzugefügt werden.
   iii. Beim Namen des Prozesses wird zwischen Groß- und Kleinschreibung unterschieden.

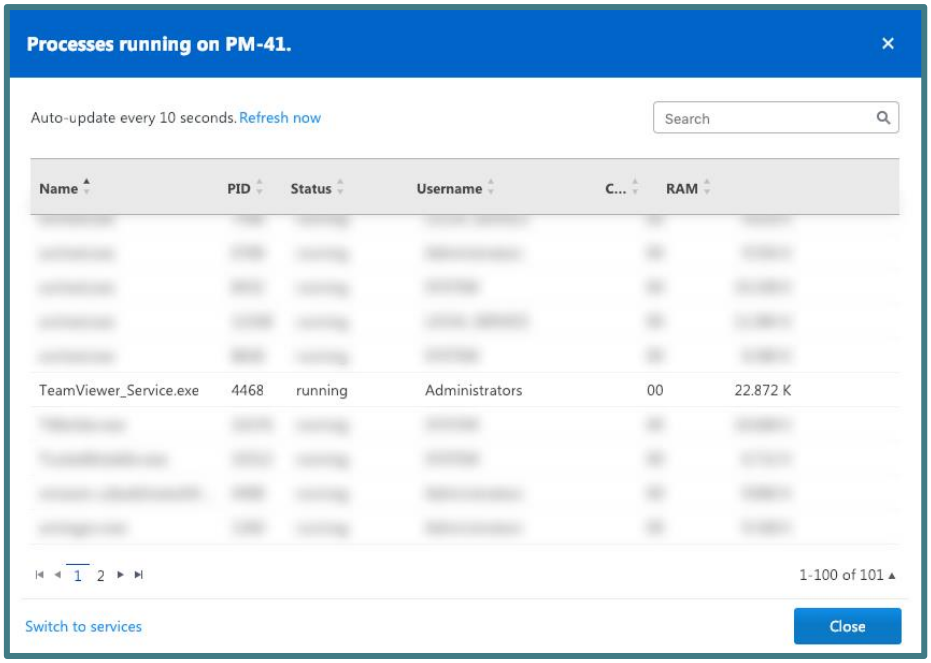


Bild: Prozessüberprüfung in der Management Console.

Hinweis: Laufende Prozesse auf einem Gerät können durch Öffnen des Remote Task Managers angezeigt werden.

c. Ereignisprotokoll
   i. Diese Prüfung meldet Ereignisprotokolle aus der Windows Ereignisanzeige, nachdem ein Eintrag in den konfigurierten Protokollordner geschrieben wurde.
   ii. Viele Anwendungen und kritische Windows-Operationen zeichnen Protokolle auf, so dass die Ereignisprotokoll-Prüfungen eine sehr leistungsfähige Prüfung zur Überwachung wichtiger Operationen auf einem Windows-Gerät darstellen.
   iii. Um diese Prüfung einzurichten, muss die abgefragte Kategorie ausgewählt werden:
      1. Sicherheit
      2. Anwendung
      3. System
   iv. Nach der Auswahl des Ordners, in dem die Protokolle überwacht werden sollen, muss die Quelle ausgewählt werden.
   v. Nach der Auswahl der Quelle muss die Ereignis-ID hinzugefügt werden. Mehrere Ereignis-IDs können durch "," (Komma) getrennt hinzugefügt werden.
   vi. Nach Auswahl der ID müssen eine oder mehrere Ereignisprotokollkategorien ausgewählt werden:
      1. Audit
      2. Information

3. Error

vii. Wenn ein Ereignisprotokoll geschrieben wird und den vordefinierten Prüfeinstellungen entspricht, wird eine Benachrichtigung gesendet. Eine vollständige Beschreibung des ausgelösten Ereignisprotokolls wird in der E-Mail enthalten sein.

3. **Hardware**
   a. Speicherkapazität
      i. Diese Prüfung überwacht den freien Speicherplatz auf einem Systemlaufwerk und meldet, wenn der freie Speicherplatz unter dem definierten Wert liegt.
      ii. Einer Richtlinie können mehrere Speicherplatzprüfungen mit unterschiedlichen Laufwerksbuchstaben hinzugefügt werden.
      iii. Um die Speicherplatzprüfung einzurichten, wählen Sie zunächst das gewünschte Laufwerk, das auf dem Gerät überwacht werden soll, z.B. C:\ oder G:\.
      iv. Nachdem Sie das Laufwerk ausgewählt haben, wählen Sie die benötigte Variable:
         1. % – Prozentsatz des auf dem Laufwerk verbleibenden freien Speicherplatzes.
         2. GB – Gigabyte freier Speicherplatz auf der Festplatte.
         3. MB – Auf dem Laufwerk verbleibende Megabytes an freiem Speicherplatz.
      v. Nachdem Sie die Variable ausgewählt haben, geben Sie den minimalen Schwellenwert ein. Immer wenn der Plattenplatz unter diesen Wert fällt, wird ein Alarm ausgelöst.
   b. Festplattenzustand
      i. Diese Prüfung meldet alle S.M.A.R.T.-Fehler, die im Windows-Verwaltungsinstrumentationsmodul aufgezeichnet wurden.
      ii. S.M.A.R.T. ist eine Standardisierung der Fehlerberichterstattung für Speichergerätekomponenten. Weitere Einzelheiten können hier nachgelesen werden: https://en.wikipedia.org/wiki/S.M.A.R.T.
      iii. Wenn ein Fehler ausgelöst wird, wird er gemeldet, und dann wird ein Alarm gesendet.
      iv. Falls konfiguriert, wird auch eine E-Mail-Benachrichtigung versandt, die alle notwendigen Fehlerberichte einschließlich des aufgezeichneten Fehlers enthält.
      v. Wenn S.M.A.R.T.-Alarme für ein Gerät weiterhin ausgelöst werden, untersuchen Sie bitte die gemeldeten Fehler in den Web-Ressourcen der Hersteller oder verwenden Sie die vom Hardware-Hersteller erstellten dedizierten Tools.
   c. Arbeitsspeicherauslastung
      i. Diese Prüfung überwacht die Menge des freien Random-Access-Speichers oder RAM auf dem Gerät.
   d. CPU-Auslastung
      i. Diese Prüfung überwacht die CPU-Auslastung auf dem Gerät, und ein Alarm wird ausgelöst, wenn die Auslastung höher ist als der im Konfigurationsmenü der Prüfung festgelegte Prozentsatz.

macOS Checks

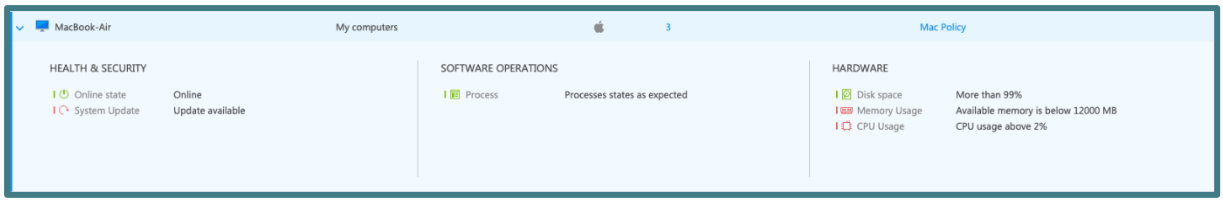


Bild: Die drei Kategorien von Monitoring Checks.

1. **Systemzustand & Sicherheit**
    a. Online state
        i. Dies ist eine proaktive Prüfung, die den Benutzer warnt, wenn das Gerät offline geht und wieder online geht.
        ii. Wenn die Prüfung auf ein Gerät angewendet wird, wird überwacht, ob das System über eine Internetverbindung verfügt. Wenn das Gerät für mehr als 1 Minute offline geht, wird ein Alarm ausgelöst.
        iii. Nachdem das Gerät offline gegangen ist, wird es die Zeitdauer in diesem Zustand verfolgen. Wenn das Gerät wieder online geht, wird zusätzlich eine Wiederherstellungsbenachrichtigung generiert und der Status der Überprüfung kehrt auf grün zurück.
        iv. Die Überprüfung kann mit einer Zeitverzögerung von 5 oder 10 Minuten angepasst werden. Wenn Sie eine Zeitverzögerung wählen, wird der Online-Zustand erst dann gemeldet, wenn das Gerät länger als den gewählten Verzögerungswert offline ist.
    b. System Update
        i. Diese Prüfung warnt den Benutzer, wenn ein System-Update verfügbar ist
2. **Softwareausführung**
    a. Prozesse
        ii. Bei dieser Prüfung wird ein definierter Prozess überwacht, und es wird eine Warnung ausgelöst, ob der Prozess läuft oder nicht läuft.
        iii. Um diesen Check einzurichten, muss der unter "Activity Monitor" aufgeführte Prozessname im Check-Konfigurationsmenü hinzugefügt werden.
3. **Hardware**
    e. Speicherkapazität
        i. Diese Prüfung überwacht den freien Speicherplatz auf einem Systemlaufwerk und meldet, wenn der freie Speicherplatz unter dem definierten Wert liegt.
        ii. ii. Einer Richtlinie können mehrere Speicherplatzprüfungen mit unterschiedlichen Laufwerksbuchstaben hinzugefügt werden.
        iii. iii. Um die Plattenplatzprüfung einzurichten, fügen Sie zunächst den "Volumepfad" hinzu, der überwacht werden muss (z.B. Macintosh HD)
        iv. Nachdem Sie das Laufwerk ausgewählt haben, wählen Sie die benötigte Variable aus:
            1. % – Prozentsatz des auf dem Laufwerk verbleibenden freien Speicherplatzes.
            2. GB – Gigabyte freier Speicherplatz auf der Festplatte.

3. MB – Auf dem Laufwerk verbleibende Megabytes an freiem Speicherplatz.

v. Nachdem Sie die Variable ausgewählt haben, geben Sie den minimalen Schwellenwert ein. Immer wenn der Plattenplatz unter diesen Wert fällt, wird ein Alarm ausgelöst.

f. Arbeitsspeicherauslastung
   i. Diese Prüfung überwacht die Menge des freien Random-Access-Speichers oder RAM auf dem Gerät.

g. CPU-Auslastung
   i. Diese Prüfung überwacht die CPU-Auslastung auf dem Gerät, und es wird ein Alarm ausgelöst, wenn die Auslastung höher ist als der im Konfigurationsmenü der Prüfung festgelegte Prozentsatz.

Linux Checks

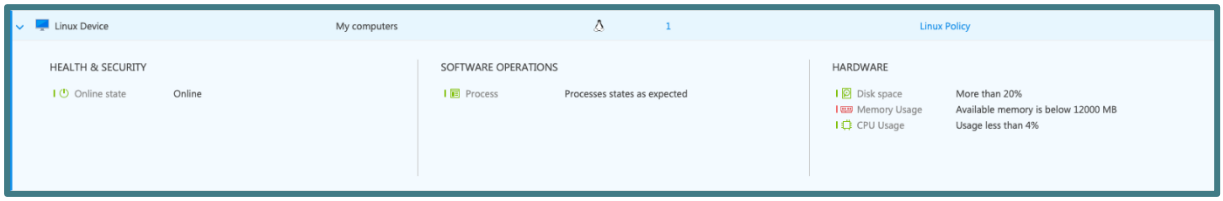


Bild: Die drei Kategorien von Monitoring Checks.

1. **Systemzustand & Sicherheit**
   a. Online state
      i. Dies ist eine proaktive Prüfung, die den Benutzer warnt, wenn das Gerät offline geht und wieder online geht.
      ii. Wenn die Prüfung auf ein Gerät angewendet wird, wird überwacht, ob das System über eine Internetverbindung verfügt. Wenn das Gerät für mehr als 1 Minute offline geht, wird ein Alarm ausgelöst.
      iii. Nachdem das Gerät offline gegangen ist, wird es die Zeitdauer in diesem Zustand verfolgen. Wenn das Gerät wieder online geht, wird zusätzlich eine Wiederherstellungsbenachrichtigung generiert und der Status der Überprüfung kehrt auf grün zurück.
      iv. Die Überprüfung kann mit einer Zeitverzögerung von 5 oder 10 Minuten angepasst werden. Wenn Sie eine Zeitverzögerung wählen, wird der Online-Zustand erst dann gemeldet, wenn das Gerät länger als den gewählten Verzögerungswert offline ist.
   b. System Update
      i. Diese Prüfung warnt den Benutzer, wenn ein System-Update verfügbar ist
2. **Softwareausführung**
   a. Prozesse
      ii. Bei dieser Prüfung wird ein definierter Prozess überwacht, und es wird eine Warnung ausgelöst, ob der Prozess läuft oder nicht läuft.
      iii. iii. Um diese Prüfung einzurichten, muss der Prozessdateiname oder der absolute Pfad eines Prozesses (z.B. Dateiname: bash oder teamviewerd ;

absoluter Pfad: /usr/bin/bash oder /opt/teamviewer/tv_bin/teamviewerd) im Konfigurationsmenü des Checks hinzugefügt werden.

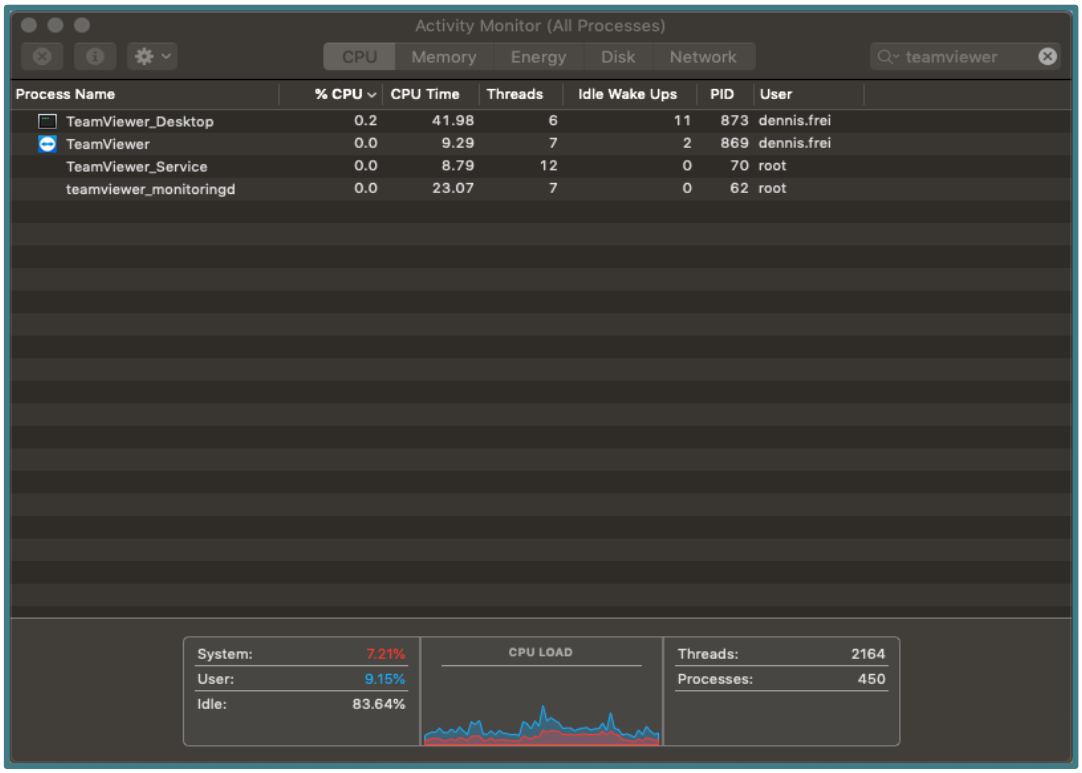


Bild: Aktivitätsmonitor und Dienst.

3. **Hardware**
    a. Speicherkapazität
        i. Diese Prüfung überwacht den freien Speicherplatz auf einem Systemlaufwerk und meldet, wenn der freie Speicherplatz unter dem definierten Wert liegt.
        ii. Einer Richtlinie können mehrere Speicherplatzprüfungen mit unterschiedlichen Laufwerksbuchstaben hinzugefügt werden.
        iii. Um die Speicherplatzprüfung einzurichten, fügen Sie zunächst den "Einhängepunkt" hinzu, der überwacht werden soll (z.B. /home oder /media/data)
        iv. Wählen Sie nach der Auswahl des Laufwerks die benötigte Variable:
            1. % – Prozentsatz des auf dem Laufwerk verbleibenden freien Speicherplatzes.
            2. GB – Gigabyte freier Speicherplatz auf der Festplatte.
            3. MB – Auf dem Laufwerk verbleibende Megabytes an freiem Speicherplatz.
        v. Nachdem Sie die Variable ausgewählt haben, geben Sie den minimalen Schwellenwert ein. Immer wenn der Plattenplatz unter diesen Wert fällt, wird ein Alarm ausgelöst.
    b. Arbeitsspeicherauslastung
        i. Diese Prüfung überwacht die Menge des freien Random-Access-Speichers oder RAM auf dem Gerät.

c. CPU-Auslastung
    i. Diese Prüfung überwacht die CPU-Auslastung auf dem Gerät, und es wird ein Alarm ausgelöst, wenn die Auslastung höher ist als der im Konfigurationsmenü der Prüfung festgelegte Prozentsatz.

4.3 Monitoring Richtlinie

Die Standardpolitik für Überwachung und Asset Management umfasst die folgenden Prüfungen, die unter

4.2 Monitoring Checks.

1. Ist Antiviren-Software installiert und aktiv?
2. Ist mehr als 500 MB RAM verfügbar?
3. Ist die CPU-Auslastung höher als 75%?
4. Wie ist der Zustand der Festplatte?
5. Ist der verfügbare Speicherplatz auf der Festplatte weniger als 10%?
6. Ist Windows Update aktiv?
7. Ist die Windows-Firewall aktiviert?

Für weitere politische Optionen lesen Sie bitte: 3.2 .

4.4 Remote Task Manager

Der Remote Task Manager kann für jedes Gerät geöffnet werden, auf dem Monitoring & Asset Management installiert ist. (Fenster)

Das Fenster zeigt eine aktuelle Liste von Prozessen oder Diensten auf dem entfernten Gerät an, die bei Bedarf beendet werden können.

> **Hinweis:** Dies ist ein sehr wichtiges Werkzeug, wenn Benutzer Fehler auf einem entfernten Computer beheben müssen, ohne eine Fernverbindung zu diesem Computer herzustellen.

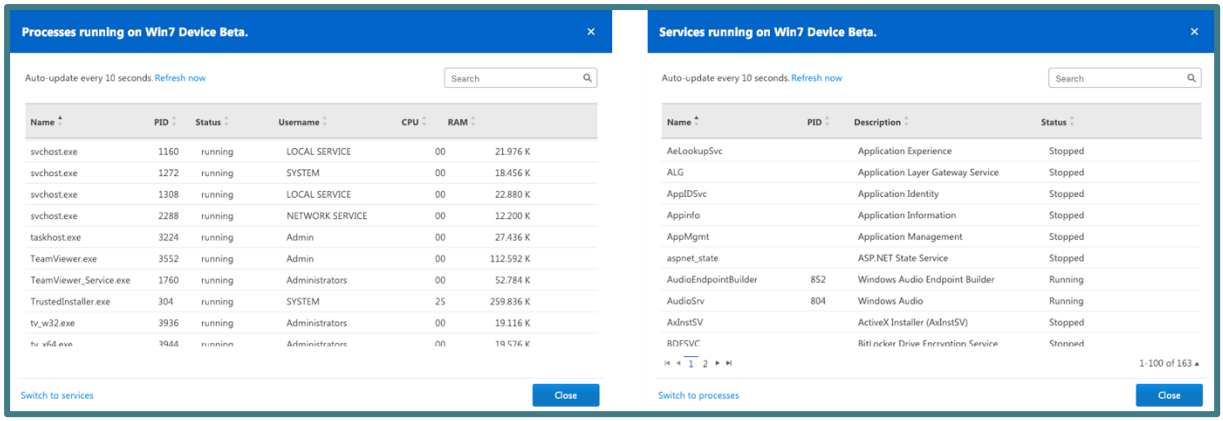


Bild: Remote Task Manager.

4.5 Alarme und Benachrichtigungen

4.5.1 Alarme

Alarme werden generiert, wenn das Risiko besteht, einen in der Überwachungsrichtlinie festgelegten Schwellenwert zu verletzen.

Alarme werden in der TeamViewer-Verwaltungskonsole und der TeamViewer-Anwendung angezeigt.

Es gibt verschiedene Alarmtypen:

1. Erhöhter Alarm
    a. Wenn bei einer Prüfung die Gefahr besteht, dass der konfigurierte Schwellenwert überschritten wird, wird ein Alarm erstellt und in der Verwaltungskonsole gemeldet.
    b. Der Alarm ist durch ein rotes Dreieck gekennzeichnet.

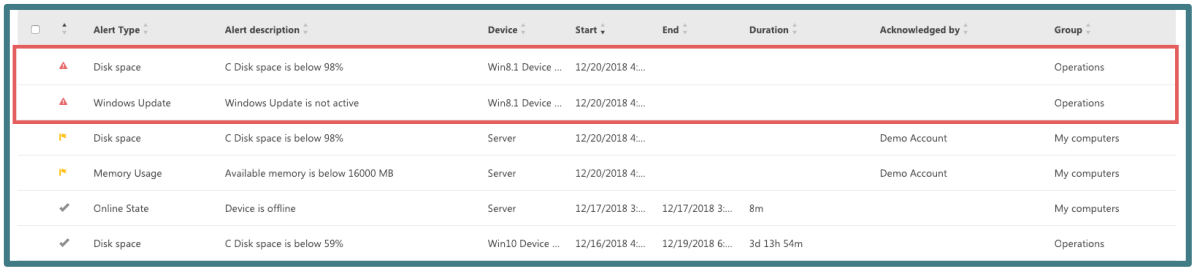
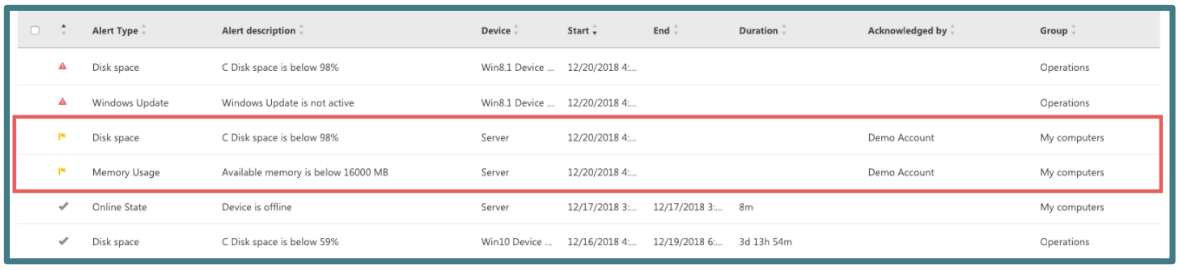


Bild: Erhöhter Alarm.

2. Bestätigter Alarm
    a. Ein ausgelöster Alarm kann vom Benutzer bestätigt werden. Sobald dies geschehen ist, wird der Alarm "quittiert".

b. Das Quittieren des Alarms bedeutet nicht, dass das Problem gelöst ist. Es bedeutet nur, dass der Supporter bestätigt hat, dass es ein Problem gibt, und es später beheben wird, da das Problem nicht kritisch genug ist, um sofort behoben zu werden.



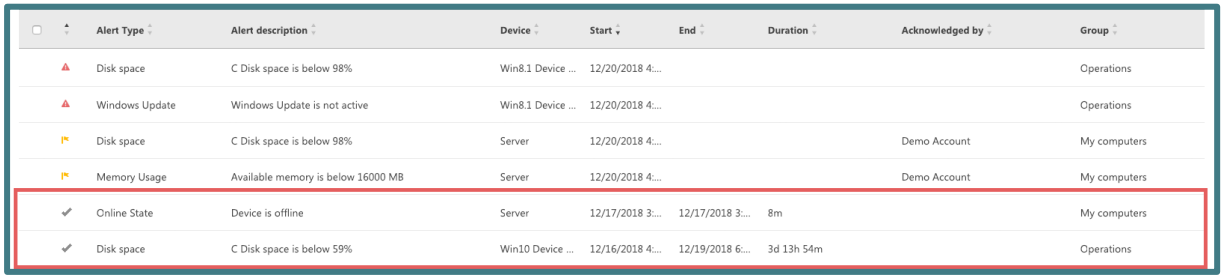
Alert Type	Alert description	Device	Start	End	Duration	Acknowledged by	Group
Disk space	C Disk space is below 98%	Win8.1 Device ...	12/20/2018 4:...				Operations
Windows Update	Windows Update is not active	Win8.1 Device ...	12/20/2018 4:...				Operations
Disk space	C Disk space is below 98%	Server	12/20/2018 4:...			Demo Account	My computers
Memory Usage	Available memory is below 16000 MB	Server	12/20/2018 4:...			Demo Account	My computers
Online State	Device is offline	Server	12/17/2018 3:...	12/17/2018 3:...	8m		My computers
Disk space	C Disk space is below 59%	Win10 Device ...	12/16/2018 4:...	12/19/2018 6:...	3d 13h 54m		Operations

Bild: Bestätigter Alarm.

3. Erholte/gelöschte Alarme

   a. Wenn ein ausgelöster Alarm zum definierten Schwellenwert zurückkehrt, erholt sich der Alarm automatisch.

   b. Bei den meisten Überwachungsprüfungen wird jede Minute versucht, zu analysieren, ob die Schwellenwerte verletzt oder wiederhergestellt wurden. Wenn die Prüfungen eine konfigurierte Zeitverzögerung haben, werden sie auf der Grundlage der Zeitverzögerung prüfen (z.B. Online-Zustandsprüfung mit einer konfigurierten 10-minütigen Verzögerung).



Alert Type	Alert description	Device	Start	End	Duration	Acknowledged by	Group
Disk space	C Disk space is below 98%	Win8.1 Device ...	12/20/2018 4:...				Operations
Windows Update	Windows Update is not active	Win8.1 Device ...	12/20/2018 4:...				Operations
Disk space	C Disk space is below 98%	Server	12/20/2018 4:...			Demo Account	My computers
Memory Usage	Available memory is below 16000 MB	Server	12/20/2018 4:...			Demo Account	My computers
Online State	Device is offline	Server	12/17/2018 3:...	12/17/2018 3:...	8m		My computers
Disk space	C Disk space is below 59%	Win10 Device ...	12/16/2018 4:...	12/19/2018 6:...	3d 13h 54m		Operations

Image: Erholter Alarm.

4.5.2 Benachrichtigungen

E-Mail-Benachrichtigungen können in der Überwachungsrichtlinie eingerichtet werden. Vom System akzeptierte E-Mail-Adressen sind diejenigen, die vom TeamViewer-Konto oder Firmenprofil erkannt werden:

- Bei TeamViewer-Accounts muss die E-Mail-Adresse in der Kontaktliste als Kontakt eingetragen sein.
- Für TeamViewer-Firmenprofile muss die E-Mail-Adresse als Kontakt oder Benutzer im Firmenprofil enthalten sein.

E-Mail-Benachrichtigungen werden gesendet von: notification@teamviewer-rm.com

> **Hinweis:** Wenn Sie mit Proxy oder benutzerdefinierten Firewalls arbeiten, kann eine Whitelist zur Domäne *.teamviewer-rm.com hinzugefügt werden.

E-Mail-Benachrichtigungen über ausgelöste oder wiederhergestellte Alarme enthalten die folgenden Informationen:

1. Name des Geräts, auf dem der Alarm ausgelöst wurde.
2. TeamViewer-ID.
3. Datum und Uhrzeit, zu der der Alarm ausgelöst wurde.
4. Name des Checks und der vordefinierte Schwellenwert.
5. Beschreibung des Alarms:
    a. Es werden prüfungsspezifische Informationen geschrieben.
    b. Dies wird für jede Prüfung unterschiedlich sein.
6. Mögliche Aktionen:
    a. Bestätigen Sie die Alarmverknüpfung.
    b. Link zum Überwachungsbericht anzeigen.
    c. Mit Geräte-Link verbinden.

4.6 Monitoring Geräte Ansicht

Die Geräteansicht ist so konzipiert, dass Metriken angezeigt werden, die für jedes Gerät relevant sind, auf dem Monitoring & Asset Management installiert ist.

In der Geräteansicht für das Monitoring kann der Benutzer alle relevanten Prüfungen sehen, die innerhalb ihrer Schwellenwerte liegen, sowie alle Prüfungen, die fehlgeschlagen sind.

Jede fehlgeschlagene Prüfung kann einzeln bestätigt und erneut geprüft werden, wenn der Benutzer entscheidet, dass der ausgelöste Alarm für den Betrieb des Geräts nicht kritisch ist.

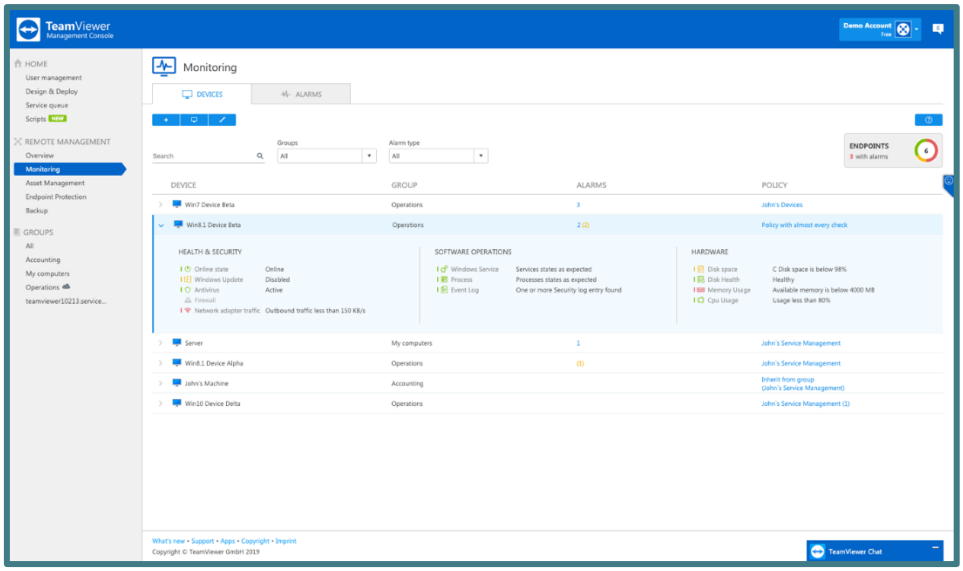


Bild: Geräte Ansicht für Monitoring für Windows

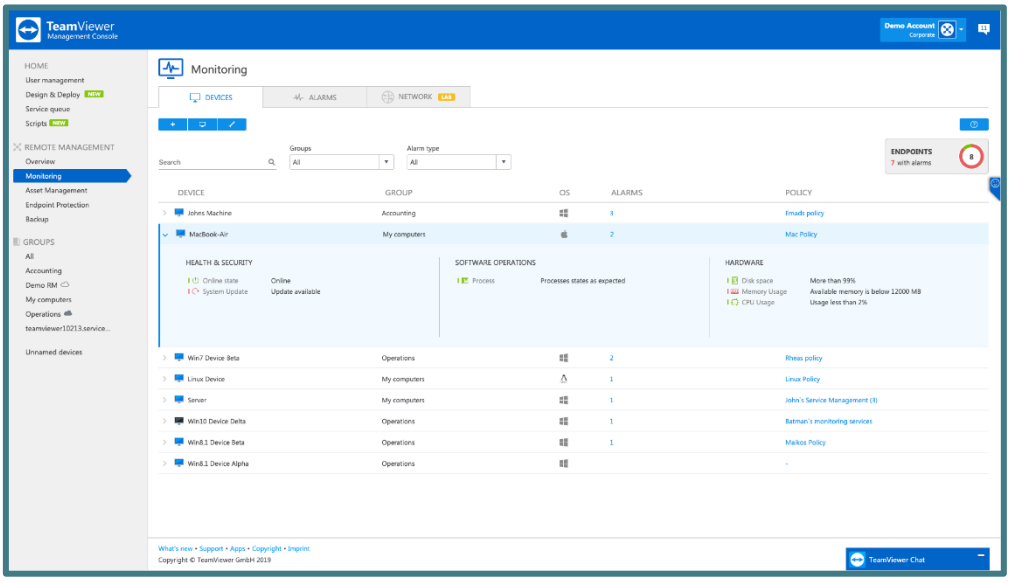


BIld: Geräte Ansicht für Monitoring für macOS.

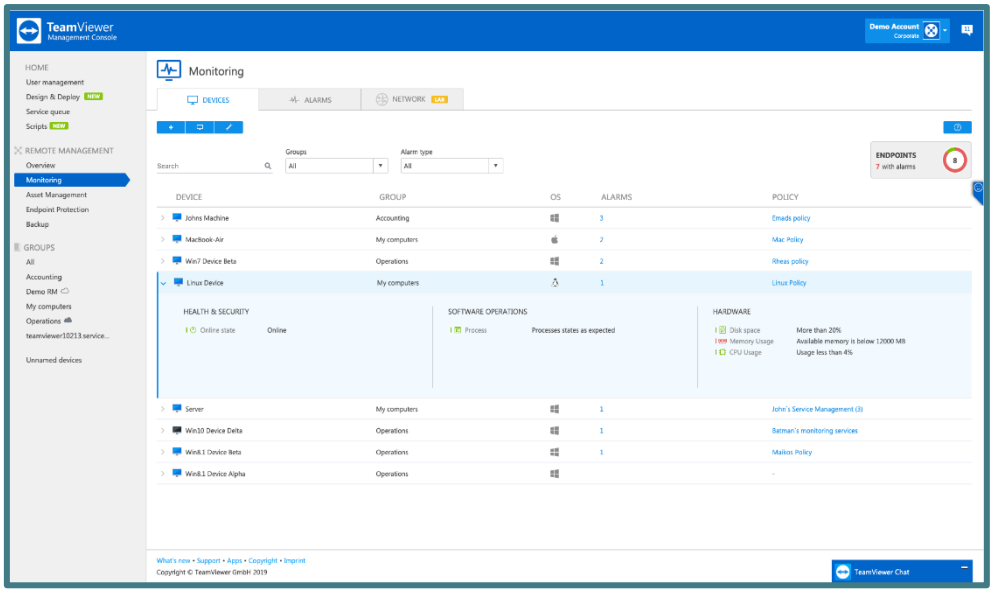


Bild: Geräte Ansicht für Monitoring für Linux.

4.7 Alarm Ansicht

Die Ansicht der Alarme konzentriert sich auf die Reaktion auf Vorfälle. Alle ausgelösten Alarme, bei denen die Prüfschwelle überschritten wurde, können gefiltert, organisiert und exportiert werden.

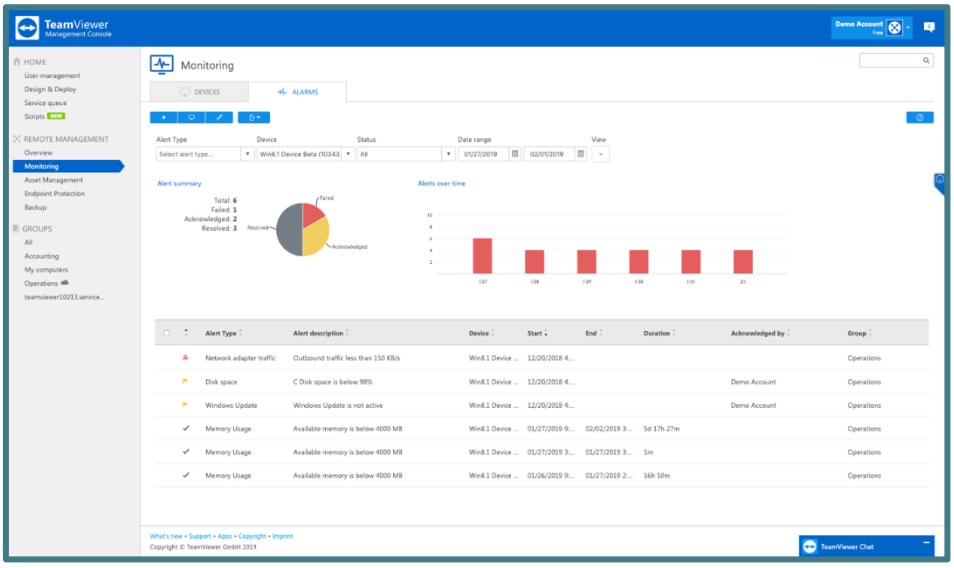


Bild: Alarm Ansicht für Monitoring.

4.7.1 Monitoring Filter

Das Filtern von Alarmen ermöglicht es dem Benutzer, einen umfassenden Überblick je nach Bedarf zu erhalten:

1. Filter nach Alarmtyp
2. Nach Gerät filtern
3. Nach Alarmstatus filtern
4. Nach Datumsbereich filternge

Ansichtseinstellungen können verwendet werden, um die Ansichtsstruktur der Berichte zu prüfen oder zu deaktivieren::

1. Spalten
    a. Alarm-Typ
    b. Alarm-Beschreibung
    c. Gerät
    d. Beginn
    e. Ende
    f. Dauer
    g. Anerkannt durch
    h. Gruppe
2. Gruppieren nach
    a. Alarm Type
    b. Gerät
    c. Keine Gruppierung
3. Andere
    a. Charts

4.7.2 Monitoring Export

Nach dem Filtern der Überwachungsalarmdaten kann die Exportfunktion verwendet werden, um die Überwachungsalarmberichte zu exportieren.

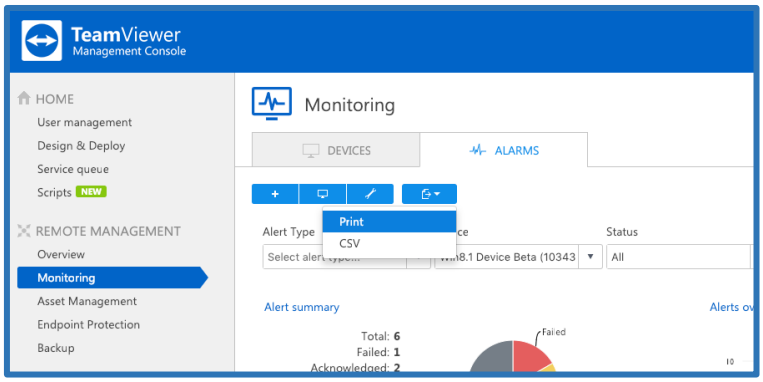


Bild: Exportfunktion im Monitoring.

Zum Drucken exportieren

Diese Funktion erzeugt eine Web-Ansicht, die mit Hilfe von Druck-Plugins ausgedruckt oder in einem beliebigen Dokumentformat gespeichert werden kann.

Exportieren nach CSV

Diese Funktion erzeugt und lädt eine CSV-Datei herunter, die gespeichert, verwaltet oder geändert werden kann, wenn dies für die Überprüfbarkeit oder andere Vorschläge erforderlich ist.

4.8 Netzwerk Monitoring

Um Netzwerkgeräte in Ihrem lokalen Netzwerk zu erkennen und zu überwachen, verwenden Sie das Netzwerk-Monitoring mit TeamViewer Monitoring.

Bei der Netzwerküberwachung werden Ihre entdeckten Netzwerkgeräte in eine der folgenden Kategorien eingeordnet:

- Computer – Für alle Windows-Computer, die während des Entdeckungsprozesses entdeckt wurden
- Router & Switch – Für alle Router und Switches, die während des Erkennungsprozesses erkannt wurden
- Drucker – Für alle Netzwerkdrucker, die während des Erkennungsprozesses erkannt wurden
- USV – Für alle Universal-Stromversorger, die während des Erkennungsprozesses erkannt wurden
- NAS – Für alle an das Netzwerk angeschlossenen Speicher, die während des Entdeckungsprozesses entdeckt werden
- Anderes Gerät – Für alle anderen Geräte, die eine IP-Adresse haben und in Ihrem lokalen Netzwerk verfügbar sind, aber in keine andere Kategorie passen

Die Netzwerküberwachung wurde als Laborversion veröffentlicht, so dass diese Funktion jetzt kostenlos genutzt werden kann. Um Netzwerk-Monitoring nutzen zu können, müssen Sie mindestens eine Lizenz für TeamViewer Monitoring besitzen, oder Sie können es während der Testphase testen. Wenn die Testphase von TeamViewer Monitoring abläuft, wird auch die Netzwerküberwachung in Ihrem Account deaktiviert.

Informationen zur Aktivierung der TeamViewer Monitoring Lizenz finden Sie unter 2.2 Lizenz .

Die **Systemanforderungen** finden Sie unter 2.3 System .

4.8.1 Netzwermonitoring Überwachung

Um das Netzwerk-Monitoring zu aktivieren, muss TeamViewer Monitoring auf dem Knoten* aktiviert werden, der Ihre Netzwerkgeräte entdecken und überwachen soll. Wenn Sie einen Knoten auswählen, auf dem TeamViewer Monitoring nicht aktiviert ist, wird es automatisch auf dem Knoten installiert.

*Node: Ist das Gerät, von dem aus die Netzwerküberwachung eine Erkennung auslöst und Ihre Netzwerkgeräte überwacht. Jeder Knoten kann sein eigenes lokales Netzwerk entdecken.

Die Netzwerküberwachung kann mit nur wenigen Klicks über die Registerkarte 'Netzwerk' in der Fernverwaltung aktiviert werden → Monitoring:

1. Klicken Sie auf "Gerät wählen" in der Registerkarte "Netzwerk".
2. Wählen Sie das entsprechende Gerät aus Ihrer Geräteliste aus. Das Gerät sollte online sein. Derzeit werden nur Windows-Geräte unterstützt.
3. Wählen Sie die erforderlichen Einstellungen und klicken Sie auf die Schaltfläche 'DISCOVER'.
    a. Vollständige Entdeckung
    b. Benutzerdefinierte Entdeckung
        i. Geben Sie den IP-Bereich ein
        ii. Geben Sie den SNMP-Community-String ein

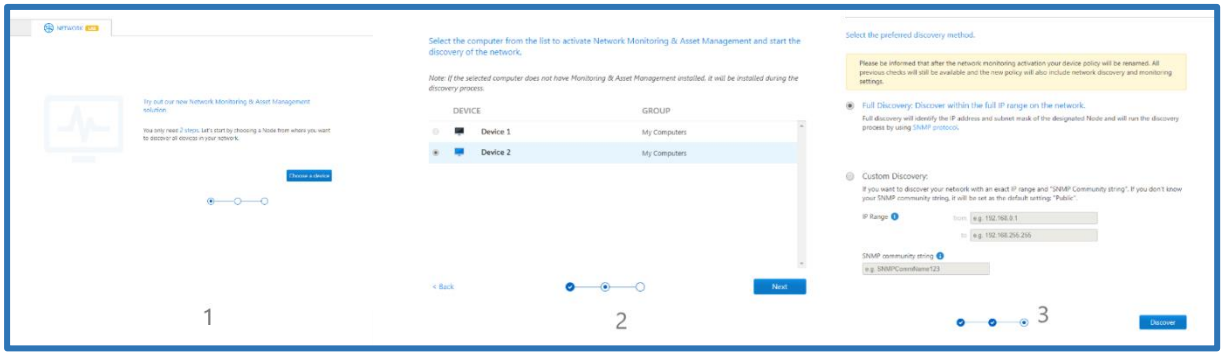


Bild: Netzwerkmonitoring Aktivierung.

Nach dem Ändern und Speichern der Sucheinstellungen startet das System eine Suche mit den neuen Einstellungen. Wenn Sie keine neue Suche durchführen möchten, drücken Sie Abbrechen.

4.8.2 Networkmonitoring Einstellungen

Nachdem die Suche abgeschlossen ist, können Sie die Sucheinstellungen jederzeit über das Einstellungsmenü ändern.

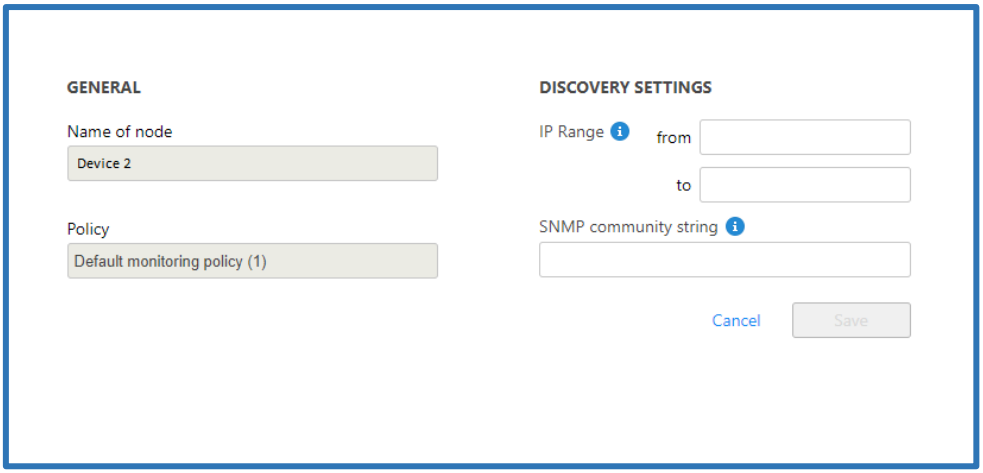


Bild: Netzwerkmonitoring Einstellungsfenster.

Nach dem Ändern und Speichern der Sucheinstellungen startet das System eine Suche mit den neuen Einstellungen. Wenn Sie keine neue Suche durchführen möchten, drücken Sie Abbrechen.

4.8.3 Überprüfungen der Netzwerküberwachung

Nachdem die Erkennung von Netzwerkgeräten abgeschlossen ist, können Sie Überprüfungen für die periodische Überwachung Ihrer Netzwerkgeräte einrichten. Derzeit unterstützt die Netzwerküberwachung die folgenden Prüfungen:

Für die Kategorie **Router & Switch**:

Port-Zustand: Falls ausgewählt, wird ein Alarm ausgelöst, wenn ein Port eines Routers oder Switches blockiert oder defekt ist. Dies funktioniert nur für Geräte mit SNMP-Unterstützung.

Für die Kategorie **Network Attached Storage (NAS)**:

Plattenplatz: Wenn dieses Kontrollkästchen aktiviert ist, wird ein Alarm ausgelöst, wenn der NAS-Festplattenplatz unter dem konfigurierten Schwellenwert liegt. Dies funktioniert nur bei Geräten mit SNMP-Unterstützung.

Festplattenzustand: Wenn dieses Kontrollkästchen aktiviert ist, wird ein Alarm ausgelöst, wenn der Zustand der NAS-Festplatte Hardwarefehler meldet. Dies funktioniert nur bei Geräten mit SNMP-Unterstützung.

Für die Kategorie **Drucker**:

Toner: Wenn dieses Kontrollkästchen aktiviert ist, wird ein Alarm ausgelöst, wenn der Toner von einem Netzwerkdrucker zu schwach ist. Dies funktioniert nur bei Geräten mit SNMP-Unterstützung.

Papier: Wenn dieses Kontrollkästchen aktiviert ist, wird ein Alarm ausgelöst, wenn das Papier von einem Netzwerkdrucker zu schwach ist. Dies funktioniert nur bei Geräten mit SNMP-Unterstützung.

Für die Kategorie **Unterbrechungsfreie Stromversorgung (USV)**:

Kapazität der Batterie: Falls ausgewählt, wird ein Alarm ausgelöst, wenn die Batteriekapazität der USV unter den konfigurierten Schwellenwert fällt. Dies funktioniert nur bei Geräten mit SNMP-Unterstützung.

Verbleibende Akkulaufzeit: Wenn dieses Kontrollkästchen aktiviert ist, wird ein Alarm ausgelöst, wenn die Energiespeicherung der USV "in Minuten" unter den konfigurierten Schwellenwert fällt. Dies funktioniert nur bei Geräten mit SNMP-Unterstützung.

Für die Kategorie **Computer**:

Überwachen Sie Ihre Computer mit dem TeamViewer Monitoring Dienst.

Die Kontrollen werden alle 1 Minute durchgeführt. Wenn ein Problem festgestellt wird, wird in der Verwaltungskonsole ein Alarm angezeigt.

Zusätzlich zu den oben genannten Überprüfungen können die Benutzer die IP-Adresse sowie den On- und Offline-Status für jedes entdeckte Gerät sehen.

Tipp: Die Netzwerküberwachung verwendet das SNMP-Protokoll zur Erkennung und Überwachung des Netzwerks. Um Ihre Netzwerkgeräte effektiv zu überwachen, sollte SNMP in Ihrem lokalen Netzwerk nicht eingeschränkt werden.

4.8.4 Netzwerkmonitoring Richtlinie

Bitte beachten Sie, dass nach der Aktivierung der Netzwerküberwachung Ihre Geräterichtlinie umbenannt wird. Alle vorherigen Überprüfungen (TeamViewer Monitoring Überprüfungen) werden weiterhin verfügbar sein, und die neue Richtlinie wird auch Einstellungen zur Netzwerkerkennung und -überwachung enthalten.

Sie können die Richtlinienseite für die Netzwerkerkennung von hier aus öffnen:

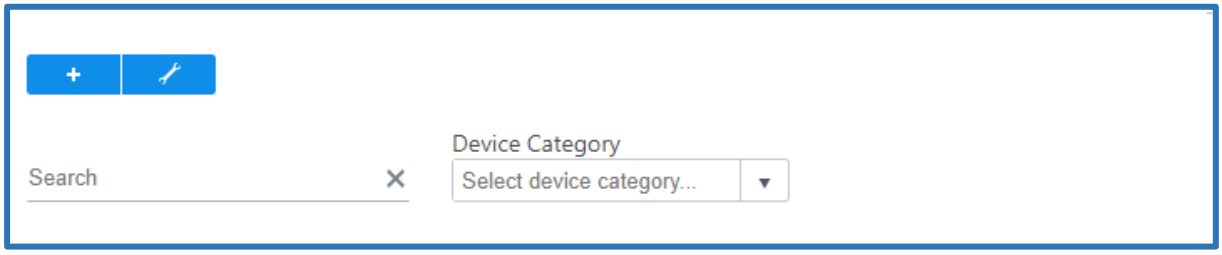


Bild: Symbol zum Öffnen der Netzwerkerkennungsrichtlinie

Wählen Sie als Nächstes aus, welche Richtlinie Sie bearbeiten möchten, und wählen Sie die erforderlichen Prüfungen für die Überwachung Ihrer Netzwerkgeräte aus.

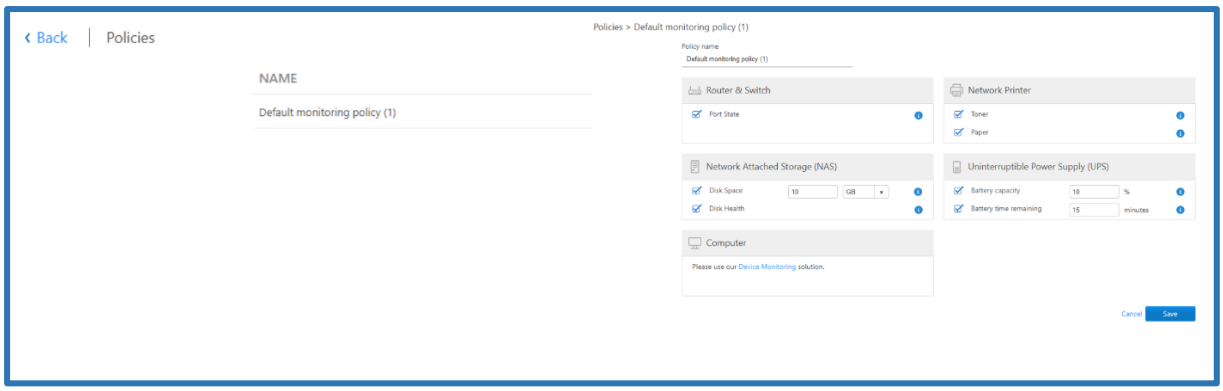


Bild: Richtlinienseite für die Netzwerkermittlung

4.8.5 Netzwerkmonitoring Ansichten

Es gibt 3 Arten von Ansichten für die Netzwerküberwachung:

Alle Nodes-Ansicht: In dieser Ansicht sehen Sie alle Ihre Netzwerke an einem Ort mit Details zu Gerätemenge und Alerts. Klicken Sie auf die Schaltfläche Home, um zu dieser Ansicht zu gelangen.

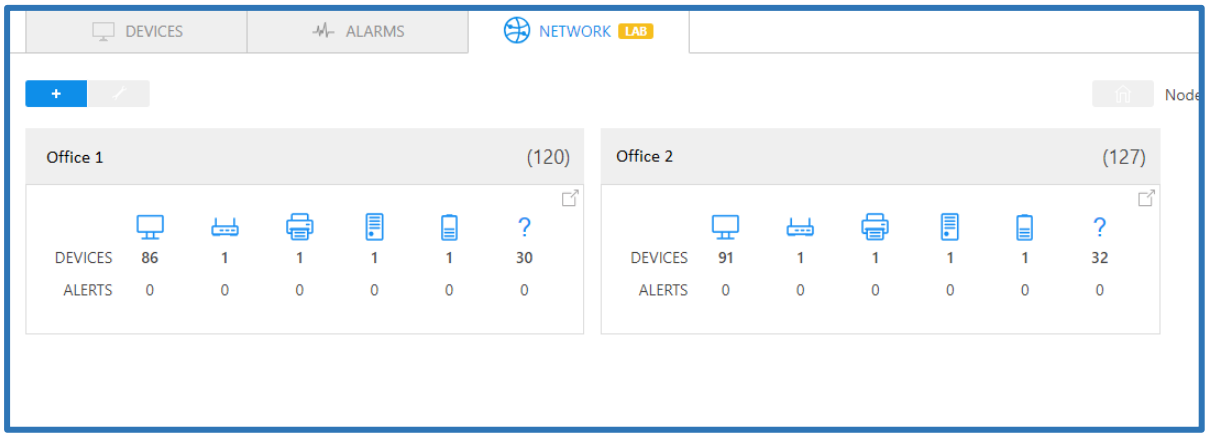


Bild: Ansicht aller Nodes in der Netzwerküberwachung.

Listenansicht: In dieser Ansicht sehen Sie alle Ihre Netzwerke an einem Ort mit Angaben zur Gerätemenge und zu Warnmeldungen. Sie können auf die Kopfzeile des Knotens klicken und zur Listenansicht gehen, um weitere Details zu erhalten. Sie können auch Zeilen erweitern, um mehr Details über jedes Gerät zu sehen.

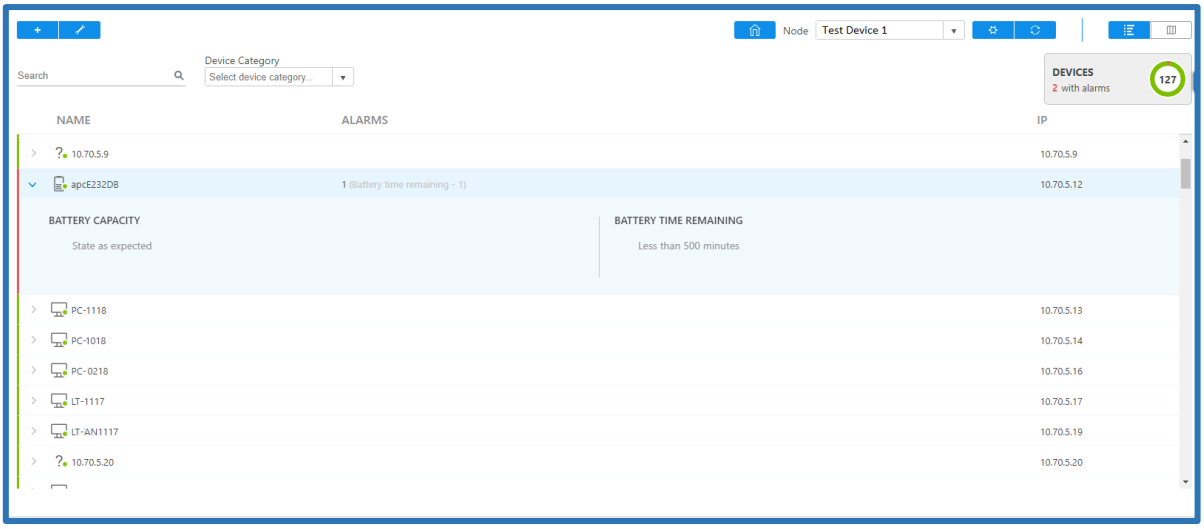


Image: List view of network monitoring.

Kartenansicht: Die Kartenansicht befindet sich derzeit im Aufbau. Sie ermöglicht es Ihnen, die Verbindungen zwischen den entdeckten Netzwerkgeräten zu sehen.

4.9 Asset Management

Nach der Installation des Dienstes Monitoring & Asset Management wird eine Momentaufnahme der installierten Software und Hardware gesammelt und in der Geräteansicht und der Asset-Ansicht organisiert. Informationen über fehlende Patches werden ebenfalls in der Asset Management Geräteansicht angezeigt.

4.9.1 Geräteansicht

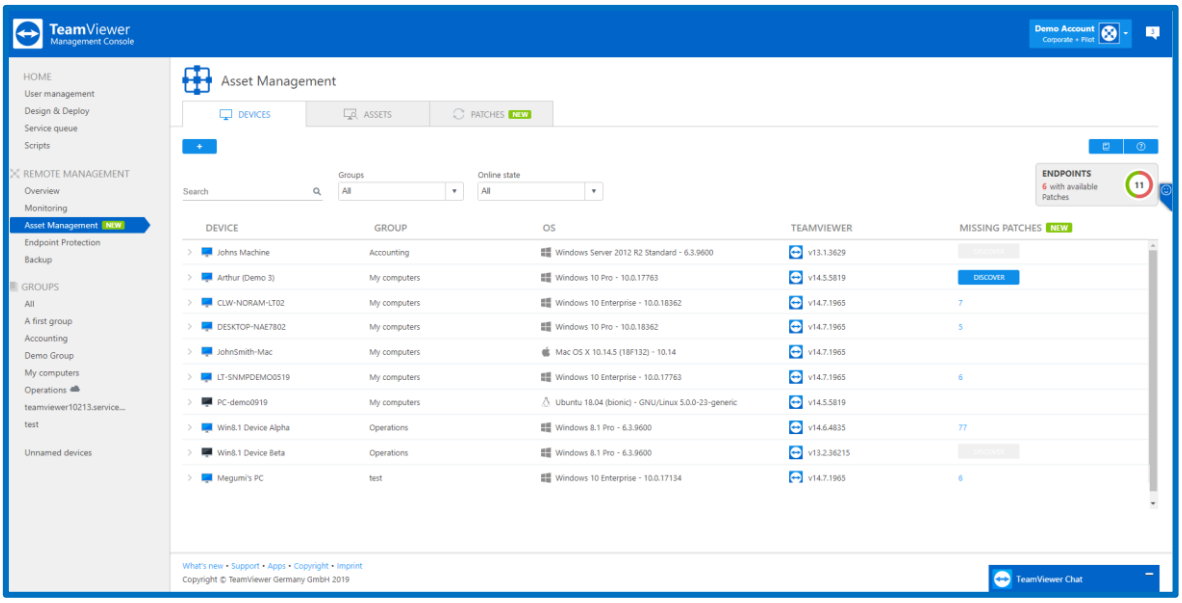


Bild: Geräteansicht in Asset Management.

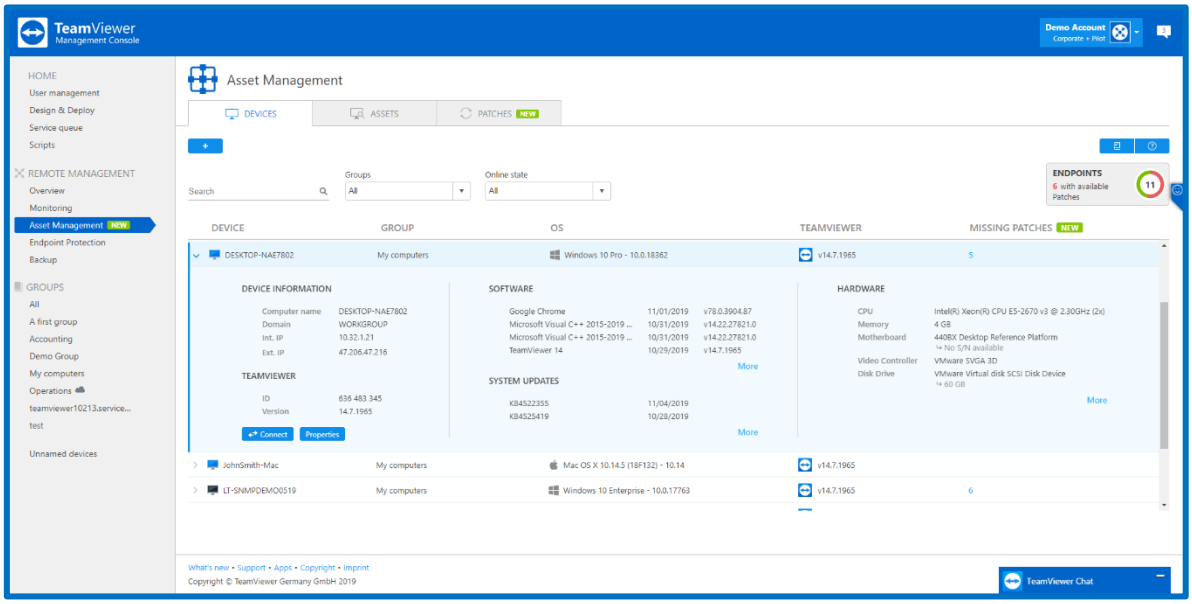


Bild: Bestandsansicht in Geräteansicht in Asset Management für Windows.

In der Geräteansicht werden die Informationen in den folgenden Kategorien sortiert und angezeigt:

Geräte-Informationen: Rechnername, Domäne, interne IP, externe IP

Fehlende Patches zählen: Fehlende Patches des Betriebssystems und von Drittanbietern werden auf dem ausgewählten Rechner gezählt.

TeamViewer: TeamViewer-ID, TeamViewer-Version

Software: Liste der kürzlich installierten Software (Windows, macOS)

Pakete: Liste aller installierten Pakete in alphabetischer Reihenfolge (Linux)

System Update: Liste der kürzlich installierten Updates

Hardware: CPU-Name und Modell, physischer Speicher (RAM), Modell und Seriennummer der Hauptplatine (falls verfügbar), Name und Modell des Video-Controllers, Name, Modell, Kapazität und Seriennummer der Festplatten (falls verfügbar).

4.9.2 Bestandsansicht

Aus der Asset-Ansicht können Berichte auf der Grundlage der unten aufgeführten Kategorien erstellt und als Web-Ansicht (Druck) oder als CSV-Datei exportiert werden.

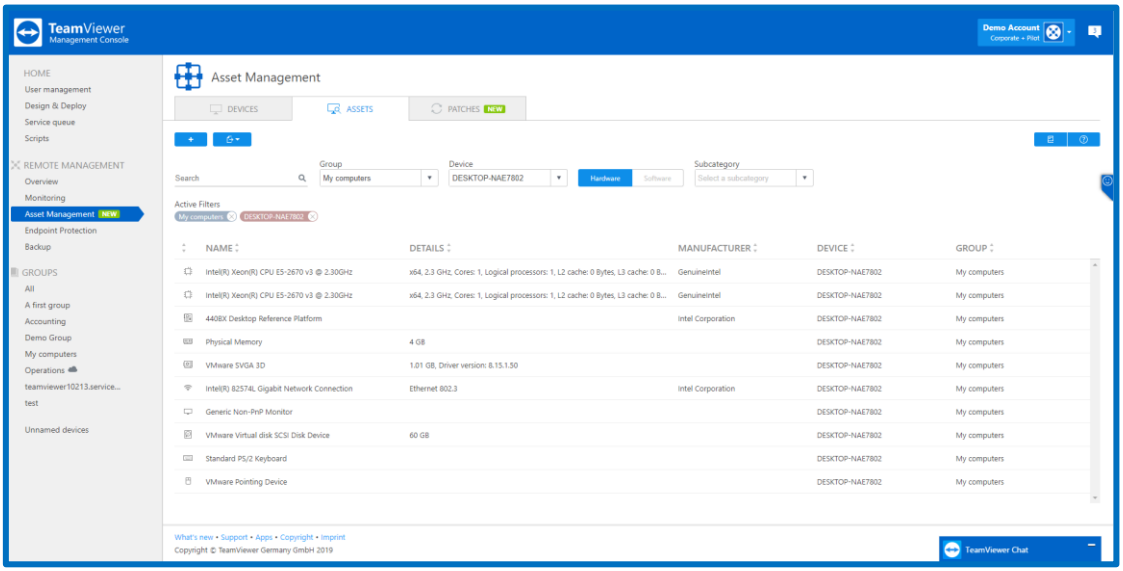


Bild: Hardware Bestand in Asset Management.

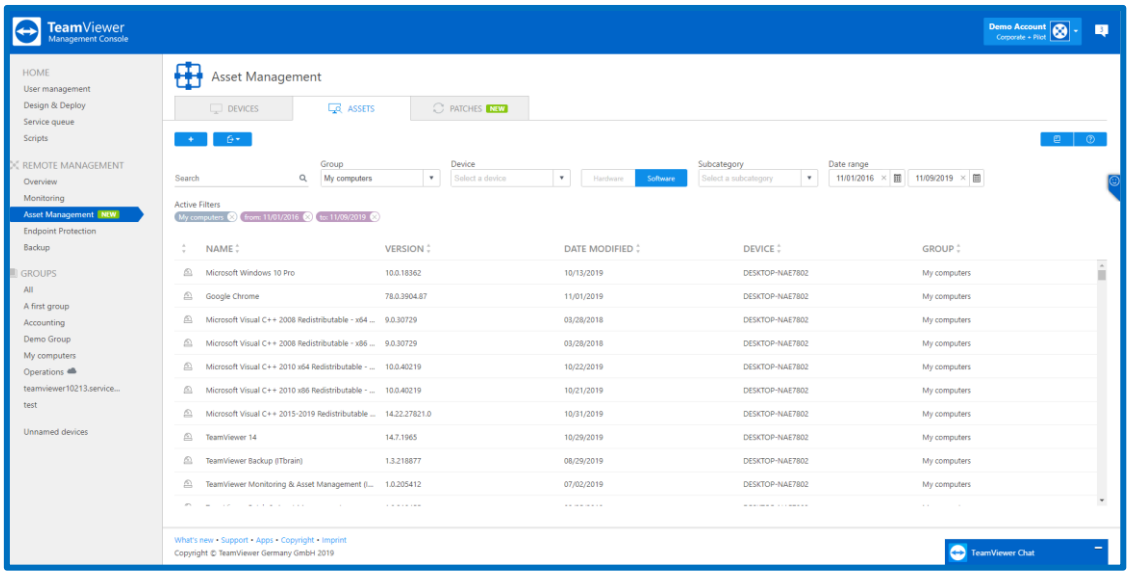


Bild: Software Bestand in Asset Management

Report	Description
Software	Überblick über die auf den Geräten installierten Anwendungen, einschließlich der Software-Version und des Datums.
Aktualisierungen	Übersicht über die installierten Windows-Updates einschließlich des Datums.
Hardware	Überblick über die installierten Hardwarekomponenten, einschließlich Typ, Name und Hersteller. Diese Übersicht enthält alle unten aufgeführten Berichte.
Bearbeiter	Überblick über die auf den Geräten installierten Prozessoren, einschließlich Name, Details und Hersteller.
Hauptplatine	Übersicht über die in den Geräten installierten Hauptplatinen, einschließlich Name, Details und Hersteller.
Physikalischer Speicher (RAM)	Übersicht über den in den Geräten installierten internen Speicher, einschließlich Name, Details und Hersteller.
Plattenlaufwerk	Überblick über die in den Geräten installierten Festplatten, einschließlich Name, Details und Hersteller.
Optisches Laufwerk	Überblick über die an die Computer angeschlossenen Eingabegeräte (einschließlich Name, Details und Hersteller).
Video-Steuerung	Übersicht über die in den Geräten installierten Grafikkarten, einschließlich Name, Details und Hersteller.
Netzwerk	Überblick über die in den Geräten installierten Netzwerkkarten, einschließlich Name, Details und Hersteller.
Tastatur	Überblick über die an die Geräte angeschlossenen Tastaturen, einschließlich Name, Details und Hersteller.
Zeigegerät	Überblick über die an die Computer angeschlossenen Eingabegeräte, einschließlich Name, Details und Hersteller

4.9.2 Patch Ansicht

In der Patch-Ansicht können Sie detaillierte Informationen über fehlende Patches des Betriebssystems und von Drittanbietern für Ihre Geräte sehen.

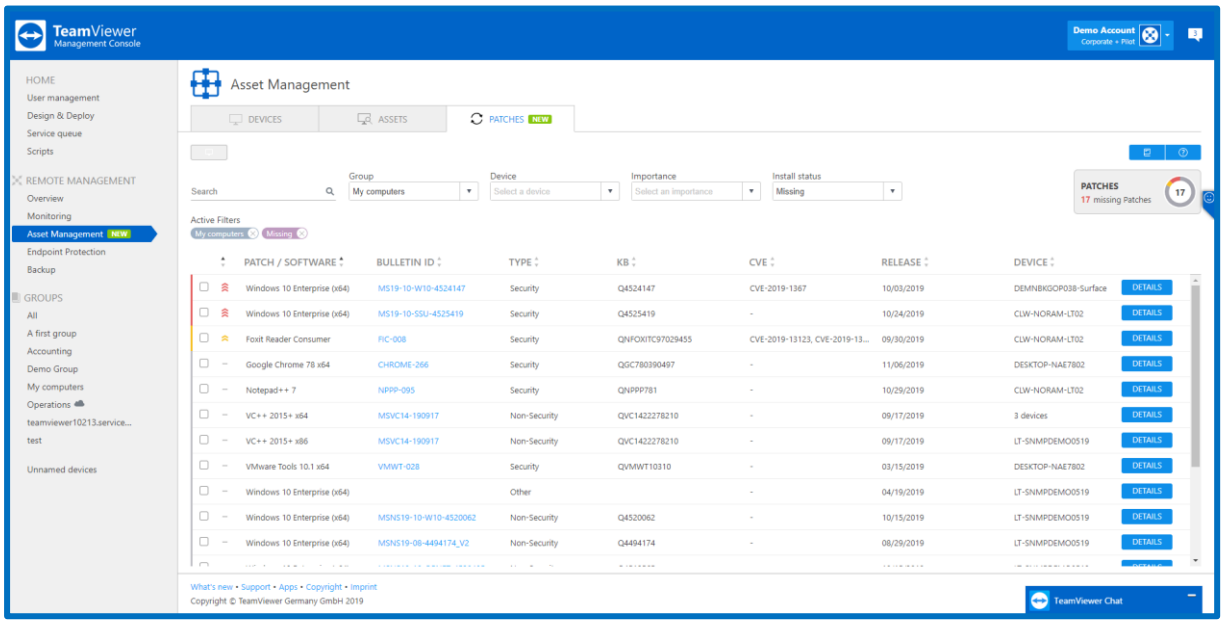


Bild: Patch Ansicht in Asset Management

Jedes einzelne Patch hat die unten beschriebenen Felder:

Symbol für den Schweregrad: Dieses Feld zeigt die Wichtigkeit des Patches an -> Kritisch, Wichtig, Niedrig, Nicht bewertet.

Patch/Software: Hier sehen Sie den Patch-Namen und die Version für einige Patches

Bulletin-ID: Die vom Anbieter angegebene Patch-ID. Die ID ist auch ein Link zum Changelog, das von jedem Softwarehersteller zur Verfügung gestellt wird.

Typ: Dieses Feld zeigt an, ob es sich bei dem Patch um einen Sicherheits- oder Nicht-Sicherheits-Patch handelt (diese Information stammt vom Software-Hersteller).

KB: Dies ist die Artikelnummer der Wissensdatenbank

CVE: Dieses Feld enthält alle häufigen Schwachstellen und Gefährdungen, die mit dem Patch zusammenhängen.

Release: Hier können Sie sehen, wann jeder Patch veröffentlicht wurde

Gerät: In diesem Feld wird der Gerätename angezeigt, auf dem der Patch fehlt. Falls es mehrere Geräte gibt, auf denen derselbe Patch fehlt, sehen Sie anstelle des Gerätenamens die Anzahl der betroffenen Geräte.

Details: Die Schaltfläche nach dem Anklicken, auf der Sie einige kurze Hinweise des Herstellers und die Patch-Größe sehen.

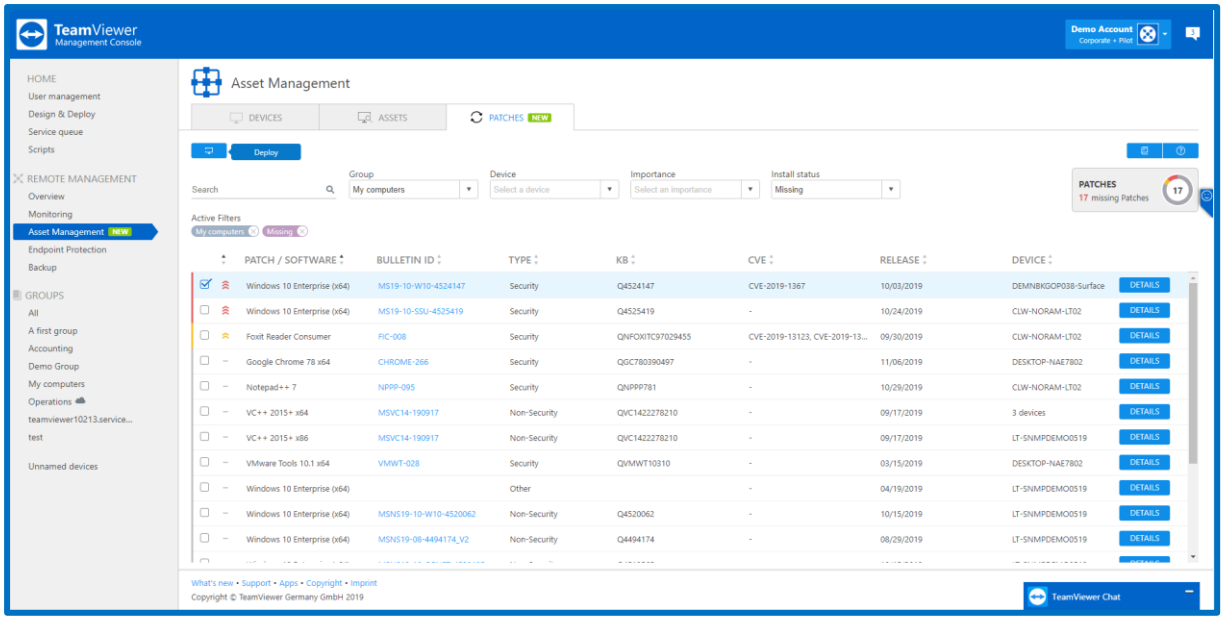


Bild: Patch Deployment Ansicht

In der Patch-Ansicht innerhalb von Asset Management können Sie einen Patch oder mehrere Patches auswählen und die ausgewählten Patches auf einem oder mehreren Geräten bereitstellen. Nachdem Sie einen Patch ausgewählt haben, brauchen Sie nur noch auf den Deploy-Button zu drücken.

In der Patch-Ansicht können Sie fehlende Patches filtern nach:

- Gruppe
- Gerät
- Bedeutung
- Installationsstatus (hier können Sie auch eine Vorschau der installierten Patches sehen)

Die Bereitstellung von Patches ist nur für Online-Geräte möglich.

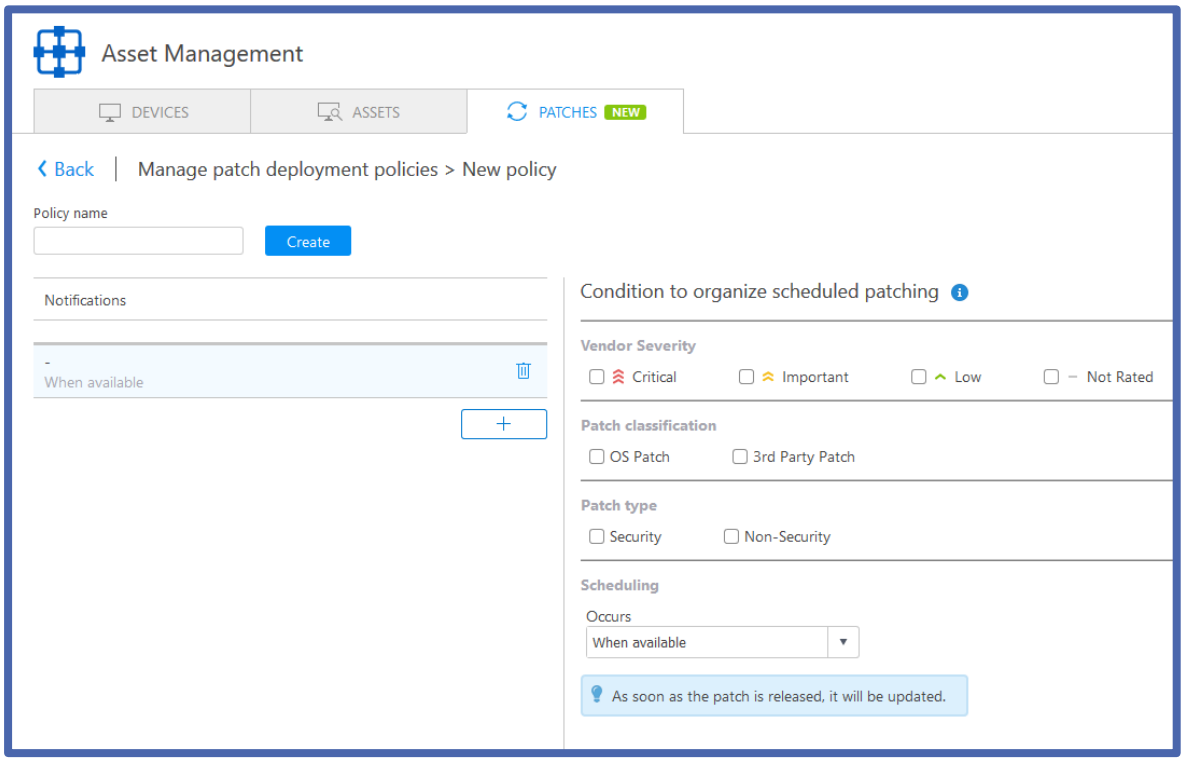
In der Patch-Ansicht können Sie einige Patches sehen, die nicht auswählbar sind, die Zeile ist mit diesem Tooltip ausgegraut: "Dieser Patch kann nicht aus der Ferne installiert werden. Bitte verbinden Sie sich mit dem Gerät und patchen Sie es manuell." Das bedeutet, dass die Patches einige zusätzliche Aktionen auf der Geräteseite erfordern, z.B. Captcha, zusätzliche Authentifizierung, EULA akzeptieren usw.

4.9.3 Patch Management Richtlinie

Mit dem Patch Management können Sie vordefinierte Kriterien festlegen, auf deren Grundlage das System die automatische Patch-Verteilung auslöst. Eine Standard-Patch-Management-Richtlinie ist eine leere Richtlinie ohne jegliche Aktion. Sie können die Einstellungen und Bedingungen in den Patchverwaltungsrichtlinien jederzeit bearbeiten und ändern.

In Asset Management können Benutzer jetzt unter der Registerkarte "Gerät" einen Richtlinienabschnitt sehen. Hier können Benutzer Richtlinien für die automatische Patch-Verteilung definieren und auswählen.

Im Patchverwaltungs-Richtlinienfenster können Benutzer neue Richtlinien erstellen und bestehende löschen oder bearbeiten. Über das 3-Punkte-Menü können Benutzer Richtlinien duplizieren. Um eine neue Richtlinie zu erstellen, müssen Benutzer auf die Schaltfläche "+" auf der rechten unteren Seite klicken. Nach der Erstellung einer neuen Richtlinie sehen die Benutzer das unten angezeigte Menü.



Die Police sollte einen Namen haben (dies ist ein Pflichtfeld), und jede Police kann bis zu 5 Bedingungen enthalten. In jeder Bedingung können Benutzer die erforderlichen Kriterien und den Zeitplan für die automatische Patch-Bereitstellung festlegen. Jede Bedingung hat mehrere Felder, die ausgefüllt werden müssen, um die Bedingung speichern zu können. Diese Felder sind:

- **Wichtigkeit**
  - (kritisch, wichtig, niedrig, nicht bewertet)
- **Einstufung des Patches**
  - Betriebssystem-Patches
  - 3rd Party Patches
- **Patch Typ**
  - Sicherheit
  - keine Sicherheitsrelevanz
- **Zeitplanung für Deployment**
  - Täglich
  - Wöchentlich
  - Monatlich
  - Sobald verfügbar

Die Erstellung einer Richtlinie ohne definierte Bedingungen löst keine Aktionen aus.

Nachdem die erforderlichen Bedingungen hinzugefügt und den Geräten Richtlinien zugewiesen wurden, überprüft das System automatisch die eingestellten Bedingungen und löst die Bereitstellung derjenigen Patches aus, die den vordefinierten Bedingungen entsprechen.

Hinweis: Um die Sicherheit Ihrer Geräte nach der ersten Richtlinienzuweisung zu gewährleisten, prüft das System die Bedingungen und löst sofort die Bereitstellung für diejenigen fehlenden Patches aus, die die festgelegten Bedingungen erfüllen (auch wenn die Planung für ein zukünftiges Datum festgelegt wurde). Danach wird die nächste Verteilung gemäß dem festgelegten Zeitplan erfolgen.

Hinweis: In Fällen, in denen das automatisch geplante Deployment nicht durchgeführt werden kann (z.B. Gerät wird offline sein), sobald das Gerät verfügbar ist, wird das Deployment nach dem ersten Rescan automatisch ausgelöst.

5. Endpoint Protection

Verwenden Sie den **TeamViewer Endpoint Protection** Dienst, um Ihre Geräte vor Malware, Ransomware und mehr zu schützen.

Informationen zur **Lizenzaktivierung** finden Sie unter 2.2 Lizenz .

Die **Systemanforderungen** finden Sie unter 2.3 Systemanforderungen.

Für die **Konfiguration von Richtlinien** und deren Zuweisung zu Geräten lesen Sie bitte: 3.2 .

Die konfigurierten Geräte werden gescannt und durch die zugewiesenen Richtlinien geschützt, die unter 3.2 . Immer wenn Malware auf dem Gerät erkannt wird, wird eine Warnung ausgelöst und als Warnmeldung in der TeamViewer-Verwaltungskonsole und der TeamViewer-Vollversion angezeigt. Eine Alarm-E-Mail-Benachrichtigung zeigt auch an, dass auf einem der Geräte Malware entdeckt wurde.

5.1 Endpoint Protection Aktivierung

Zur Aktivierung von Endpunkten siehe: 3.1

5.2 Endpoint Protection Richtlinien

Die Standardrichtlinie für den Endgeräteschutz umfasst die folgenden Scans und Einstellungen:

1. Schneller Scan, täglich 09:00 Uhr
2. Vollständiger Scan, täglich um 12:00 Uhr
3. Echtzeit-Schutz
4. Wechseldatenträger beim Anschluss scannen
5. Tray-Symbol

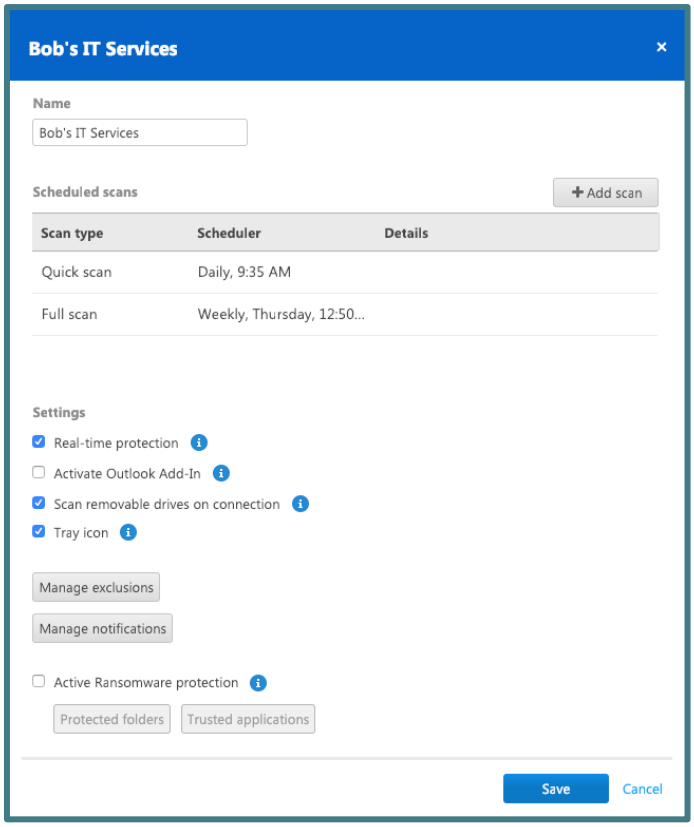


Bild: Richtlinienansicht in Endpoint Protection.

5.2.1 Endpoint Protection Einstellungen

Echtzeitschutz

Wählen Sie, ob der Echtzeitschutz für die Richtlinie aktiviert werden soll oder nicht. Wenn aktiviert, werden alle Dateien, auf die zugegriffen wird (geöffnet, ausgeführt usw.), auf Malware gescannt. Ist er deaktiviert, werden Bedrohungen nur dann erkannt, wenn ein Scan durchgeführt wird.

> **Hinweis:** Wenn der Echtzeitschutz deaktiviert ist, ist das Gerät zwischen den Scans potenziell gefährdet.

Outlook Add-In:

Das Endpoint Protection Outlook Add-In ist ein Visual Studio Tool für Office-Add-Ins für Microsoft Outlook. Dadurch kann TeamViewer Endpoint Protection infizierte Anhänge, die in den Outlook-Archivdateien (.pst,.ost) gefunden werden, während sie von Outlook verwendet werden, löschen.

Andernfalls ist TeamViewer Endpoint Protection nicht in der Lage, diese Art von Bedrohungen zu löschen, ohne zuvor Outlook zu schließen. Die Verwendung dieser Funktion erfordert die Aktivierung des Outlook-Add-Ins in der TeamViewer-Verwaltungskonsole.

Wechseldatenträger bei Anschluss scannen:

Durch die Aktivierung dieser Funktion wird automatisch ein Scan auf allen Wechsellaufwerken gestartet, wenn diese an das Gerät angeschlossen werden.

Definieren Sie eine beliebige Anzahl von Scans. Je nach Scan-Typ und Zeitplan werden alle Geräte regelmäßig auf Malware gescannt.

Klicken Sie auf die Schaltfläche "Scan hinzufügen" und definieren Sie einen Scan.

Wählen Sie zwischen den folgenden Optionen:

1. **Schneller Scan:** TeamViewer Endpoint Protection scannt nur bestimmte Daten, laufende Prozesse und die Registrierung. Auf diese Weise wird der Scan schnell abgeschlossen und die wichtigsten Daten werden geschützt.
2. **Vollständiger Scan:** TeamViewer Endpoint Protection scannt alle Festplatten Ihrer Geräte vollständig. Dieser Scan dauert länger als ein schneller Scan. Die Daten des Geräts sind vollständig geschützt.
3. **Benutzerdefinierter Scan**: TeamViewer Endpoint Protection scannt eine definierte Festplatte, einen Ordner oder eine Datei. Geben Sie dazu den Pfad wie folgt ein: C:\Folder\Filename.fileextension

> **Hinweis**: Bitte beachten Sie, dass die Geschwindigkeit Ihres Systems für die Dauer eines Scans beeinträchtigt werden kann.

Tray Icon:

Dadurch kann der Benutzer den aktuellen Status des Endpoint-Schutzes und die Benachrichtigungen über erkannte Bedrohungen einsehen. Der Benutzer wird auch in der Lage sein, schnelle und vollständige Scans auszulösen.

5.2.2 Ausnahmen

Hier kann der Benutzer bestimmte Laufwerke, Ordner, Dateien oder Dateitypen angeben, die von der Prüfung ausgeschlossen werden sollen (bspw.. D:\ um Laufwerk D auszuschließen, C:\\Directory\ um einen Ordner auszuschließen, *.xyz um einen Dateitypen auszuschließen).

5.2.3 Benachrichtigungen

Der Benutzer kann Benachrichtigungen über die Computer- und Kontaktliste einrichten. Der Endpunktschutz bietet die Möglichkeit, bei allen erkannten Bedrohungen, die sofortige Aufmerksamkeit erfordern, benachrichtigt zu werden. Der Benutzer kann auch entscheiden, ob die Benachrichtigungen in der TeamViewer-Konsole angezeigt werden sollen, und er kann auch die E-Mail-Adresse angeben, an die die Benachrichtigungen gesendet werden sollen.

Wenn eine Bedrohung erkannt wird, sendet Endpoint Protection eine E-Mail-Benachrichtigung an die definierten E-Mail-Adressen. Der Benutzer kann die E-Mail-Adressen angeben, die Benachrichtigungen über erkannte Bedrohungen erhalten sollen.

Bei der Auswahl Ihrer Benachrichtigungseinstellungen haben Sie die folgenden Optionen:

1. **Für alle erkannten Bedrohungen:** Dies ist die Standardeinstellung. Sie werden über jede Bedrohung, die auf einem Ihrer Geräte erkannt wird, benachrichtigt.
2. **Nur wenn ich Maßnahmen ergreifen muss:** Wenn eine Bedrohung erkannt wird, verschiebt Endpoint Protection die betroffene(n) Datei(en) in die Quarantäne und beseitigt so die Bedrohung. Sie werden nur dann über eine Bedrohung benachrichtigt, wenn Sie sofort Maßnahmen ergreifen müssen (z.B. wenn Sie den Computer neu starten müssen, um eine Bedrohung in Quarantäne zu verschieben).
3. **Niemals:** Alle Benachrichtigungen sind deaktiviert. Wenn Sie diese Option wählen, müssen Sie den Alarmbericht öffnen, um Informationen über erkannte Bedrohungen zu erhalten. Auch bei deaktivierten Warnmeldungen bleiben Ihre Systeme durch Endpoint Protection geschützt**.**

Vom System akzeptierte E-Mail-Adressen sind diejenigen, die vom TeamViewer-Konto oder Firmenprofil erkannt werden:

1. Bei TeamViewer-Konten muss die E-Mail-Adresse als Kontakt in der Kontaktliste enthalten sein.
2. Für TeamViewer-Firmenprofile muss die E-Mail-Adresse als Kontakt oder als Benutzer im Firmenprofil enthalten sein.

E-Mail-Benachrichtigungen werden gesendet von: notification@teamviewer-rm.com

> **Hinweis:** Wenn Sie mit Proxy oder benutzerdefinierten Firewalls arbeiten, kann eine Whitelist zur Domäne *.teamviewer-rm.com hinzugefügt werden.

5.3 Endpoint Protection Dashboard

5.3.1 Endpunkte verwalten

Dadurch erhält der Benutzer einen Überblick über alle Geräte mit aktiviertem Endpoint Protection. Der Filter oben rechts im Dialogfeld ermöglicht es dem Benutzer, anhand des Gerätenamens nach einem bestimmten Gerät zu suchen. Sie werden nach dem Geräte-Alias, der Zugehörigkeit und der auf das Gerät angewandten Richtlinie sortiert. Zusätzlich kann die Geräteliste als Tabelle in eine CSV-Datei exportiert werden. Jedes Gerät bietet einige wichtige Funktionen, wie zum Beispiel:

1. Status der Geräte
2. Bedrohungen anzeigen

3. Erkennen Sie alle Bedrohungen an
4. Die Politik ändern
5. Deinstallieren Sie die Software

5.3.2 Richtlinien verwalten

Sie können den gewünschten Scan-Typ auswählen und die Scans wie folgt planen:

1. Scan Typ
    a. Schneller Scan
    b. Vollständiger Scan
    c. Benutzerdefinierter Scan: Dies ermöglicht es dem Benutzer, einen bestimmten Datenträger, Ordner oder eine Datei hinzuzufügen, die gescannt werden soll.
2. Kalender: kann der Benutzer die Häufigkeit der Scans einstellen. Der Benutzer kann zwischen einem täglichen, wöchentlichen oder einem bestimmten Zeitintervall (das der Benutzer individuell einstellen kann) wählen.

5.3.3 Manuelle Scans

Starten Sie einen manuellen Scan für einzelne Endpunkte. Überprüfen Sie die Endpunkte unabhängig von geplanten Scans aus den Endpoint Protection-Richtlinien jederzeit auf Malware. Ein manueller Scan wird innerhalb der TeamViewer-Verwaltungskonsole oder der TeamViewer-Vollversion für jedes Online-Gerät gestartet.

1. Klicken Sie in der TeamViewer-Verwaltungskonsole auf den Namen des Endpunkts und wählen Sie "Schnellscan" oder "Vollständiger Scan".
2. Wählen Sie in der TeamViewer-Vollversion die Option 'Schnellscan' oder 'Vollständiger Scan' im Kontextmenü (Rechtsklick) des Endpunkts.

5.3.4 Status des Geräts

Für jeden Endpunkt kann der Status des Endpoint Protection-Scans angezeigt werden. Der Status enthält Informationen über Zeit und Datum der vorherigen und nächsten geplanten Scans sowie allgemeine Details über den Schutz des Geräts.

1. Klicken Sie auf den Namen eines Gerätes und wählen Sie die Option "Status" aus dem Kontextmenü.
2. Die folgenden Informationen werden im Dialogfeld "Endpoint Protection-Status" angezeigt:
    a. Status – der Status des Geräts kann durch seine Farbe identifiziert werden.
        i. Grün: Der Endpunkt ist geschützt.
        ii. Gelb: geringfügiges Problem, z. B. alte Malware-Definitionen oder ein geplanter Scan wurde nicht durchgeführt.
        iii. Rot: laufendes Problem, z.B. Malware wurde gefunden, aber nicht entfernt.
    b. Letzter Scan – Datum, Uhrzeit und Scantyp des letzten Scans.
    c. Endpunktschutzrichtlinie – die zugewiesene Endpunktschutzrichtlinie.

d. Zeitplan – alle geplanten Scans für den Endpunkt, wie in der Endpoint Protection-Richtlinie definiert.

5.3.5 Quarantäne

Dieser Bericht zeigt alle Bedrohungen in Quarantäne an. Sie können nach Gerät und nach einem bestimmten Zeitintervall gefiltert werden.

5.3.6 Active Ransomware Protection

Der aktive Schutz vor Lösegeldforderungen schützt bestimmte Ordner, die von unbekannten Anwendungen wie Lösegeldforderungen oder anderer bösartiger Software gelesen oder beschrieben werden können. Wir verfügen über ein intelligentes System, das Lese-/Schreibversuche von Anwendungen überprüft und den Zugriff auf diese Ordner gewährt oder verweigert. Um diese Funktion zu nutzen, müssen Sie das Kontrollkästchen "aktiver Schutz vor Lösegeldforderungen" anklicken und Ihre Konfigurationen einrichten.

Geschützte Ordner:

Dies sind die Speicherorte, die der Benutzer vor Zugriff oder Veränderung durch nicht vertrauenswürdige Anwendungen schützen möchte.

Vertrauenswürdige Anwendungen:

Dies sind die Anwendungen, die dem Benutzer bekannt sind und auf Dateien in den geschützten Ordnern zugreifen oder diese ändern können.

Gesperrte Anwendungen:

Dies ist der Bericht über die Anwendungen, die durch aktiven Lösegeld-Schutz blockiert werden, wenn sie versuchen, auf Dateien oder Ordner in den benutzergeschützten Speicherorten zuzugreifen.

> **Hinweis:** Der aktive Schutz vor Lösegeldforderungen wird nicht standardmäßig eingestellt. Um diese Funktion nutzen zu können, muss der Benutzer sie in der Endpoint Protection-Richtlinie aktivieren. Dann muss der Benutzer sicherstellen, dass

5.3.7 Geräteansicht

Die Geräteansicht von TeamViewer Endpoint Protection ist darauf ausgelegt, die Effizienz der Benutzer bei der Verwendung der Software zu verbessern. Sie gibt dem Benutzer einen Überblick über alle Geräte mit aktiviertem Endpoint Protection, so dass der Benutzer bei Bedarf schneller reagieren kann. Die GerÃ€teansicht zeigt zuerst die GerÃ€te mit Alarmen an, die sofortige

Aufmerksamkeit erfordern. Diese Ansicht ist sehr nützlich für die Benutzer, die eine große Anzahl von Endpunkten verwalten.

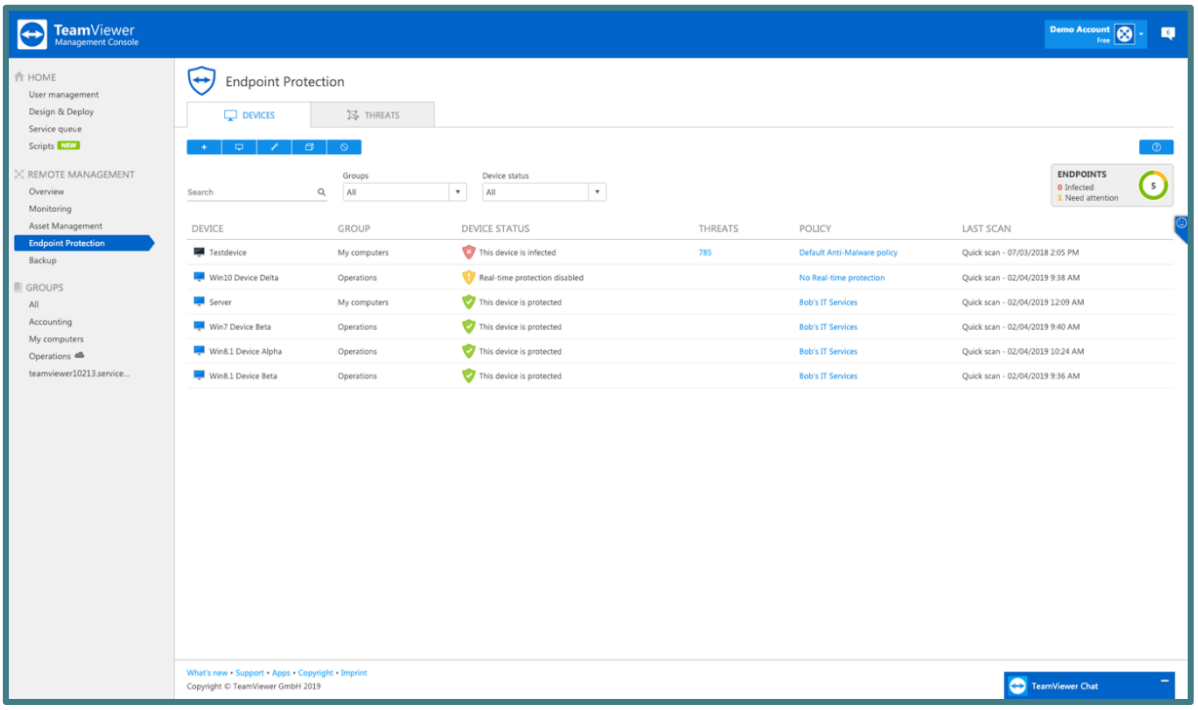


BIld: Endpoint Protection Geräteansicht.

Suchfunktion: Damit können Benutzer nach Geräten anhand des Gerätenamens suchen. Es werden nur die Endgeräte mit aktiviertem Endpoint Protection angezeigt.

Filterung:

Nach Gruppen: Benutzer können nur die Gruppen mit Endpunkten mit Endpoint Protection auswählen.

Nach Gerätestatus: Benutzer können die Geräte auf der Grundlage ihres Status auswählen (Einzel- und Mehrfachauswahl ist möglich).

Endpunkte: Benutzer können sehen, wie viele Endpunkte auf dem Konto verfügbar sind, wie viele in Gebrauch sind und wie viele infiziert sind oder behandelt werden müssen.

Status der Geräte:

Das rote Symbol wird zur Identifizierung der infizierten Geräte verwendet.

Das gelbe Symbol wird verwendet, um die Geräte zu identifizieren, die Aufmerksamkeit benötigen, weil:

1. Die Definitionen sind veraltet.
2. Der Echtzeitschutz ist deaktiviert.
3. Es wurde seit langer Zeit kein Scan durchgeführt.
4. Auf diesem Gerät ist keine Richtlinie aktiviert.

Das grüne Symbol dient zur Kennzeichnung der Geräte, die sicher sind.

Durch Auswahl der 3 Punkte können Benutzer

1. Direkt mit dem Endpunkt verbinden.
2. Endpoint Protection auf dem Endpunkt deinstallieren.
3. Auslösen eines schnellen oder vollständigen Scans.

5.3.8 Bedrohungen Ansicht

Die Bedrohungsansicht zeigt alle Warnungen für jeden Computer, auf dem Endpoint Protection installiert ist, und wird in der TeamViewer Management-Konsole angezeigt. Eine Warnmeldung wird ausgelöst, sobald Unregelmäßigkeiten bei einem Gerät festgestellt werden. Dies hängt von den definierten Fernverwaltungsrichtlinien ab.

Die Standardrichtlinie für den Endgeräteschutz umfasst die folgenden Scans, die im Abschnitt 5.2 Endpoint Protection .

1. Schneller Scan, täglich 09:00 Uhr
2. Vollständiger Scan, täglich um 12:00 Uhr

Der Alarmbericht kann auf eine der folgenden Arten abgerufen werden:

1. Klicken Sie in der Seitenleiste auf Remote Management → Wählen Sie die Registerkarte Endpunktschutz → Wählen Sie die Registerkarte Bedrohungsansicht.
2. Klicken Sie in der Seitenleiste auf eine Gruppe aus Ihrer Computer- und Kontaktliste → Wählen Sie die Registerkarte Endpunktschutz.

Bedrohungsdetails

Sie können detaillierte Informationen über erkannte Malware anzeigen. So erhalten Sie schnell Informationen über die Art der Malware und können die Bedrohung durch die Malware besser einschätzen.

Auf die Bedrohungsdetails können Sie auf eine der folgenden Arten zugreifen:

1. Klicken Sie auf das Symbol neben einer Warnmeldung und wählen Sie die Option "Details".
2. Wählen Sie alle Warnmeldungen aus, die Sie bestätigen möchten, und klicken Sie darauf: Werkzeuge → Details.

Die folgenden Informationen werden im Dialogfeld Bedrohungsdetails angezeigt:

1. Gerät – Name des Geräts, auf dem die Malware gefunden wurde.
2. Name – Name der Malware.
3. Gefunden in – Pfad oder Datei, in der die Malware gefunden wurde.

Optionen: Wählen Sie aus, wie Sie mit der Malware verfahren möchten:

1. Aus der Quarantäne löschen - wählen Sie dies, wenn Sie die Malware aus der Quarantäne entfernen und dauerhaft löschen möchten.

2. Aus der Quarantäne wiederherstellen - wählen Sie dies, wenn Sie die Malware an ihrem ursprünglichen Speicherort wiederherstellen und aus der Quarantäne entfernen möchten.

Filtern

Sie können Alarmmeldungen nach Alarmtyp, Gerät, Status und Datumsbereich filtern. Wenn Sie auf einen Eintrag in der Tabellenüberschrift klicken, können Sie die Alarmmeldungen innerhalb der Spalte sortieren. Über das Menü Ansicht können Sie festlegen, welche Spalten in der Tabelle angezeigt werden sollen, und Sie können die Diagramme aktivieren oder deaktivieren.

1. Wenn bei einem Scan eine Bedrohung entdeckt wird, wird die erkannte Malware sofort in den Quarantäneordner verschoben. Dort kann die Malware keinen Schaden anrichten. Zusätzlich wird eine E-Mail-Benachrichtigung an die E-Mail-Adressen gesendet, die Sie für die Richtlinie definiert haben.
2. Der Status der Benachrichtigungen wird durch verschiedene Symbole angezeigt.

Icon Farben	Beschreibung
Rot 	Auf dem Gerät wurde Malware gefunden. Die Bedrohung konnte nicht neutralisiert oder in Quarantäne verschoben werden.
Gelb 	Auf dem Gerät wurde eine Bedrohung gefunden. Die Bedrohung wurde neutralisiert und in die Quarantäne verschoben.
Grau 	Sie haben die Bedrohung bestätigt. Die Bedrohung wird nicht mehr angezeigt.

3. Bedrohung bestätigen
   Bedrohungen (Malware), die während eines Scans entdeckt werden, werden im Alarmbericht angezeigt und können dort bestätigt werden. Bestätigen Sie eine Warnmeldung, wenn Sie die Bedrohung kennen oder verifizieren können, und beginnen Sie mit der Fehlerbehebung. Wenn Sie eine Bedrohung bestätigen, wird die Bedrohung nicht mehr in den Benachrichtigungen des Geräts angezeigt, sondern mit einem Haken im Alarmbericht.

   > Beispiel: Bei einem Scan wurde Malware gefunden. Als Administrator des Gerätes erhalten Sie eine entsprechende Benachrichtigung per E-Mail. Überprüfen Sie die Benachrichtigung in der TeamViewer-Verwaltungskonsole. Nun, da Sie wissen, um was es sich bei der Bedrohung handelt, können Sie die Entdeckung der Malware bestätigen und gegebenenfalls Maßnahmen einleiten, um zukünftige Entdeckungen zu vermeiden.

   Sie können Bedrohungen auf eine von zwei Arten anerkennen:

   a. Klicken Sie auf das Symbol neben einer Warnmeldung und wählen Sie die Option "Bestätigen".

b. Wählen Sie alle Warnmeldungen aus, die Sie bestätigen möchten, und klicken Sie auf "Ausgewählte bestätigen".

Hinweis: Die Bedrohung wird in Quarantäne bleiben, nachdem Sie sie bestätigt haben. Löschen Sie die Malware nach Ihrem Ermessen vom Gerät.

Tipp: Es ist auch möglich, eine Bedrohung innerhalb der Computer- und Kontaktliste (TeamViewer-Vollversion und TeamViewer-Verwaltungskonsole) zu bestätigen.

Exportieren

Dadurch können Sie eine Liste der Bedrohungen exportieren, die auf allen Ihren Endpunkten gefunden wurden.

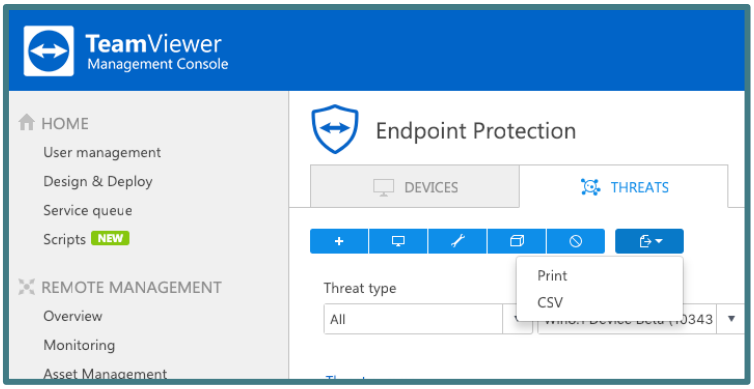


Bild: Exportfunktionalität in Endpoint Protection.

Zum Drucken exportieren

Diese Funktion erzeugt eine Web-Ansicht, die mit Hilfe von Druck-Plugins ausgedruckt oder in einem beliebigen Dokumentformat gespeichert werden kann.

Exportieren nach CSV

Mit dieser Funktion wird eine CSV-Datei erzeugt und heruntergeladen, die gespeichert, verwaltet oder geändert werden kann, wenn dies für die Überprüfbarkeit oder andere Vorschläge erforderlich ist.

6. Backup

Um Dateien auf Ihren Geräten zu sichern, verwenden Sie den **TeamViewer Backup** Dienst.

Für die **Lizenzaktivierung** siehe 2.2 Lizenz g.

Die **Systemanforderungen** finden Sie unter 2.3 System .

Zur Konfiguration von Richtlinien und deren Zuweisung zu Geräten siehe: 3.2 .

Die konfigurierten Geräte werden gemäß den zugewiesenen Richtlinien, die in Abschnitt 3.2 definiert sind, gesichert. Wann immer ein Backup nicht ordnungsgemäß durchgeführt werden konnte, wird ein Alarm ausgelöst und als Warnmeldung in der TeamViewer Management Console und der TeamViewer Vollversion angezeigt.

Service Symbol: Der Benutzer kann die Hauptfunktionen von TeamViewer Backup über das Servicesymbol ausführen. Hier kann er auf einfache Weise den Backup-Status auf dem Gerät überprüfen, ein Sofortbackup starten, ein laufendes Backup pausieren oder eine Wiederherstellung auslösen, ohne sich bei der Verwaltungskonsole anmelden zu müssen. Im Abschnitt über TeamViewer Backup finden Sie Informationen über die Version der Software, die derzeit auf dem Gerät läuft.

Hinweis:

1. Systemdateien sind von jeder Sicherung ausgeschlossen.
2. Wenn Sie Vollsicherung oder Schnellauswahl gewählt haben, werden auch Dateien auf angeschlossenen externen Speicherlaufwerken gesichert.
3. Sobald eine Sicherung oder Wiederherstellung gestartet wird, kann sie nicht angehalten oder gestoppt werden.

6.1 Backup Aktivierung

Zur Aktivierung von Endpunkten siehe: 3.1

6.2 Richtlinien

Nach der Aktivierung von TeamViewer Backup auf einem Gerät wird eine Standard-Sicherungsrichtlinie erstellt, die einige grundlegende Einstellungen enthält, und der Benutzer kann sofort die erste Sicherung durchführen. Der Benutzer kann die individuelle Backup-Richtlinie anpassen, festlegen, welche Daten gesichert werden sollen, die Häufigkeit der Backups anpassen und sogar die Verwendung bestimmter Prozesse, wie z.B. die Bandbreitendrosselung, definieren. Diese Richtlinien können auf einzelne Geräte oder eine Gruppe von Geräten angewendet werden. Um Ihre Richtlinien anzupassen, sollte der Benutzer durch die Option navigieren: Richtlinie verwalten → Backup Richtlinien verwalten → Editieren.

Dies ist der Ausgangspunkt für die Entwicklung und Änderung der Politik. Es gibt verschiedene Einstellungen, die in den TeamViewer Backup-Richtlinien konfiguriert werden können und dem Benutzer helfen, das Produkt effizient zu nutzen.

6.2.1 Richtlinien Name

Das erste, was bei der Erstellung einer Richtlinie definiert werden muss, ist der Name der Richtlinie. Benutzer können viele verschiedene Richtlinien erstellen, daher ist der Name der Richtlinie entscheidend.

Als Nächstes müssen Sie den Namen für die erstellte Richtlinie definieren. Dieser Name wird verwendet, um die Richtlinie in der Übersicht aller erstellten Richtlinien zu identifizieren.

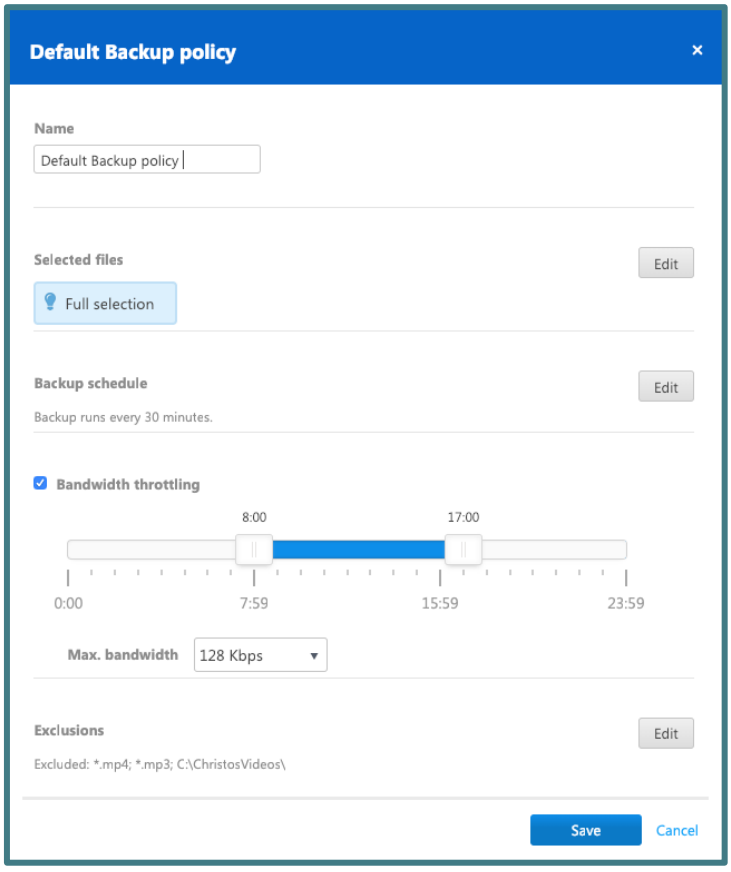


Bild: Backup Richtlienansicht.

6.2.2 Backup Richtlinie hinzufügen

Für weitere politische Optionen lesen Sie bitte: 3.2 .

6.2.3 Dateiauswahl

Um TeamViewer Backup zu verwenden, muss der Benutzer zunächst Daten in die Cloud hochladen. TeamViewer Backup bietet mehrere Optionen zur Festlegung der Daten, die in das Backup aufgenommen werden sollen. Dies vermeidet die Möglichkeit, unnötige Dateien zu sichern, und optimiert die Leistung des Backups.

Backup Auswahl

1. Komplettes Backup
    a. Dies ist die Standardsicherungsauswahl. Sie wählt automatisch alle von TeamViewer Backup unterstützten Dateien auf dem Gerät aus.
2. Schnellauswahl
    a. Die Schnellauswahl bietet die Möglichkeit, bestimmte Dateitypen auf dem Gerät auszuwählen, die in die Sicherung einbezogen werden müssen.
3. Erweiterte Auswahl
    a. Mit der erweiterten Auswahl kann der Benutzer einen oder mehrere spezifische Pfade angeben, die gesichert werden müssen, indem er einfach den Pfadnamen.

> **Hinweis:** Bei der Wahl von 'Vollständige Auswahl' ist es wichtig zu berücksichtigen, dass einige Speicherorte oder Laufwerke automatisch ausgeschlossen werden und die Dateien innerhalb dieser Speicherorte nicht gesichert werden.

Befolgen Sie die folgenden Schritte, um alle Dateien auszuwählen, die mit Hilfe der Richtlinie in Backups einbezogen werden sollen.

1. Klicken Sie auf **Bearbeiten**.
2. Wählen Sie je nach Ihren Anforderungen eine der folgenden Optionen:
    a. **Vollständige Sicherung**: Ein Voll-Backup umfasst alle Dateien ohne Einschränkungen hinsichtlich Dateityp oder Speicherort auf einem Gerät.
    b. **Schnelle Auswahl**: Wählen Sie aus den wichtigsten Dateitypen die Dateien aus, die in die Sicherung einbezogen werden sollen. Sie können zwischen **Office-Dateien** (Dokumente, Präsentationen, Tabellenkalkulationen, Textdateien usw.), **E-Mails**, **PDFs**, **eBooks** und **Bildern** wählen.
    c. **Erweiterte Auswahl**: Definieren Sie eine Festplatte (z.B. D:\), einen Ordner (z.B. C:\Ordner), eine Datei (z.B. C:\Ordner\Report.xlsx) oder einen Dateityp (z.B. *.mp3), die in die Sicherung einbezogen werden sollen. Auf diese Weise können Benutzer bestimmte Dateien von einzelnen Geräten sichern**.**
3. Klicken Sie auf **Pfad hinzufügen**.

> **Hinweis:** Wenn Sie Vollsicherung oder Schnellauswahl wählen, werden auch Dateien auf angeschlossenen externen Speicherlaufwerken gesichert.

Tipp: Sie können Platzhalter verwenden, um Dateipfade zu sichern, die bestimmte Schlüsselwörter enthalten (z.B. C:\Benutzer\Dokumente).*

6.2.4 Backup Einstellungen

TeamViewer Backup bietet verschiedene Optionen, die eine flexible Einrichtung und einfache Bedienung ermöglichen.

6.2.5 Backup Zeitplanung

TeamViewer Backup bietet die MÃ¶glichkeit, den Backup-Zyklus zu definieren und festzulegen, wie oft das automatische Backup durchgefÃŒhrt werden soll - innerhalb eines bestimmten Zeitintervalls, jeden Tag zu einer bestimmten Zeit oder an bestimmten Tagen zu einer bestimmten Zeit.

Definieren Sie, wann das Backup für die ausgewählten Dateien auf dem Gerät gestartet werden soll.

1. Klicken Sie dazu auf **Bearbeiten**.
2. Wählen Sie je nach Ihren Anforderungen eine der folgenden Optionen:
    a. **Führen Sie alle [X] eine Sicherung aus:** Definieren Sie das Intervall für eine Sicherung. Die Dateien werden unabhängig von Datum und Uhrzeit regelmäßig gesichert.
    b. **Planen Sie die Sicherung für:** Definieren Sie den Zeitpunkt, zu dem das Backup ausgeführt wird. Darüber hinaus können Sie die spezifischen Tage auswählen, an denen ein Backup durchgeführt werden soll**.**

6.2.6 Bandbreitenbegrenzung

Mit dieser Option kann der Benutzer einfach den Durchsatz des an die Backup-Server gesendeten Datenverkehrs begrenzen, indem er eine maximale Bandbreite und den Zeitrahmen für die Drosselung festlegt.

Begrenzen Sie die Bandbreite, die für Ihre Backups verwendet wird, z.B. während der Arbeitszeiten. Dadurch wird die Auswirkung, die ein Backup auf die Geschwindigkeit Ihrer Internetverbindung hat, verringert.

Die folgenden Einstellungen können konfiguriert werden:

1. **Zeitlicher Rahmen:** Definieren Sie die Zeit, wann die Bandbreitendrosselung beginnt und wann sie endet. Zwischen Start- und Endzeitpunkt ist die Bandbreite begrenzt**.**

2. **Bandbreite**: Wählen Sie die maximale Bandbreite, die während der Drosselung verwendet wird.

> **Hinweis:** Wenn die Bandbreite nicht begrenzt ist, verwendet TeamViewer Backup die maximal verfügbare Bandbreite.

6.2.7 Ausnahmen

TeamViewer Backup bietet die Möglichkeit, bestimmte Daten einfach von der Sicherung auszuschließen, ohne die gesamte Sicherungsauswahl zu beeinflussen. Dies kann durch Angabe des Pfades der Laufwerke, der Ordner, der Dateien oder der Dateitypen erfolgen, die nicht in die Sicherung einbezogen werden sollen.

Gehen Sie wie folgt vor, um Dateien von der Sicherung auszuschließen: Klicken Sie auf Bearbeiten → Ausnahme hinzufügen.

Definieren Sie ein Laufwerk (z.B. D:\), einen Ordner (z.B. C:\Ordner), eine Datei (z.B. C:\Ordner\Report.xlsx) oder Dateitypen (z.B. *.mp3), die von der Sicherung ausgeschlossen werden sollen.

6.2.8 Benachrichtigungen

TeamViewer Backup benachrichtigt den Benutzer durch Senden einer E-Mail an das Admin-Konto in den folgenden Fällen:

1. Wenn eine Web-Wiederherstellung abgeschlossen ist, wird der Download-Link in einer E-Mail-Benachrichtigung gesendet.
2. Wenn ein Backup auf einem Gerät fehlgeschlagen ist, wird der Download-Link in einer E-Mail-Benachrichtigung gesendet.
3. Wenn eine Wiederherstellung auf dem Originalgerät oder auf einem anderen Gerät abgeschlossen ist, wird der Download-Link in einer E-Mail-Benachrichtigung gesendet.
4. Wenn der verwendete Backup-Speicher 75% des gekauften Speichers erreicht.

E-Mail-Benachrichtigungen werden gesendet von: notification@teamviewer-rm.com

> **Hinweis:** Wenn Sie mit einem Proxy oder benutzerdefinierten Firewalls arbeiten, kann eine Whitelist zur Domäne *.teamviewer-rm.com hinzugefügt werden.

6.3 Aufbewahrungsfrist

TeamViewer Backup bietet Benutzern die Möglichkeit zu definieren, wie lange die ältere Version jeder Datei in der Cloud aufbewahrt werden soll. Dies kann unter der Schaltfläche 'Globale Einstellungen' auf dem Dashboard eingestellt werden.

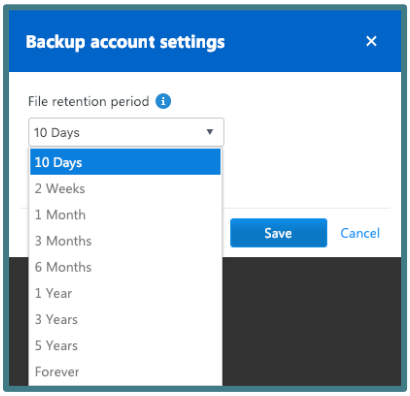


Bild: Benutzerdefinierte Einstellungen für die Aufbewahrungsdauer von Dateien.

> **Hinweis:** Die Aufbewahrungsfrist gilt nur für das Konto, das die Einstellungen geändert hat, und betrifft alle Geräte, bei denen das Backup für dieses Konto aktiviert ist.

6.4 Backup verwalten

TeamViewer Backup bietet flexible Optionen zur Verwaltung Ihrer Backups und erleichtert Ihnen die Arbeit innerhalb des Produkts.

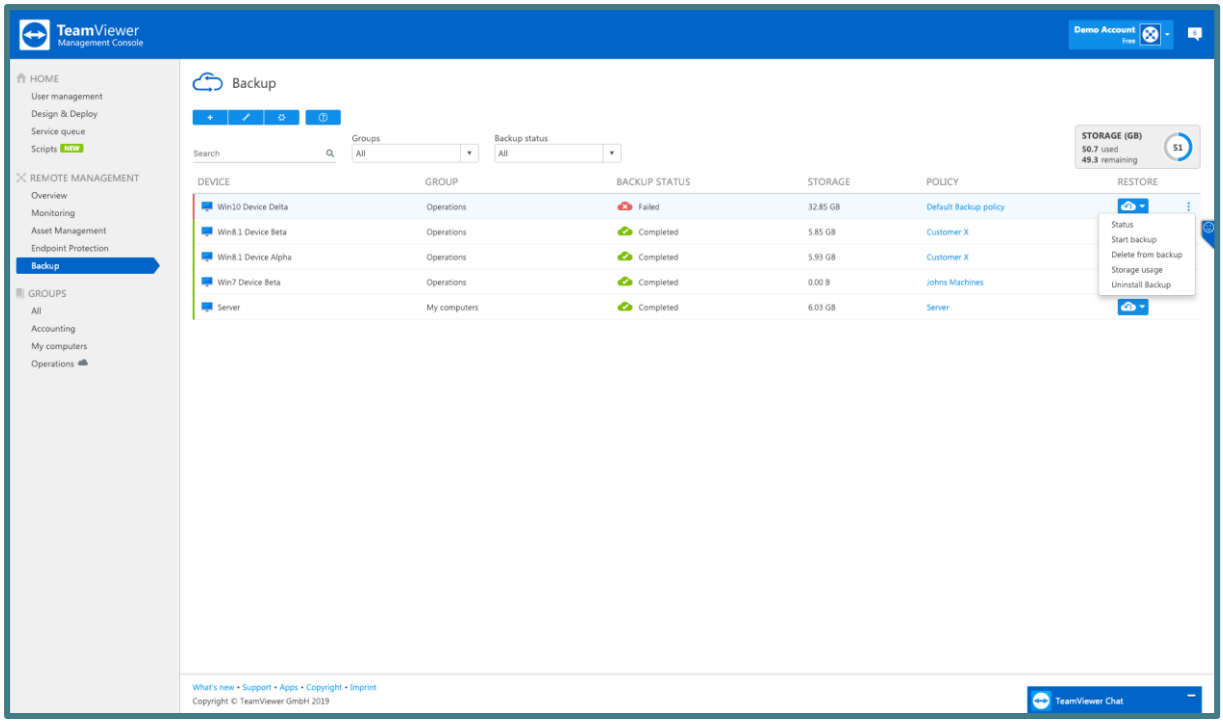


Bild: Backupverwaltungsoptionen

6.4.1 Backup Status

Für jedes Gerät kann der Status seiner Backups in der Verwaltungskonsole oder über das Symbol für den Backup-Dienst angezeigt werden.

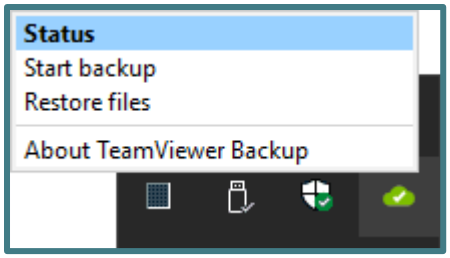


Bild: Backupstatus Ansicht vom Service Symbol.

Der Status enthält Informationen über die Zeit und das Datum der vorherigen und nächsten geplanten Sicherung sowie allgemeine Details über den Sicherungsstatus des Geräts.

1. Klicken Sie auf den Namen eines Gerätes und wählen Sie 'Status' aus dem Kontextmenü.
2. Klicken Sie in der TeamViewer-Vollversion mit der rechten Maustaste auf 'Status' im Kontextmenü des Geräts.

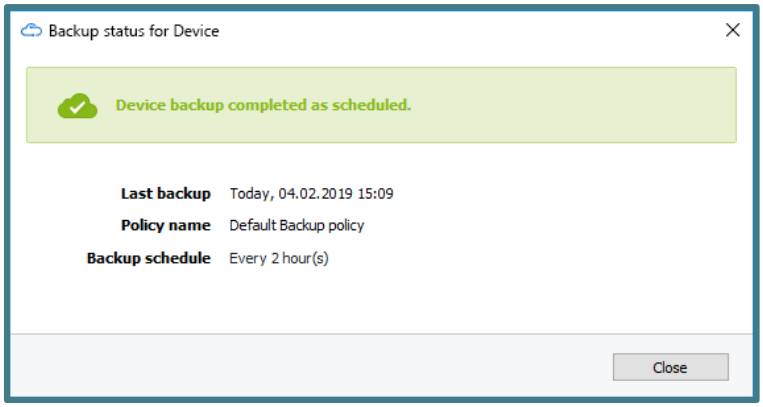


Bild: Backupstatus Service Symbol.

6.4.2 Status Beschreibung

Die folgenden Informationen werden im Dialogfenster Sicherungsstatus für angezeigt:

1. TeamViewer Backup meldet 3 verschiedene Gerätezustände, die durch die folgenden Farben gekennzeichnet sind:

Status	Beschreibung
Grün	Die Sicherung wird wie geplant abgeschlossen.
Gelb	Das Backup wurde aufgrund eines kleineren Problems nicht wie geplant ausgeführt, z.B. konnte das letzte geplante Backup nicht durchgeführt werden.
Rot	Die Sicherung auf dem Gerät ist aufgrund eines laufenden Problems fehlgeschlagen, z.B. ist die letzte Sicherung fehlgeschlagen, oder mehrere geplante Sicherungen konnten nicht durchgeführt werden.
In Bearbeitung	Die Sicherung wird gerade durchgeführt.
Backup pausiert	Die Sicherung wird angehalten.

2. Letzte Sicherung: Datum der letzten erfolgreichen Sicherung.
3. Backup-Richtlinie: Die zugewiesene Backup-Richtlinie.

6.4.3 Tägliche Speichernutzung pro Gerät

Um den Backup-Speicher zu überwachen, kann der Benutzer außerdem sehen, wie viel Speicherplatz monatlich genutzt wird. Der Benutzer kann auch sehen, wie viel Speicherplatz täglich auf jedem Gerät in einem Zeitintervall von 2 Wochen verwendet wird.

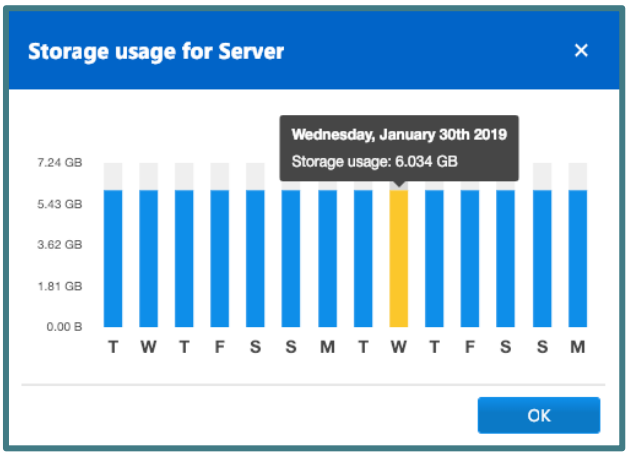


Bild: Tägliche Speichernutzung pro Gerät.

6.4.4 Löschen von Dateien aus der Sicherung

TeamViewer Backup bietet die Möglichkeit, unerwünschte Dateien, Ordner und/oder Laufwerke aus dem Backup-Speicher zu löschen. Dies maximiert die Wirksamkeit des Produkts.

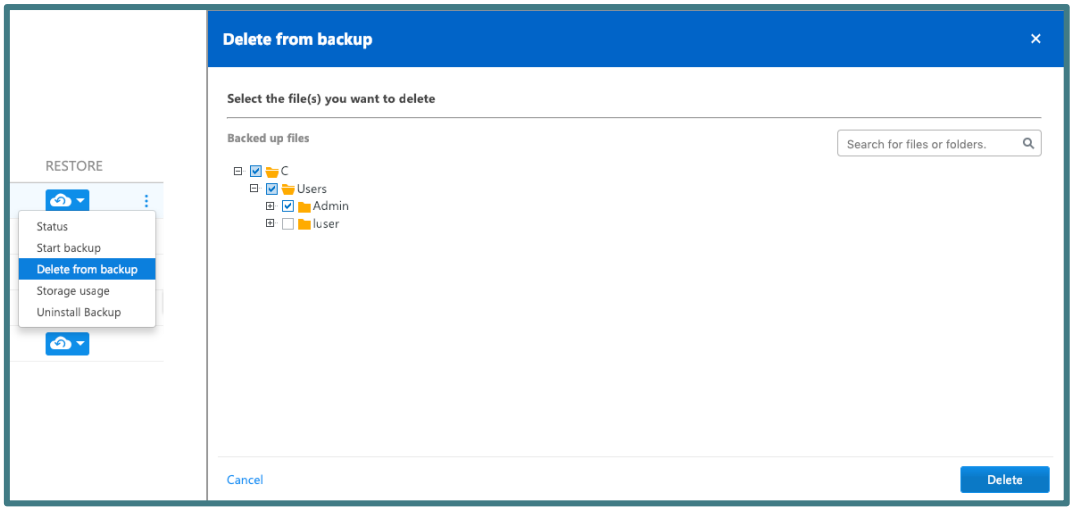


Bild: Löschen Sie eine Datei aus dem Sicherungsspeicher.

6.5 Wiederherstellen gesicherter Dateien

Nachdem eine Sicherung erfolgreich durchgeführt wurde, kann der Benutzer wählen, wie die Dateien wiederhergestellt werden sollen:

1. Stellen Sie die Dateien auf dem Gerät (Geräte-Alias) wieder her.
2. Wiederherstellen der Dateien auf einem anderen Gerät.
3. Wiederherstellen von einer früheren Sicherung.

6.5.1 Wiederherstellen auf das Originalgerät

Der Benutzer hat die Möglichkeit, Dateien aus der Ferne auf dem Gerät wiederherzustellen, auf dem die Sicherung läuft.

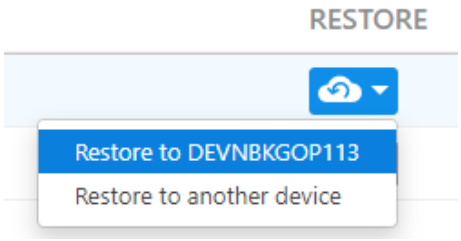


Bild: Wiederherstellung auf das Originalgerät.

6.5.2 Wiederherstellen auf einem anderen Gerät

Der Benutzer kann Dateien aus der Ferne auf einem anderen Gerät wiederherstellen, falls das Originalgerät beschädigt wird oder verloren geht.

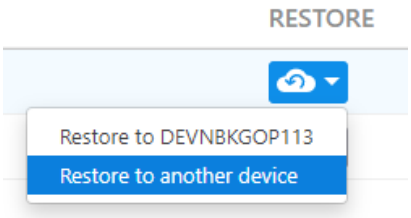


Bild: Wiederherstellung auf ein neues Gerät.

6.5.3 Wiederherstellen aus vorheriger Sicherung

Benutzer haben die Möglichkeit, eine Sicherung wiederherzustellen, die zuvor auf einem früheren Gerät durchgeführt wurde. Dies ermöglicht dem Benutzer die Wiederherstellung älterer gesicherter Dateien für den Fall, dass TeamViewer Backup erneut auf einem Gerät installiert wird, auf dem bereits ein Backup durchgeführt wurde.

6.6 Dateiauswahl zum Wiederherstellen

Bei der Auswahl der Dateien für die Wiederherstellung kann der Benutzer wählen, ob er 1) eine einzelne Version einer Datei oder 2) Dateien innerhalb eines bestimmten Zeitintervalls wiederherstellen und die Dateien nach diesem bestimmten Datumsbereich auswählen möchte. Der Benutzer kann eine Datei oder einen Ordner auch über den Namen im Suchfeld suchen oder die Datei oder den Ordner über den Baum auswählen.

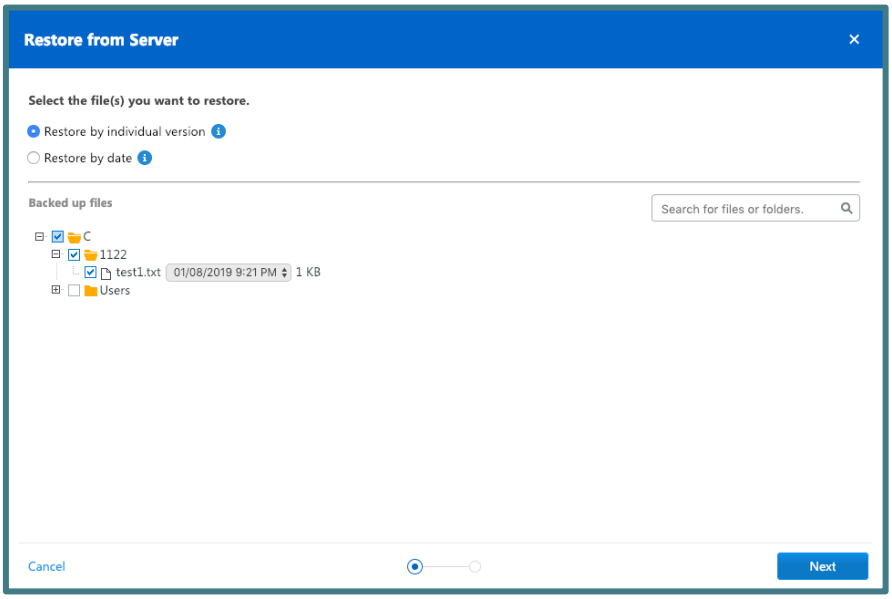


Bild: Dateien zur Wiederherstellung auswählen.

Nachdem die Dateien ausgewählt wurden, kann der Benutzer angeben, wohin die Dateien wiederhergestellt werden sollen. Es gibt zwei Optionen:

1. Wiederherstellen am ursprünglichen Speicherort: Die Dateien werden am gleichen Ort wiederhergestellt, an dem sie sich auf dem ursprünglichen Gerät befanden.

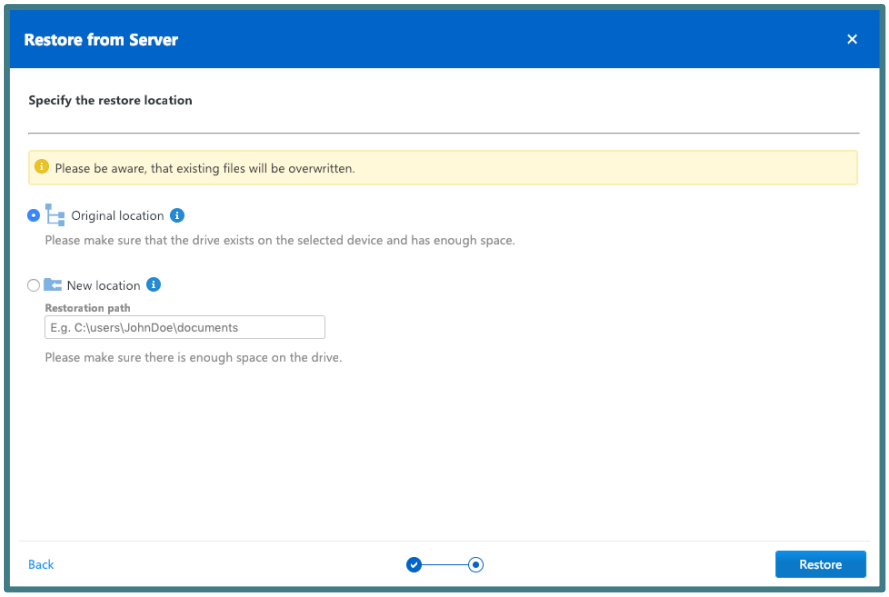


Bild: Dateien am ursprünglichen Speicherort wiederherstellen.

2. Wiederherstellen an einem neuen Speicherort: Ein neuer Speicherort für die Dateien kann gewählt werden, indem der Pfad des neuen Speicherorts hinzugefügt wird.

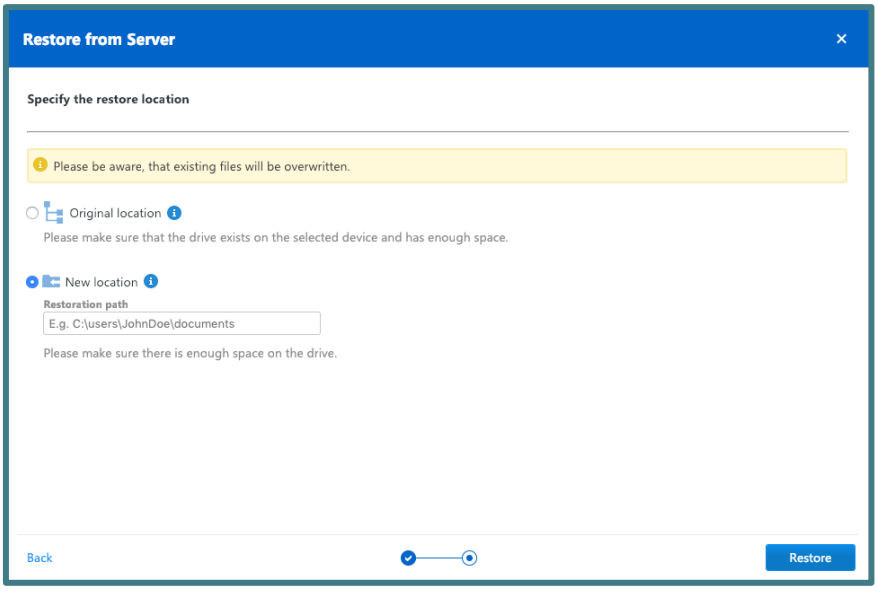


Bild: Dateien an einem neuen Speicherort wiederherstellen.

Hinweis: Es ist wichtig, sicherzustellen, dass das/die Laufwerk(e), auf dem/denen die Dateien wiederhergestellt werden sollen, auf dem ausgewählten Gerät vorhanden ist/sind und über genügend Speicherplatz verfügt.

6.7 Backup Geräteansicht

Die Geräteansicht von TeamViewer Backup soll sicherstellen, dass der Benutzer die wichtigsten Informationen im Blick hat. Sie wurde entwickelt, um die Arbeit mit TeamViewer Backup einfacher und effizienter zu gestalten. Mit den Suchfunktionen und Filtern kann der Benutzer nach einem bestimmten GerÃ€t ÃŒber den GerÃ€tenamen, eine GerÃ€tegruppe oder den Backup-Status suchen.

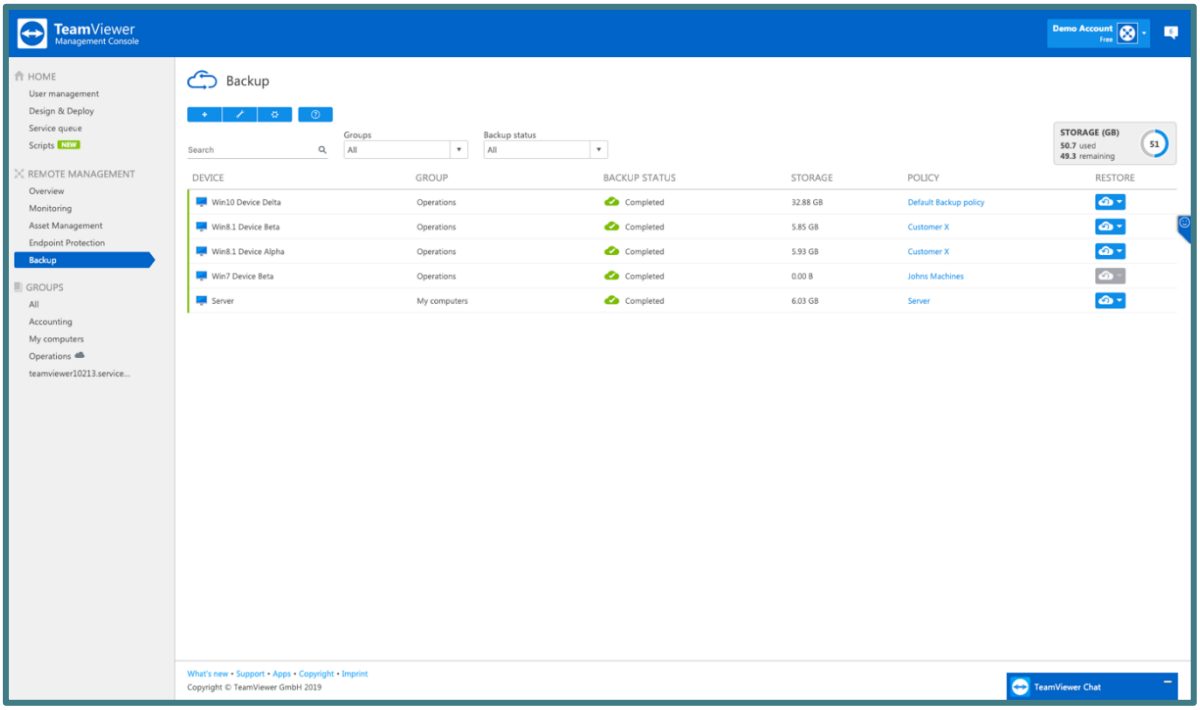


Bild: Geräteansicht für Backup.

6.7.1 Filtern

Der Benutzer kann nach Geräten anhand des Gerätenamens suchen oder die Geräte nach den Gruppen und dem Sicherungsgerätestatus filtern.

6.7.2 Übersicht über den verwendeten Speicher

Dies gibt einen Überblick über die Anzahl der verwendeten Endpunkte und zeigt die Menge des verwendeten Speichers im Vergleich zum gekauften Speicher an.

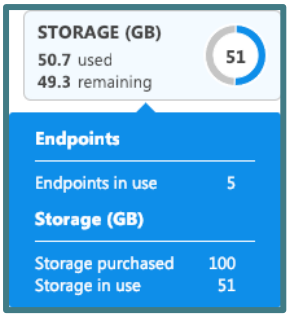


Bild: Überblick über Backup-Speicher.

7. Web Monitoring

Um Ihre Web-Ressourcen zu überwachen, verwenden Sie den Dienst **TeamViewer Web Monitoring.**

Für die Lizenzaktivierung sehen Sie bitte den Abschnitt 2.2 Lizenz g.

Wenn alle definierten Bedingungen für eine Prüfung erfüllt sind, wird ein Alarm ausgelöst und als Nachricht in der TeamViewer-Verwaltungskonsole angezeigt. Eine E-Mail-Benachrichtigung wird ebenfalls gesendet, wenn dies in den Monitorkonfigurationen konfiguriert wurde. Eine Alarmmeldung zeigt an, dass in einem der überwachten Web Ressourcen ein Problem aufgetreten ist.

7.1 Web Monitoring Aktivierung

Zur Aktivierung des Web Monitoring siehe: 3.1 .

7.2 Web Monitoring Monitor Typen

Es gibt 3 Arten von Web-Monitoren - Uptime, Page Load und Transaction.

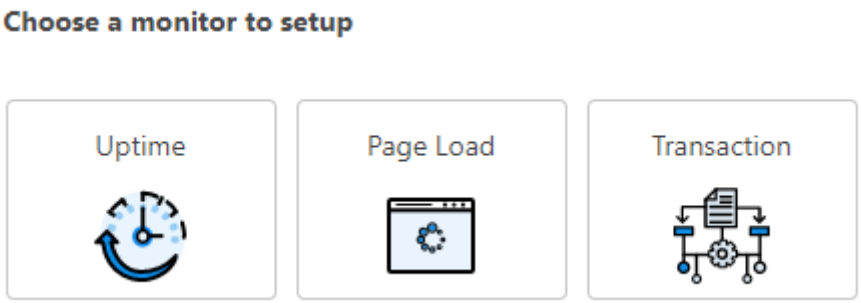


Bild: Web Monitoring Monitor Typen.

7.2.1 Uptime Monitore

Überprüft die Verfügbarkeit und die Antwortzeiten Ihrer Website von mehreren Standorten auf der ganzen Welt. Uptime Monitoring warnt Sie sofort bei Problemen mit Ihren externen IT-Diensten. Diese sind für Benutzer und Kunden oft am sichtbarsten, was sie zu den kritischsten macht.

Uptime Monitoring kann Sie innerhalb von 1 Minute nach einem Problem durch E-Mail-Benachrichtigungen über kostspielige Ausfallzeiten informieren.

Sie haben die Möglichkeit, 3 Subtypen von Uptime-Monitoren zu erstellen - HTTP, HTTPS und ICMP (Ping).

HTTP und HTTPS – Die HTTP(S)-Überwachung ermöglicht es Ihnen, die Verfügbarkeit und die Antwortzeiten Ihrer Website von mehreren Standorten auf der ganzen Welt aus zu testen.

Sie sollten HTTPS oder verwenden. HTTP-Überwachung, wenn Ihre Website das HTTPS-Protokoll für sichere Kommunikation verwendet.

Sobald Sie einen HTTP(S)-Monitor für Ihre Website hinzugefügt haben, beginnt die Web-Überwachung damit, HTTP(S)-Anfragen in Ihren voreingestellten Zeitintervallen an Ihre Website zu senden, um zu prüfen, ob Ihre Website zugänglich ist.

ICMP – Mit der ICMP- oder Ping-Überwachung können Sie die Erreichbarkeit Ihres Servers über ein IP-Netzwerk von mehreren Standorten auf der ganzen Welt testen.

Sobald Sie einen PING-Monitor hinzugefügt haben, wird Web Monitoring in den von Ihnen voreingestellten Zeitintervallen einen Ping auf Ihrem Server durchführen, um zu prüfen, ob Ihre URL/IP zugänglich ist.

7.2.2 Page Load Monitore

Sehen Sie, wie lange es dauert, eine komplette HTML-Seite in echten Browsern zu laden. Durch die Verfolgung der Ladezeiten jedes einzelnen Bildes, CSS, JavaScript, RSS, Flash und Frames/Frames misst das Tool die Benutzererfahrung Ihres Web-Besuchers.

Der Page Load Monitor von Web Monitoring ist nützlich, um u.a. Dinge zu verstehen und zu analysieren:

- welche Elemente am längsten zum Laden benötigen,
- wie interne und externe Links beim Laden betroffen sind,
- wie lange es dauert, eine Verbindung herzustellen,
- die Start- und Endzeit der Ladung für jedes Element auf der Seite.

7.2.3 Transaction Monitore

Die Transaktionsüberwachung ist eine proaktive Website-Überwachung, die durch den Einsatz von Verhaltensskripten in einem Webbrowser erfolgt, um den Weg zu simulieren, den ein echter Kunde (oder Endbenutzer) durch eine Website nimmt.

Sie ermöglicht es Ihnen, Interaktionen mit einer webbasierten Anwendung - dem Transaktionsrecorder - Schritt für Schritt aufzuzeichnen und als Skriptdatei zu speichern.

Weitere Informationen über die Installation des Transaction Recorder Plugins und die Aufzeichnung eines Transaktionskripts finden Sie in den entsprechenden Kapiteln.

Um die Interaktionen genau zu lokalisieren, können Sie die Aufzeichnung im Transaktionsrecorder wiederholt abspielen und alle Schritte, die eine Überarbeitung erfordern, bearbeiten.

Nachdem das aufgezeichnete Skript fertiggestellt ist, sollte es auf Ihr lokales Laufwerk heruntergeladen und dann auf das Web-Monitoring-Dashboard hochgeladen werden, um mit der Konfiguration der Transaktionsmonitore zu beginnen.

Sobald die Testergebnisse verfügbar sind, können Sie die gesammelten Daten auf den Dashboards in Tabellen- und Diagrammansicht anzeigen: siehe Abschnitt7.3 Monitor Datenvisualisierung.

7.3.4 Einrichten von Konfigurationen für Monitore

Die Konfiguration der Web-Monitoring-Monitore ist in Schritte unterteilt und ist ein einfacher Prozess, der in wenigen Sekunden abgeschlossen ist. Um den Prozess zu erleichtern, haben wir informative Tooltips zu den meisten Feldern hinzugefügt, die Ihnen helfen zu verstehen, wofür die einzelnen Felder stehen. Die Schritte 2 und 3 sind für alle Monitortypen gleich.

Uptime Monitore

Wenn Sie in Schritt 1 einen Uptime-Monitor konfigurieren, sollten Sie dies tun:

- Richten Sie einen Monitor-Namen ein, geben Sie die URL oder die IP-Adresse an,
- wählen Sie das Protokoll (http, https oder icmp), darauf aufbauend wird der entsprechende Monitor-Subtyp erstellt,
- stellen Sie die Port-Nummer ein, standardmäßig ist sie 80 für http und 443 für https,
- Wählen Sie die Option Monitorsammlung, falls vorhanden, sonst ist das Feld Monitorsammlung nicht sichtbar, um den neu erstellten Monitor zu einer Sammlung (einer Gruppe) hinzuzufügen. Die Organisation von Monitoren in Sammlungen ist hilfreich bei der Definition des Zugriffs auf Monitore in der Benutzerverwaltung.
- Wählen Sie die Anforderungsmethode GET oder POST (für die POST-Methode sollten Sie auch die POST-Daten so bereitstellen, wie Ihr Server sie erwartet),
- die Timeout-Schwelle einstellen (in Millisekunden) - die Zeit, die wir warten werden, bis wir Ihre Website als defekt betrachten,
- die Prüffrequenz so oft wie einmal pro Minute bis zu einmal alle 6 Stunden einstellen,

Schritt 2

Wählen Sie aus den zahlreichen Standorten in Amerika, Europa, Asien, Afrika und Ozeanien aus, von denen aus Ihre Website überwacht werden soll,

Schritt 3

- die Konfigurationen der Benachrichtigungen einrichten: siehe Abschnitt 7.4 Alarme und Benachrichtigungen.

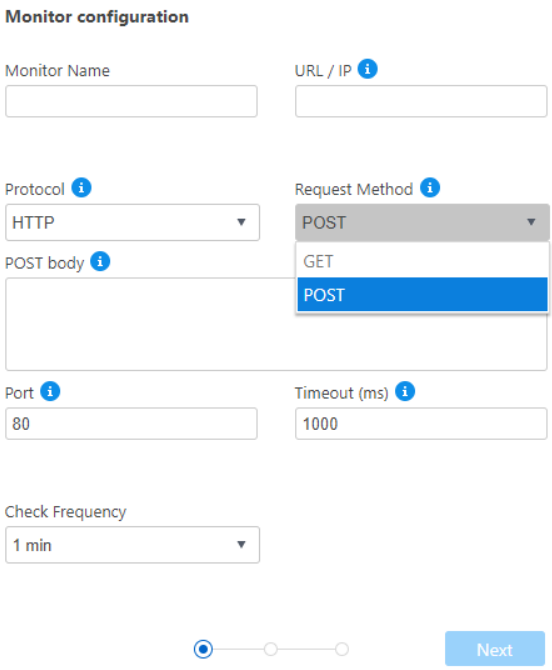


Bild: Uptime Monitor Konfiguration – Schritt 1

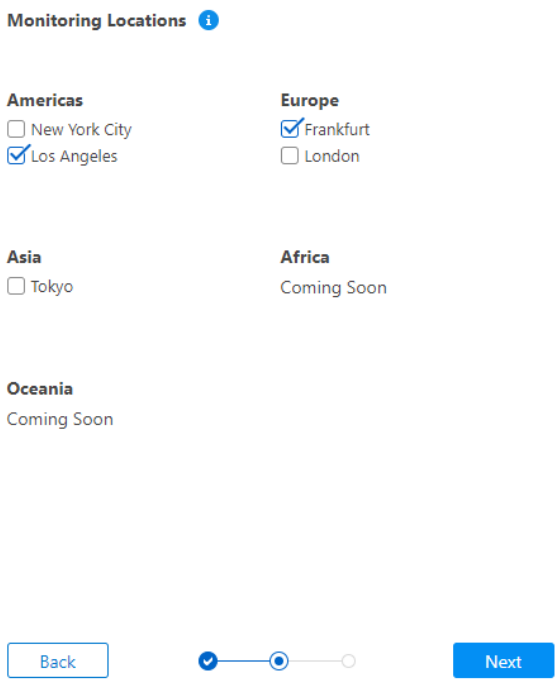


Image: Monitor configuration – step 2

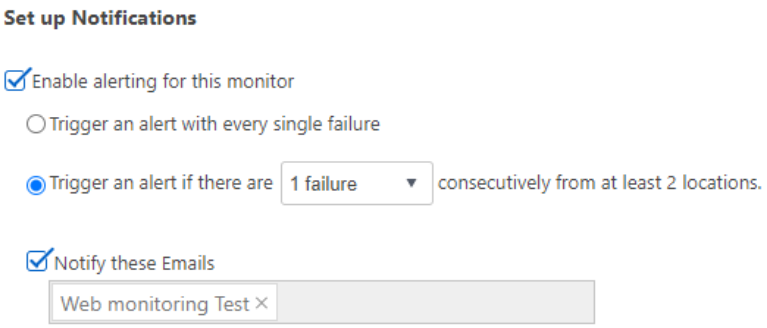


Image: Monitor configuration – step 3

Page Load Monitore

Wenn Sie in Schritt 1 einen Seitenlademonitor konfigurieren, sollten Sie dies tun:

- Richten Sie einen Monitor-Namen ein, geben Sie die URL oder die IP-Adresse an,
- Wählen Sie Monitorsammlung, falls vorhanden, sonst ist das Feld Monitorsammlung nicht sichtbar, um den neu erstellten Monitor zu einer Sammlung (einer Gruppe) hinzuzufügen. Die Organisation von Monitoren in Sammlungen ist hilfreich bei der Definition des Zugriffs auf Monitore in der Benutzerverwaltung,

- Wählen Sie den Browser-Typ - Sie können wählen, von welchem Browser aus die Seitenladeprüfungen durchgeführt werden sollen. Derzeit unterstützen wir nur Firefox und Chrome. Sie können die Browser-Auswahl der Einstellungen Ihres Monitors jederzeit ändern,
- wählen Sie das Protokoll (http, https) - https ist die Standardoption,
- stellen Sie die Port-Nummer ein, standardmäßig ist sie 80 für http und 443 für https,
- die Timeout-Schwelle (in Sekunden) festlegen - die Zeit, die wir warten, bis wir Ihre Website als nicht mehr verfügbar betrachten,
- die Kontrollhäufigkeit so oft wie 5 Minuten bis zu einmal alle 6 Stunden einstellen,

Schritt 2 und 3 sind die gleichen wie bei den Uptime-Monitoren

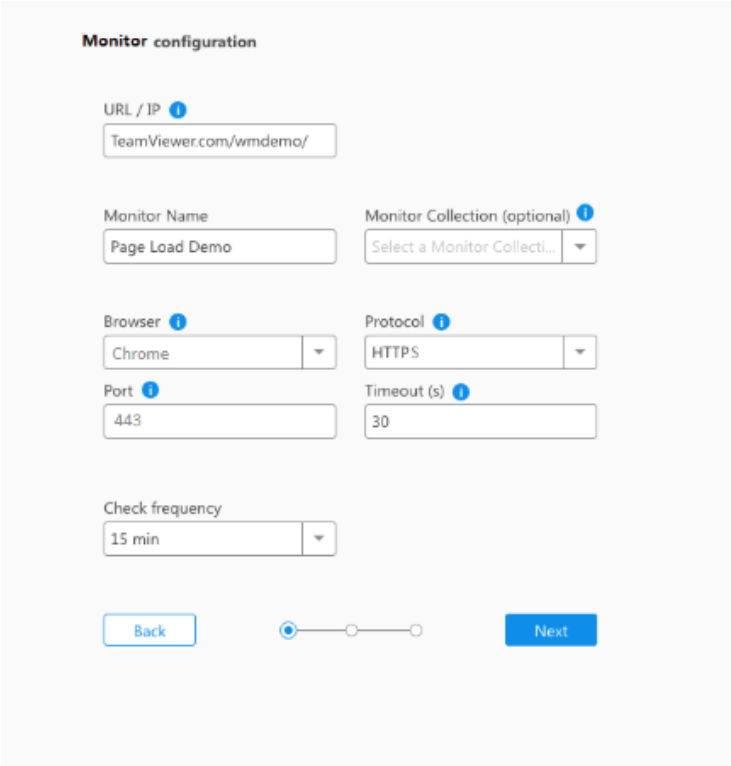


Bild: Page Load Monitor Konfiguration – Schritt 1

Transaction Monitore

Wenn Sie in Schritt 1 einen Transaktionsmonitor konfigurieren, sollten Sie dies tun:

- Durchsuchen Sie die Skript-Datei von Ihrem lokalen Laufwerk, um die Konfiguration zu starten,
- Richten Sie einen Monitor-Namen ein,
- Wählen Sie Monitorsammlung, falls vorhanden, sonst ist das Feld Monitorsammlung nicht sichtbar, um den neu erstellten Monitor zu einer Sammlung (einer Gruppe) hinzuzufügen. Die Organisation von Monitoren in Sammlungen ist hilfreich bei der Definition des Zugriffs auf Monitore in der Benutzerverwaltung,

- Wählen Sie den Browser-Typ - Sie können wählen, von welchem Browser die Transaktionsprüfungen durchgeführt werden sollen. Derzeit unterstützen wir nur Firefox und Chrome. Sie können die Browser-Auswahl der Einstellungen Ihres Monitors jederzeit ändern,
- die Kontrollhäufigkeit so oft wie 5 Minuten bis zu einmal alle 6 Stunden einstellen,

Schritt 2 und 3 sind die gleichen wie bei den Monitoren Uptime und Page Load

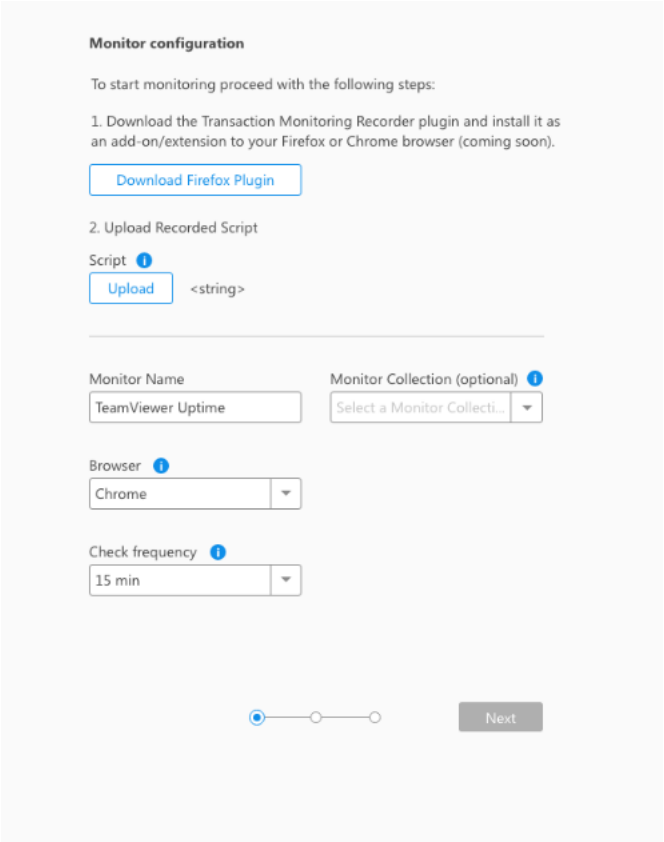


Bild: Transaction Monitor Konfiguration – Schritt 1

7.3.5 Transaction Recorder Plugin Installation

Um mit der Aufzeichnung von Skripten zu beginnen, müssen Sie zunächst den Transaktionsüberwachungs-Recorder herunterladen und als Add-on / Erweiterung für Ihren Firefox-Browser installieren.

- Um den Recorder herunterzuladen, klicken Sie einfach auf die Schaltfläche Firefox-Plugin herunterladen in Schritt 1 von Hinzufügen eines Transaktionsmonitors,

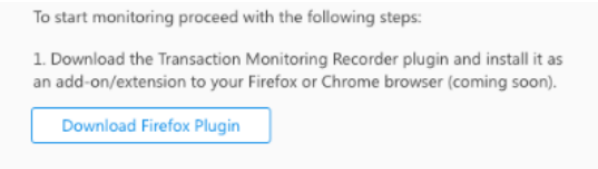
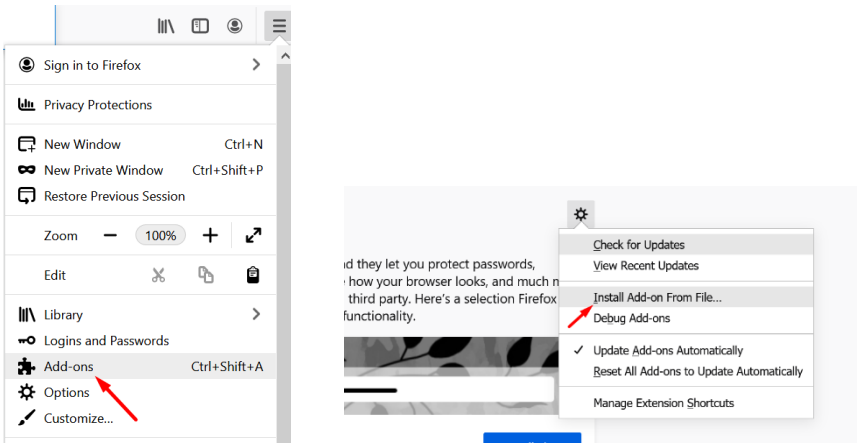


Image: Download Firefox plugin

- Öffnen Sie Firefox und gehen Sie zu Add-ons,
- Klicken Sie in der Registerkarte Erweiterungen auf das Zahnradsymbol und wählen Sie Add-on aus Datei installieren.
- Navigieren Sie im Dialog Add-on zur Installation auswählen zu der heruntergeladenen Rekorderdatei und wählen Sie sie aus, um die Installation zu starten.



Images: Adding Add-ons (left), Installing Add-on from file (right)

- Der Transaktionsrekorder wird nun als Erweiterung in Ihrem Firefox hinzugefügt.

7.3.6 Aufnahme des Transaktionsskripts

Um ein Skript aufzuzeichnen, öffnen Sie den Transaktionsrecorder über das Symbol in der Taskleiste.

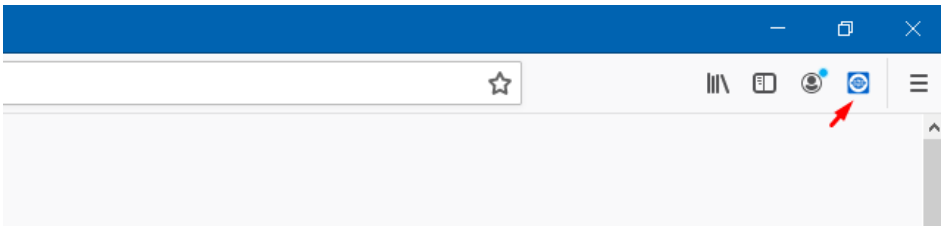
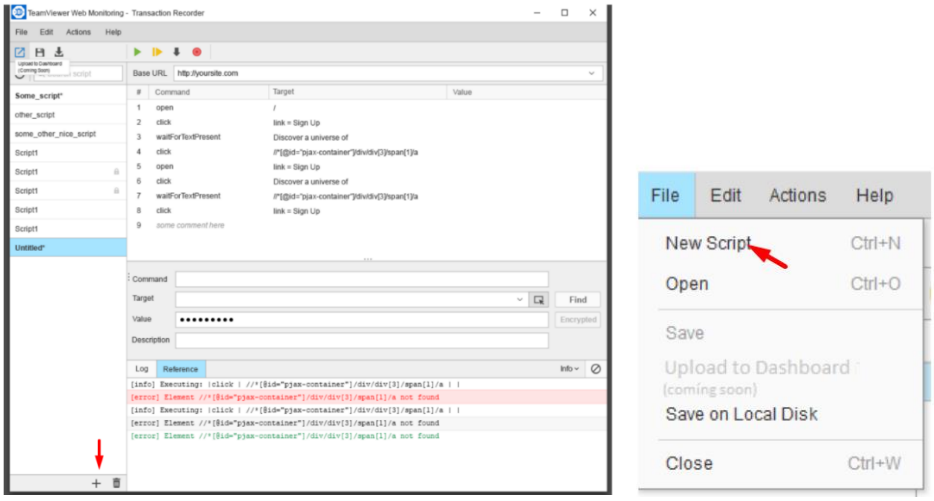


Bild: Transaction Recorder Icon im Firefox Browser



Bilder: Erstellung eines neuen Skripts

1. Klicken Sie auf die Schaltfläche +, um die Aufzeichnung zu starten und Ihre Skripte im unteren Teil oder Neues Skript im Datei-Menü hinzuzufügen.
2. Geben Sie die URL der Site, die Sie überwachen möchten, in das Feld Basis-URL ein (z.B. example.com), und klicken Sie auf die Schaltfläche Aufzeichnung starten, um die Aufzeichnung des Skripts zu starten.
3. Öffnen Sie die Site, die Sie überwachen möchten, in Firefox und beginnen Sie, durch die Site zu navigieren und mit ihr zu interagieren.

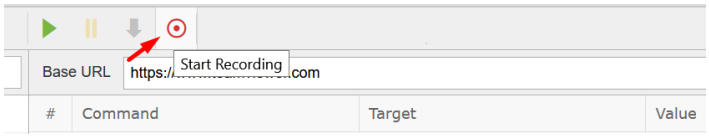


Bild: Aufnahme starten

Hinweis: Wenn Sie das Feld Basis-URL leer lassen und dann auf die Schaltfläche Aufzeichnung starten klicken und die Website öffnen, auf der Sie ein Skript aufzeichnen möchten, wird die Basis-URL automatisch mit der Adresse der Website ausgefüllt, und zwar nach dem Öffnen-Befehl, den der Rekorder in Ihrem Skript hinzugefügt hat.

- Der Transaktionsrecorder zeichnet alle Ihre Schritte auf. Während der Aufzeichnungsphase können Sie jeden aufgezeichneten Befehl bearbeiten, indem Sie ihn auswählen und den Wert im Feld Befehl bearbeiten. Sie können auch Befehle einfügen/löschen (verwenden Sie die entsprechende Option nach einem Rechtsklick auf einen Schritt).

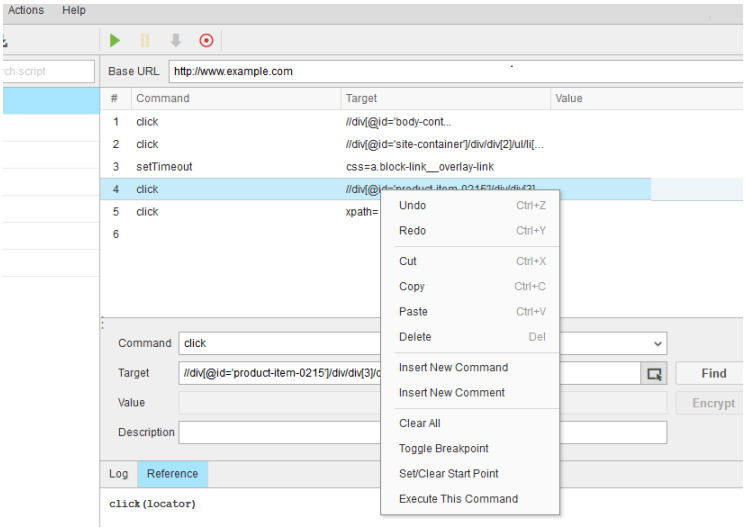


Bild: Befehle verwalten

Hinweis: Die Beschreibung des ausgewählten Befehls wird auf der Registerkarte Referenz unten im Fenster des Transaktionsrecorders angezeigt.

- Um das aufgezeichnete Skript auf Ihre lokale Festplatte herunterzuladen, klicken Sie auf die Schaltfläche Download. Sie können dies auch über das Menü Datei tun. Beachten Sie, dass ein Sternchen '*' neben dem Namen des Skripts bedeutet, dass Sie ungespeicherte Änderungen in diesem Skript vorgenommen haben.
- - Um einen zuvor aufgezeichneten Test zu bearbeiten, gehen Sie zum Register Skripte, wählen Sie einen Test aus der Liste im linken Bereich des Aufnahmefensters und klicken Sie darauf.

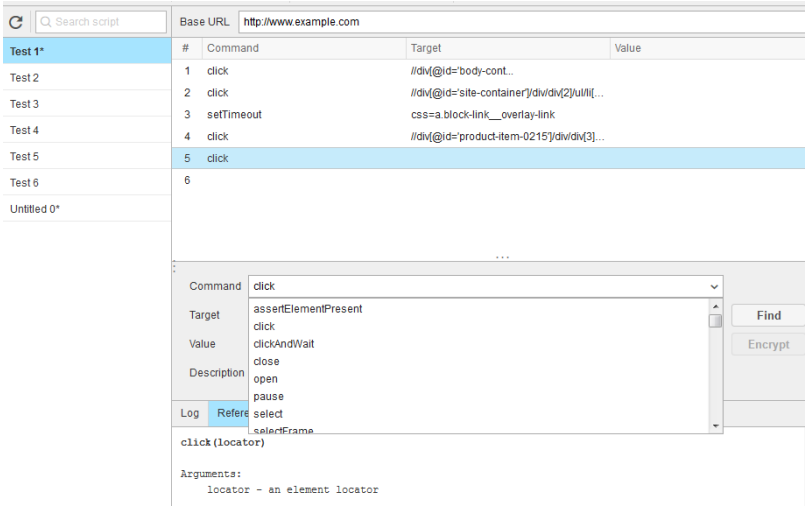


Bild: Skript editieren

- Um die Skriptänderungen zu speichern, klicken Sie auf die Schaltfläche Speichern, entweder im Recorder oder im Menü Datei. Beachten Sie, dass die Schaltfläche Speichern inaktiv bleibt, wenn keine Änderungen im Skript vorgenommen wurden.
- Um den aufgezeichneten Ablauf anzusehen, klicken Sie auf die Schaltfläche Skript ausführen.
- Sie können auch andere Skripte öffnen/auf den Rekorder hochladen, um sie zu bearbeiten oder auch, um das Skript auf dem Rekorder zu behalten.

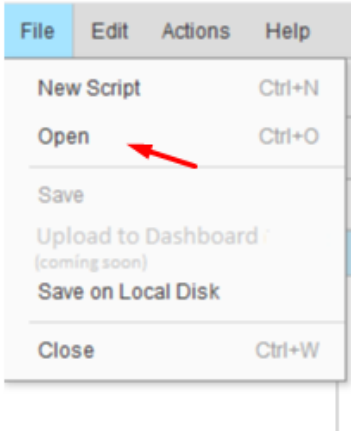


Bild: Skript zum Rekorder uploaden

In Zukunft werden Sie auch die Möglichkeit haben, Ihre Skripte direkt auf das Web-Monitoring-Dashboard hochzuladen und das gleiche Recorder-Plugin für einen Chrome-Browser zu verwenden.

Technische Hinweise zur Aufnahme eines Skripts

- Es gibt drei Felder, die wesentliche Informationen über jeden Schritt im Skript speichern - Befehl, Ziel und Wert. Für jedes auf der Webseite vorhandene Element bildet der Transaktionsrecorder seine Aktion mit diesen drei Werten ab: Befehl, Ziel und Wert. Wenn Sie z.B. einen Benutzernamen in das Textfeld Benutzername eingeben, übersetzt der Transaktionsrecorder ihn als COMMAND=TYPE , TARGET=USERNAME_TEXT_BOX und VALUE=YOUR_USERNAME. Bei Befehlen, die sich auf Asserts beziehen, kann ein bestimmter Wert zum Vergleich mit einem anderen Wert angegeben werden. Zum Beispiel: COMMAND=ASSERTTEXT, TARGET=LABEL und VALUE=SOMETHINGTOCOMPARE.
- Der Transaktionsrekorder bietet genügend Funktionalität im Hinblick auf die Identifizierung des Ziels. Zum Beispiel kann der Kunde das Ziel über DOM, ID, Name, XPath usw. lokalisieren oder identifizieren. Möglicherweise finden Sie es auch nützlich, Firefox-Erweiterungen wie DOM Inspector oder XPath Viewer auszuprobieren, um Informationen über den XPath oder die DOM-Informationen des zu testenden GUI-Elements zu erhalten.

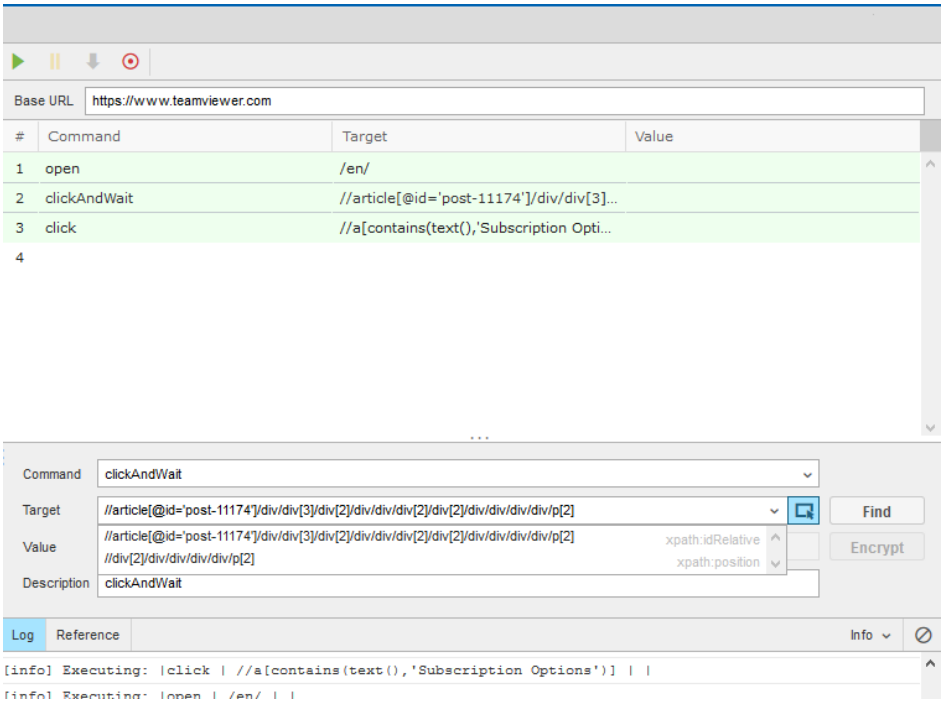


Image Identifying the target

- Verwenden Sie die Schaltfläche Zielauswahl, um das Ziel auf der Webseite auszuwählen. Klicken Sie auf die Schaltfläche und dann auf ein Element auf der Webseite, um es auszuwählen. Um die Auswahl zu ändern, klicken Sie auf ein anderes Element. Um die Auswahl aufzuheben, klicken Sie erneut auf die Schaltfläche.
- - Nachdem Sie das Element ausgewählt haben, können Sie je nach Bedarf zwischen ID, Name oder XPath als Ziel des Elements wählen, indem Sie den Wert aus dem Kombinationsfeld Ziel auswählen.
- - Sie können auch die Drucktaste Suchen verwenden, um das Element zu finden, das Sie unter Ziel angegeben haben.
- - Es gibt auch speziell entwickelte Befehle: **if**, **else** und **for**.
- - Wenn es notwendig ist, den Ablauf eines Transaktionsskripts durch Einfügen einer Bedingung zu ändern, dann können Sie die "**if/else**"-Anweisung verwenden. Die Bedingung der "**wenn**"-, "**sonst**"- und "**für**"-Klauseln wird in der Spalte Ziel angezeigt. Wenn die "**else**"-Klausel nicht benötigt wird, sollten Sie die "**if**"-Klausel mit dem "**endif**"-Befehl schließen. Wenn Sie den Befehl "else" verwenden, sollten Sie ihn mit dem Befehl "**endElse**" schließen.
- - In einigen Fällen muss der standardmäßig hinzugefügte Befehl "**click**" in "**clickAndWait**" geändert werden, da das Laden des Elements oder der Seite einige Zeit in Anspruch nimmt.
- - Verwenden Sie die "**for**"-Anweisung, um die gleichen Befehle mehrmals zu wiederholen.

7.3.7 Liste der vom Transaktionsrekorder verwendeten Befehle

N	Befehl Name	Befehl Beschreibung
1	click	Klicken Sie auf das Element. Die "..andWait"-Version wartet dann ebenfalls auf ein Seitenladeereignis.
2	open	Open unterstützt relative und vollständige URLs.
3	type	Dieser Befehl löscht Box-Inhalte, sendkey jedoch nicht.
4	pause	Die Zeit zum Schlafen in Millisekunden. Zum Beispiel: "5000" bedeutet Schlaf für 5 Sekunden.
5	waitForElementPresent	Prüft, ob sich das angegebene Element irgendwo auf der Seite
6	setTimeout	Gibt die Zeitspanne an, die der Rekorder auf den Abschluss von Aktionen wartet. Zu den Aktionen, die ein Warten erfordern, gehören "offene" und "Warten auf" Aktionen. Die Standardzeitüberschreitung beträgt 30 Sekunden.
7	clickAndWait	
8	clickHiddenElement	Klickt auf einen verborgenen Link, eine Schaltfläche, ein Kontrollkästchen oder ein Optionsfeld. Wenn die Klickaktion das Laden einer neuen Seite bewirkt (wie es bei einem Link normalerweise der Fall ist), rufen Sie waitForPageToLoad auf.
9	storeEval	Ruft das Ergebnis der Auswertung des angegebenen JavaScript-Snippets ab. Das Snippet kann mehrere Zeilen haben, aber es wird nur das Ergebnis der letzten Zeile zurückgegeben. Beachten Sie, dass das Snippet standardmäßig im Kontext des "Selen" ausgeführt wird.
10	select	Objekt selbst, also bezieht sich dies auf das Selen-Objekt. Verwenden Sie window, um auf das Fenster Ihrer Anwendung zu verweisen, z.B. window.document.getElementById('foo')
11	storeElementPresent	Überprüft, ob sich das angegebene Element irgendwo auf der Seite befindet.
12	waitForPageToLoad	Wartet auf das Laden einer neuen Seite. Sie können diesen Befehl anstelle der Suffixe "AndWait", "clickAndWait", "selectAndWait", "typeAndWait" usw. verwenden.
13	if	
14	waitForVisible	Bestimmt, ob das angegebene Element sichtbar ist. Ein Element kann unsichtbar gemacht werden, indem die CSS-Eigenschaft "visibility"

		auf "hidden" oder die Eigenschaft "display" auf "none" gesetzt wird, entweder für das Element selbst oder für einen seiner Vorfahren.
15	fireEvent	Ein Ereignis explizit simulieren, um den entsprechenden "Ein-Ereignis"-Handler auszulösen.
16	endIf	
17	selectFrame	Wählt einen Rahmen innerhalb des aktuellen Fensters aus. (Sie können diesen Befehl mehrmals aufrufen, um verschachtelte Rahmen auszuwählen).
18	selectWindow	Wählt ein Popup-Fenster mit Hilfe eines Fenster-Locators aus; sobald ein Popup-Fenster ausgewählt wurde, gehen alle Befehle zu diesem Fenster. Um das Hauptfenster erneut auszuwählen, verwenden Sie null als Ziel.
19	setDimension	Legen Sie die Größe des aktuellen Fensters fest. Dadurch wird die äußere Fensterabmessung geändert, nicht nur der Ansichtsport.
20	waitForText	Ruft den Text eines Elements ab. Dies funktioniert für jedes Element, das Text enthält.
21	clickHiddenElementAndWait	Klickt auf einen verborgenen Link, eine Schaltfläche, ein Kontrollkästchen oder ein Optionsfeld. Wenn die Klick-Aktion das Laden einer neuen Seite bewirkt (wie es bei einem Link normalerweise der Fall ist), rufen Sie waitForPageToLoad
22	else	
23	sendKeys	Simuliert Tastendruck-Ereignisse auf dem angegebenen Element, als ob Sie den Wert Taste für Taste eingegeben hätten. Dies simuliert einen echten Benutzer, der jedes Zeichen in der angegebenen Zeichenfolge eingibt; es ist auch an die Einschränkungen eines echten Benutzers gebunden, wie z.B. nicht in der Lage zu sein, in ein unsichtbares oder schreibgeschütztes Element einzugeben
24	endElse	
25	chooseCancelOnNextConfirmation	
26	mouseOver	Simuliert einen Benutzer, der mit der Maus über das angegebene Element fährt.
27	waitForElementNotPresent	Überprüft, ob sich das angegebene Element irgendwo auf der Seite befindet.
28	store	Gibt den angegebenen Ausdruck zurück. Dies ist wegen der JavaScript-Vorverarbeitung nützlich und wird verwendet, um Befehle wie

		assertExpression und waitForExpression zu generieren.
29	assertElementPresent	Überprüft, ob sich das angegebene Element irgendwo auf der Seite befindet.
30	mouseDown	Simuliert einen Benutzer, der die linke Maustaste (ohne sie noch loszulassen) auf dem angegebenen Element drückt.
31	runScript	Erstellt ein neues "Skript"-Tag im Körper des aktuellen Testfensters und fügt den angegebenen Text in den Körper des Befehls ein. Skripte, die auf diese Weise ausgeführt werden, lassen sich oft leichter debuggen als Skripte, die mit dem Befehl "getEval" von Selenium ausgeführt werden.
32	close	Simuliert, dass der Benutzer auf die Schaltfläche "close" in der Titelleiste eines Popup-Fensters oder Tabs klickt.
33	verifyElementPresent	Überprüft, ob sich das angegebene Element irgendwo auf der Seite befindet.
34	waitForCondition	Führt das angegebene JavaScript-Snippet wiederholt aus, bis es als "true" ausgewertet wird. Das Snippet kann mehrere Zeilen haben, aber nur das Ergebnis der letzten Zeile wird berücksichtigt.
35	endFor	
36	for	
37	waitForNotVisible	Bestimmt, ob das angegebene Element sichtbar ist. Ein Element kann unsichtbar gemacht werden, indem die CSS-Eigenschaft "Sichtbarkeit" auf "versteckt" oder die Eigenschaft "Anzeige" auf "keine" gesetzt wird, entweder für das Element selbst oder für einen seiner Vorfahren. Diese Methode schlägt fehl, wenn das Element nicht vorhanden ist.
38	storeText	Ruft den Text eines Elements ab. Dies funktioniert für jedes Element, das Text enthält. Dieser Befehl verwendet entweder den textContent (Mozilla-ähnliche Browser) oder den innerText (IE-ähnliche Browser) des Elements, d.h. den gerenderten Text, der dem Benutzer angezeigt wird.
39	assertEval	Ruft das Ergebnis der Auswertung des angegebenen JavaScript-Snippets ab. Das Snippet kann mehrere Zeilen haben, aber es wird nur das Ergebnis der letzten Zeile zurückgegeben.

40	mouseMove	Simuliert einen Benutzer, der mit der Maus über das angegebene Element fährt.
41	echo	Druckt die angegebene Nachricht in die dritte Tabellenzelle in Ihren Selenese-Tabellen. Nützlich für das Debugging.
42	assertElementNotPresent	Überprüft, ob sich das angegebene Element irgendwo auf der Seite befindet.
43	focus	Bewegen Sie den Fokus auf das angegebene Element; wenn das Element beispielsweise ein Eingabefeld ist, bewegen Sie den Cursor auf dieses Feld.
44	storeVisible	Bestimmt, ob das angegebene Element sichtbar ist. Ein Element kann unsichtbar gemacht werden, indem die CSS-Eigenschaft "Sichtbarkeit" auf "versteckt" oder die Eigenschaft "Anzeige" auf "keine" gesetzt wird, entweder für das Element selbst oder für einen seiner Vorfahren. Diese Methode schlägt fehl, wenn das Element nicht vorhanden ist.
45	storeTextPresent	Es wird überprüft, ob das angegebene Textmuster irgendwo auf der gerenderten Seite erscheint, die dem Benutzer angezeigt wird.
46	addSelection	Fügen Sie dem Satz ausgewählter Optionen in einem Mehrfachauswahl-Element mit Hilfe eines Options-Locators eine Auswahl hinzu.
47	assertConfirmation	Ruft die Nachricht eines JavaScript-Bestätigungsdialogs ab, der während der vorherigen Aktion generiert wurde. Standardmäßig gibt die Bestätigungsfunktion den Wert true zurück, was den gleichen Effekt hat wie das manuelle Klicken auf OK. Dies kann durch vorherige Ausführung des Befehls chooseCancelOnNextConfirmation geändert werden.
48	verifyConfirmation	
49	createCookie	Erstellen Sie ein neues Cookie, dessen Pfad und Domäne mit denen der aktuell getesteten Seite übereinstimmen, es sei denn, Sie haben explizit einen Pfad für dieses Cookie angegeben.
50	refresh	Simuliert den Benutzer, der auf die Schaltfläche "Aktualisieren" in seinem Browser klickt.
51	mouseUp	Simuliert das Ereignis, das eintritt, wenn der Benutzer die Maustaste auf dem angegebenen Element loslässt (d.h. aufhört, die Taste gedrückt zu halten).
52	assertTitle	Ruft den Titel der aktuellen Seite ab.

53	verifyElementNotPresent	Überprüft, ob sich das angegebene Element irgendwo auf der Seite befindet.
54	assertExpression	Gibt den angegebenen Ausdruck zurück. Dies ist wegen der JavaScript-Vorverarbeitung nützlich und wird verwendet, um Befehle wie assertExpression und waitForExpression zu generieren.
55	chooseOkOnNextConfirmation	Standardmäßig gibt die von Selenium überschriebene Funktion window.confirm() den Wert true zurück, als ob der Benutzer manuell auf OK geklickt hätte; nach Ausführung dieses Befehls gibt der nächste Aufruf von confirm() den Wert false zurück, als ob der Benutzer auf Cancel geklickt hätte. Selenium verwendet dann für zukünftige Bestätigungen wieder das Standardverhalten und gibt automatisch true (OK) zurück, es sei denn, Sie rufen diesen Befehl bei jeder Bestätigung explizit auf.
56	highlight	Ändert kurzzeitig die Hintergrundfarbe des angegebenen Elements gelb. Nützlich für die Fehlersuche.
57	waitForTextNotPresent	Überprüft, ob das angegebene Textmuster irgendwo auf der gerenderten Seite erscheint, die dem Benutzer angezeigt wird.
58	waitForTitle	Ruft den Titel der aktuellen Seite ab.
59	waitStoreElementPresent	Speichert, ob das Element auf der Seite vorhanden ist.
60	verifyTitle	Ruft den Titel der aktuellen Seite ab.
61	check	Markieren Sie eine Umschalttaste (Checkbox/Radio).
62	waitForConfirmation	Ruft die Nachricht eines JavaScript-Bestätigungsdialogs ab, der während der vorherigen Aktion generiert wurde. Standardmäßig gibt die Bestätigungsfunktion den Wert true zurück, was den gleichen Effekt hat wie das manuelle Klicken auf OK.
63	assertLocation	Ruft die absolute URL der aktuellen Seite ab.
64	mouseMoveAt	Simuliert einen Benutzer, der die Maustaste auf dem angegebenen Element drückt (ohne sie noch loszulassen).
65	clickAtAndWait	Klickt auf einen Link, eine Schaltfläche, ein Kontrollkästchen oder einen Auswahlknopf. Wenn die Klick-Aktion das Laden einer neuen Seite bewirkt (wie es ein Link normalerweise tut), rufen Sie waitForPageToLoad auf.
66	verifyLocation	Ruft die absolute URL der aktuellen Seite ab.

67	typeJavaScript	Setzt den Wert eines Eingabefeldes, als ob Sie ihn eingegeben hätten. Kann auch verwendet werden, um den Wert von Kombinationsfeldern, Kontrollkästchen usw. festzulegen. In diesen Fällen sollte Wert der Wert der gewählten Option sein, nicht der sichtbare Text.
68	storeValue	Ruft den (durch Leerzeichen getrimmten) Wert eines Eingabefeldes (oder alles andere mit einem value-Parameter) ab. Bei Checkbox-/Radio-Elementen ist der Wert "ein" oder "aus", je nachdem, ob das Element markiert ist oder nicht.
69	typeAndWait	Legt den Wert eines Eingabefeldes so fest, als ob Sie ihn eingegeben hätten. Kann auch verwendet werden, um den Wert von Kombinationsfeldern, Kontrollkästchen usw. festzulegen. In diesen Fällen sollte Wert der Wert der gewählten Option sein, nicht der sichtbare Text.
70	waitForValue	Ruft den (durch Leerzeichen getrimmten) Wert eines Eingabefeldes (oder alles andere mit einem Wert-Parameter) ab. Bei Checkbox-/Radio-Elementen wird der Wert "ein" oder "aus" sein, je nachdem, ob das Element markiert ist oder nicht.
71	deleteCookie	Löschen Sie ein benanntes Cookie mit angegebenem Pfad und Domäne. Seien Sie vorsichtig; um ein Cookie zu löschen, müssen Sie es unter Verwendung genau desselben Pfades und derselben Domäne löschen, die zur Erstellung des Cookies verwendet wurden. Wenn der Pfad falsch ist oder die Domäne falsch ist, wird das Cookie einfach nicht gelöscht.
72	verifyEval	Ruft das Ergebnis der Auswertung des angegebenen JavaScript-Snippets ab. Das Snippet kann mehrere Zeilen haben, aber es wird nur das Ergebnis der letzten Zeile zurückgegeben.
73	verifyVisible	Ermittelt, ob das angegebene Element sichtbar ist. Ein Element kann unsichtbar gemacht werden, indem die CSS-Eigenschaft "Sichtbarkeit" auf "versteckt" oder die Eigenschaft "Anzeige" auf "keine" gesetzt wird, entweder für das Element selbst oder eines seiner Vorfahren. Diese Methode schlägt fehl, wenn das Element nicht vorhanden ist.
74	submit	Reichen Sie das angegebene Formular ein. Dies ist besonders nützlich für Formulare ohne Submit-Schaltflächen, z.B. "Suche"-Formulare mit einfacher Eingabe.

75	verifyValue	Ruft den (durch Leerzeichen getrimmten) Wert eines Eingabefeldes (oder alles andere mit einem Wert-Parameter) ab. Bei Checkbox-/Radio-Elementen ist der Wert "ein" oder "aus", je nachdem, ob das Element markiert ist oder nicht.
76	windowMaximize	Ändern Sie die Größe des aktuell ausgewählten Fensters so, dass es den gesamten Bildschirm einnimmt.
77	openWindow	Öffnet ein Popup-Fenster (falls ein Fenster mit dieser ID nicht bereits geöffnet ist). Nachdem Sie das Fenster geöffnet haben, müssen Sie es mit dem Befehl selectWindow auswählen.
78	storeAttribute	Ruft den Wert eines Elementattributs ab. Der Wert des Attributs kann sich von Browser zu Browser unterscheiden (dies ist z.B. beim Attribut "style" der Fall).
79	goBack	Simuliert, dass der Benutzer auf die Schaltfläche "Zurück" in seinem Browser klickt.
80	removeSelection	Entfernt eine Auswahl aus der Menge der ausgewählten Optionen in einem Mehrfachauswahl-Element unter Verwendung eines Optionslocators.

7.3 Monitors Daten Visualisierung

7.3.1 Tabellenansicht

Die Tabellenansicht dient zur Anzeige der Liste der Monitore und der für sie relevanten Informationen, wie z.B::

- Name des Monitors,
- Die Reaktionszeit der letzten Überprüfung.
- Der Status des Monitors - OK oder Ausgefallen, die linke Seite der ausgefallenen Monitore ist rot gefärbt.
- Der Monitortyp und die Subtypen - z.B. Uptime (HTTP), Uptime (ICMP), Page Load oder Transaktion.
- Die URL oder IP - auf der der Monitor läuft.
- Die Monitorsammlung - die Gruppe oder Gruppen, zu der/denen der Monitor gehört.

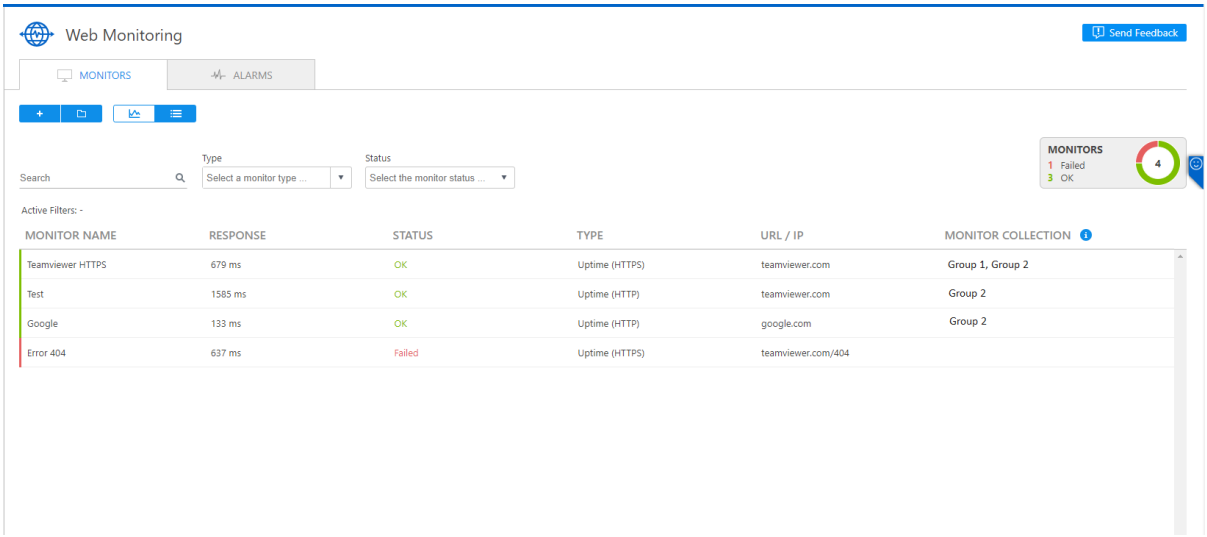
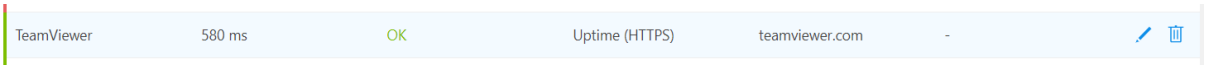


Bild: Web-Monitoring-Tabellenansicht

Wenn Sie den Mauszeiger genau auf die Monitorzeile in der rechten Ecke bewegen, können Sie die Aktionssymbole des Monitors sehen, bearbeiten und löschen.



Die Web-Monitoring-Tabellenansicht hat, wie die meisten anderen Fernverwaltungsprodukte, auch die folgenden Funktionen:

Suchfunktion: Damit können Benutzer den Monitor nach Name und URL oder IP suchen.

Filterung: nach Monitortyp, Status und Monitorsammlung.

Nach Gerätestatus: Benutzer können die Geräte nach ihrem Status auswählen (Einzel- und Mehrfachauswahl ist möglich).

Monitors Status-Kachel

Die Monitor-Status-Kachel ist sowohl im Dashboard der Tabellen- als auch der Diagrammansicht sichtbar und spiegelt alle Arten von statusbezogenen Informationen der Monitore wider:

- Die Gesamtzahl der Monitore
- Die Anzahl der ausgefallenen und die Anzahl der OK-Statusmonitore

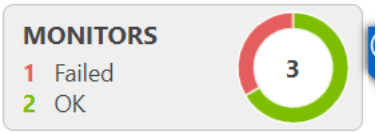


Bild: Monitors Status-Kachel

7.3.2 Chart Ansicht

Die Web-Monitoring-Chart-Ansicht zeigt die historischen Überwachungsdaten-Ergebnisse pro Check für die angegebenen Zeitintervalle wie die letzte Stunde oder 3, 6, 12 und 24 Stunden, bald können Sie auch die aggregierten Daten-Zeitintervalle wie die letzten 3 Tage oder 7, 30 Tage sowie die Möglichkeit, zu einem bestimmten Datum oder Datumsbereich zu wechseln, erhalten.

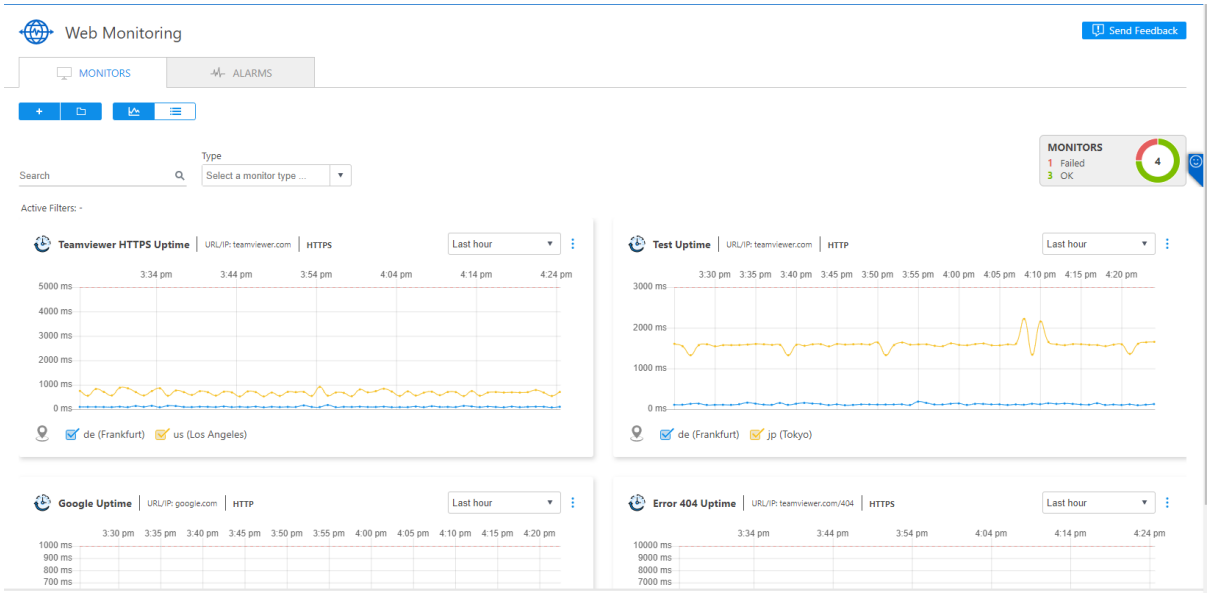


Bild: Web Monitoring chart Ansicht

Im oberen Teil des Monitordiagramms Uptime zeigt der Monitorname, -typ, URL/ IP und der Subtyp des Uptime-Monitors an, im unteren Teil wird angezeigt, von welchen Standorten aus die Überwachung läuft. Im oberen Teil des Monitordiagramms Page Load wird auch der Browser (Firefox oder Chrome) angezeigt, von dem aus die Überwachung ausgeführt wird.

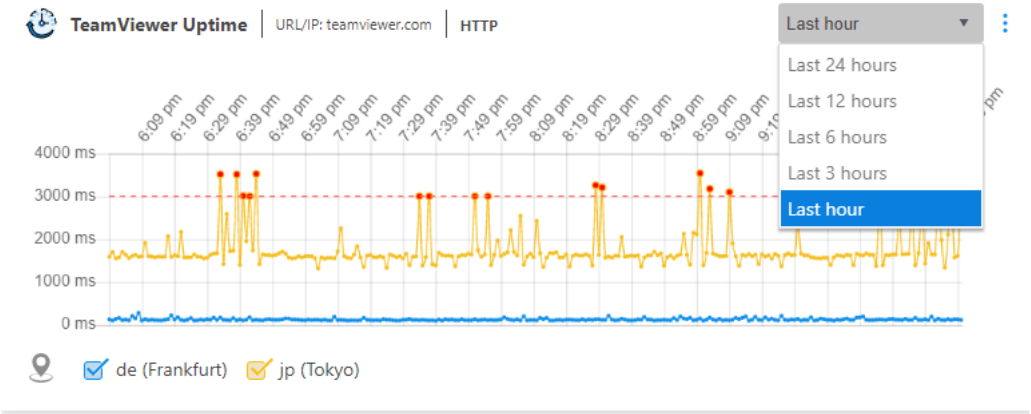


Image: Web Monitoring chart Ansicht – Datenbereiche

Die Diagrammansicht zeigt deutlich an, ob eine Prüfung fehlgeschlagen ist. Die fehlgeschlagenen Überprüfungen werden durch rote Punkte angezeigt, wenn Sie auf den roten Punkt schweben, werden die Zeit, zu der der Fehler aufgetreten ist, die Fehlerort-ID und der Fehlergrund im Tooltip angezeigt.

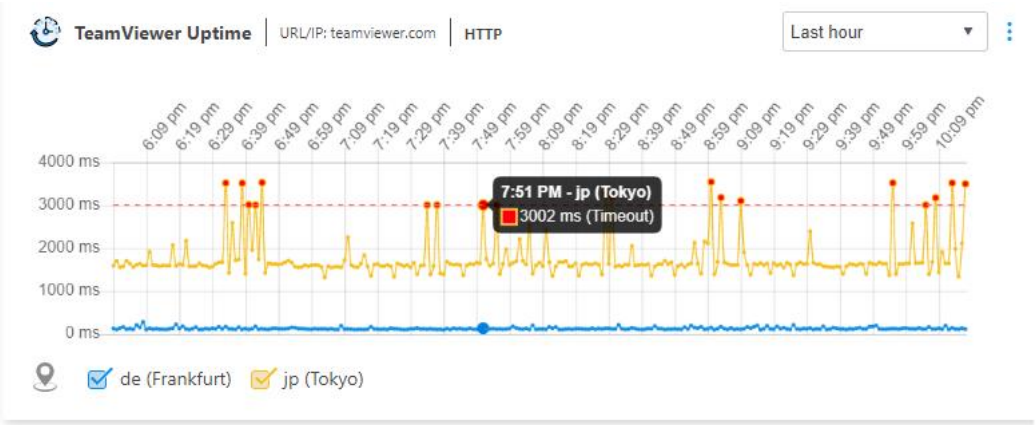


Bild: Web Monitoring Chart Ansicht, Rote Punkte

7.4 Alarme und Benachrichtungen

7.4.1 Alarme

Die Ansicht der Alarme konzentriert sich auf die Reaktion auf Vorfälle. Alle ausgelösten Alarme, bei denen die Prüfschwelle überschritten wurde, können gefiltert, organisiert und exportiert werden.

In der Alarmansicht können Sie den Schweregrad der Alarme sehen und bei Bedarf schnelle Maßnahmen ergreifen. Die erweiterbaren Zeilen ermöglichen es Ihnen, die Details der fehlgeschlagenen Prüfung zu sehen, wie z.B. Orte, von denen der Fehler stammt, Reaktionszeit, Host, Fehlermeldung, Browser, Schritt, auf dem der Fehler aufgetreten ist usw.

Neue Alarme werden am Anfang der Alarmliste hinzugefügt und die linke Seite der Zeile wird rot gefärbt.

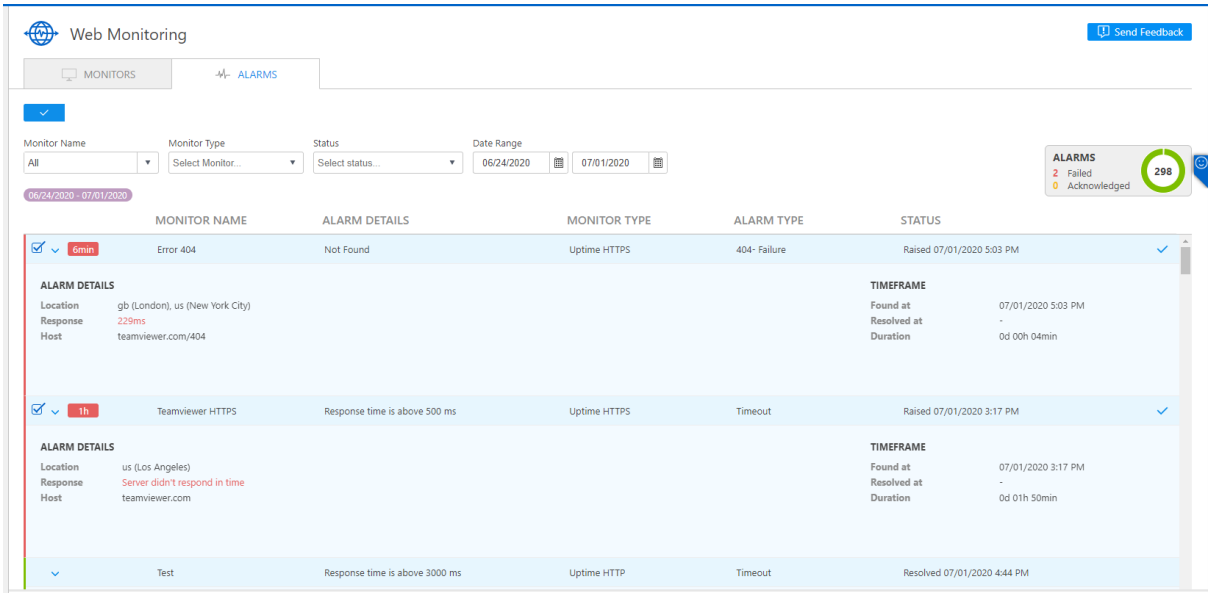


Bild: Web Monitoring Alarmansicht

Sie können den Alarm quittieren, indem Sie die offenen Status-Alarmzeilen mehrfach überprüfen und dann auf die Schaltfläche Quittieren im linken oberen Teil des Armaturenbretts oder eine nach der anderen im rechten Teil der Alarmzeile klicken. Nach der Bestätigung wird der linke Teil des Alarms gelb gefärbt.

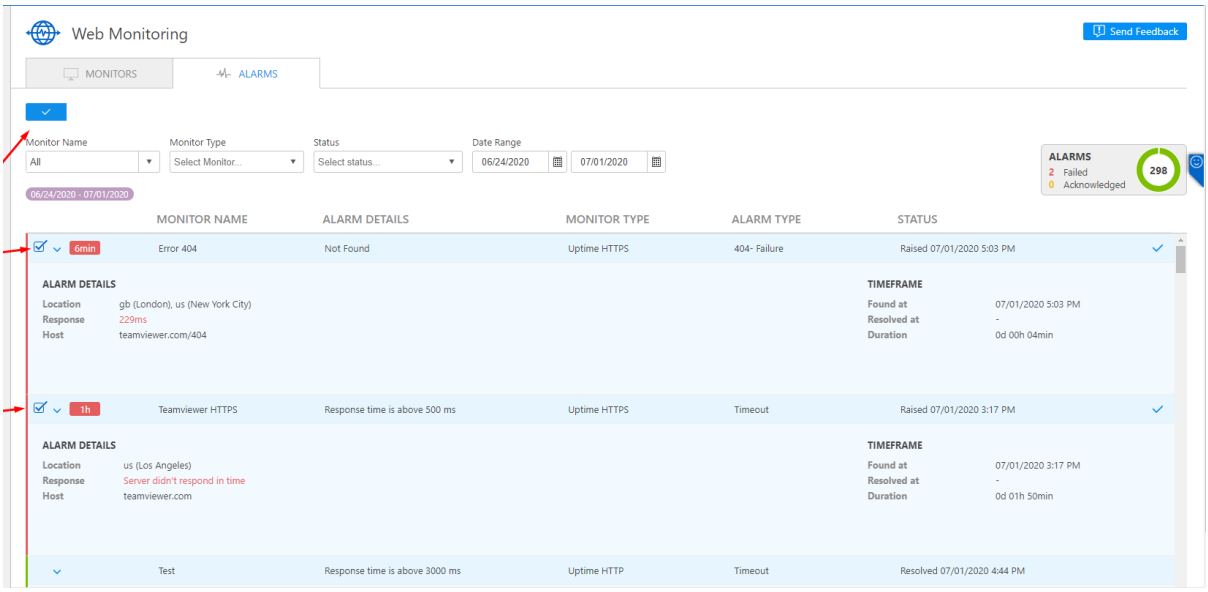


Bild: Web Monitoring Alarme bestätigen

Quittieren bedeutet, dass bestätigt wird, dass der Alarm bemerkt wird und gegebenenfalls Maßnahmen ergriffen werden, so dass andere sich darüber keine Sorgen machen müssen. Bei der Bestätigung werden die Zeit und die Person, die den Alarm bestätigt hat, im Zeitrahmen-Teil des Alarms festgelegt.

Gelöste Alarme werden grün gefärbt.

Ähnlich wie in den Tabellen- und Diagrammansichten ist auch in der Alarmansicht eine Filterung nach; Monitorname möglich. Monitortyp, Status und Datumsbereiche.

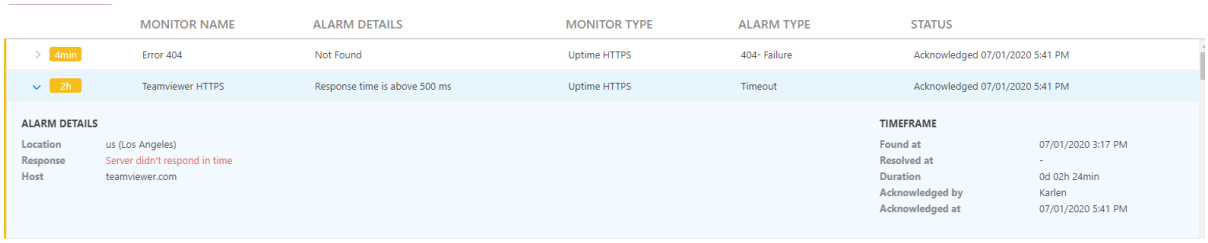


Bild: Web Monitoring Bestätigungsdetails

7.4.5 Benachrichtigungen

Alarmbenachrichtigungsbedingungen können in den Monitorkonfigurationen in Schritt 3 oder 4 je nach Monitortyp eingerichtet werden. Sie können benachrichtigt werden, wenn vom System akzeptierte E-Mail-Adressen diejenigen sind, die vom TeamViewer-Konto oder Firmenprofil erkannt werden:

- Bei TeamViewer-Konten muss die E-Mail-Adresse als Kontakt in der Kontaktliste enthalten sein.
- Für TeamViewer-Firmenprofile muss die E-Mail-Adresse als Kontakt oder als Benutzer im Firmenprofil enthalten sein.

E-Mail-Benachrichtigungen werden gesendet von: notification@teamviewer-rm.com

> **Hinweis:** Wenn Sie mit Proxy oder benutzerdefinierten Firewalls arbeiten, kann eine Whitelist zur Domäne *.teamviewer-rm.com hinzugefügt werden.

Um die Benachrichtigungen so einzurichten, dass Sie die E-Mails erhalten, wenn Ihre Monitore ausfallen, sollten Sie zwischen 2 Optionen wählen

- bei jedem einzelnen Fehler einen Alarm auslösen oder
- Auslösen eines Alarms bei einigen (1,2 oder 3) aufeinanderfolgenden Ausfällen von zwei beliebigen Standorten aus

Ihr Monitor wird ausfallen, wenn;

- Die Reaktionszeit liegt über dem Einrichtungs-Timeout
- - Es gibt DNS-Lösungsprobleme
- - Es gibt Konfigurationsprobleme
- - Fehlerantworten wie 404 Nicht gefunden oder 500 Interne Fehler werden empfangen
- - Es gibt unbekannte Fehler im System

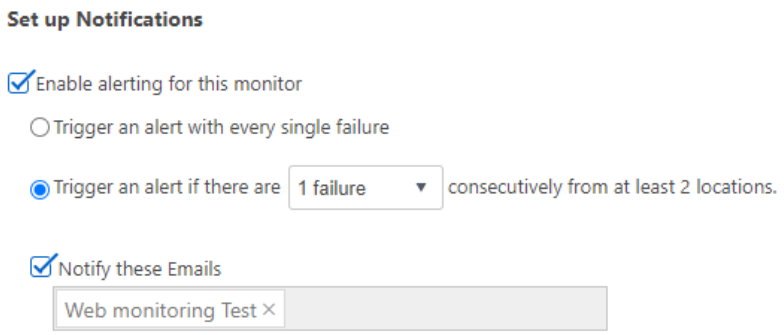


Bild: Einrichten von Benachrichtigungsbedingungen

E-Mail-Benachrichtigungen zu ausgelösten oder wiederhergestellten Alarmen und Monitortypen enthalten die folgenden Informationen:

- Alarm-Details
- Name des Monitors
- Monitor-Typ
- URL/ IP
- Protokoll
- Anfrage-Methode
- Orte, wo Misserfolge herkommen
- Sammlung Monitore
- Fehlerbeschreibung des Transaktionsmonitors
- Schritt Nummer
- Schritt Details
- Schritt Dauer
- Fehler Inhalt
- Alarm-Start
- Alarm Ende
- Ausfall Dauer

7.5 Monitor-Sammlung

Mit Monitorsammlungen können Sie Monitore in verschiedenen Sammlungen gruppieren. Die Anzahl der Monitore, die zu einer Sammlung hinzugefügt werden können, ist nicht beschränkt. Ein und derselbe Monitor kann an mehr als eine Sammlung angeschlossen werden.

Um eine Monitorsammlung hinzuzufügen, sollten Sie auf das Ordnersymbol im oberen linken Teil der Dashboards der Tabellen- oder Diagrammansicht klicken.

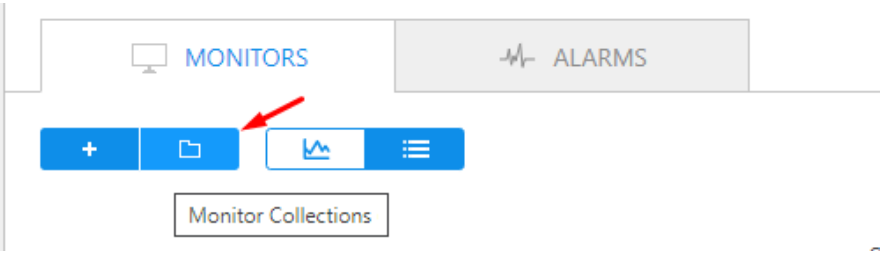


Bild: Monitor Sammlung hinzufügen - Schritt 1

Auf der Seite Monitorsammlungen verwalten sollten Sie einen eindeutigen Namen eingeben und mindestens einen Monitor aus der Liste unten auswählen, um eine Sammlung (eine Gruppe) zu erstellen.

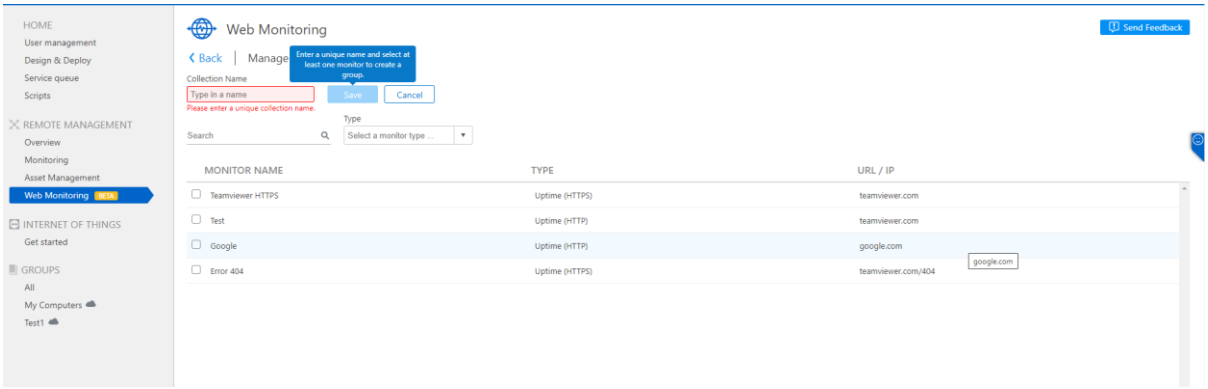


Bild: Monitorsammlung hinzufügen - Schritt 2

Ihre hinzugefügten Monitorsammlungen werden auf der linken Seite in der Liste sichtbar sein, und auf der rechten Seite der ausgewählten Sammlung werden die in der Sammlung enthaltenen Monitore angezeigt.

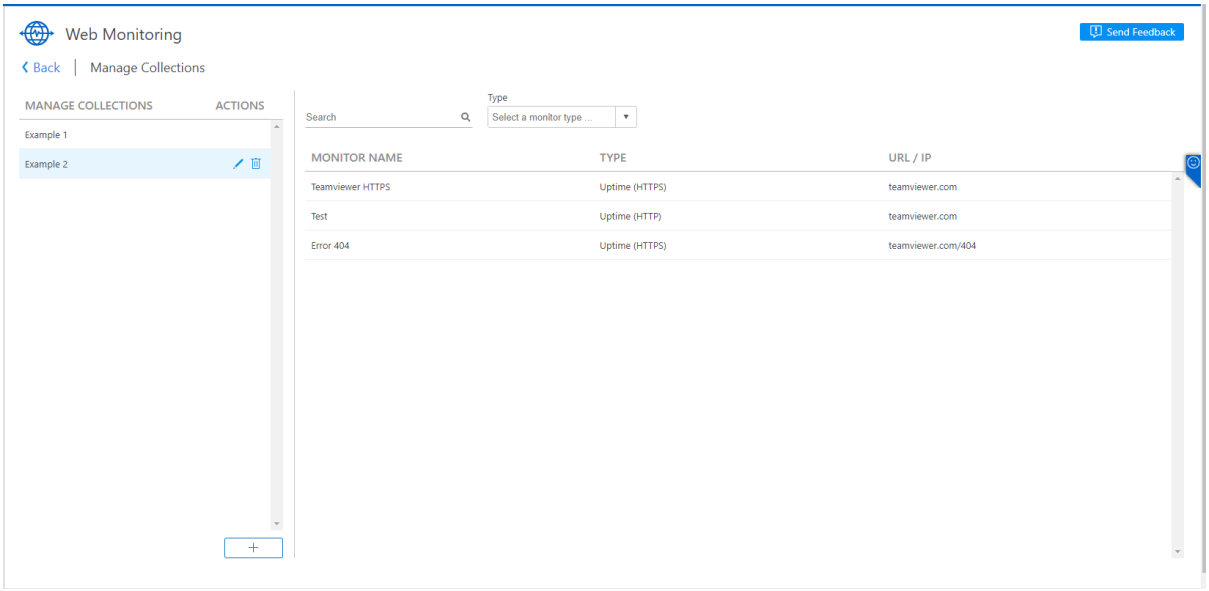


Bild: Liste der Monitorsammlung

Sie können ganz einfach eine weitere Monitorsammlung hinzufügen und Monitore darin aufnehmen, indem Sie auf die Schaltfläche + unten auf der Seite klicken.

7.6 Datenexport

Sie können auch die historischen Daten Ihres Monitors zur späteren Verwendung in eine csv-Datei exportieren. Klicken Sie einfach auf die Schaltfläche CSV exportieren aus dem Untermenü des

Moduls Diagrammansicht des Monitors. Die CSV-Datei wird automatisch auf Ihr lokales Laufwerk heruntergeladen.

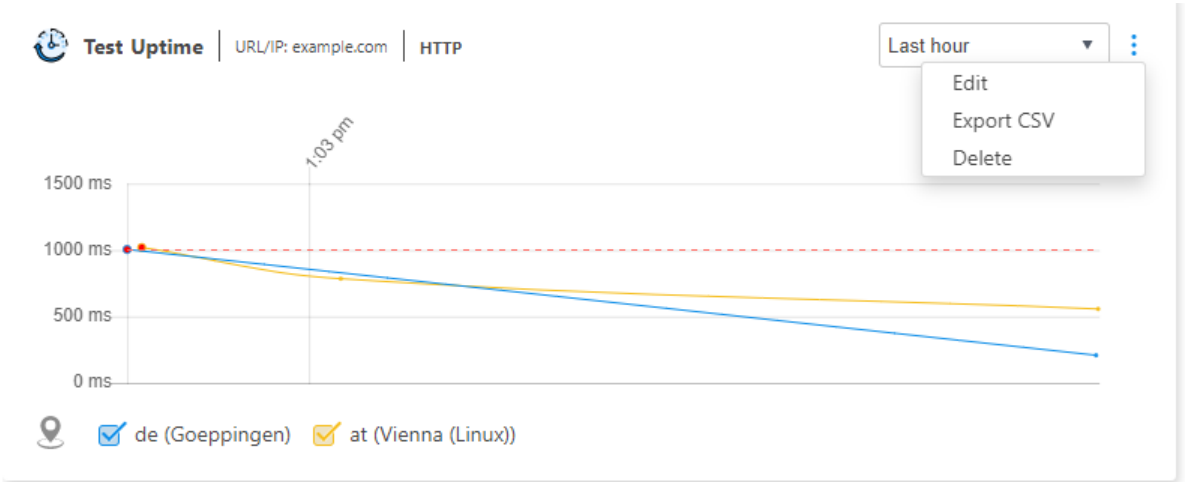


Bild: Datenexport

8. Support

Für Fragen, zusätzliche Hilfe und Unterstützung wenden Sie sich bitte an unser erfahrenes Support-Team, indem Sie ein Ticket einreichen. Sie können auch unsere Community Seite für weitere Unterstützung besuchen. Wir helfen immer gerne!

V6.02.2008

TeamViewer Germany GmbH
Jahnstr. 30
73037 Göppingen
Germany

©2020 TeamViewer Germany GmbH. All rights reserved.