What's new in Enterprise Alert® 9

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

1 WHAT'S NEW IN ENTERPRISE ALERT 9.6?

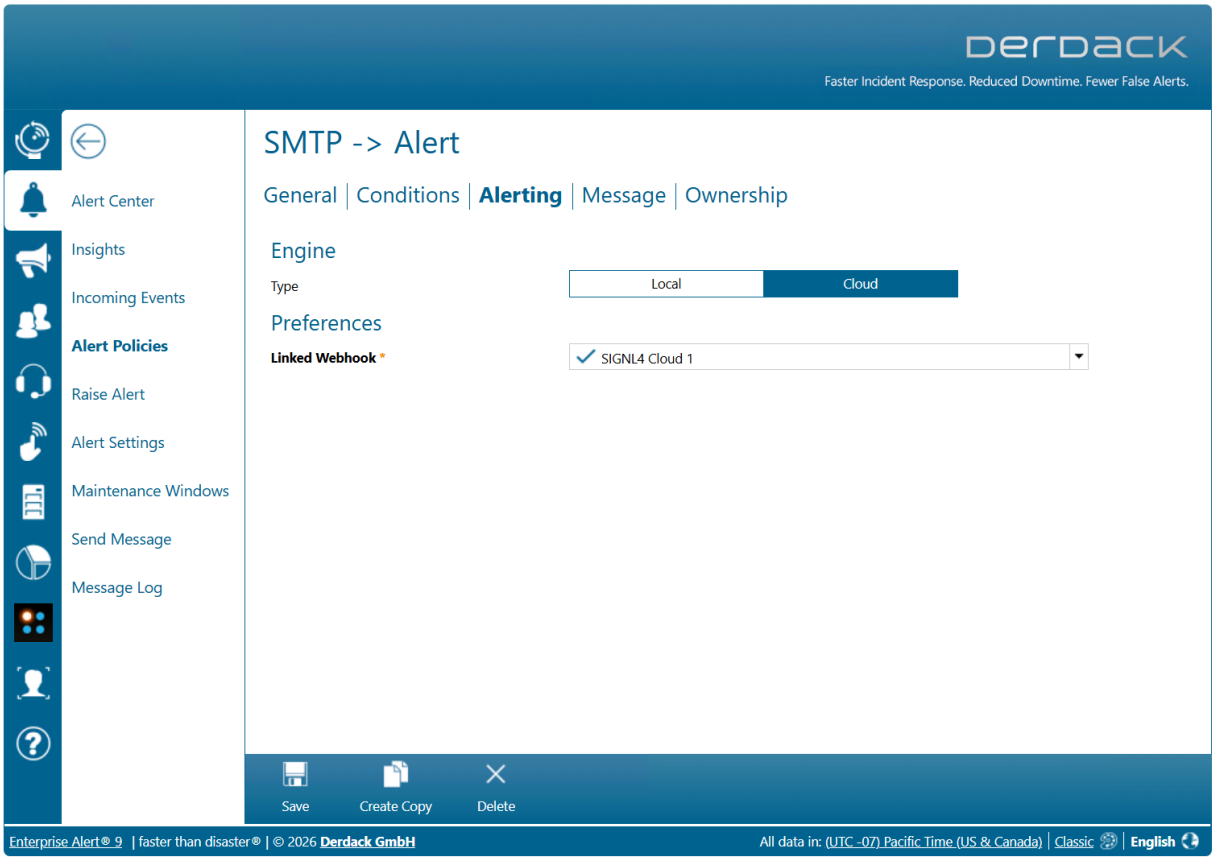
1.1 NEW: Cloud alerting engine in Alert Policies

We have enhanced alert policies with the option to use the SIGNL4 cloud platform as the alerting engine for on-premises events. This integration is based on so-called "Linked Webhooks", which are configured in the Enterprise Alert Cloud Bridge.

Each Linked Webhook is associated with an inbound webhook in your SIGNL4 account. When a Linked Webhook is selected as the target of an Enterprise Alert policy, events are forwarded directly to the SIGNL4 cloud. There, SIGNL4 workflow rules can be used for filtering, duplicate suppression, enrichment, and intelligent routing to the appropriate recipients or teams.

In this configuration, no alert is created within Enterprise Alert. Instead, alert processing, notification delivery, escalation handling, and response tracking are performed entirely within the SIGNL4 cloud platform.

This approach provides greater control over the data leaving your on-premises environment while enabling the use of SIGNL4's intelligent, AI-powered workflow capabilities in the cloud.



1.2 Latest Version of Node.js v24.14 LTS in the Connector Host

Node.js, as a platform for certain third-party system integrations, has been updated to Long-Term Support (LTS) version 24.14 to ensure continued platform support, security updates, and compatibility with current connector technologies.

1.3 Updated Microsoft Visual C++ Runtime Environment 2022

The Microsoft Visual C++ Runtime environment included with Enterprise Alert has been updated to the 2022 version. This ensures compatibility with the latest Microsoft development platform components and security updates.

1.4 Support for SQL Server 2025

Enterprise Alert 9.6 includes support for SQL Server 2025.

1.5 Support for Windows Server 2025

Enterprise Alert 9.6 can be operated on Windows Server 2025. Existing support for Windows Server 2022 remains unchanged.

Important Note for Windows Server 2025

The Enterprise Alert Scripting Host requires the classic Microsoft JScript engine when running on Windows Server 2025. Therefore, the following registry entry is automatically configured during installation:

[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main]
"JScriptReplacement"=dword:00000000

Without this setting, the Enterprise Alert Scripting Host cannot be used on Windows Server 2025.

1.6 Support for .NET Framework 4.8.1

Enterprise Alert 9.6 now supports Microsoft .NET Framework 4.8.1, enabling operation on the latest supported Windows Server platforms and benefiting from Microsoft's latest framework updates.

2 WHAT'S NEW IN ENTERPRISE ALERT 9.5?

Enterprise Alert 9.5 is a maintenance update focused on security aspects and includes the features described below.

2.1 Support for EntraID Login in the Web Portal

Version 9.5 introduces the ability to log in to the web portal using EntraID accounts. It is possible to either allow only EntraID login or to use a hybrid mode, where login with an EnterpriseAlert user account is also permitted.

Maximum security is achieved by allowing only EntraID login, as EntraID provides significantly more authentication methods and can enforce two-factor authentication.

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

At the same time, the Single Sign-On (SSO) provided in this way offers a significantly improved user experience when managing identities and authentication processes within your organization.

A local Windows Active Directory is therefore no longer required for SSO with EnterpriseAlert from version 9.5 onwards, although it may still be relevant for service accounts, etc., within your domain.

2.2 Support for the Latest jQuery Version 3.7 in the Web Portal

The web portal has been updated and now uses jQuery version 3.7, which receives regular security updates. The previously used version recently showed vulnerabilities in some DAST scanners and could therefore lead to compliance issues.

2.3 Latest Version of Node.js v22.14 LTS in the Connector Host

Node.js, as a platform for certain third-party system integrations, has been updated to Long-Term Support (LTS) version 22.14, which will receive security updates until April 2027.

2.4 Support for SQL Server 2022

EnterpriseAlert 9.5 includes support for SQL Server 2022.

2.5 Support for Windows Server 2016 to Windows Server 2022

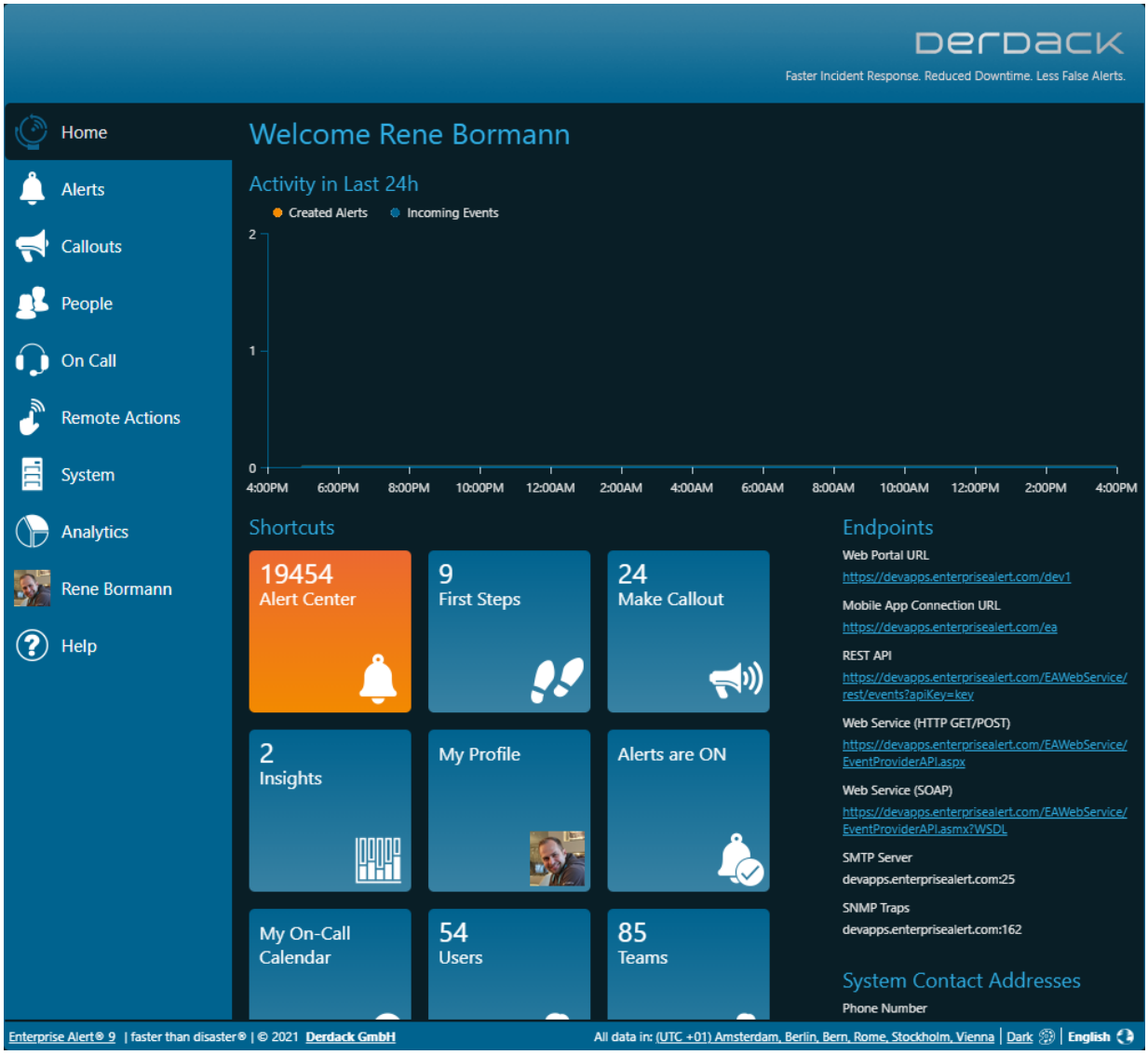
EnterpriseAlert 9.5 can be operated on Windows Server versions 2016 to 2022. Support for earlier server versions, such as 2012, is no longer provided.

3 WHAT'S NEW IN ENTERPRISE ALERT 9?

Enterprise Alert 9 contains exciting new features, all the details are in this section.

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

3.1 Dark mode in Web portal



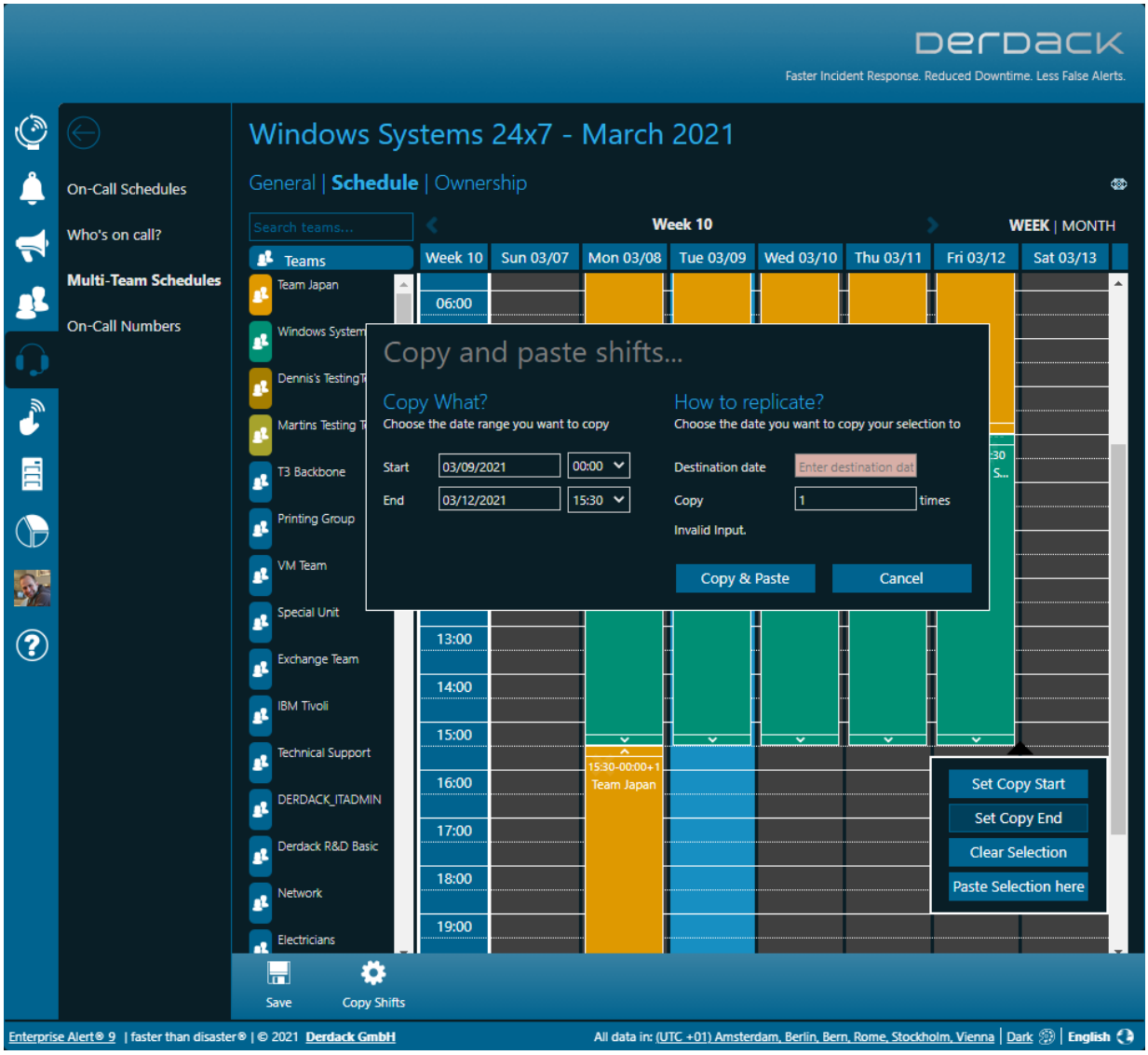
A new dark mode has been added to the Web Portal. This theme can be activated in the footer by each user and is stored user-related in the database. The classic theme of the Web portal can still be used as a classic mode.

In Internet Explorer 11 (no longer recommended) only the classic mode is supported. The default mode for every new Enterprise Alert installation is the dark mode. It is possible to customize the default mode of the Enterprise Alert installation in the configuration file "web.config" (just open the file and search for "ColorThemeDefault"):

```
        <!--
        Default Color Theme: Classic or Dark
        -->
        <add key="ColorThemeDefault" value="Dark"/>
    </appSettings>
```


PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

3.2 Copy & Paste in Multi-Team Schedules



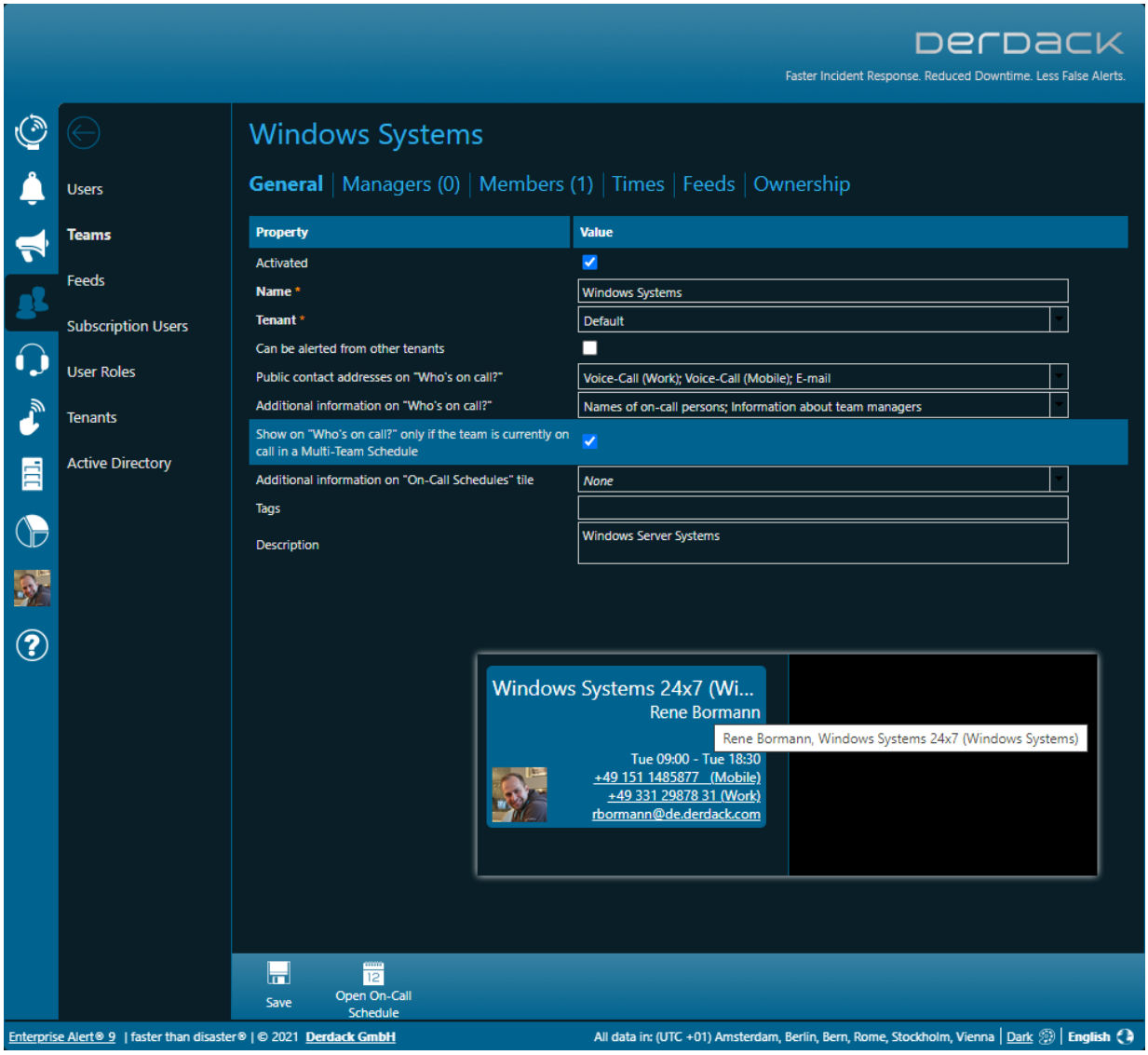
Multi-team schedules are ideal for scheduling teams across time zones. Unlike the on-call calendar of those teams, multi-team schedules did not have a supporting feature to quickly replicate planning into the future (e.g. so-called "auto-rotation").

In EntperiseAlert 9 we have added a copy function to the multi-team schedules. This allows you to transfer the planning into the future with just a few clicks and replicate it as often as you like.

To copy, simply click with the mouse in a calendar cell, define the area to be copied ("Set copy start", "Set copy end") and then select "Copy Shifts" in the action bar. In the following dialog, you can fine-tune the period to be copied and then specify the insertion date and the number of copies (one after the other).

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

3.3 Who's on-call supports Team shifts in Multi-Team Schedules



The on-call overview in Enterprise Alert was previously based exclusively on the on-call times of the respective teams. Teams with or without on-call times were displayed on the overview. In scenarios where several of these teams cover an entire service in turn (so-called "follow-the-sun" scheduling), it was previously difficult to see which of the teams involved was currently actively scheduled via a multi-team schedule.

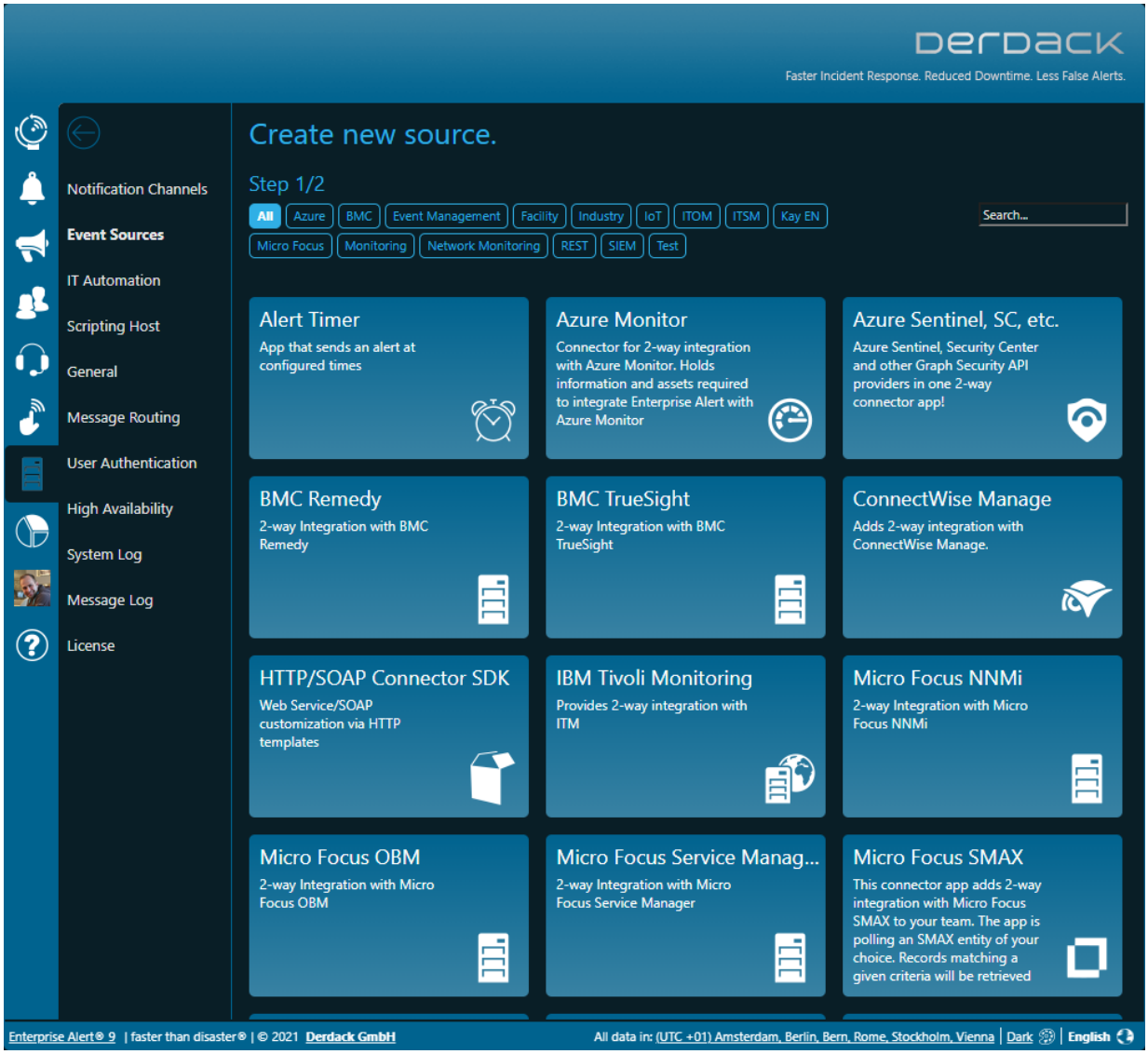
In Enterprise Alert 9, it is now possible to consolidate the display of these teams involved in the service. In this case, only the team that is currently on duty according to the multi-team schedule is displayed on the overview (requires scheduling of the teams involved in the multi-team schedule as well as the planning of the responsibilities of the individual colleagues in the on-call schedule of the individual teams).

In the scenario described above, enable the option "*Show on 'Who's on call?' only if the team is currently on call in a Multi-Team Schedule*" in the details of the teams involved in the service (see screenshot).
All teams with this option enabled will only be displayed on the on-call overview if they have a covered on-call duty and are also currently on shift in a multi-team schedule.
In this scenario, the name of the multi-team schedule should be the name of the service that is provided

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

and that end users or customers can use. In the screenshot above, the name of the multi-team schedule or the service provided is "Windows Systems 24x7".

3.4 New no-code and low-code connectors with new hosting environment ('Node.js')



Enterprise Alert 9 brings support for a new runtime environment, 'Node.js'. With 'Node.js', we have integrated an additional extension platform into the product besides the "Application Programming Toolkit" (with JScript and VB Script). Based on 'Node.js' we are now able to develop connectors and even notification channels in 'Node.js' and extend Enterprise Alert faster than before.

With the release of version 9, the portfolio of available no-code and low-code connectors and notification channels in Enterprise Alert is also extended as follows:

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

3.4.1 Connector (Event Sources)

- Micro Focus Service Management X (SMAX) – IT Service Management
    - No-Code integration
    - 2-way integration via REST
    - Polling of a SMAX entity of your choice
    - Multiple Enterprise Alert 9 instances can access the same SMAX environment at the same time
- ConnectWise Manage – IT Service Management
    - No-Code Integration
    - 2-way integration via REST
    - Polling of Tickets
    - Multiple Enterprise Alert 9 instances can access the same Manage environment at the same time
- Microsoft Azure Monitor - IT Monitoring
    - Low-Code Integration
    - Requires creation of a Registered Application for Enterprise Alert in Azure Active Directory (PowerShell Script is part of the connector)
    - 2-way integration via REST
    - Polling of Alerts from Azure Monitor
- Microsoft Azure Sentinel - Cloud based SIEM
    - Low-Code Integration
    - Requires creation of a Registered Application for Enterprise Alert in Azure Active Diectory (PowerShell Script is part of the connecotr)
    - 2-way integration via REST
    - Polling of Incidents from Azure Sentinel
    - Augmentation of security events with data from the source object from LogAnalytics and GraphAPI
- SIEMENS Siematic S7 Connector – Factory Automation
    - No-Code-Integration
    - Connects to Programmable Logic Controllers (PLCs) with Siemens S7 Ethernet-Protocol (RFC1006 / "ISO over TCP")
    - Polling of configurable address values and triggering of events when address values meet a desired (configurable) criteria
    - Can run on separate machines in appropriate factory networks as a Windows service and communicate with Enterprise Alert via REST API

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

- Telekom Cloud of Things – Factory Automation IoT Platform
    - No-Code-Integration
    - Connects to a Cloud of Things tenant and thus enables alarm triggering via push-button (Telekom IoT service button) in scenarios such as a maintenance call
    - 2-way Integration with Cloud of Things
    - Integration via REST API

3.4.2 Notification Channels

- Threema OnPremise – Enterprise Collaboration
    - No-Code-Integration
    - Sends instant messages to Threema via REST API
    - Users can either be addressed via their e-mail, their UPN or their user ID

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

3.5 Flexible 2-way REST API with easily customizable outbound message formats

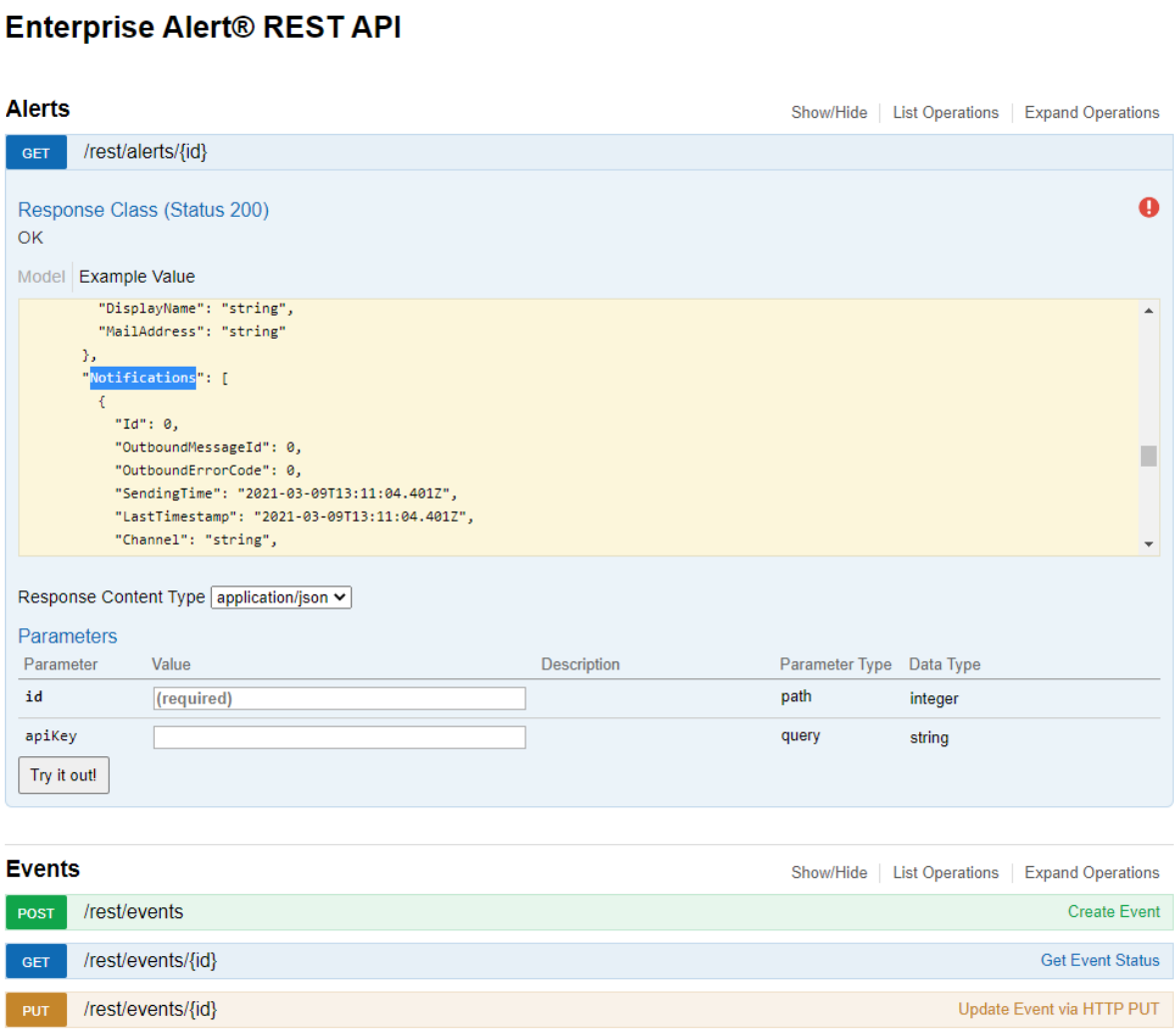
The REST API in Enterprise Alert 9 has now also been extended with a 2-way functionality. This allows to call webhooks or REST endpoints from third party systems on alarm status changes (acknowledge, close). Thus, in Enterprise Alert 9, it becomes child's play to establish a 2-way integration with almost any REST enabled third party system.

The formatting of the outgoing REST call is possible in a specially provided 'Node.js' file with a few script lines of code. This means that Enterprise Alert does not require a mandatory format for the outgoing communication to a third party system but allows for example to send a JSON payload that the respective third party system expects (see the path link to the JavaScript file in the configuration of the respective REST API source).

For use cases where a 2-way integration needs to be implemented via polling from the third-party system towards Enterprise Alert (firewall), we have also extended the REST API itself and added a new alerts

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

controller.
It now makes it possible, based on an alert ID (can be previously determined by the Events Controller using an EventID), to query all details about the alert and the alerting process in Enterprise Alert. This allows the third-party system to track what has happened to an event previously submitted to Enterprise Alert. The JSON object returned on a GET to /alerts/{id} even contains all notifications including the delivery status.



3.6 Improved Security with TLS 1.3 support

All components of Enterprise Alert 9 have been explicitly made compatible with TLS version 1.3 with regarding to any TLS communication. Which TLS version is applied to incoming requests depends largely on the desired version that the client supports. Enterprise Alert itself does not enforce a specific minimum version.

Instead, this must be explicitly implemented in the Windows Server environment, via appropriate group policies. The negotiation of the TLS version to be applied is otherwise based on Microsoft standard implementation in .NET Framework 4.8, against which Enterprise Alert 9 has been compiled.

Please note that at the time of writing (March 2021), Microsoft has not yet released support for TLS 1.3 on Windows Server 2019 for production workloads. Instead, TLS 1.3 availability on Windows Server is currently limited to Server 2019 BUILD 18362 (1903) as Preview. Once Microsoft releases TLS 1.3 support for Windows Server 2019 and newer versions, Enterprise Alert 9 is intended to support TLS 1.3 as well.

3.7 Dependencies & System requirements

With Enterprise Alert 9 there are slight changes in the system requirements, which are summarized below.

3.7.1 Software

- Operating system: Windows Server 2012 R2 - Windows Server 2019
- Database: SQL Server with no significant version restrictions, embedded version in the product setup is a redistributable edition of SQL Server 2019
- Web Browser: Latest versions of Firefox, Chrome, Safari or Microsoft Edge. Microsoft Internet Explorer 11 supported as a long term supported browser on the Windows server to a minimum extent, but not recommended.

3.7.2 Hardware

- Memory requirement for the Enterprise Alert Machine increases to 8GB, additional memory may be required depending on the scenario.

3.8 How to upgrade?

The upgrade procedure itself has not changed and remains a child play. You can upgrade your existing installation in-place. We have tested this with version 2019 and 2017.

Before you take any action, backup the current installation folder on all our EA nodes and also backup the database!

Please also keep in mind to request an updated product license from Derdack sales before you update.

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

4 ABOUT

Derdack designs software for mission-critical alert notifications and anywhere incident response. Derdack's Enterprise Alert® supports IT & business operations of large enterprises and global services organizations in over 50 countries. It provides customers with the ability to reliably distribute critical information to the right people and to respond to critical incidents and emergency situations before they can impact business continuity and customer service levels. Founded in 1999, Derdack has its headquarters in Glen Allen, Virginia, and Potsdam, Germany.

5 FURTHER INFORMATION

Please visit www.derdack.com or:

Corporate Blog:	https://www.derdack.com/news/
Technical Blog:	https://www.derdack.com/category/technical-blog/
Youtube:	http://www.youtube.com/derdack
Facebook:	http://www.facebook.com/derdack
LinkedIn:	http://www.linkedin.com/groups?gid=1701707
Twitter:	http://twitter.com/#!/derdack

6 CONTACT

Please visit www.derdack.com for further information on Enterprise Alert® or contact us:

US:	+1 (202) 4700885
UK:	+44 (20) 88167095
Germany/Intl.:	+49 (331) 29878-20 (German, English, Spanish), Fax: +49 (331) 29878-22
Email:	info@derdack.com

6.1 Mailing Address

Derdack Corp.
4470 Cox Road, Suite 250
Glen Allen, VA 23060
USA

Derdack GmbH
Friedrich-Ebert-Straße 8
14467 Potsdam
Germany

7 DISCLAIMER

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585