

derdack

EnterpriseAlert® 9 Getting Started



1	INTRODUCTION.....	6
1.1	How does it work.....	6
1.2	What is new in version 2019?	9
1.2.1	Updated UI design	17
1.2.2	Multi-tenancy	17
1.2.3	Support for ADFS authentication in the web portal	18
1.2.4	Turn receiving of alerts on or off in the mobile app	19
1.2.5	Android app enhancements	20
1.2.6	Scripting Host script synchronization in HA deployments	21
1.2.7	Support for Windows Server 2019 and SQL Server 2017	21
2	DEPLOYMENT AND ACTIVATION	22
2.1	Upgrading previous versions	22
2.2	Deployment Scenarios	22
2.2.1	Standard (Single Server).....	22
2.2.2	High Availability (Multi-Instance)	23
2.3	System Requirements	25
2.4	Backend Server Setup	25
2.4.1	Plug-and-Play Mode	25
2.4.2	Advanced Mode.....	27
2.5	Product Activation.....	31
2.6	Mobile App Setup	35
2.6.1	Supported Platforms	35
2.6.2	Backend Connectivity (Inbound Traffic)	36
2.6.3	Push Notifications (Outbound Traffic).....	36
2.6.4	App Deployment Options	37
3	QUICK START SCENARIO	38
3.1	Step 1 - Create a User Account.....	38
3.2	Step 2 - Set up a Notification Channel	39
3.3	Step 3 - Set up an Event Source	42
3.4	Step 4 - Create an Alert Policy	43
3.5	Step 5 - Set up integration with IT automation systems.....	46

3.6	Step 6 - Create a Remote Action Policy	47
3.7	Step 7 - Simulate a Problem to trigger an Alert.....	49
3.8	Step 8 - Acknowledge the Alert.....	49
3.9	Step 9 - Execute the Remote Action to troubleshoot the Problem	50
4	REFERENCE GUIDE	52
4.1	Terminology	52
4.1.1	What is a Notification Channel?	52
4.1.2	What is a Connection?	52
4.1.3	What is Message Routing?.....	52
4.1.4	What is an Alert Policy?	52
4.1.5	What is a Remote Action?	53
4.1.6	What is a Notification Profile?	53
4.1.7	What is a User Profile?	53
4.1.8	What is a Team?	53
4.1.9	What is an On-Call Schedule?	53
4.1.10	What is a Multi-Team Schedule?	54
4.1.11	What is a Notification Feed?	54
4.1.12	What is a Subscription User Profile?	54
4.1.13	What is a Callout?.....	55
4.1.14	What is a Maintenance Window?.....	55
4.1.15	What is an escalation, what is a tier escalation?	55
4.1.16	What is a Tenant?	55
4.2	User Roles	56
4.2.1	Understanding All- and Tenant Scopes	56
4.2.2	Setting role permissions and role members	57
4.3	Active Directory Integration	59
4.4	Setting up Notification Channels	64
4.4.1	Setting up Emails.....	64
4.4.2	Setting up Voice Calls.....	69
4.4.3	Setting up Push Notifications	74
4.4.4	Setting up Microsoft Skype for Business IM and Voice-Calls	76
4.4.5	Setting up SMS text messaging	80

- 4.5 Integration in 3rd party Systems83
 - 4.5.1 Integration in System Center Operations Manager (SCOM).....83
 - 4.5.2 Integration in System Center Service Manager (SCSM).....90
 - 4.5.3 Integration in System Center Orchestrator (SCO).....93
 - 4.5.4 Integration IBM Tivoli Monitoring (ITM)97
 - 4.5.5 Integration in HP Operations Manager99
 - 4.5.6 Integration in HP Network Node Manager (HP NNM)101
 - 4.5.7 Integration in HP Service Manager (HPSM).....105
 - 4.5.8 Integration in Windows Task Scheduler110
 - 4.5.9 Standard Interfaces.....113
 - 4.5.10 Integration in other ITSM Products121
- 4.6 Advanced Notifications.....122
 - 4.6.1 Duplicate Event Suppression.....122
 - 4.6.2 Multiple Event Occurrences.....122
 - 4.6.3 Team Broadcast Alerts122
 - 4.6.4 Team Escalation Alerts123
 - 4.6.5 Acknowledgement and Closure Workflows123
 - 4.6.6 Acknowledgement Time Limit.....123
 - 4.6.7 Tier Escalation124
 - 4.6.8 Alert Severity.....124
 - 4.6.9 Find me, follow me Notifications125
 - 4.6.10 First Channel Notifications126
 - 4.6.11 Channel Broadcast Notifications126
 - 4.6.12 On-Call Notifications126
 - 4.6.13 Notifications to Teams on duty (e.g. "Follow the Sun" notifications).....130
 - 4.6.14 One-way Outbound Notifications131
 - 4.6.15 Time based Notification Channels134
 - 4.6.16 Anti Flood Protection.....136
 - 4.6.17 Maintenance Windows137
- 4.7 On-Call Scheduling141
 - 4.7.1 On-Call Times141
 - 4.7.2 On-Call Scheduling144

4.7.3 Auto Rotation	148
4.7.4 Public Holidays	150
4.7.5 PDF-Export.....	151
4.7.6 Gap-Reminders	152
4.7.7 Publishing Contact Address Information	153
4.8 On-Call Management	153
4.8.1 My On-Call Calendar	154
4.8.2 ics-Export to Outlook and others	155
4.8.3 Who is on call?	157
4.9 Remote IT Management	157
4.9.1 Remote Action Policies	157
4.9.2 Security and Rights Management.....	158
4.9.3 Remote Action Parameter Values.....	159
4.10 Multi-tenancy	160
4.10.1 Managing tenants	160
4.10.2 Entity/tenant relationships	161
4.10.3 Integrity Checker.....	164
5 SUPPORT	166
5.1 Important Links.....	166
6 ABOUT.....	167
7 FURTHER INFORMATION	167
8 CONTACT	167
8.1 Mailing Address	167
8.2 Hours of Operation	168
9 DISCLAIMER.....	168

1 INTRODUCTION

1.1 How does it work

Enterprise Alert® automates alerting processes and enables a fast, reliable and effective response to incidents threatening the continuity of services and operations. This is in particular importance for 24/7 operated mission-critical systems and IT. The enterprise notification software combines three pillars to effectively respond to incidents – automated alert notifications, ad-hoc collaboration and anywhere incident remediation.



Never miss a critical Alert

Enterprise Alert provides automated, and persistent alert notifications by voice, text, push, email and IM. It tracks the delivery of notifications, acknowledgements and replies and reacts automatically on non-delivery or non-reply by utilizing escalation chains, on-call schedules and presence information.

Enterprise Alert provides automated, persistent alert notifications going far beyond the common 1- or 2-way alert notifications offered by other systems. It tracks the delivery of notifications, acknowledgements and replies and reacts automatically on non-delivery or non-reply by utilizing escalation chains, on-call schedules and presence information.

- Parallel, multi-target, multi-channel alert notifications
- Persistent, closed-loop notifications
- Accurate notifications to single users and teams (broadcast & escalations)
- Automated, real-time tracking of notification delivery
- Automated processing of responses (alert acknowledgements)
- Fully automated escalation chains
- Automated 'hopping' of communication channels, i.e. Find-Me/Follow-Me
- Visually appealing schedules and duty rosters
- "Alert Policies" for convenient management of alert workflows
- "On-the-fly" compilation of alert notification messages

- Easy holiday and absence management
- Context- and incident-related alert notifications workflows
- Destination-related message composing
- Alert storm/flood prevention
- Powerful suppression of duplicate events
- Real-time reporting
- Full audit trailing of notification and alarm processes

Always know who's on call

Enterprise Alert enables convenient scheduling of on-call duties by drag & drop in any browser. Based on scheduling information it can then alert the right engineers at the right time. Backup engineers and stand-ins are also available.

The on-call scheduling 'engine' provides

- Easy scheduling of duties via drag & drop in your browser
- Primary, Backup, Stand-ins or full-team rotations
- 24/7, custom times and custom duty lengths (e.g. 1 week, 1 day)
- Auto-rotation (one-up)
- Support for holidays, half days, special days
- Follow-the-sun schedules (multi-team duty schedules)
- Planning gap alerts
- Calendar integration & sync, e.g. for Outlook or iPhone
- On-call scheduling PDF Export
- 3rd Integration, e.g. export to SAP HR possible
- "Who is on call?" page with future lookup
- Sharepoint integration of "who is on call"
- Mobile app with instant "who is on call" access incl 1-touch contact
- And much more

Anywhere ChatOps, Incident Sharing and Conferencing.

IT service staff or engineers who are alerted often need to communicate with managers, on-call staff of other teams or subject-matter experts. Derdack's Enterprise Notification Software provides perfect toolset for a real-time, anywhere collaboration experience.

Leave your Notebook at Home

Handling critical incidents shouldn't stop with acknowledging an alert. With our mobile app you can comfortably manage alerts, troubleshoot problems and even resolve them by triggering parameter-based IT automation tasks.

Remote Execution of IT Automation Tasks

Handling critical incidents shouldn't stop when acknowledging an alert. That is why we have created "remote actions" that enable you to trigger IT automation tasks directly from your smartphone. You build your incident remediation actions with Windows PowerShell or Orchestration tools and Enterprise Alert puts them on your smartphone's screen. Now, you truly hold your IT and other systems in the palm of your hand!

Seamless Integrations

Enterprise Alert has a unique way of integrating itself with 3rd party IT and enterprise systems. It provides plug & play, 2-way smart connectors for major IT management systems like Microsoft System Center, as well as numerous open and customizable APIs like SOAP, HTTP, SMTP, XML, ASCII, CLI, OPC, RS232, SNMP and many others. If you find one system that Enterprise Alert cannot link to – do let us know.

Unrivalled Usability, Live Insights and Audit Trailing

When it comes to usability, Enterprise Alert is second to none. Though enterprise-class alerting, alarm management and incident response is a sophisticated topic, we have made things really easy. Even setting up complex alerting scenarios only takes minutes, which reduces your maintenance effort enormously. With Enterprise Alert, you get convenient, instant and real-time insights into what is going on, who is alerted, who has responded and who has taken ownership. You will also be able to see if problems have been resolved or not.

Designed for Large and Global Enterprises

Enterprise Alert has been specifically designed for enterprises and organizations with the highest demands in reliability, productivity, integrations and security. That is why our product is one of the very few, if not the only one, that fully addresses the needs that come with running business-critical operations such as enterprise IT, manufacturing lines, energy & utility creation and distribution.

2 CHANGELOG

2.1 What's new in EnterpriseAlert 9 (Released March 2021)?

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

2.1.1 Dark mode in Web portal

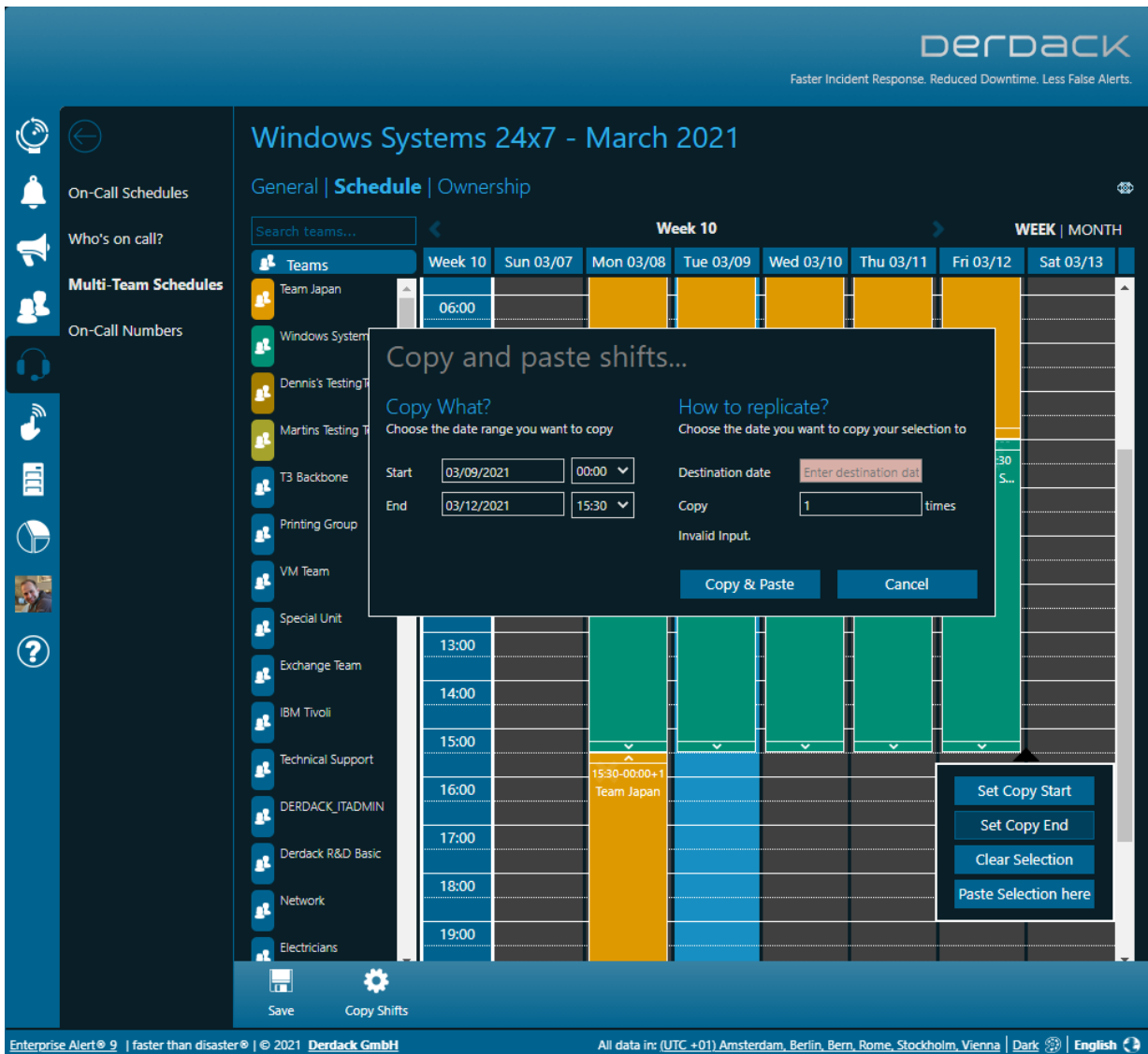
A new dark mode has been added to the Web Portal. This theme can be activated in the footer by each user and is stored user-related in the database. The classic theme of the Web portal can still be used as a classic mode.

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>
```

2.1.2 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 EnterpriseAlert 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).

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

The screenshot displays the 'Windows Systems' configuration page in the Enterprise Alert interface. The page is divided into a left sidebar and a main content area. The sidebar contains navigation icons for Users, Teams, Feeds, Subscription Users, User Roles, Tenants, and Active Directory. The main content area features a 'Windows Systems' header with tabs for General, Managers (0), Members (1), Times, Feeds, and Ownership. Below this is a 'Property Value' table with the following data:

Property	Value
Activated	<input checked="" type="checkbox"/>
Name *	Windows Systems
Tenant *	Default
Can be alerted from other tenants	<input type="checkbox"/>
Public contact addresses on "Who's on call?"	Voice-Call (Work); Voice-Call (Mobile); E-mail
Additional information on "Who's on call?"	Names of on-call persons; Information about team managers
Show on "Who's on call?" only if the team is currently on call in a Multi-Team Schedule	<input checked="" type="checkbox"/>
Additional information on "On-Call Schedules" tile	None
Tags	
Description	Windows Server Systems

Below the table, there is a pop-up card for 'Windows Systems 24x7 (Wi...)' featuring a profile picture of Rene Bormann and the following contact information:

- Name: Rene Bormann
- Time: Tue 09:00 - Tue 18:30
- Mobile: +49 151 1485877
- Work: +49 331 29878 31
- Email: rbormann@de.derdack.com

At the bottom of the main content area, there are buttons for 'Save' and 'Open On-Call Schedule'. The footer of the interface includes the text 'Enterprise Alert® 9 | faster than disaster® | © 2021 Derdack GmbH' and 'All data in: (UTC +01) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna | Dark | English'.

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 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".

2.1.4 New no-code and low-code connectors with new hosting environment (nodejs)



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:

Connectors (Event Source)

- Micro Focus Service Management X (SMAX) – IT Service Management
 - o No-Code integration
 - o 2-way integration via REST
 - o Polling of a SMAX entity of your choice
 - o Multiple Enterprise Alert 9 instances can access the same SMAX environment at the same time
- ConnectWise Manage – IT Service Management
 - o No-Code Integration
 - o 2-way integration via REST
 - o Polling of Tickets
 - o Multiple Enterprise Alert 9 instances can access the same Manage environment at the same time
- Microsoft Azure Monitor - IT Monitoring
 - o Low-Code Integration
 - o Requires creation of a Registered Application for Enterprise Alert in Azure Active Directory (PowerShell Script is part of the connector)
 - o 2-way integration via REST
 - o Polling of Alerts from Azure Monitor
- Microsoft Azure Sentinel - Cloud based SIEM
 - o Low-Code Integration
 - o Requires creation of a Registered Application for Enterprise Alert in Azure Active Directory (PowerShell Script is part of the connector)
 - o 2-way integration via REST
 - o Polling of Incidents from Azure Sentinel
 - o Augmentation of security events with data from the source object from LogAnalytics and GraphAPI
- SIEMENS Siematic S7 Connector – Factory Automation
 - o No-Code-Integration
 - o 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
- 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

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

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

The screenshot displays the configuration page for a '2way-REST' notification channel in Enterprise Alert 9. The interface is dark-themed with a blue sidebar on the left containing navigation icons and labels. The main content area is titled '2way-REST' and features a toggle switch set to 'Activated'. Below this, there are input fields for 'Name' (2way-REST), 'Tenants' (All Tenants (Public)), and 'API Key' (jqk1s8bf6d8z2j23itp8ab81l60tdq). There are 'Generate New' and 'Copy' buttons next to the API key field. A checkbox labeled 'Enable outbound REST (2-way)' is checked. The 'Target Url' field contains 'https://requestbin.enterprisealert.com/inza1ain' and has a tooltip that reads 'Enable outbound webhook for sending REST calls on alert status updates to external system.' To the right, there is a box with links for 'REST API Documentation', 'Outbound Webhook Status' (OK), and a 'Customizable Node.js source file' path: 'C:\Program Files (x86)\EnterpriseAlert\ConnectorHost\OutboundWebhooks\2way-REST\Main.js'. Below the configuration fields is a table of 'Event Parameters' with columns for Name, Path, Value of Last Event, and External ID. The table lists parameters such as Title, Description, Severity, Gateway, Impact, NodeID, Id, Type, Source, Message, and State. The 'Id' parameter has a value of '637317974967361756' and its 'External ID' checkbox is checked. At the bottom of the configuration area are 'Save', 'Delete', and 'Add Parameters from Last Event' buttons. The footer of the interface includes 'Enterprise Alert® 9 | faster than disaster® | © 2021 Deraldack GmbH' and 'All data in: (UTC +01) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna | Dark | English'.

Name	Path	Value of Last Event	External ID
Title	\$.Title		<input type="checkbox"/>
Description	\$.Description		<input type="checkbox"/>
Severity	\$.Severity		<input type="checkbox"/>
Gateway	\$.Gateway		<input type="checkbox"/>
Impact	\$.Impact		<input type="checkbox"/>
NodeID	\$.NodeID		<input type="checkbox"/>
Id	\$.Id	637317974967361756	<input checked="" type="checkbox"/>
Type	\$.Type	Security alert	<input type="checkbox"/>
Source	\$.Source	Gate agent	<input type="checkbox"/>
Message	\$.Message	Agressive passenger	<input type="checkbox"/>
State	\$.State	ACTIVE	<input type="checkbox"/>

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

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.

Enterprise Alert® REST API

Alerts Show/Hide | List Operations | Expand Operations

GET /rest/alerts/{id}

Response Class (Status 200)
OK

Model Example Value

```

{
  "DisplayName": "string",
  "MailAddress": "string"
},
"Notifications": [
  {
    "Id": 0,
    "OutboundMessageId": 0,
    "OutboundErrorCode": 0,
    "SendingTime": "2021-03-09T13:11:04.401Z",
    "LastTimestamp": "2021-03-09T13:11:04.401Z",
    "Channel": "string",
  }
]

```

Response Content Type

Parameters

Parameter	Value	Description	Parameter Type	Data Type
id	<input type="text" value="(required)"/>		path	integer
apiKey	<input type="text"/>		query	string

Events Show/Hide | List Operations | Expand Operations

POST /rest/events Create Event

GET /rest/events/{id} Get Event Status

PUT /rest/events/{id} Update Event via HTTP PUT

2.1.6 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.

2.2 What is new in version 2019 (Released March 2019)?

All new enhancements and features in Derdack's brand new Enterprise Alert® 2019 release are introduced and discussed in this document. You will learn about new capabilities, possible scenarios and resulting benefits for your enterprise.

2.2.1 Updated UI design

We have done a very moderate update to the UI design for the web portal and our mobile app. The key change are rounded corners for most tile and button elements.

2.2.2 Multi-tenancy

Enterprise Alert® 2019 does now support multi-tenancy, i.e. data from different departments or branches can be separated much better. This enables you to ensure that each department or branch or each of your "customers" can only see the data that affects them in system.

However, multi-tenancy was designed for enterprise use, i.e. public hosting scenarios are not officially supported. The data segmentation does not take place on the database level, but rather on the application level. All data is still stored in the same database.

The handling of multi-tenancy in the product is essentially based on a new entity, the so-called "tenant". Global administrators can create and manage these tenants. The rest of the principle is quite simple and is essentially based on assigning almost* all other entities in Enterprise Alert® 2019 to one or more** tenants.

The role model has been extended so that you can now create tenant-administrators. Members of this role cannot configure the system configuration (for example, the database connection), but can access all entities (for example, alarms) that belong to their tenant. The assignment of the entities in Enterprise Alert® 2019 (for example, an event source) to a tenant is done by the global system administrator in the Web Portal.

When the product is updated to the new version 2019, your existing data is migrated and assigned to a default tenant. You can then create new tenants and start assigning corresponding entities from the default tenant to the new tenants. It is recommended that you use the "Integrity Checker", a mechanism that shows you inconsistencies in your tenant assignments. An example of an inconsistency is the assignment of a user from a team to a tenant "A", while the team itself was assigned to a tenant "B".

Multi-tenancy requires the "User Role Add-On" to be part of your Enterprise Alert® license. Please contact Derdack sales if you are unsure whether this component is part of your license.

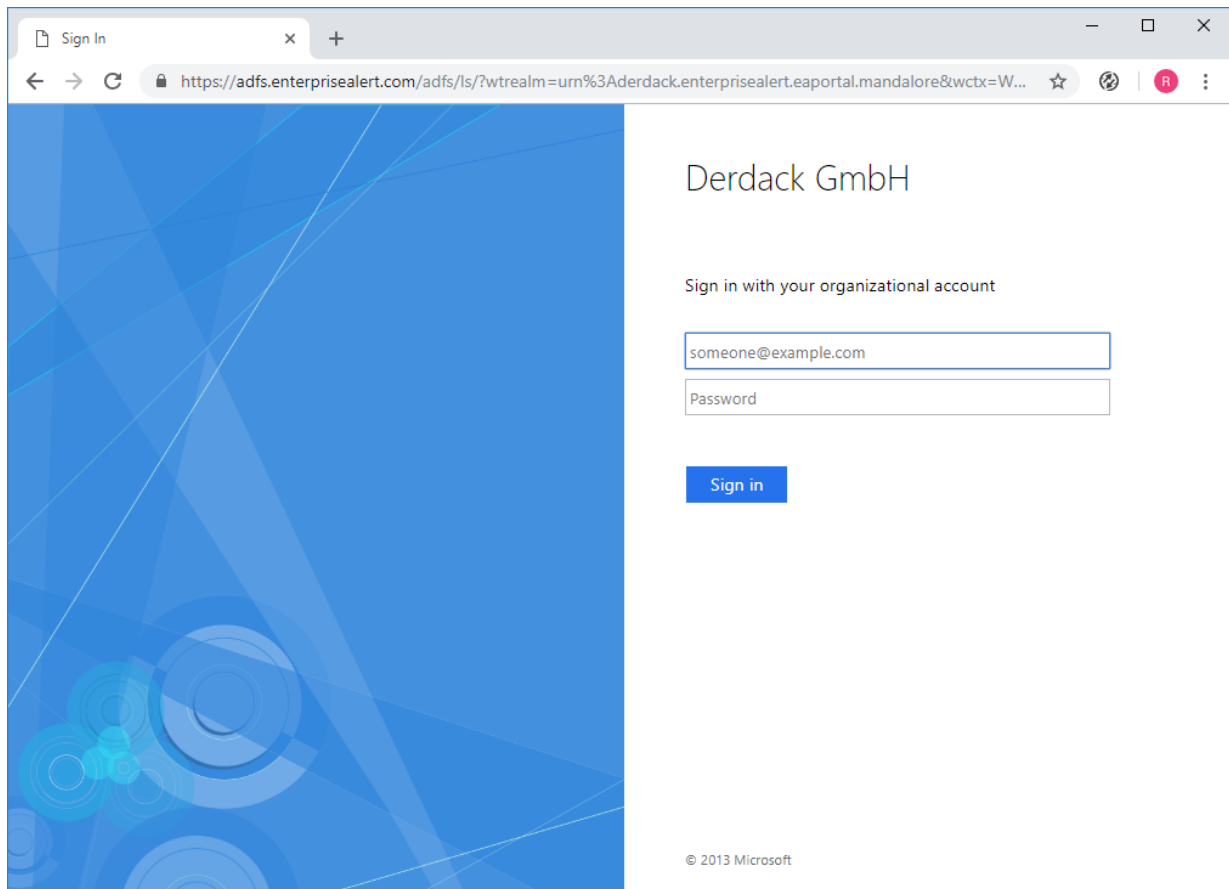
* Notification channels are still global and are used to send or receive messages from all mandates

** There are entities that can belong to multiple tenants, an example of this is a user profile

The screenshot displays the Derdack Enterprise Alert web portal interface. The top right corner features the Derdack logo and the tagline "Faster Incident Response. Reduced Downtime. Less False Alerts." The left sidebar contains a navigation menu with icons and labels for: Users, Teams, Feeds, Subscription Users, User Roles, Tenants (highlighted), and Active Directory. The main content area is titled "Tenants" and includes a search bar labeled "Search tenants...". Below the title, there is a sub-section "Tenant Management | Integrity Checker" and four blue tiles representing different tenant categories: IT, Facility, Manufacturing, and Default. Each tile contains a white icon of a server rack. At the bottom of the main content area, there is a "Create New" button with a plus sign icon. The footer of the page contains copyright information: "Enterprise Alert® 2019 | faster than disaster® | © 2019 Derdack GmbH" and "All data in: (UTC +01) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna | English" with a globe icon.

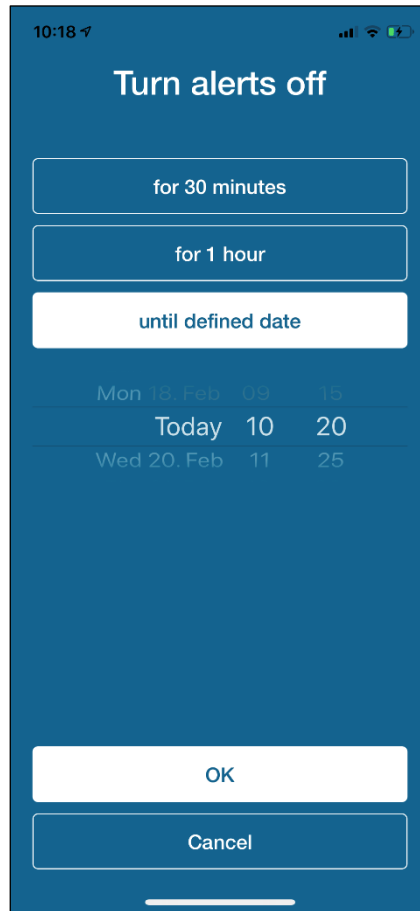
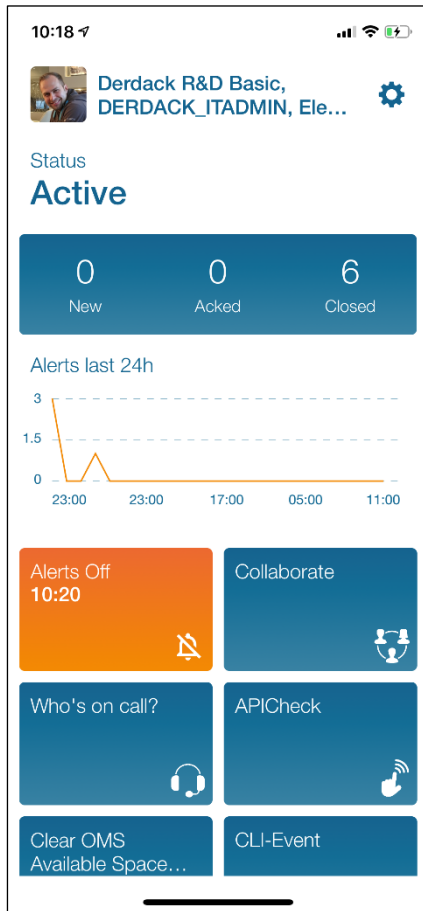
2.2.3 Support for ADFS authentication in the web portal

Das EnterpriseAlert Web Portal unterstützt nun neben AD- auch die SSO-Authentifizierung mittels ADFS. Sollten sie Multi-Faktor Authentifizierung mit ADFS verwenden, so kann diese nun auch bei EnterpriseAlert Nutzern eingesetzt werden. Die Aktivierung der ADFS-Authentifizierung erfolgt über die web.config Datei des Web Portals, in dem hier die entsprechend auskommentierten Konfigurationsblöcke einfach einkommentiert werden.



2.2.4 Turn receiving of alerts on or off in the mobile app

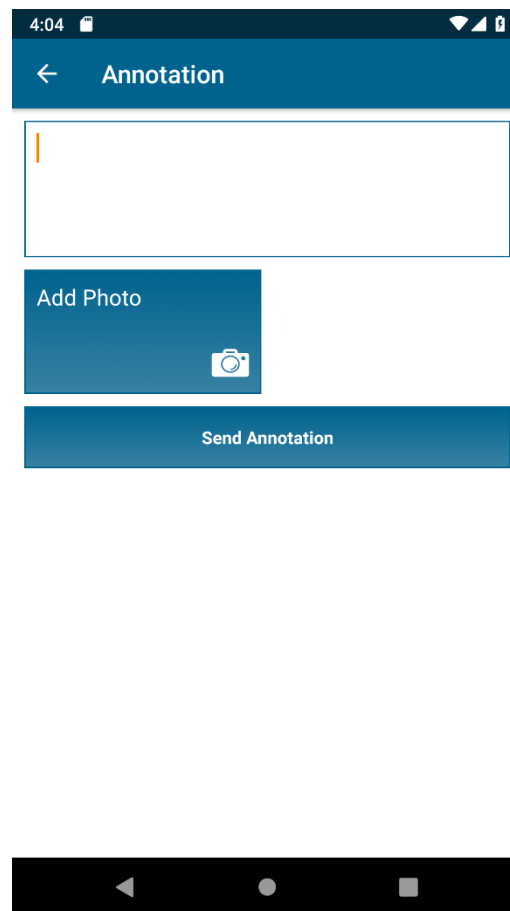
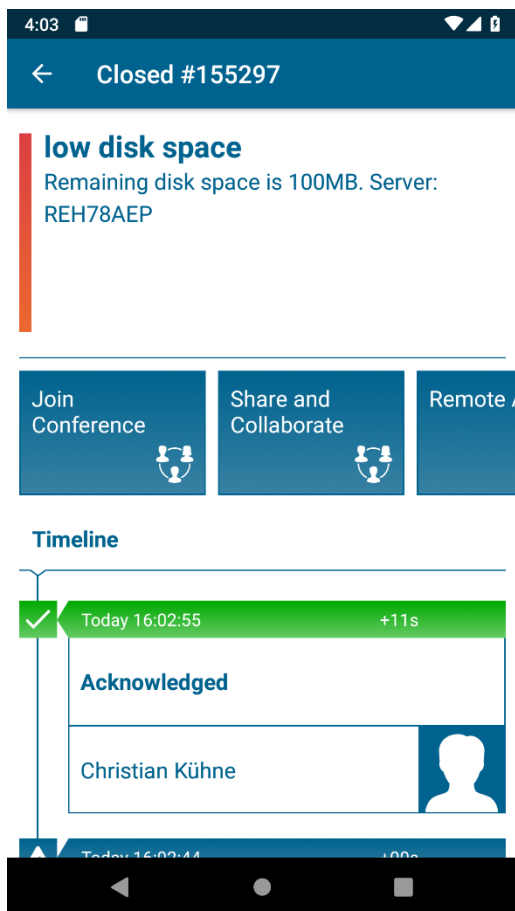
In the mobile app, there is now a tile on the dashboard that can be used to turn receiving of alerts on or off. Users can deactivate alarm receiving for a selectable period of time, e.g. for holidays or other absences. After the set time has elapsed, the user is automatically reactivated for receiving alerts from Enterprise Aler®.



2.2.5 Android app enhancements

The Enterprise Alert® mobile app for Android now also provides support for commenting on alerts (annotations) and joining or initiating ad-hoc telephone conferences related to incidents.

In addition, the Enterprise Alert® Android app now also supports "Android for Work", i.e. you can configure the server URL in your MDM software, so that it does not have to be entered by your end-users themselves.



2.2.6 Scripting Host script synchronization in HA deployments

Scripting Host script applications are now synchronized between Enterprise Alert® instances in a multi-server deployment. In previous versions, scripts needed to be manually replicated to all other Enterprise Alert® machines. This process is now automated which means, that you can now assume that your newly created script applications are available all all Enterprise Alert® nodes or that deleted scripts are removed from all nodes the same way.

2.2.7 Support for Windows Server 2019 and SQL Server 2017

Enterprise Alert® 2019 now officially supports Windows Server 2019 and is built on the latest .NET Framework 4.7.2.

The installation routine for new installations now ships with SQL Server 2017.

The SystemCenter connectors in Enterprise Alert® 2019 were compiled for the latest SystemCenter product releases (release 1801).

3 DEPLOYMENT AND ACTIVATION

This chapter contains important information related to the deployment of Enterprise Alert®. Please read carefully before executing the setup on your preferred machine.

3.1 Upgrading previous versions

The setup wizard of Enterprise Alert® 2019 supports the in-place upgrade of the following previous product versions:

- Enterprise Alert 2017

Before you start the upgrade process, we recommend that you back up your whole system or at least perform a database backup. Backing up the whole Windows server e.g. via a snapshot is however recommended.

Please be aware that the upgrade process *will* change the run-as account of all Enterprise Alert® Windows services to LOCAL_SYSTEM. You will therefore have to change the accounts back to their previous values if needed.

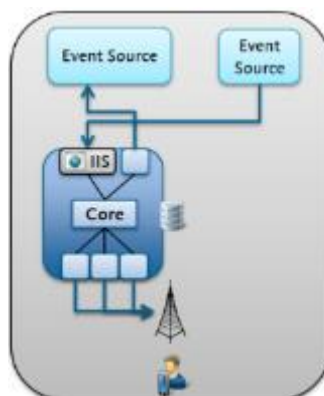
Alternatively, you can set the connection credentials for most configurations in the Enterprise Alert® Web portal itself, which will then be used instead of the run-as account.

3.2 Deployment Scenarios

Enterprise Alert® is shipped with two standard deployment scenarios which are introduced in this section more in detail.

3.2.1 Standard (Single Server)

The standard deployment scenario involves only one instance of the server system. This deployment will therefore not be highly available, but can be deployed in a shorter amount of time. The high-level architecture of the standard scenario is displayed below:



3.2.2 High Availability (Multi-Instance)

The second deployment scenario is a high availability scenario and involves two instances of the server system on two separate machines.

Furthermore, the HA scenario involves one shared database which must also be highly available itself, e.g. SQL Server Availability Groups. The deployment of the high available database is not the subject of this document; rather it is considered as a prerequisite for this scenario.

Enterprise Alert® supports essentially three HA operations modes which are introduced in the following section:

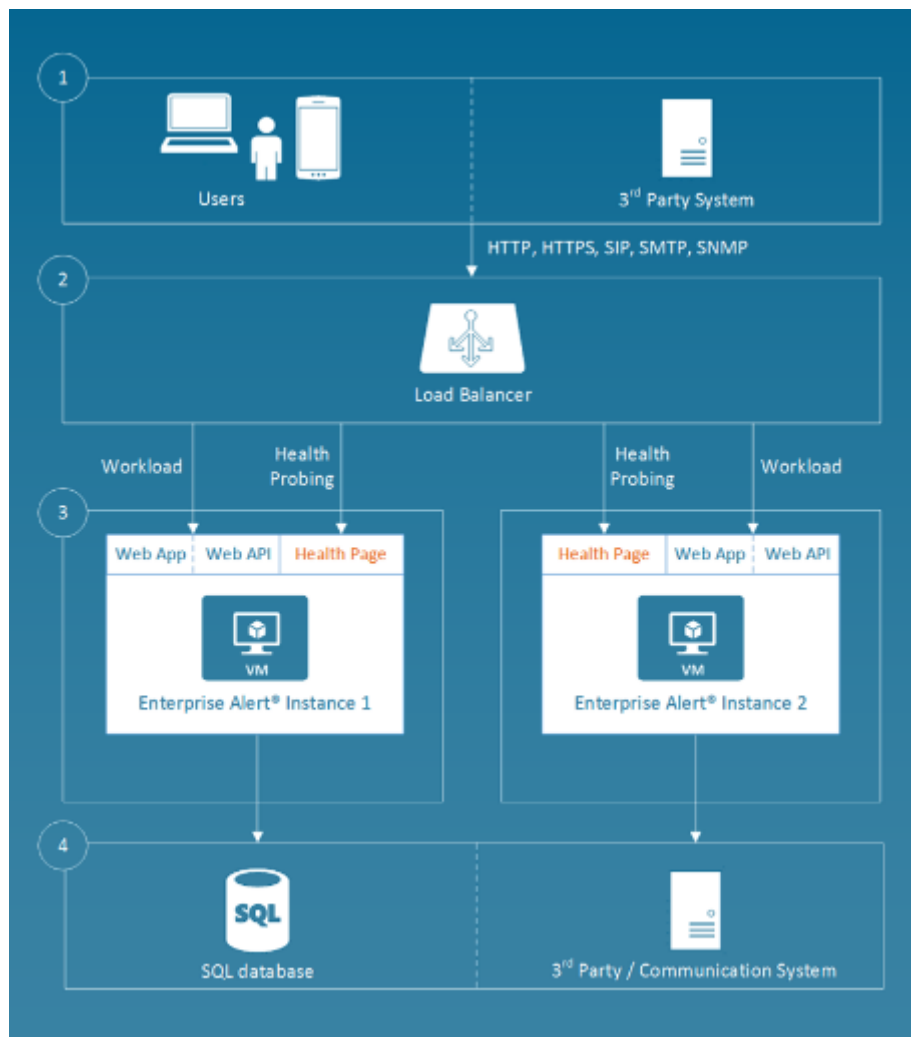
HA operations mode	Description
Node Cluster (Active/Active)	<p>In this scenario both instances of Enterprise Alert® are active at the same time and process alerts simultaneously. As both instances are run using this mode, they may consume more infrastructure resources. Both nodes share the same configuration and are accessed via a Load Balancer (not part of Enterprise Alert®). The load balancer can make use of a Web-based probe handler which either returns a 5xx response if the node becomes unhealthy or a 2xx response if the node is still healthy. The probe handler is accessible under the following URI per default: http://localhost/eaportal/pages/HealthMonitor.ashx</p>
Failover System (Active/Passive)	<p>In this mode, only one node is active at a given point in time for processing alerts and notifications. The other node is passive and is only involved in the heartbeat mechanism. The heartbeat mechanism operates via the high available database itself. If the active node no longer reports a heartbeat, it is regarded as being down and the passive node becomes active and takes over.</p>
Failover System with Source and Channel Clustering	<p>In this mode, only one node is active at a given point in time for processing alerts and notifications. However, in this scenario it is possible to activate some workloads on the passive node as well. Here, sources and channels can be active on passive nodes as well and can be used e.g. for querying 3rd party systems or sending notification messages.</p> <p>In this mode, the Enterprise Alert® core process runs in active/passive mode and monitors fellow core processes using a heartbeat mechanism via the shared database. In contrast to the active/passive mode of the core process, connectors typically run in active/active mode.</p> <p>The core process of Enterprise Alert® contains a duplicate recognition engine that will process only one event in the event that both</p>

	connectors retrieve the same event from a 3 rd party source at the same time. Otherwise, if only a single connector receives an event, it will forward the event to the <u>active</u> Enterprise Alert® core process. This behavior depends on the implementation of the 3 rd party system.
--	---

The installation instructions provided in the next section must be performed on each machine if you would like to deploy Enterprise Alert® as being highly available with multiple nodes. The workflow for deploying an HA system is the following:

- Deploy a high available SQL database server if not already available
- Install Enterprise Alert® on the first node
 - The HA SQL server on which the database should be deployed can be specified in the advanced mode product setup
- Install Enterprise Alert® on the second node
 - The HA SQL server on which the database should be deployed can be specified in the advanced mode product setup

The high-level architecture of the high availability deployment scenario is displayed below:



3.3 System Requirements

The hardware and software requirements of Enterprise Alert® can be found in the document “Hardware and Software Requirements” and relate to required computer hardware as well as operating system requirements.

3.4 Backend Server Setup

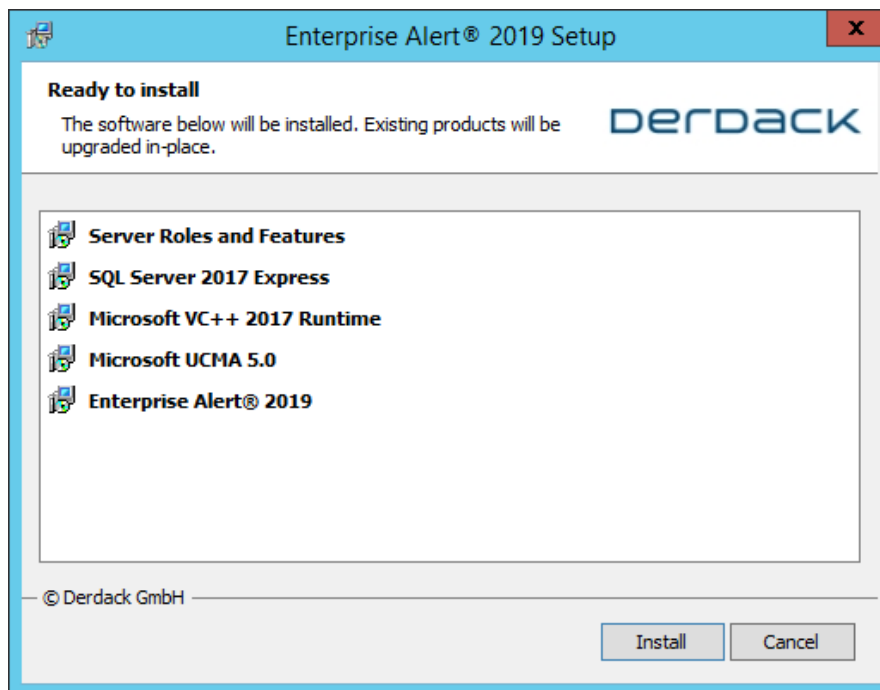
3.4.1 Plug-and-Play Mode

In order to start the setup wizard double click the file “EA2019.exe”. Afterwards, select your preferred language and click **OK** to load the welcome page.

On the welcome page click **Next** to proceed.

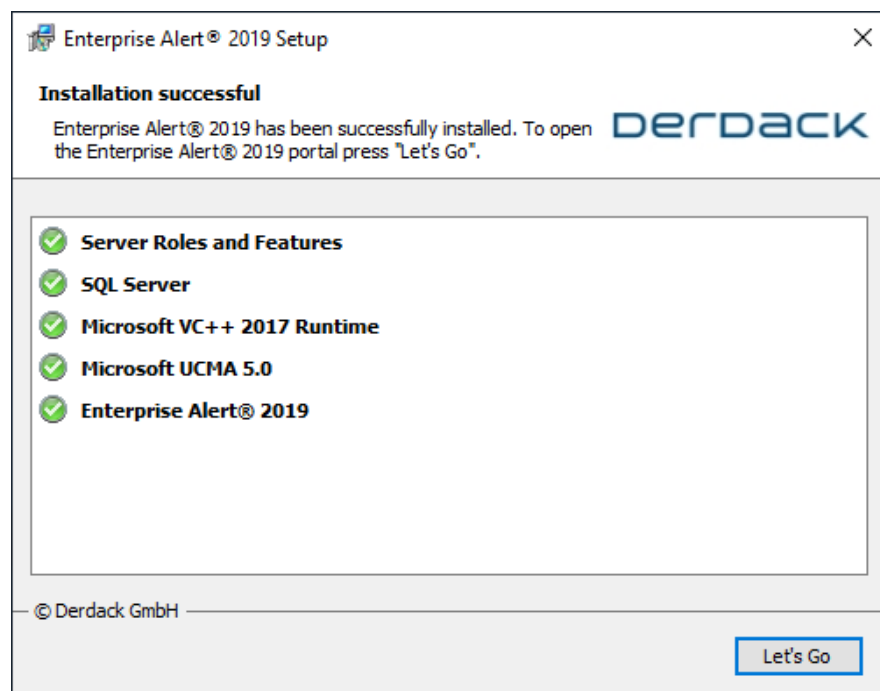
Please accept the license agreement and click **Next** to load the main setup page.

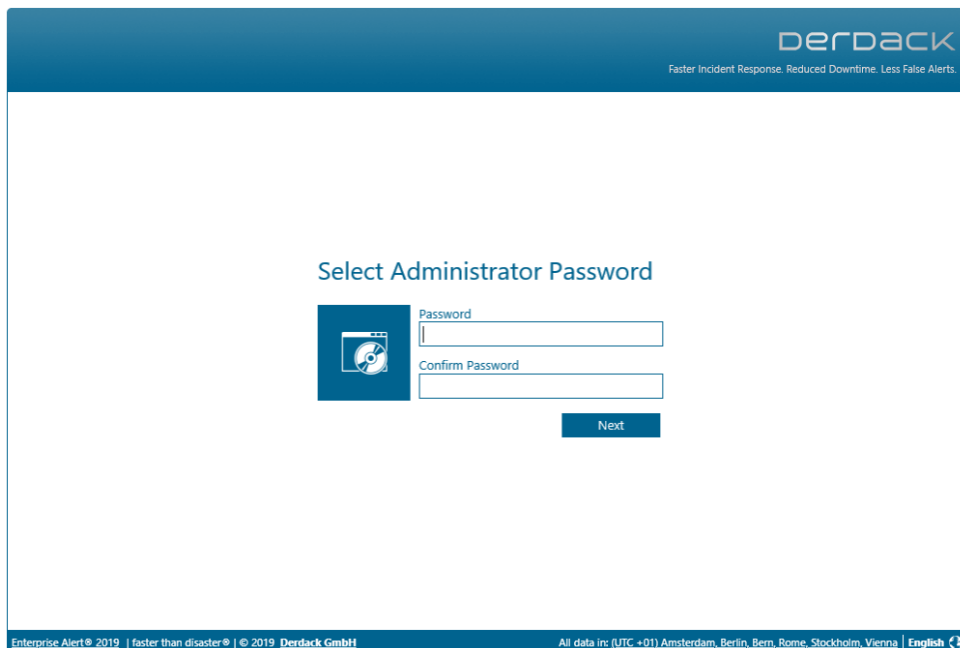
The main page will first analyze your system environment in order to identify the components required for installation. Once the list of required installation components is displayed, click [Install](#) to start the installation process.



Restarts of Windows may be required during the installation of the listed prerequisites. In this case, the setup will continue automatically after the reboot and after the Administrator has logged on to the system.

After the installation has finished, please click [Let's Go](#) to launch the Web portal of Enterprise Alert®. Afterwards proceed with the product activation in section 2.5.





3.4.2 Advanced Mode

Enterprise Alert® can also be installed in advanced mode. This is especially useful if you do not want to deploy the Enterprise Alert® database on a local SQL Server Express edition, but would rather deploy the database on a remote database server. Another advanced mode setup scenario is the addition of a further Enterprise Alert® instance linked to an existing database for the purpose of an HA system deployment.

The installation procedure is as follows:

- Download the setup executable from Derdack and launch it
- The Bootstrapper will be loaded and can be used to automatically install missing prerequisites
- Next, the setup wizard collects various information e.g. the database server instance and copies the bits to the machine
- After the installation has finished and once you have registered your license file, you will be able to log in to the Web portal

The following section provides detailed information for all these installation steps.

Step 1 – Bootstrapper and Prerequisites

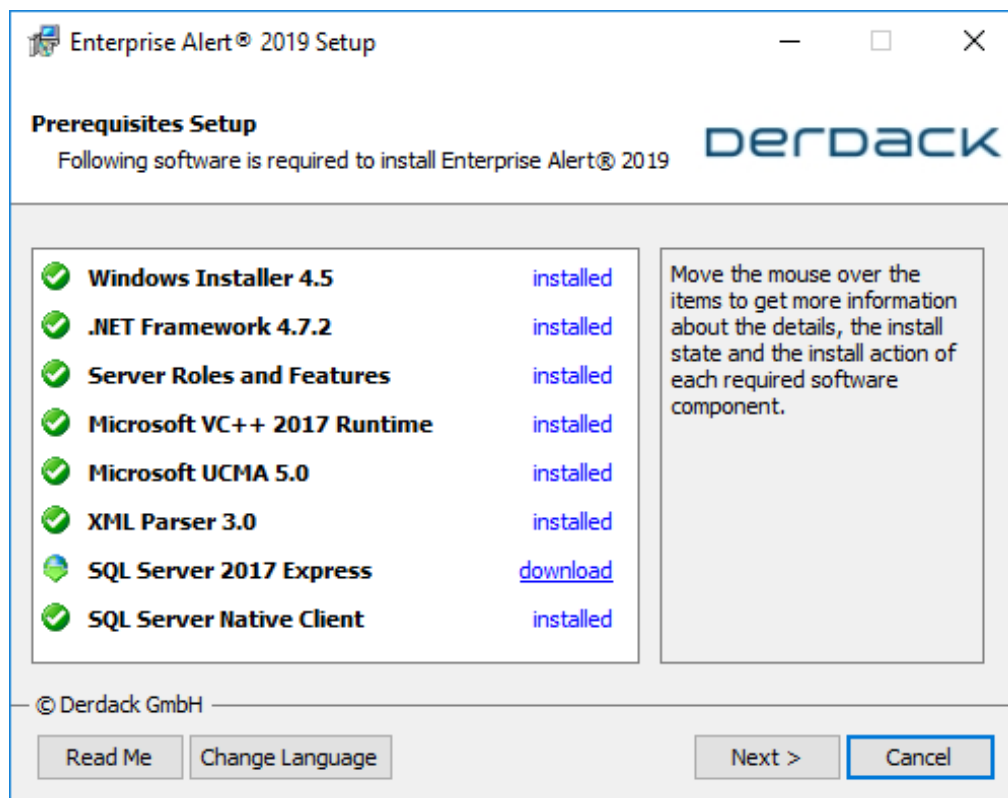
After you have downloaded the setup file from Derdack (EA2019.exe), open the command prompt with administrative permissions on the target machine and specify the advanced attribute `-a` when launching the setup:

```
EA2019.exe -a
```

The Bootstrapper application will then be loaded and verifies that all prerequisites have been installed or are available. If not, each prerequisite that is not available can be installed directly from the bootstrapper application by clicking on the associated [Install](#) link.

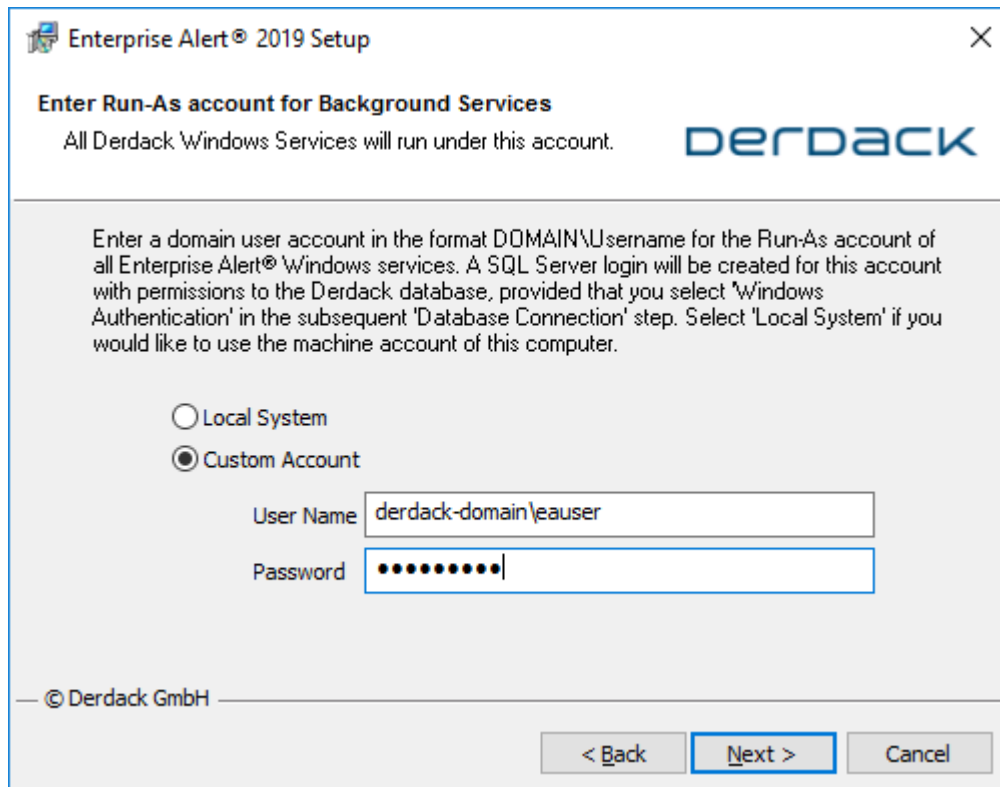
The Bootstrapper application also scans your network for available instances of Microsoft SQL Server. Even if there are instances available, you can always install a local express edition by clicking on the corresponding [Install](#) link.

Once all prerequisites are available, the Next button will be enabled and can be clicked in order to launch the Setup Wizard.



Step 2 – Run-As Accounts

Click [Next](#) to proceed. Enter the Run-As accounts for the background services in the application layer and for the web portal / APIs of Enterprise Alert®. A custom domain account can be granted with access permission to the Enterprise Alert® database by the Setup application. If you select local system/network service, the machine account of the windows system must be granted access to the Enterprise Alert® database which can be difficult to accomplish by company security policy.



Step 3 - Database Connection, Deployment and Logins

In this dialog, you specify if the Enterprise Alert® database should be created as part of the installation. If you want the database to be created you must specify the SQL Server instance on which it should be created. In this case you can also enter a desired name for the Enterprise Alert® database.

Check the box "Don't create the database during install" if the database should not be created as part of the installation (e.g. when installing an additional instance to an existing HA cluster).

Otherwise, if you specify a SQL Server instance, access credentials and a database name the tool will automatically compile the resulting connection string used by Enterprise Alert® when accessing the database.

The following table lists standard instance strings that you might use when specifying your instance:

String	Description
(local)	Local default instance of SQL Server (MSSQLSERVER)
HOSTNAME\MSSQLSERVER	Default instance of SQL Server (MSSQLSERVER) on the host 'hostname'
HOSTNAME\INSTANCENAME	Instance with the name 'instancename' on the host 'hostname'

Select the preferred database authentication mechanism to use with Enterprise Alert®. For security reasons, we recommend you select [Windows Authentication](#).

Database Connection

SQL Server Connection
Specify an SQL Server Instance to be used by Derdack. Please also enter a database name and choose log on credentials.

Server Name: Refresh

Database Name:

Log on to the server

Use Windows Authentication
 Use SQL Authentication

User name:
Password:

Resulting Odbc Connection String for Windows Services, Web Portal and Web APIs

```
Driver=SQL Server Native Client
11.0;Server=eawin2019\ENTERPRISEALERT;Trusted_Connection=Yes;Database=EnterpriseAlert
```

Don't create database during install. Only configure product by connection string above.

© Derdack GmbH

< Back Install Cancel

Step 4 – Setup Wizard and Installation

By clicking on the Install button in the Bootstrap application, the Setup Wizard will be started. Accept the license agreement and click [Next](#). This will display the language selection.

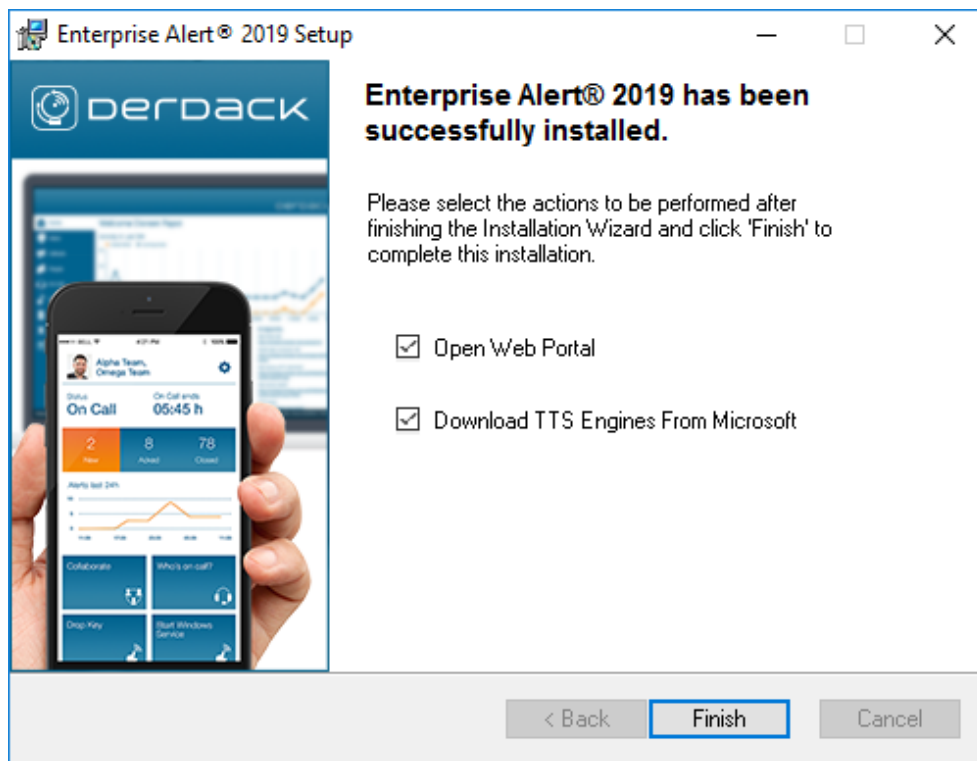
Step 5 - Installation Language

On this wizard step you select the language of the documents to be installed as well as the language of the Windows start menu entries for Enterprise Alert®. The language you select here will also be set as the initial language of the Enterprise Alert® Web portal. However, the Web portal language can be switched later to German or English regardless of what you select here. Click [Next](#) to display the installation type.

Step 5 - Installation Type

Select [Complete](#) as installation type and click [Next](#) to start the installation process.

A final setup page will be displayed after Enterprise Alert® has been installed on the target system. It allows you to select what should be done next. Check "Open Web Portal" to open a browser and to load Enterprise Alert®.



You will now need to select the administrator password and enter some contact address information. After the first login you need to deploy a valid license file. These steps are the same as described in section 2.4.2

3.5 Product Activation

When the Web portal of Enterprise Alert® is opened for the very first time it starts in activation mode in which you can select an administrator password and deploy a license.

Follow the instructions provided in this section in order to initialize Enterprise Alert® and to deploy a license file.


Step 1 – Administrator Account Setup

Enterprise Alert® is installed with a default administrator user account. The user name is "Administrator". Before you can start using Enterprise Alert® with this user account, you must select a password.

Select a password, confirm it and click [Next](#) to proceed.

DERDACK
Faster Incident Response. Reduced Downtime. Less False Alerts.

Select Administrator Password



Password
.....

Confirm Password
.....

Next

Enterprise Alert® 2019 | faster than disaster® | © 2019 Deraldack GmbH | All data in: (UTC +01) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna | English ↻

Now enter the e-mail address and optionally the phone number that Enterprise Alert® should use when notifying the Administrator user. Afterwards click [Proceed to Login](#).

Type in the password that you have selected previously and click [Login](#)

Step 2 – License Deployment

In the next step the system will verify the product license. In most cases you will be requested to deploy a new license as there is normally no license available after a fresh installation:

License Required
Please deploy a license.

Deploy
Deploy your license.

Purchase
Contact Derdack sales to purchase a full license.

Generate Hardware ID
If required generate a hardware id file.

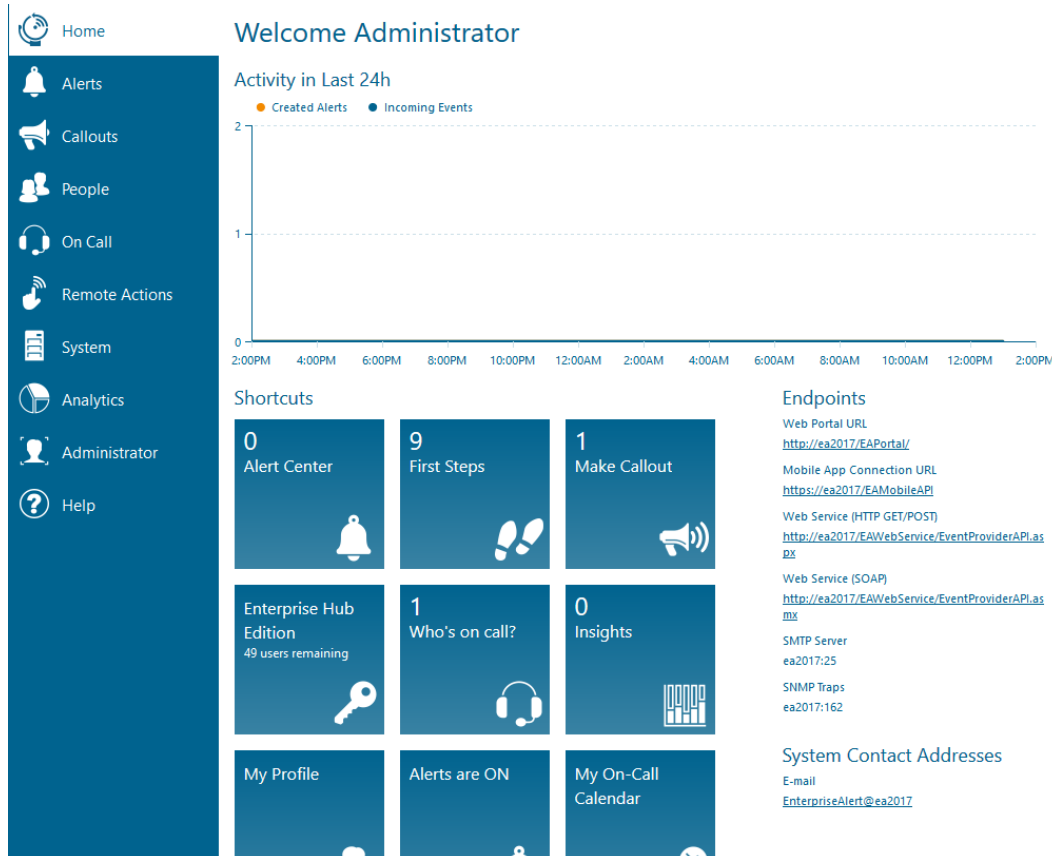
Either paste the license file URL in the Textbox below or save it manually on your hard disk and click 'Browse my computer...' to upload it:

License File URL:
Paste URL here... [Browse my computer...](#)

At this point, you would normally have already been in contact with a Derdack representative, who would have already sent you a license. Should this not be the case, you can click on [Purchase](#) to re-request a trial license from Derdack via e-mail.

As soon as you have received your license from Derdack, please open the Web portal by double clicking on the Enterprise Alert® icon on your desktop, log in and click on [Deploy](#).

After you have uploaded the license, a start page dashboard will appear and the system is ready for use:



3.6 Mobile App Setup

This section contains prerequisites and deployment options for the Enterprise Alert® Mobile App.

3.6.1 Supported Platforms

The following table lists all supported platforms of the Enterprise Alert® Mobile App:

Platform	Constraints
Apple iOS	Supported iOS version is 9 or higher.
Android	Supported versions of Android are 4.1 (API16) or higher.

3.6.2 Backend Connectivity (Inbound Traffic)

The following table displays the required Enterprise Alert® mobile APIs categorized by app or platform. The mobile app implementations for the various platforms are heterogeneous and partly access different backend APIs to work with system data.

As part of the app deployment the API URL must be accessible from the smartphone. This can be done with different techniques such as VPN or Web access through the DMZ with proxies or load balancers.

Derdack recommends usage of Microsoft technologies such as Active Directory Federation Services (ADFS) and Web Application Proxy (WAP) to make the below listed APIs publicly available for the Enterprise Alert® Mobile App. More details can be found online in Derdack video channels on e.g. vimeo or YouTube.

Platform	Used API	API URL ("EAFQDN" to be replaced by the EA host name)	TCP Port	TLS Encryption
iOS, Android	EAMobileAPI	https://EAFQDN/eamobileapi/	443	Mandatory Self-signed certificates are supported but not recommended. On iOS custom CA trust must be enabled under Settings-> General -> About -> Certificate Trust Settings Self signed certificates must be signed by your CA.

3.6.3 Push Notifications (Outbound Traffic)

Push notifications are sent via cloud infrastructure of each smart device platform vendor. The target server URL, port and protocol is different for each vendor. The following table lists outbound connections established by the backend server in order to send push notifications to the Enterprise Alert® Mobile App. The table is structured with focus on information you need when configuring firewalls, etc.

Platform	Server URL	Port	Protocol

Apple iOS	gateway.push.apple.com ("Apple Push Notification Server URL")	2196, 5223, 2195, 2196, 443 ("Apple Push Notification Server Port")	TCP
Android	https://android.googleapis.com/gcm/send ("Android Push Notification Server URL")	5228-5230, 443	HTTPS

3.6.4 App Deployment Options

The Enterprise Alert® mobile app can be deployed via the public (app) stores of the corresponding platform vendors. Additionally there are enterprise or manual deployment options which are explained below.

Platform	Store Item Name	Enterprise or manual deployment option
iOS	Derdack	The iOS app can be downloaded from Derdack in ipa format. In the Enterprise Alert® Web app open the page "Get the mobile App" from the dashboard. On this page there is an action item "Download Mobile Apps". Once you have downloaded and extracted the zip file you can find the complete iOS app content in the iOS subfolder. You may now use the ipa file to deploy the app to your mobile device using various desktop applications, an email attachment or using appropriate MDM software.
Android	Enterprise Alert®	The Android app can be downloaded from Derdack in apk format. In the Enterprise Alert® Web app open the page "Get the mobile App" from the dashboard. On this page there is an action item "Download Mobile Apps". Once you have downloaded and extracted the zip file you can find the complete Android app content in the Android subfolder. You may now use the apk file to deploy the app to your mobile device using various desktop applications, as an email attachment or by using appropriate MDM software. Please note that if you intend to install the app manually, you will first need to activate the option "allow the installation of apps from unknown sources" on your smartphone. This option can be found on most Android phones under Settings > Applications > Unknown sources .

4 QUICK START SCENARIO

This chapter contains a quick start scenario that helps to bring Enterprise Alert® into operation after the product has been installed on the target machine. Before reading this chapter, we recommend you first familiarize yourself with the terminology of Enterprise Alert® by reading through section 5.1 *Terminology* first.

4.1 Step 1 - Create a User Account

After the installation of Enterprise Alert®, the first step is to log in to the Web portal and create a new user account to which to send your first notification.

On the Enterprise Alert® machine, double click on the Enterprise Alert® icon on the desktop or open a browser and type in the following URL to load the portal:

<http://localhost/EAPortal/>

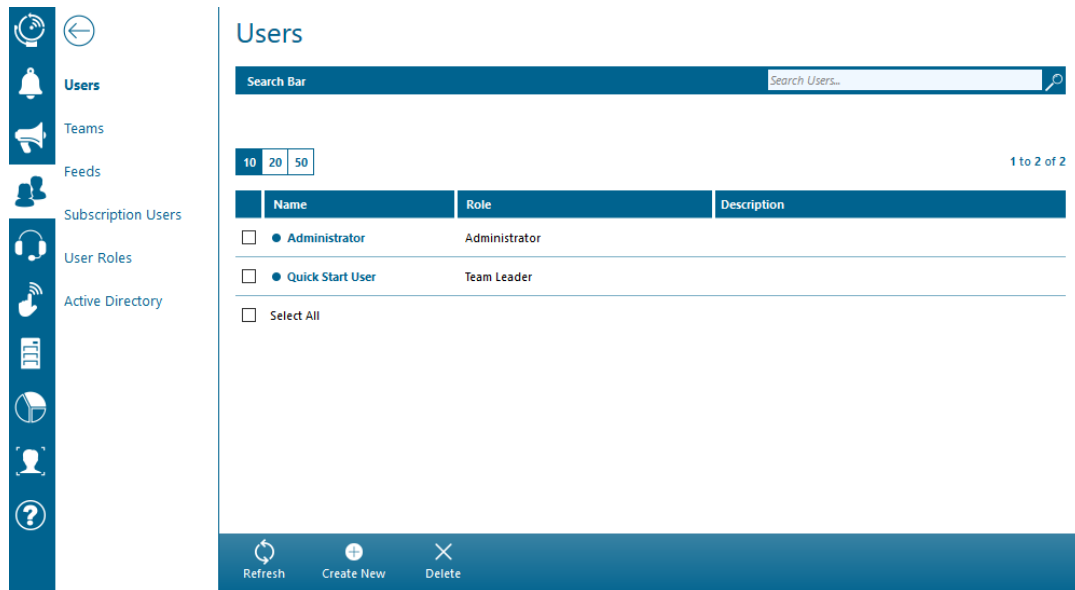
Log in by using the following credentials:

- User name: Administrator
- Password: <the password you have entered during the setup process>

After you have logged in, open the user profiles management section under [People > Users](#). On the action bar at the bottom of the page, click on [Create New](#) to create a new User Profile. Fill in the following information on the general tab and once finished, click [Next](#):

- Activated: Yes
- User Name: quickstartuser
- Profile Password: Derdack13#
- Confirm Profile Password: Derdack13#
- Role: Team Leader
- Full Name: Quick Start User

Click [Next](#) on the action bar to continue to the "Contact Addresses" tab. Fill in your email address and click [Save](#). To proceed to the notification profiles of the new user account click on the "Notification Profiles" tab at the top of the screen. The default notification profile will always be active, unless you create a profile that applies for a specific time period during the day. The default notification profile automatically contains the email notification channel that you entered. To navigate back to the user profiles overview, click on the "Users" tab on the side-bar, the overview now appears as below:



4.2 Step 2 - Set up a Notification Channel

Now that you have created the user account that will be notified, you will now configure the notification channel through which a notification will be sent to the user. In the previous section, you entered your email address as being the only contact address available for the user. You will therefore create an email notification channel in this section.

In Enterprise Alert®, each notification channel that you plan to send notifications through must be configured with at least one corresponding connection. For example, entering a mobile number for SMS messaging as contact address without having set up at least one connection through which SMS's can be transmitted is invalid and will result in failed notification messages.

In order to set up a new email connection, first open the configuration of the email notification channel under [System > Notification Channels > E-Mail – DirectSend on the side panel](#).

The following page will be displayed:

E-Mail - DirectSend

Activated

Name *
Corporate email server

Account Type *
1 - Internet Mail

Push Notification Public Callback URL

Mailbox E-mail Address *
enterprisealert@de.derdack.com

Username

Password

Receiving Protocol *
0 - Off

Sending Protocol *
2 - Direct SMTP Delivery

Standard Domain of the E-mail Recipient
de.derdack.com

Send High Priority E-mails *

Pending messages in queue
0

Status
OK

Save Delete

The connection in this scenario is used to send emails directly to the according SMTP server in each target email domain (and not through a relay server).

Fill in the following configuration details and click on ["Save"](#):

- Name: "Corporate email server"
- Account Type: "1 – Internet Mail"
- Mailbox E-mail Address: Enter an email address that should be used as originator address, e.g. "enterprisealert@derdack.com"
- Username/Password: Leave these fields blank as no authentication is required.
- Receiving Protocol: 0 – Off
- Sending Protocol: 2 – Direct SMTP Delivery
 - Note: Direct delivery will extract the domain portion from any recipient email address and will attempt to query for an MX record in that domain. The record MX server will afterwards be used to submit the email in the destination domain.
- Send High Priority E-mails: 2 – Only for alerts with critical severity

Leave the remaining properties with their default values and click on ["Save"](#).

A new route in the message routing section of Enterprise Alert® will automatically be created for the activated email connection. Message routing is a built-in mechanism that controls through which connection for a particular notification channel a message is sent through. Message routing can be accessed via [System > Message Routing](#).

Each message route can use prefixes, postfixes or wildcards to match the destination address of messages that should be routed through the connection configured for the route. A new route will only be created automatically for the first connection of a notification channel i.e. routes for any further connections will have to be created manually.

After the creation of your email connection, message routing will appear as follows:

The screenshot shows the 'Message Routing' configuration page. On the left is a sidebar with navigation icons and labels: Notification Channels, Event Sources, IT Automation, Scripting Host, General, Message Routing (highlighted), User Authentication, High Availability, System Log, and License. The main panel is titled 'Message Routing' and contains a table with the following data:

<input type="checkbox"/>	Notification Channel	Matching Destinations	Primary Connection	Fallover Connections	
<input type="checkbox"/>	E-mail	*;	Corporate email server	-	
<input type="checkbox"/>	MMS	*@*;	Corporate email server	-	
<input type="checkbox"/>	Push Notification	Android	Push - Android	-	
<input type="checkbox"/>	Push Notification	Blackberry	Push - BlackBerry	-	
<input type="checkbox"/>	Push Notification	iPhone	Push - iPhone	-	
<input type="checkbox"/>	Push Notification	Windows Phone	Push - Windows Phone	-	
<input type="checkbox"/>	SMS	*@*;	Corporate email server	-	
<input type="checkbox"/>	Select All				

At the bottom of the main panel, there are three action buttons: Delete (with an 'X' icon), Create New (with a '+' icon), and Refresh (with a circular arrow icon).

In order to test the email connection you've set up, you can send a notification message manually. Manual notifications can be sent via the Messenger, which you can access under your personal menu e.g. [Alerts > Send Message](#) on the side-panel, as in the screenshot below:

Enter a subject and message text and click on [Submit and Track](#) to take you to the message journal, where you can track the message.

If the email fails, please check the connection settings and ensure that valid credentials have been entered (if applicable). Also check that the email server will accept emails from the Enterprise Alert® machine. For troubleshooting purposes, you can enable file logging on the details page of the email connection. Log files can be found in the subfolder “Logs” of the Enterprise Alert® root installation folder under program files.

The 1-way email connection is recommended in test scenarios only. For productive scenarios we recommend to either configure a dedicated Microsoft Exchange connection or 2-way Internet email connection. Details can be found in section 4.3.1.

4.3 Step 3 - Set up an Event Source

So far you have created a new user profile and configured a new notification channel. In the next section, you will set up a new event source.

Similar to notification channels, event sources contain one or more connections to remote systems. The difference is that these connections are not used for sending notification messages, but rather for integrating 3rd party event source systems.

Examples of such event source systems are IT monitoring systems like System Center Operations Manager or ITSM systems like HP Service Manager. Integration into these systems is used for implementing automated notifications in Enterprise Alert® for events forwarded from the data center / event source system to Enterprise Alert®.

Integration into event source systems can be implemented either by means of built-in smart connectors or by using the standard APIs and interfaces of Enterprise Alert®. The difference between the built-in smart connectors and the standard APIs and interfaces is that the smart connectors have been developed by Derdack with the use of SDKs and frameworks provided for the 3rd party systems, while the standard interfaces and APIs utilize generic protocols and standards, in which case interoperability between both products must be configured manually.

For the purpose of this quick start scenario, you will make use of a standard interface, namely the file interface of Enterprise Alert®. To configure this interface, open its configuration under [System > Event Sources > File Interface](#). By default, Enterprise Alert® reads files from the "FileInterface" folder in the root installation folder of Enterprise Alert®. The standard reading interval is 10 seconds. We recommend you leave the configuration as is and proceed directly to the next step.

4.4 Step 4 - Create an Alert Policy

In this section, you will create a new alert policy to automate an email notification based on the content of the file you write to the file interface of Enterprise Alert®. In general, alert policies are rules used for automating notification workflows. They are created for specific event sources and are applicable to incoming events matching given criteria, triggering new notification workflows for a given destination.

To start with, open the alert policy management section under [Home > Alert Policies](#). You will see a list of default policies shipped with Enterprise Alert® that are based on smart connector event sources.

On the bottom of the page, click on [Create New](#) and then enter in the following values on the following screen and click [Next](#):

- Activated: Yes
- Name: FileInterface to Email policy
- Event Source: Event Sources -> File Interface (Events from File Interface)
- Tags: Quick Start

On the next tab, you can add conditions that the incoming events must adhere to, before they can trigger the policy. Click on [Add Condition](#) to add a new condition with the following characteristics:

- Event parameter to evaluate: Event Text
- Type of condition: starts with
- Value to match: "Quick Start:"

Click [Next](#).

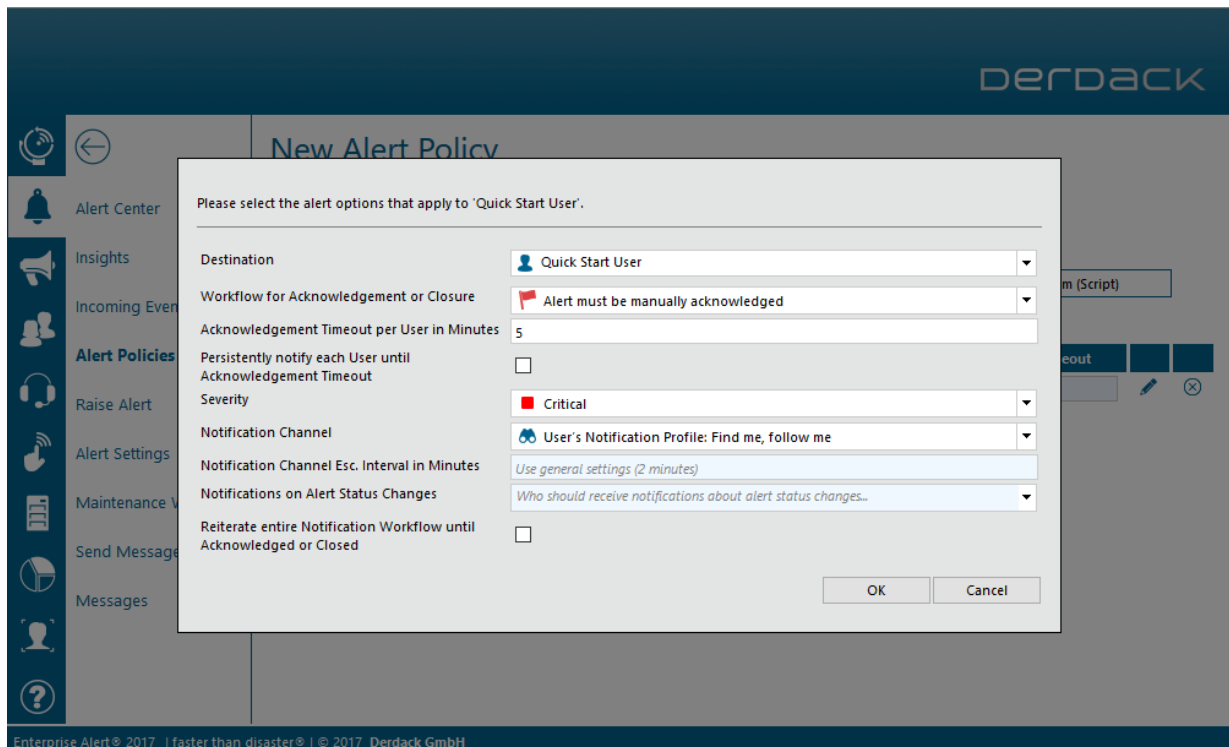
On the next tab, you can select the alert destination by clicking on "Tier Escalation". Afterwards add the following user from the Dropdown in the Destination Column.

- Destination: Quick Start User.

Once you have selected a destination, click the [Edit](#) button in the newly added destination tier to proceed.

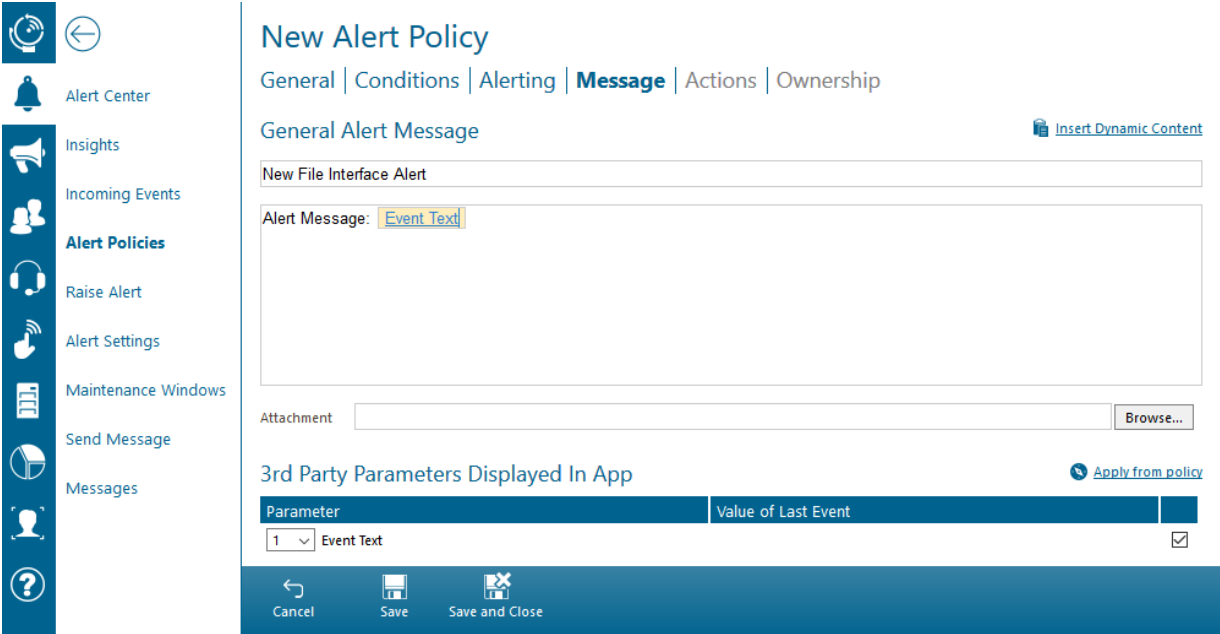
Here you can configure which alert notification workflow must be triggered for the incoming event (in this example files that start with "Getting Started"). Configure the following properties and click [OK](#):

- Workflow for Acknowledgement or Closure: Alert must be manually acknowledged
- Severity: Critical
- Acknowledgement Timeout per User in Minutes: 5, or use general settings
- Notification Channel: User's Notification Profile: Find me, follow me



Click [Next](#) to compose the layout and content of your notification message. The editor enables you to mix the parameter values from the triggering event with static text fragments. Format the message fields as displayed below and click [Next](#). Event parameter values can be inserted by clicking on "Insert Dynamic Content".

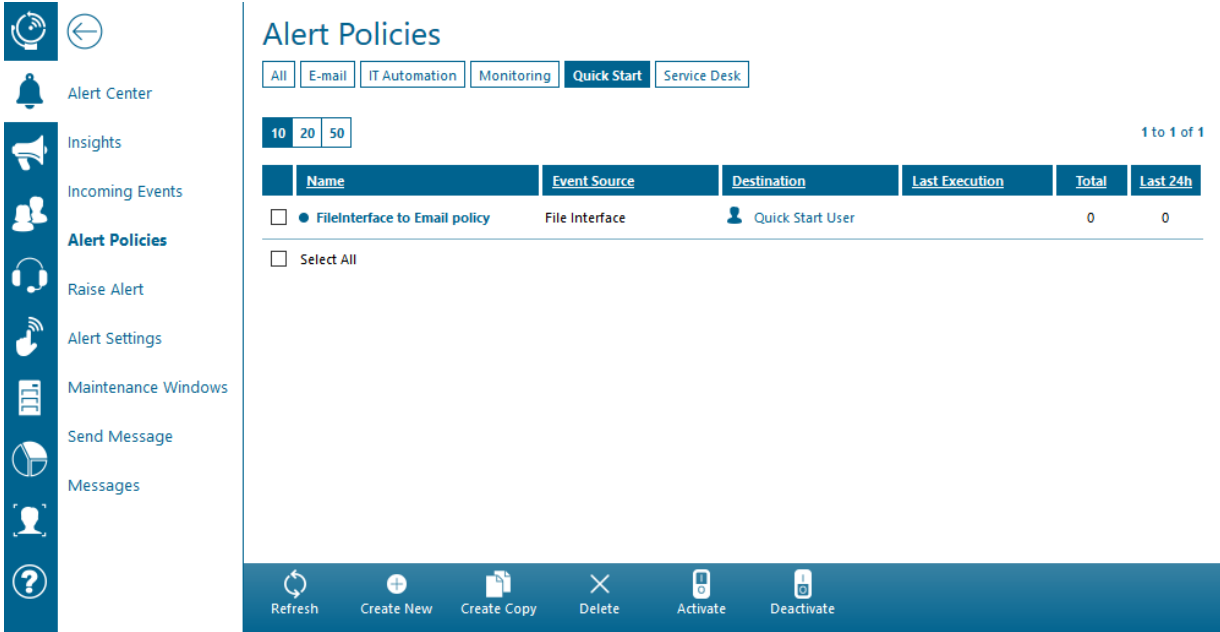
- Enter Subject... : New File Interface Alert
- Enter Message Text... : Alert Message: <Event Text>



Click on [Save](#) to create the policy and afterwards click on [Ownership](#) which will take you to the ownership management tab of the policy.

As you are the creator of the policy, you are automatically set as the primary owner of the policy. Click on [Save and Close](#) to create your first alert policy.

Click on [Alert Policies](#) to go back to the policy management overview. Click on the tag [Quick Start](#) to only display the policy that you have just created.



4.5 Step 5 - Set up integration with IT automation systems

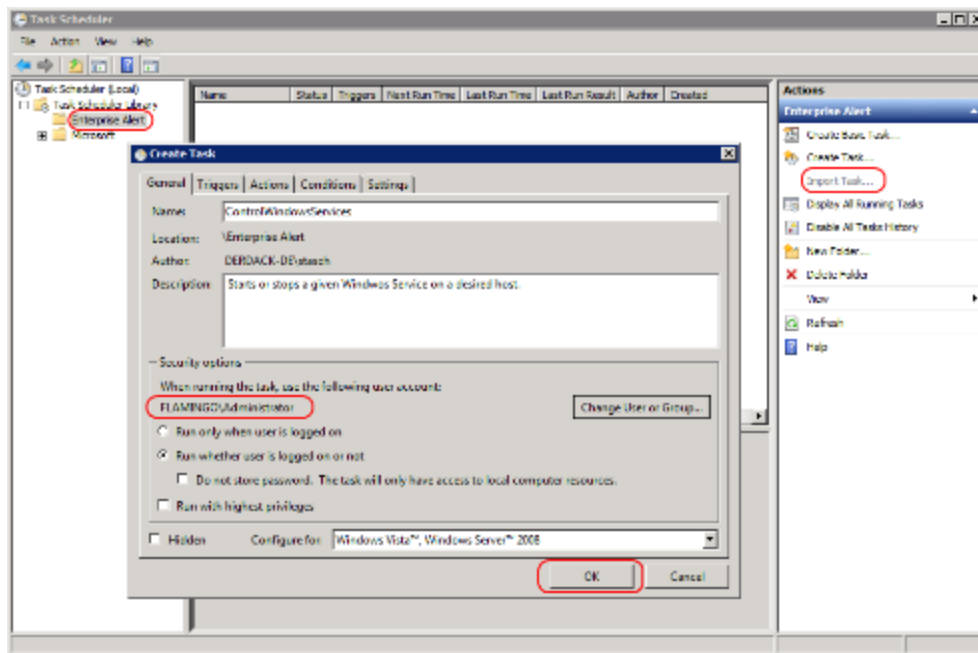
Automated and intelligent notification workflows via alert policies form only one of the core features of Enterprise Alert®. Another core feature is the concept of remote actions. Remote actions are basically tasks in IT automation systems that you can make available as remote actions with Enterprise Alert®. Remote actions are intended for remote troubleshooting of critical incidents in the data center, typically after you have been alerted via an alert policy in Enterprise Alert®.

In this quick start scenario, we will assume that the reason for the file being written to the file interface is a Windows service that is no longer running. To troubleshoot this problem, you will execute a remote action in Enterprise Alert®. The remote action is based on a task in Windows Task Scheduler – the IT automation system that you will work with in this quick start scenario. In this section, you will create a connection to the Windows Task Scheduler on the Enterprise Alert® machine.

To create a connection to the Windows Task Scheduler on the Enterprise Alert® machine, open [System > IT Automation](#) from the main menu. Click on [New Connection](#) at the bottom of the page. Select "Windows Task Scheduler" from the [Connection Type](#) drop down menu. Leave all the default values as they are and then click [Save](#).

All tasks in this folder can be made available as remote actions. Go to [System ->IT Automation ->New Task Scheduler Connection](#)

Enterprise Alert® is shipped with a sample task that can control selected Windows services. This task is available as an XML file and can be found in the Windows start menu of Enterprise Alert®. Copy this task to the desktop and import the file to the "Enterprise Alert" task folder by first right-clicking on the folder and selecting [Import Task...](#) from the actions panel. Locate the XML file on the desktop and double click it. The task will then be loaded. Before you can finish the import by clicking [OK](#), you must change the execution credentials that are saved with the task. Click on the button [Change User or Group](#) and select a [local administrator](#) on the Enterprise Alert® machine. Finish the import by clicking on [OK](#).



4.6 Step 6 - Create a Remote Action Policy

In this section, you will make the action that you have created in your IT automation system available for remote execution. This is achieved by means of remote action policies. To create a new remote action policy, select [Remote Actions > Remote Actions](#) from the main menu. On the bottom of the page, click on [Create New](#). Configure the following properties and click [Next](#):

- Name: Start NT Service
- Execute From: Incoming Messages -> E-Mail (E-Mail)
- Execute In: Windows Task Scheduler
- Tags: Quick Start

On the next tab, you can add the conditions that the incoming email must meet for the policy to be executed. Click on [Add Condition](#) to add a new condition with the following characteristics:

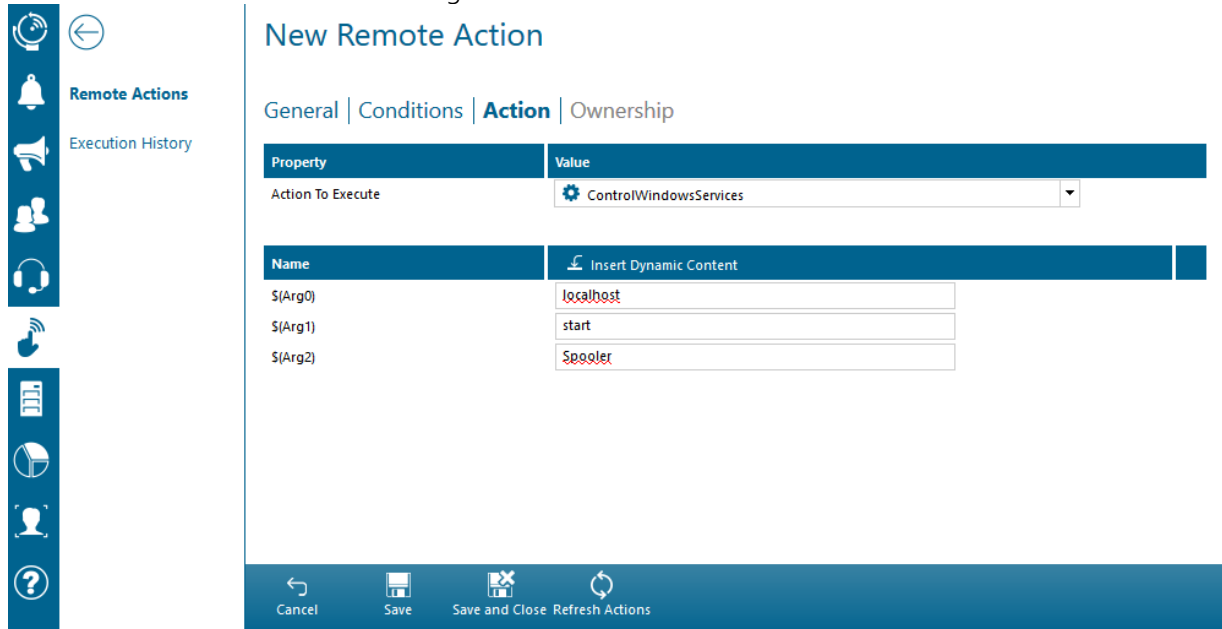
- Event parameter to evaluate: Subject
- Type of condition: contains
- Value to match: "Quick Start"

On the next tab, click the [Refresh](#) button in the Action Bar and then select the following value under "Task to Execute": localhost -> Enterprise Alert -> Start Windows Service (ControlWindowsServices).

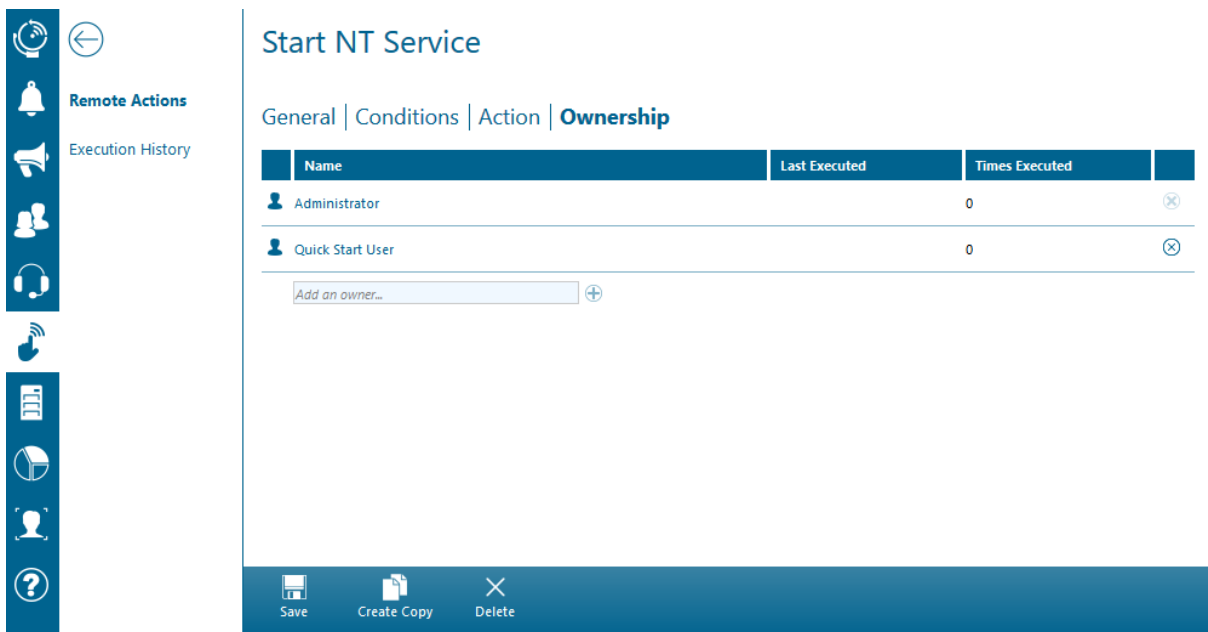
The command line arguments that have been configured for the task in the Windows Task Scheduler are as follows:

Argument	Meaning
\$(Arg0)	Host name on which to start a Windows service e.g. "localhost"
\$(Arg1)	Action to perform e.g. "start" or "stop"
\$(Arg2)	The name of the service to start or stop

For each of the arguments, enter suitable default values that Enterprise Alert® will pass as input parameters when the action is executed. Your configuration will look as follows:



Click on **Save and Close** to save your remote action policy. You can select ownership management tab of the remote action policy, however as you are the creator of the policy, you are automatically set as the primary owner of the policy. Only owners of the remote action policy may execute the policy. Next, grant permission to the "Quick Start User" so that they may execute the remote action. The permissions will then appear as follows:



Click on **Save** to save your new remote action policy and navigate back to the remote action policy overview. Click on the "Quick Start" tag to only display the remote action policy that you have just created:

Remote Actions

Search Bar

All

10 20 50 1 to 1 of 1

Name	Execute From	Execute In	Last Execution	Last Executed By
<input type="checkbox"/> Start NT Service	E-mail	Windows Task Scheduler	-	-
<input type="checkbox"/> Select All				

Refresh Create New Create Copy Delete Activate Deactivate

Please note that you will troubleshoot a data center problem in this quick start scenario by sending an email to Enterprise Alert®. In case you have already deployed the smart app and configured the connection from the app to the Enterprise Alert® Web service, you can also select "Smart App" as execution channel for this remote action.

4.7 Step 7 - Simulate a Problem to trigger an Alert

You will now kick off your quick start scenario! Simulate a critical problem with your printing services by stopping the print spooler Windows service on the Enterprise Alert® machine. Normally, there would be some automated monitoring system in place that would detect this problem and for example write a new file to the file interface of Enterprise Alert® as a result. But, we will perform this step manually instead by creating the text file by hand.

Create a new text document on your desktop that has the following content:

Quick Start: The print spooler is no longer running.

Save the file and copy it to the file interface of Enterprise Alert® (by default `C:\Program Files (x86)\Enterprise Alert\FileInterface`).

The file will be processed as an incoming event and the alert policy created in step 4 will trigger a new alert workflow that you can track and acknowledge by following the guidelines provided in the next step.

4.8 Step 8 - Acknowledge the Alert

First of all, log out of the Web portal as Administrator under [Administrator > Logout](#) and then log back in as the user you have created in step 1. You will otherwise *not* be able to acknowledge the alert in the web portal.

Log in as Quick Start User by entering the following credentials:

- User name: quickstart
- Password: Derdack13#

On the dashboard click on the tile "Alert Center" to view the new alert created by the alert policy. In order to acknowledge the alert, drag it on the "Acknowledged" tab and drop it there.

The alert details and especially the notifications for each particular recipient can be displayed via a double click on an alert.

4.9 Step 9 - Execute the Remote Action to troubleshoot the Problem

As you have acknowledged the alert, you are now responsible for resolving the problem that caused the alert. To do this, you will need to restart the print spooler. Instead of doing this manually, you will execute an automated IT task in Enterprise Alert® via Smart App or by sending a message to Enterprise Alert® through one of the unified communication channels such as email.

You will now simulate an incoming email by copying another file to the file interface of Enterprise Alert®.

On the desktop, create a new XML file with the following content, but replace quickstart@enterprisealert.com with the email address you entered in step 1!

```
<mm_message>
  <mm_header type="user" subtype="inbound" index="" sessionid="0"
  from="quickstart@enterprisealert.com" to="enterprisealert@enterprisealert.com"
  service_from="/Internal SMTP Manager" service_to="" subject="Quick Start"
  username="user" password="" timestamp="" msg_options="0" priority="" strref="" />
  <mm_body>Only the subject of this mail matters.</mm_body>
  <mm_attachments>
    <item name="attachments">
      <value>
      </value>
    </item>
  </mm_attachments>
</mm_message>
```

Copy the XML file from the desktop to the file interface folder of Enterprise Alert® (by default *C:\Program Files (x86)\Enterprise Alert\FileInterface*).

From the main menu, select [Remote Actions-> Execution History](#). You will see an entry for the remote action that has been executed. Once the status is 'Executed', verify that the print spooler is now running again.



Remote Actions

Execution History

Execution History

Search Bar

All Quick Start

Auto Refresh

10 20 50

1 to 1 of 1

Remote Action	Executed From	Executed By	Timestamp	Status	
Start NT Service	E-mail	Quick Start User	5/18/2017 3:51:12 PM	Executed	

Refresh Actions

5 REFERENCE GUIDE

5.1 Terminology

The following is a basic introduction to the essential concepts and terms used in Enterprise Alert®.

5.1.1 What is a Notification Channel?

A *Notification Channel* defines the media or means of notification transmission. Enterprise Alert® provides the following notification channels:

- SMS/MMS
- Voice-Call
- Email
- Instant Messaging
- Push Notifications
- Fax
- Paging

Most channels are bidirectional, not only allowing the transmission of messages, but also the receiving of replies.

5.1.2 What is a Connection?

A *Connection* is a configured integration to either a notification endpoint (SMSC, VoIP Server etc.) or to an event source (SCOM, ITM, etc.). These connections enable Enterprise Alert® to gather events from 3rd party systems and send out notifications.

Multiple *Connections* can be configured, allowing you to gather events from multiple sources of the same type or configure failover for notification connections using *Message Routing*.

5.1.3 What is Message Routing?

Message Routing defines which *Connection(s)* will be used when transmitting a message for a certain *Notification Channel*. Multiple *Connections* can be configured for a single *Notification Channel* to enable connection failover, but at least one *Connection* must be configured for the notification channel to be usable.

Additionally, simple conditions can be set to enable the use of different *Connections* for different messages, depending on their destination.

5.1.4 What is an Alert Policy?

An *Alert Policy* is the core component in Enterprise Alert's automated alerting process. It defines a set of conditions for incoming events or messages as well as the form of alert created when these conditions are fulfilled. *Alert Policies* enable the suppression of non-critical or duplicate events and the creation of alerts specific to the problem that caused the events.

The *Alert Policy* allows the complete configuration of the resulting alert, from different alerting procedures, priorities and notification channels to the dynamic composition of the alert message.

5.1.5 What is a Remote Action?

A *Remote Action* enables remote IT management by Enterprise Alert® users. A *Remote Action* consists of an executable action (provided by an IT automation connection) and user based execution permissions.

Remote Actions can either be triggered from the Enterprise Alert® Smart App or by incoming messages. If the policy is triggered by an incoming message, a set of trigger conditions can be configured similar to the trigger conditions of *Alert Policies*.

5.1.6 What is a Notification Profile?

Notification Profiles allow User Profiles to configure how they want to be alerted at specific times (business hours, after hours etc.). A *Notification Profile* defines the order of and *Notification Channels* used when alerting the user. At the time of an alert, *Notification Channels* will be used according to the user's currently active notification profile.

5.1.7 What is a User Profile?

A *User Profile* is the basic user account in Enterprise Alert® and has a number of functions. It is used to give the user access to the software, to send messages, manage the system and receive alerts.

User Profiles contain basic information about users, contact addresses and *Notification Profiles*. They also define a user's role, which specifies the features of Enterprise Alert® available to the user.

User Profiles can be imported from Active Directory or created manually.

5.1.8 What is a Team?

User Profiles can be grouped into *Teams*. These *Teams* are usually responsible for problems in particular areas and typically represent actual teams in your enterprise. *Teams* consist of *members* and *managers*.

Grouping users in a *Team* allows for advanced notification procedures such as alerting all *team members* at the same time (*Team Broadcast*) or each individual member sequentially until one of the team members acknowledges the alert (*Team Escalation*).

In contrast to earlier Enterprise Alert® versions, Enterprise Alert® 2012 only uses *Teams* for grouping *User Profiles*. This allows you to either apply an escalation or a broadcast notification procedure when alerting the *Team*.

Team managers are not part of the regular notification process. However, they can receive informational notifications about alert status changes. They can also cancel alerts addressed to their *Teams*.

5.1.9 What is an On-Call Schedule?

An *On-Call Schedule* belongs to a *Team* in Enterprise Alert®. For each *Team* you are able to create and maintain a corresponding on-call schedule. An on-call service is usually operated for a specific area or service that a team of engineers is responsible for. On-Call Schedules can be managed by team leaders who are *Managers* of the corresponding *Team* in Enterprise Alert®. Once the schedule has been completed, you can then send automated notifications to the corresponding on-call engineer by means of an *Alert Policy*. Please refer to section 3.4 and 4.5.10 for more detailed information.

On-Call Schedules were specifically designed for on-call service management. An on-call service typically has one on-call engineer who is on duty for an extended period of time e.g. one week. The on-call service may be operated on a 24x7 basis or only after hours and on weekends. If this description does not fit with

your scenario and you are looking for scheduling multiple resources for specific hours or periods during the day, for example for scheduling shifts or follow-the-sun scheduling, there are also Multi-Team Schedules, which you can use. You can read more about this in the following section.

5.1.10 What is a Multi-Team Schedule?

Multi-Team Schedules allow scheduling multiple *Teams* throughout the day for the purpose of notifying only the *Team* that is on duty at the time the alert has to be sent. The smallest interval for a shift is 30 minutes i.e. the shortest shift for a *Team* can be half an hour. Scheduling of shifts is done in a week view, which provides a good overview of the hours or shifts covered by the various *Teams*.

In contrast to *On-Call Schedules*, *Multi-Team Schedules* can be used to schedule shifts and follow-the-sun-based schedules. In both scenarios, you can schedule teams at the times of the day when they are on duty. An example for scheduling shifts is where three *Teams* cover a day that is split into 8-hour business hour, swing and night shifts respectively. An example for a so-called follow-the-sun schedule would be an onsite *Team* of engineers that is scheduled during local business hours and an external contracting *Team* who is in charge during the night and is typically located eastwards (hence follow-the-sun).

When an incident occurs, notifications to the *Team* on duty can either be broadcast, escalated through the team members or sent directly to the on-call engineer in the *Team* (but only if the *Team* maintains an *On-Call Schedule*). For further information about how to send notifications automatically to the *Team* on duty, please refer to section 4.5.11.

5.1.11 What is a Notification Feed?

A *Notification Feed* represents areas of interest that users in the system can self-subscribe to. Using *Notification Feeds*, you can send simple one-way notifications to users subscribed to the feeds.

In contrast to alert notifications sent to internal users or teams, where people are expected to solve problems and fix systems, *Notification Feeds* are used when you do not require users to respond to the notifications via acknowledgements or when you do not wish to work with teams.

Notification Feeds can also be made public, meaning that you can set up feeds, which external users such as customers or suppliers can subscribe to. An example is where a feed is used to represent particular products or services used by external users and which may be affected by problems. In the event of an incident affecting the associated products or services, notifications are sent to all users subscribed to the feed.

5.1.12 What is a Subscription User Profile?

A *Subscription User* is a user that may only receive notifications sent to *Notification Feeds*. Functionality such as sending messages via the Web portal, team memberships, time-related *Notification Profiles*, alert acknowledgment and so forth are not available - any other task in Enterprise Alert® beyond managing subscriptions and contact addresses cannot be performed by *Subscription Users*.

Subscription Users may either be external (public) users or internal users that have been imported from Active Directory as *Subscription Users*. There is a distinction between the usual internal users such as Team Leaders, Alert Users or Standard Users and *Subscription Users* in terms of security and licensing.

Before external users can subscribe to *Notification Feeds*, they must first register themselves with Enterprise Alert®. Once they have signed in, they can see feeds that were made available to external users and can subscribe to their fields of interest.

Subscription Users cannot directly be a destination for alerts or even basic notifications; they will only receive notifications directed to the *Notification Feeds* they are subscribed to.

5.1.13 What is a Callout?

Callouts in Enterprise Alert® have been designed for manually triggering notifications in emergency situations. Emergency scenarios that have been identified can thereby be created as a *Callout Plan*. Such a plan contains an alert text and consists of one or more alert recipients. Recipients can be individual Users, Teams, Notification Feeds or even Schedules.

Created Callout Plans can also be provisioned to users who will then be able to trigger and track the *Callout* in an emergency situation. Depending on the scenario, *Callouts* can be triggered via the Web Portal, an incoming SMS text message or even an inbound voice call.

5.1.14 What is a Maintenance Window?

Maintenance Windows are designed to stop incoming alerts from interrupting users while working in any systems monitored by Enterprise Alert®. If the maintenance work being done causes alerts to be sent out, there is no reasoning in receiving notifications when the alerts are intentional.

A *Maintenance Window* can be utilized for a specific Alert Policy, or for an Alert Policy Tag. The difference being between stopping an individual policy, or any policies of a particular type. (SMS, E-mail, etc..)

5.1.15 What is an escalation, what is a tier escalation?

In Enterprise Alert® there are two forms of alert escalation. The first one is an escalation from one team member to another. The typical scenario behind is an escalation from the primary person on-call to a backup person within the same team. This type of escalation can be activated by selecting "Escalation" as team notification method/procedure.

The second type of escalation is a tier escalation. The typical scenario is an escalation from a subject matter expert team, e.g. a team responsible for operating databases to a team of managers. Both teams may schedule on-call duty with primary and backup people. In case the backup(s) in the network team did finally not respond, the alert will be escalated to the next team, and here to the manager on duty. Team to team escalation is only one example for tier escalation. The alert target of a tier can be an individual User, a Team or a Multi-Team Schedule. A tier escalation can be setup by adding more than only one tier on the alerting tab in the details of an Alert Policy.

5.1.16 What is a Tenant?

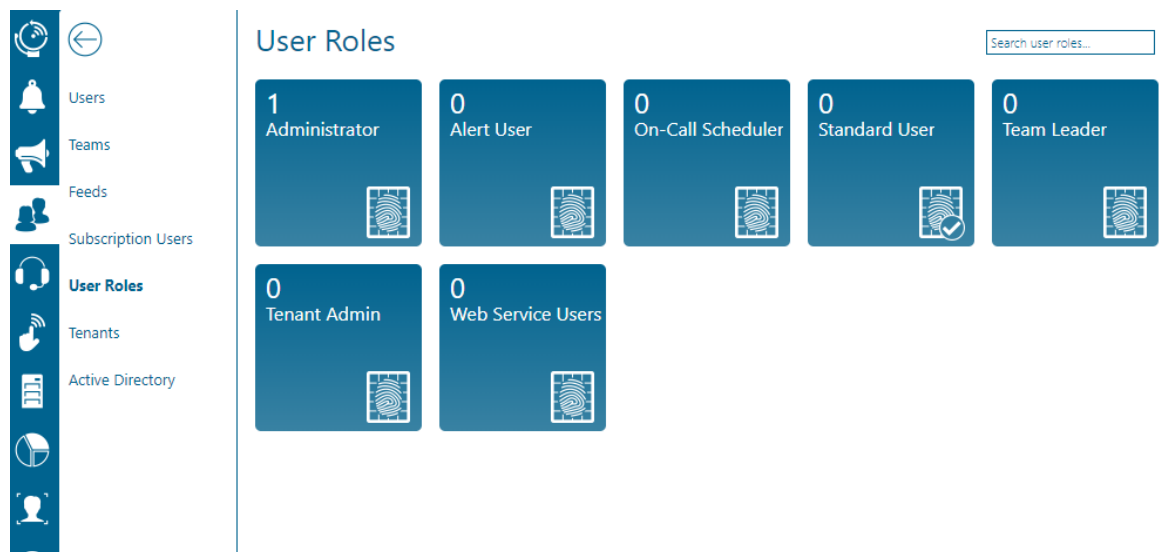
A tenant is an entity that allows to segregate data on your Enterprise Alert® instance. Lets say you provide alerting services to different departments or branches in your organization where each of them should only be able to see their own data (e.g. users or alerts). In this scenario the department or branch is a tenant in Enterprise Alert®. You can create tenants and assign most of the other entities such as users, policies, teams, etc. to these tenants. Each tenant member can then only see and work with their own assets.

5.2 User Roles

User Roles are a feature of Enterprise Alert® that help define the purpose and abilities of every user. Each Enterprise Alert® user is assigned to a role, which has a general description and a set list of permissions for the person assigned to it. A user can also be assigned to multiple roles.

There are default roles created with every deployment of Enterprise Alert®, however you can also create and customize user roles as you please. The default roles created with Enterprise Alert® are: Administrator, Alert User, On-Call Scheduler, Standard User, Team Leader and Tenant Admin.

To navigate to the User Roles page, select [People->User Roles from the side menu:](#)



5.2.1 Understanding All- and Tenant Scopes

When you set permissions in a role (see next section) you grant/deny permission or access to data in the system based on so called scopes. Scopes include "Own", "Team", "Tenant" and "All".

An example is the permission to view alerts. You can grant ("scope") this permission to:

- Own – Only view alerts that the user has triggered or where he was the notification target
- Team – Only view alerts that were sent to the team where the user is a member or owner of
- Tenant – View all alerts belonging to the tenant that the user also belongs to
- All – View all alerts in the system without any restrictions

The meaning of the scope "own" sometimes changes per permission. E.g., in contrast to the above example, the scope "own" for viewing teams means, "where the user is part of the ownership list of the particular team" (an alert does not have such a list).

In each role details, the very first permission defines if the possible scopes are restricted to all data within the tenant of the current user or if the role member can see data beyond his/her tenant:

General | **Permissions** | Members

Global System Access
Can manage Tenants and access all data in the system

No Yes

Active Directory
Import teams and users from the active directory

No Yes

Can manage Tenants and access all data in the system

If global system access is enabled in a role, the highest access level scope per permission in the role is "All", otherwise the highest scope is "Tenant". System owners or administrators of Enterprise Alert® should belong to a role where this permission is enabled and the remaining permissions are scoped to "All". Such role can be considered as "(Global System) Administrator". All remaining users should have this permission disabled in their role.

Members of a role in which the global system access permission is disabled but the remaining permissions are scoped to "Tenant", can be considered as "Tenant Administrators". These users can see/manage all data within their tenant.

5.2.2 Setting role permissions and role members

To edit an already existing role, simply click on the desired tile to edit. To create a new role, select the "Create New" button from the action bar at the bottom of the page. When editing or creating a new User Role, there are three tabs for configuration: the *General*, *Permissions*, and *Members* tabs.

First, give the role a name and a brief description in the *General* tab:

Alert User

General | Permissions | Members

Name

Alert User

Description

Default role for alert users.

Then, on the *Permissions* tab you can select which actions each user assigned to this role can perform and which aspects of Enterprise Alert® they are able to see:

Alert User

General | **Permissions** | Members

Active Directory

Import teams and users from the active directory
 Edit the active directory mappings

No	Yes
No	Yes

Alert Policies

Create alert policies
 See alert policies
 Edit alert policies

No	Yes	
None	Own	All
None	Own	All

Alerts


Raise alerts to other users and teams
 See alerts
 Acknowledge or decline alerts
 Cancel alerts
 Forward alerts to other users and teams
 Move overdue alerts to closed
 Change the alert severity
 See the insights page
 See alert reports
 Disable alerts
 View the alert settings page
 Edit the alert settings
 See incoming events
 Manage maintenance windows

No	Yes		
None	Own	Team	All
Own	Team		
None	Own	Team	All
None	Own	Team	All
None	Own	Team	All
None	Own	Team	All
No	Yes		
No	Yes		
No	Yes		
No	Yes		
No	Yes		
No	Yes		

Emergency Callouts



















Make emergency callouts

None	Own	All
------	-----	-----

Finally on the *Members* tab, you can add or remove members from the group of users assigned to this role. To assign someone to the role, simply search for and select an existing user from the 'Add Member...' text bar at the bottom of the list. To remove a user, simply click the  on the right side of their name.

Alert User

General | Permissions | **Members**

Name	
Chris Johnson	
Doreen Jacobi	
Doreen Papot (Custom)	
Fred Luddy	
General Lee	
John Smith	
Kathleen Zachieschang	
Kay Connor	
Kay Ramos	
Kyle Coder	
Ulus Khan (Alert User)	
Laura McCartney	
Marjin MeHES	
Matthias Derdack	
Spock	
Susann Grogger	
Sven Lehmann	
Sven Swanson	
Add member...	

When all settings are configured to your satisfaction, click the *Save* button from the action-bar at the bottom of the page to finalize your changes.

5.3 Active Directory Integration

Active Directory integration allows you to import Active Directory groups and all of their members into Enterprise Alert® fully automatically. You thereby do not have to create all users manually. The most important information that is being imported from AD is the contact address information such as a corporate e-mail address. On the other hand, when AD integration is being activated, all users who access the web portal of Enterprise Alert® can be automatically authenticated via Windows SSO.

Active Directory groups will be created as *Teams* in Enterprise Alert®, whereas users will be created as *User Profiles*. *Teams* will not however be created if the Active Directory group's users are imported as *Subscription Users*. In this case, the users will simply be created as *Subscription User Profiles* and will not be assigned to any *Teams*.

The *User Profile's* contact addresses can be mapped to properties of their Active Directory profile. These property values and changes to group memberships will be updated from Active Directory in configurable intervals to automatically keep Enterprise Alert's *Teams* and *User Profiles* in synch.

To configure Active Directory integration, open [People -> Active Directory \(under the Import&Synchronization section\)](#) in the Web portal of Enterprise Alert® and follow these steps.

Active Directory

48 of 50 remaining users 10 of 10 remaining subscription users

Synchronization | **Settings**

Background synchronization

Synchronization interval in minutes:

AD Access Credentials / DN

Domain / Distinguished Name	Account
+	

Default Notification Profile for imported users

Order	Channel	
1	SMS	<input type="checkbox"/>
2	E-mail	<input type="checkbox"/>
3	MMS	<input type="checkbox"/>

User field mappings

Address	AD field name	Format Address	Synchronize
SMS/MMS	mobile	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Voice-Call (Work)	telephoneNumber	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Voice-Call (Mobile)	mobile	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Voice-Call (Home)	homePhone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco IP Phone	ipPhone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fax	facsimileTelephoneNumber	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Pager	pager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Synchronize User Authentication

On the *Settings* tab, you can change the general import settings.

- **Background synchronization and the synchronization interval**

If you would like Enterprise Alert® to routinely import and synchronize Active Directory groups, you can enable the Background Synchronization property. Enabling this property allows Enterprise Alert® to automatically update Active Directory groups. If you want to perform the import only once, you do not have to check it. The Synchronization interval simply defines how often Enterprise Alert® will automatically import and synchronize groups; it is defined in minutes.

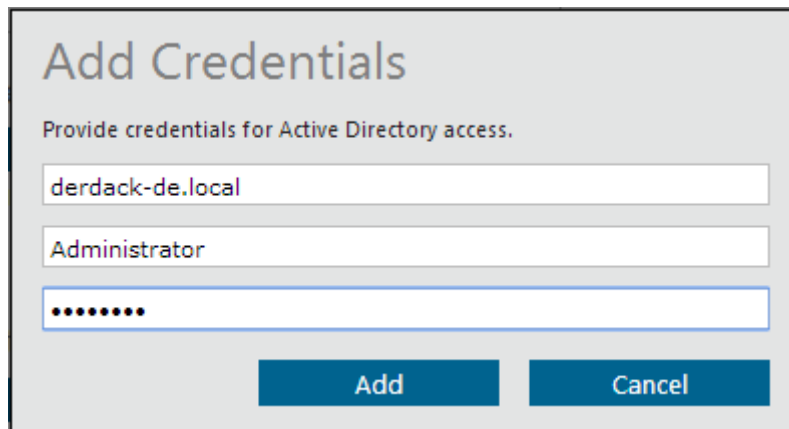
- **AD Access Credentials / DN**

This section defines the domains from which Enterprise Alert® will find and synchronize Active Directory groups. By default, this domain address is defined by the local domain of the machine currently running Enterprise Alert®. The default credentials are generated from the Run-As account of the Active Directory's Windows Service. In most cases this will be sufficient to begin adding groups. However, if no groups are available you must delete the default created domain and add your own domain address and credentials. You can do so by clicking the '+' button under the Domain Credentials section. You must enact the same process when integrating any additional domains.

Example Default Credentials:



Adding new credentials:



- **Set the default notification profile for imported users.**

The notification profile configured here will be the default profile for newly imported users. Manually created / changed notification profiles will not be changed when updating user profiles. The order number defines the order that Enterprise Alert® will escalate through notification profiles. You can assign as many Notification Channels that are available.

Default Notification Profile for imported users

Order	Channel	
1	SMS	<input type="checkbox"/>
2	E-mail	<input type="checkbox"/>
3	MMS	<input type="checkbox"/>

D field name	Format Address	Synchronize
mobile	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
telephoneNumber	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
mobile	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
homePhone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ipPhone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- **Set the contact address property mappings.**

Contact addresses that are mapped to Active Directory properties cannot be edited manually during Active Directory integration. They will always be kept in synch with their Active Directory values. However, you can remove these mappings at a later stage, and after the next (automatic or manually triggered) import, these addresses will be editable.

With each item in the contact address field, there are two options: Format Address and Synchronize. When a contact address field is enabled for formatting, it will be converted into E.164 format using the regular expression rules that you specify below. E.164 format is a general format for telephone numbers to communicate internationally and the format in which enterprise alert works with phone numbers. Similar to the UTC format for times it is the standard format for phone numbers used in Enterprise Alert. The synchronize option enables or disables syncing of specific contact addresses for each user imported. If you deselect one of the items, then that contact address will not be synchronized.

- **Save the settings by clicking Save or Synchronize at the bottom of the page.**

Saving the settings on the *Settings* tab will not initiate an import process. It will simply update the settings for the next automatic or manually triggered import.

Synchronizing the settings on the *Settings* tab will initiate an import process, as well as saving the desired settings for future reference.

Active Directory

183 of 300 remaining users 98 of 200 remaining subscription users 5/23/2017 10:27:46 AM last synchronization

Synchronization | Settings

Search synchronized groups...

Group	Roles in Enterprise Alert	AD Container	
DERDACK_DIRECTORS (2)	Co-Admin	Security Groups (derdack-de.local)	⊗
DERDACK_MARKETING (4)	Administrator	Security Groups (derdack-de.local)	⊗
DERDACK_RD_BASIC (11)	Co-Admin	Security Groups (derdack-de.local)	⊗
DERDACK_SALES (6)	Administrator	Security Groups (derdack-de.local)	⊗
DERDACK_SUPPORT (4)	Administrator	Security Groups (derdack-de.local)	⊗
Print Operators (3)	Alert User	Builtin (derdack-de.local)	⊗
WSUS Administrators (1)	Administrator	Users (derdack-de.local)	⊗

Save Synchronize Add Groups User Authentication

On the *Synchronization* tab, you configure the groups that will be imported from the Active Directory and manually trigger an import process.

- **Click 'Add Groups' at the bottom of the page, select the desired domain, then click 'Find' to list all available groups from that Active Directory that can be added to Enterprise Alert®.**

Searching through groups via a key-word is also available, use the *"Find groups..."* search bar to do so. In most cases, the user context in which the Web application runs, namely the NETWORK_SERVICE account, has sufficient access rights to read from Active Directory. However, if this is not the case you will have to provide specific domain access credentials that should be used to query Active Directory (these credentials will only be used for the query and not be saved anywhere, they can be edited in the 'Settings' tab. You can do so by clicking the '+' button under the Domain Credentials section).

- **Select the groups that should be imported into Enterprise Alert®.**

You will also have to select a role for users belonging to this group. If a user belongs to multiple imported groups, the user will receive the highest role selected for any of their groups. The list of available groups also displays groups that have been previously synchronized, shown by an 'Already synchronized' text field where User Role selection would normally be. Groups cannot be edited from the Add groups page. If you want to change a groups role, you can do so from the Synchronization tab. If the group has switched domains, you must re-import that group entirely.

Please note that any previously imported groups that have not been selected will be deleted from Enterprise Alert® along with all their member profiles. Be especially aware of this when using the *Distinguished Name* field to reduce the query results. Only groups selected in the query result will be imported / kept in the system; everything else will be removed.

- **Click 'Add Groups(#)' then 'Synchronize' to start the import process.**
 The import process will now be started. When the synchronization process has been started successfully, a message will appear in the lower right hand corner. This is an asynchronous process and depending on the number of users to be imported may take some time. A synchronization summary will be written to the System Log ([System->System Log](#)) when the process is finished. You can look into more detail about the summary by clicking the magnifying glass on the right side of the page. At the end of the import process, the Web portal will be set to use Windows Authentication if this is not already the case.
- **Removing Synchronized Groups**
 Removing groups from the synchronized list is very simple. Just click on the small, encircled 'X' on the right of the group that you want to remove.
- **Search Synchronized Groups**
 At any point in time, the user can search through all Active Directory groups that have been previously synchronized. To do so simply type a keyword into the "Search synchronized groups..." search bar above the list of groups.
- **Remaining Users & Other Information**
 At the top of the page there are three important pieces of information displayed: Remaining users, remaining subscription users, and last synchronization. The number of remaining users and subscription users is directly related to your product license with Enterprise Alert®. To acquire more available users, you must update your subscription edition. The last synchronization information field simply displays the last time your Active Directories were synchronized and imported.

If you have activated the synchronization interval, a new import process will automatically be started in the configured interval. This process will update the mapped contact addresses, add new group members to the system and remove *User Profiles* that are no longer members of any synchronized group, thus keeping your Enterprise Alert® system in synch with Active Directory.

5.4 Setting up Notification Channels

5.4.1 Setting up Emails

Enterprise Alert® supports Email notifications via your Microsoft Exchange server or by using standard E-mail protocols such as SMTP, IMAP or POP3.

Exchange Integration

Integration of Enterprise Alert® into Microsoft Exchange Server involves the provisioning of a dedicated Enterprise Alert® user in your Active Directory. This user should be assigned an email address like "enterprisealert@yourcompany.com" and then be provisioned with a corresponding mailbox in your Exchange Server. The last configuration step is then to create a new Exchange email connection in Enterprise Alert® as described below.

Please note that Exchange Web Services (EWS) must be enabled on your Exchange server for Enterprise Alert® to be able to integrate with it.

To integrate Enterprise Alert® with Microsoft Exchange, open [System](#) then select "New Channel" from the action-bar. Select E-mail as the Media entry. Enter the following configuration information and click [Save](#):

- **Activated:** Please check this box in order to activate the connection to Microsoft Exchange.
- **Name:** Enter a name for the new connection e.g. "Corporate Exchange"
- **Account Type:** Select "0 – Exchange"
- **Mailbox E-mail Address:** Enterprise Alert® will monitor a dedicated inbox on your Exchange Server. It is therefore recommended that you create a domain account for Enterprise Alert® in your AD and to provision a mailbox for this user in your Exchange server. Afterwards enter the mailbox email address in this field. An example would be "enterprisealert@yourdomain.com".
- **Account Credentials:** Either select "0 – Configure Account Credentials" or select "1 – Use Windows Service Account". If you select the first option, you can enter the credentials for the mailbox on the configuration page. Otherwise you must set the AD account of the mailbox user account as Run-As account for the Windows Service "Enterprise Alert® E-mail Module" on the server where Enterprise Alert® has been installed.
- **Domain:** Enter the domain part of the mailbox user credentials
- **Username:** Enter the username of the mailbox user credentials
- **Password:** Enter the password of the mailbox user credentials
- **Exchange Server:** If Exchange server auto discovery is working in your domain, you can leave this field empty. Otherwise, please enter the IP or the FQDN of your Exchange server.
- **Send High Priority E-mails:** This property defines whether the priority of an e-mail is set to high.
 - *0-Never:* No e-mail is marked with a high priority when sent via this account.
 - *1-Always:* The e-mail is always marked with a high priority when sent via this account.
 - *2-For high prioritized alert notifications only:* The priority of an e-mail is set to high if the corresponding notification has a high priority.
- **Save Copy of Sent Emails:** If this option is enabled, all emails that are sent through this connection will be saved in the "Sent Items" folder of the mailbox. Otherwise the emails are not saved in this folder, which would help in preventing the mailbox size from increasing over time.
- **Standard Domain of the E-mail Recipient:** This property can be used to specify the standard domain of the e-mail recipient. In cases where the recipient's address is not complete e.g. where @yourdomain is left out of the address, the standard configured domain will be added.

- **E-mail Receiving:** Use this property to configure 2-way emails or to turn email receiving off. This property specifies the method to use when monitoring changes to the Exchange folder. Changes that are monitored include the 'New Email', 'Email Moved' and 'Email Deleted' events. Each method has its own advantages and disadvantages. The option "1 – Poll Exchange Server" increases network traffic and is not real-time, while option "2 – Receive Push Notifications" involves opening up a port on the server where Enterprise Alert® is installed, in which case a port may have to be unblocked on the firewall.
- **Poll Interval (sec):** Specify the interval in seconds between which the account connection polls the Exchange server for updates. The minimum value is 5 seconds. If you would like to reduce this value, please consider using push instead. This property is only displayed when you select "1 – Poll Exchange Server" as method for 'Email Receiving'.
- **After Mail Retrieval:** Select whether the emails that have been received should be marked as read, moved to the "Deleted Items" folder or should be deleted from the mailbox in order to reduce the mailbox size.
- **Include Attachments:** Email attachments will only be processed and included in the inbound messages when this property is activated, otherwise attachments will be dropped from the messages. Dropping the attachments may result in faster processing of the messages and reduced disk space usage.

The screenshot below displays a sample configuration for Exchange server integration:

New Channel

Media *
Email

Activated

Name *
New Email Account

Account Type *
0 - Exchange

Mailbox E-mail Address *

Account Credentials *
0 - Configure Account Credentials

Domain *
derdack-de

Username *
dpapst

Password *

Exchange Server

Send High Priority E-mails *
2 - For high prioritized alert notifications only

Save Copy of Sent Emails

Standard Domain of the E-mail Recipient

E-mail Receiving *
1 - Poll Exchange Server

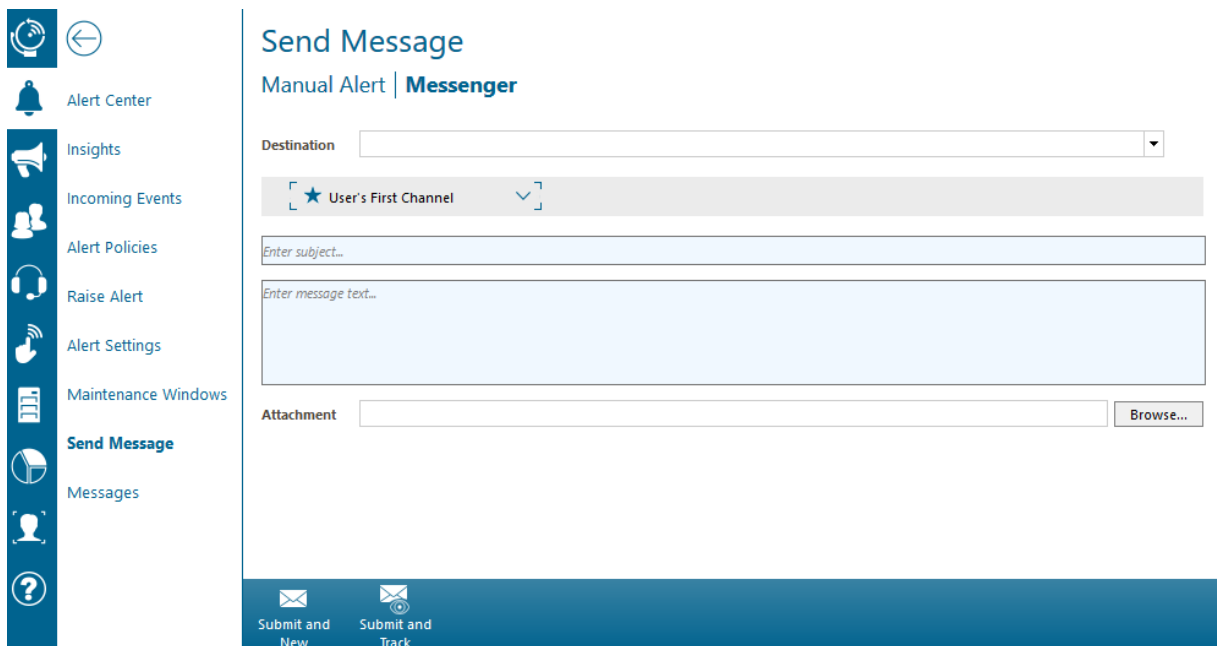
Poll Interval (sec)
5

After Mail Retrieval *
1 - Mark As Read

Include Attachments

Preserve HTML from E-mails

Once you have saved your new connection it will be initialized. Enterprise Alert® will attempt to connect to the Microsoft Exchange Server. If the connection was successful, the connection status 'OK' will be displayed. In this case you may want to send a test email with the Messenger. The Messenger can be found under [Alerts](#)
-> [Send Message:](#)



Standard Email Accounts

Besides direct Exchange server integration via EWS you can also implement email notifications via standard email protocols such as SMTP, POP3 or IMAP. Enterprise Alert® allows you to configure any email account that can be accessed with these protocols. In order to create a corresponding email connection, open [System > Notification Channels](#) in the Web portal of Enterprise Alert®. Afterwards click [New Channel](#). Select Email as the Media type, enter the following configuration information and click [Save](#):

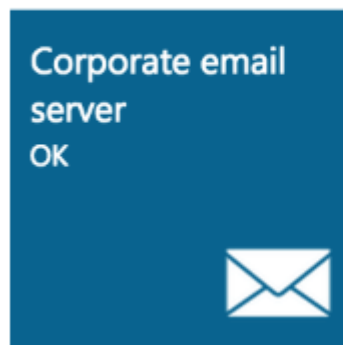
- **Activated:** Check this box in order to activate the connection.
- **Name:** Enter a name for the new connection e.g. "Gmail Email Account"
- **Account Type:** Select "1 – Internet Mail"
- **Mailbox E-mail Address:** Enter the email address of the mailbox account. This Email address will also be used as originator email address when Enterprise Alert® sends email notifications.
- **Username:** Enter the username of the mailbox user credentials.
- **Password:** Enter the password of the mailbox user credentials.
- **Receiving Protocol:** Select the protocol for receiving emails from the server. You can either use POP3 or IMAP depending on the supported protocol of the mailbox server. Using IMAP is recommended. If you do not want to enable incoming emails for this connection you can also select "0 – Off" to disable incoming emails.
- **Incoming Mail Server Address:** Enter the IP address or DNS of the email server e.g. pop.google.com. A port other than the default port can be specified by appending the port to the IP address or DNS separated by a colon e.g. 192.168.8.1:8723.
- **Use Secure Connection (Incoming):** If activated, emails will always be received via a secure connection (SSL encrypted connection).
- **Delete Email From Server After Reading:** If this property is activated, messages read by this connection will be deleted from the server, otherwise they will remain on the server.
- **Include Attachments:** Email attachments will only be processed and included in the inbound messages when this property is activated, otherwise attachments will be dropped from the messages. Dropping the attachments may result in faster processing of the messages and reduced disk space usage.

- Interval For Querying POP3 Account In Minutes: This property only applies if POP3 was selected as protocol for receiving emails. In this case enter the interval in minutes in which the mailbox should be queried for new emails.
- Sending Protocol: This property specifies whether e-mails can be sent through using this account and which method should be used for e-mail submission.
 - SMTP Relay Server: E-mails are sent via the given e-mail host specified in 'Outgoing Mail Server Address'.
 - SMTP Server Direct: E-mails are sent directly to the SMTP host as determined from the domain specified in the destination e-mail address. In this case, the domain needs to contain a valid MX record.

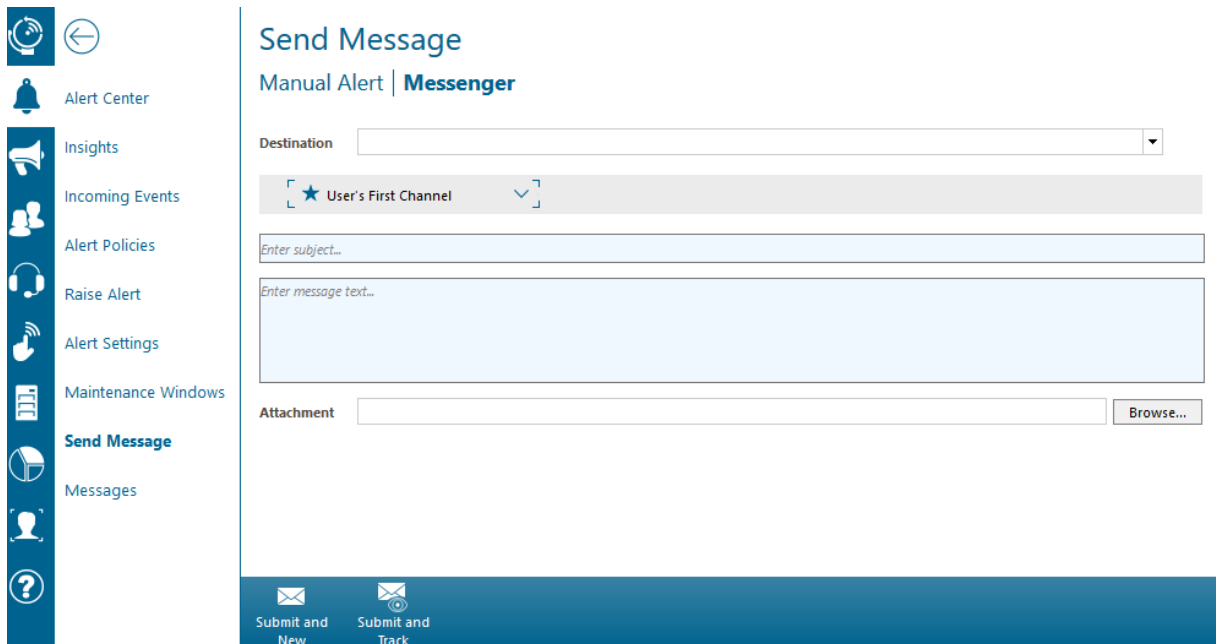
If you do not want to enable outgoing emails for this connection you can also select "0 – Off" to disable outgoing emails.

- Outgoing Mail Server Address (SMTP): Enter the IP address or DNS of the email server e.g. smtp.google.com. A port other than default port can be specified by appending the port to the IP address or DNS separated by a colon e.g. 192.168.8.1:8723.
- Authentication Required: Activate this property if the outgoing email server requires authentication with the credentials you specified in the Username/Password properties.
- Use Secure Connection (Outgoing): If this property is activated, emails will always be transmitted via a secure connection (SSL).
- Standard Domain of the E-mail Recipient: This property can be used to specify the standard domain of the e-mail recipient. In cases where the recipient's address is not complete, the standard domain configured here will be added.
- Send High Priority E-mails: This property defines whether the priority of an e-mail is set to high.
 - *0-Never*: No e-mail is marked with a high priority when sent via this account.
 - *1-Always*: The e-mail is always marked with a high priority when sent via this account.
 - *2-For high prioritized alert notifications only*: The priority of an e-mail is set to high if the corresponding notification has a high priority.

Notification Channels



Once you have saved your new connection it will be initialized. Enterprise Alert® will attempt to connect to the mail server. If the connection was successful, the connection status 'OK' will be displayed. In this case you may want to send a test email with the Messenger. The Messenger can be found in the alert menu:



5.4.2 Setting up Voice Calls

Enterprise Alert® realizes voice calls through a custom SIP based VoIP integration. This allows for great flexibility in your voice call scenarios, ranging from Cisco Unified Call Manager (CUCM) integration to complete replacements of outdated TAPI integrations. The Enterprise Alert® VoIP component can act as SIP Endpoint or as SIP Trunk.

The VoIP component has the following characteristics.

- Signaling is done according to the SIP RFC3261 (does not support H.232), supporting the “early offer” call/answer model.
- Media Sessions are negotiated using SDP (RFC2327) and transport is realized using RTP (RFC3550)
- Security SIPS or SRTP is currently not supported
- DTMF supports SIP-INFO requests (RFC2976) and RTP Payload for DTMF (RFC4733)
- Supported audio codec is G711 aLaw or uLaw (WAV file support but no PCM)



Before you configure a VoIP connection in Enterprise Alert you have to prepare your VoIP system i.e. create SIP Profiles and trunks. The preparation steps needed greatly depend on your VoIP system. A sample preparation workflow for CUCM would be:



Once your VoIP system is prepared, open [System > Notification Channels](#) and select VoIP as the media type in the Web portal of Enterprise Alert® to configure a VoIP connection. Configuration will look as below:

New Channel

Media *

Activated

Name *

VoIP Server *

Account Name or SIP URI *

Account Password

Connection Type *

SIP Transport *

TTS Engine *

TTS Rate *

Inbound Menu *

Call Transfer Mode *

Maximum Inbound & Outbound Lines

Enable Inbound Calls

Reserved Inbound Lines

Local Listening Address

Local Public Address

Call Initialization Timeout (ms)

Call Pickup Timeout (ms)

Input Timeout (ms)

Input Terminator

Redial Attempts

Redial Sleep Time (ms)

Called Number Format Rules (Phone number formatting before calling with Regular Expressions)

Rule Name	Regular Expression	Replacement
There are currently no number format rules.		

The following settings are required to set up a VoIP connection:

- **Connection name:** A unique name identifying the connection in Enterprise Alert®
- **VoIP Server:** IP address of your VoIP server
- **Account Credentials:** SIP URI or an account name and password if required for authentication on the VoIP server
- **Connection Type:** SIP Trunk or SIP Endpoint
- **TTS Engine:** The TTS engine which will be used for voice calls. TTS engines are gathered through .NET and UCMA interfaces. Legacy and nonstandard TTS engines may not be available. The TTS engine will be automatically switched to the first matching engine if the selected TTS engine does not support the current alert's language.

Other optional settings allow you reserve or disable inbound lines, reduce the amount of concurrent calls and fine tune call and input timeouts.

Notification Channels



Notification Channels



If the connection has been configured correctly, the new VoIP connection will appear dark-blue in the Notification Panels page, with 'OK' displayed in the bottom right corner. Otherwise it will appear orange with a short error message along the bottom of the tile.

Creating the first VoIP connection will automatically create a message route directing ALL voice-calls through this connection. You should modify the message routes if you also have active Lync integrations to prevent failed submission of messages through the wrong connections. Setting the

destination condition for your Lync connection to its domain suffix will only route messages sent into your Lync domain through this connection and everything else through your VoIP connection.

Message Routing

Notification Channel	Matching Destinations	Primary Connection	Failover Connections
<input type="checkbox"/> E-mail	*	Corporate email server	-
<input type="checkbox"/> MMS	*@*	Corporate email server	-
<input type="checkbox"/> Push Notification	Android	Push - Android	-
<input type="checkbox"/> Push Notification	Blackberry	Push - BlackBerry	-
<input type="checkbox"/> Push Notification	iPhone	Push - iPhone	-
<input type="checkbox"/> Push Notification	Windows Phone	Push - Windows Phone	-
<input type="checkbox"/> SMS	*@*	Corporate email server	-
<input type="checkbox"/> Select All			

Buttons: Delete, Create New, Refresh

To finalize the VoIP integration, you have to configure SIP URIs or phone numbers dialable by your VoIP system in your user's voice call address fields. You can either configure these manually or import the values through Active Directory integration.

Administrator

General | **Contact Addresses** | Notification Profiles | Teams | Notification Feeds

Notification Channel	Address
SMS	Mobile: +49177723432
E-mail	Office E-Mail: rbormann@de.derdack.com
Voice-Call	Office Phone
Voice-Call	Home Phone
Voice-Call	Mobile Phone
Push Notification	iPhone: Get Login Details
Push Notification	Android: Get Login Details
Push Notification	BlackBerry: Get Login Details
Push Notification	Windows Phone: Get Login Details
Instant Message	SIP Address
MMS	(same as SMS mobile number)
Pager Message	Pager Number
Fax	Fax Number
Add...	New Contact Address Name... Enter Contact Address...

Buttons: Save, Delete

See 3 Active Directory Integration for more information on Enterprise Alert® Active Directory Integration.

5.4.3 Setting up Push Notifications

Push Notifications are sent to smart devices via push infrastructure of according platform vendors such as Google, Microsoft or Apple.

On the other hand, they may also be sent to BlackBerry devices through an internal BES Server or to on campus Cisco IP Phone devices using CUCM.

Google, Microsoft or Apple Push Notifications

To be able to send push notifications to the Enterprise Alert® Mobile App on these platforms you need to configure each a push notification channel. Push notification channels can be created in the Enterprise Alert® Web Portal under [System > Notification Channels](#). Click on [New Channel](#) and select Push.

Enter a name for the new Channel (e.g. "Apple Push") and if applicable enter the push service URL and port.

You can find the Push Server URL and port to enter in section 2.6.3.

New Channel

Media *
Push

Activated

Name *
New Smartphone Push Connection

Device Type *
3 - iPhone

Apple Push Notification Server URL *
gateway.push.apple.com

Apple Push Notification Server Port *
2195

BlackBerry Push Notifications

To set up BlackBerry BES push integration, you need to provide the following configuration settings:

- [MDS Push URL](#): URL of the Mobile Data System (MDS) Web service of the BES
- [BES Access Credentials](#): Login credentials for the BES server
- [Device Port](#): The port on which the Enterprise Alert® App on your BlackBerry device will listen for incoming push messages. Make sure this port is not in use for anything else on your device.

Cisco IP Phone Push

The IP Phone notification requires more configuration than the rest of the Push devices. It allows for a very detailed type of notification. Definition requires:

- [Real-time Interface Service \(RIS\) Port URL](#)
- [RIS Username](#)

- RIS Password
- Soundfile Name
- Length of Vibration in Seconds
- Interval between Vibrations in Seconds
- Number of Vibrations
- EA Client API Rest URL

New Channel

Media *

Activated

Name *

Device Type *

Real-time Interface Service (RIS) Port URL *

RIS Authentication enabled

RIS Username *

RIS Password *

Attempt to resolve MAC address to User ID

IP Phone Authentication Enabled

Play Sound on Alert

Soundfile Name *

Vibrate on Alert

Length of Vibration in Seconds *

Interval between Vibrations in Seconds *

Number of Vibrations *

Push Confirmation of Alert Acknowledgments

EA Client API REST URL *

5.4.4 Setting up Microsoft Skype for Business IM and Voice-Calls

Enterprise Alert® enables you to send and receive instant messages and voice calls through the Microsoft Skype for Business Server.

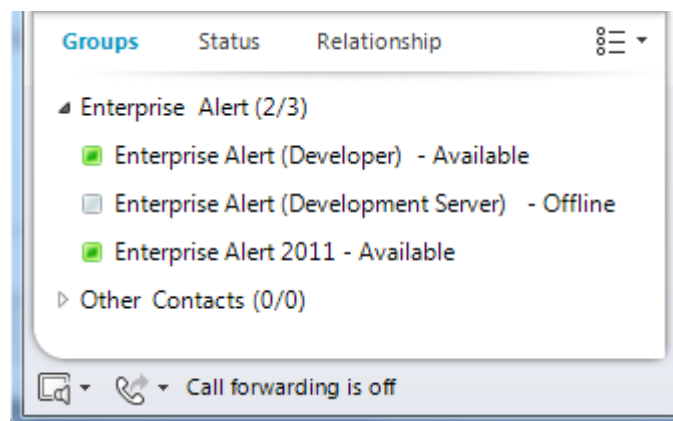
Skype for Business Server integration is based on the Unified Communications Managed API (UCMA). Depending on the Skype for Business Server setup, this enables Enterprise Alert® to make calls across domains, to public IM providers or public phones. Additionally, Enterprise Alert® subscribes to presence state changes on the Lync server, keeping the availability of Enterprise Alert® users up-to-date.

Supported server versions are:

- OCS 2007 (R2)
- Lync Server 2010
- Lync Server 2013
- Skype for Business Server 2015



The first step in setting up Skype for Business Server integration is the creation of a dedicated Enterprise Alert® domain user account. Provisioning this account in Skype for Business Server allows Enterprise Alert® to send IMs and voice calls as this user. This account will also appear as a contact in the Skype for Business Client, enabling users to call Enterprise Alert® directly.



There are no special trust relationships and certificates beyond those a normal Skype for Business Client installation would require. To verify this, you can install a Skype for Business Client on the Enterprise Alert® server. If you can use the account to successfully log in, the Enterprise Alert® Skype for Business integration will be able to connect to the server as well.

To configure a Skype for Business Server connection, open [System > Notification Channels](#) then select Skype for Business as the media type in the Web portal of Enterprise Alert®.

Setting up a Skype for Business server connection in Enterprise Alert® is really easy. All you need is the domain name of the Skype for Business Server and the dedicated domain account.

New Channel

Media *
 Lync

Activated

Name *
 MyLyncConnection

Server FQDN *
 YourLyncHost.Domain.com

Account SIP URI *
 enterprisealert@domain.com

Account Credentials *
 0 - Configure Account Credentials

Account Name *
 Username

Account Password *

Account Domain *
 Domain

TTS Engine *
 Microsoft Anna - English (United States)

TTS Rate *
 0 - Normal

Maximum Inbound & Outbound Lines
 10

Server Port
 0

Transport Type *
 0 - TLS

Allowed Authentication Protocols *
 0 - Kerberos & NTLM

Enable Inbound Calls

The following settings are required to set up a Skype for Business connection:

- **Connection name:** A unique name identifying the connection in Enterprise Alert®
- **Server FQDN:** Full Qualified Domain Name of the Microsoft Skype for Business Server
- **Account SIP URI:** The SIP URI of the domain account Enterprise Alert® will use to send and receive calls
- **Account Credentials:** Either enter the account credentials on this configuration page (the account password will be saved encrypted) or set the credentials mode to use the credentials the Enterprise Alert® Skype for Business Windows service is running under. In any case, the account used must be the owner of the SIP URI configured above.

Please note that there are additional requirements when changing the run-as-account of the Skype for Business integration Windows service. The new run-as-account needs full access to all four *mmocsmodule* message queues in MSMQ as well as the installation directory of Enterprise Alert® (by default "Program Files/Enterprise Alert").

- **TTS Engine:** The TTS engine which will be used for voice calls. TTS engines are gathered through .NET and UCMA interfaces. Legacy and nonstandard TTS engines may not be available. The TTS engine will be automatically switched to the first matching engine, if the selected TTS engine does not support the current alert's language.

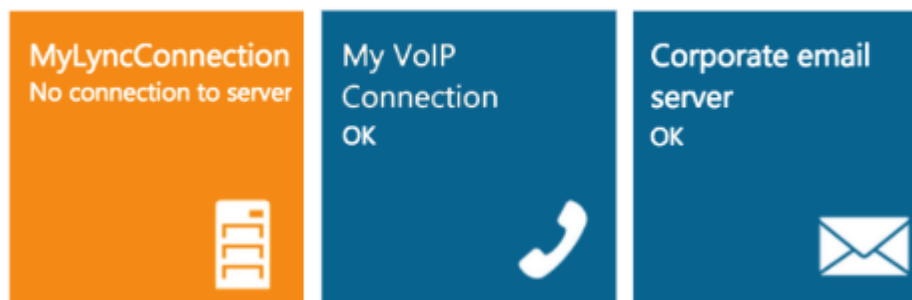
Additional UCMA TTS engines can be downloaded here:

<http://www.microsoft.com/download/en/details.aspx?DisplayLang=en&id=19549>

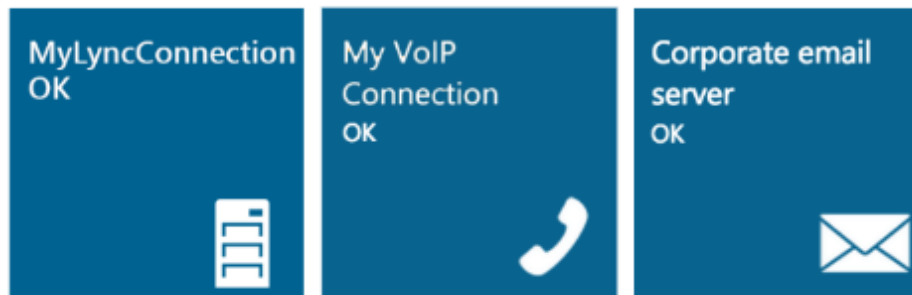
- **Transport Type:** TLS/TCP
- **Allowed Authentication Protocols:** Kerberos/NTLM

Other optional settings allow you reserve or disable inbound lines and fine tune call and input timeouts. You should not need to change the default values in most cases.

Notification Channels



Notification Channels



If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.

Creating the first Skype for Business connection will automatically create a message route directing ALL voice-calls/IMs through this connection. You should modify this message route if you also have active VoIP integrations to prevent failed submission of messages. Setting the destination condition to your Lync domain suffix will only route messages sent into your Skype for Business domain through this connection.

To finalize the Skype for Business integration, you have to configure SIP URIs or Skype for Business dialable phone numbers in your user’s voice call and instant message address fields. You can either configure these manually or import the values through Active Directory integration.

General | **Contact Addresses** | Notification Profiles | Teams | Notification Feeds

Notification Channel	Address	
SMS	Mobile	
E-mail	Office E-Mail *	derdack_test@freenet.de
Voice-Call	Office Phone	+4915612345678
Voice-Call	Home Phone	
Voice-Call	Mobile Phone	
Push Notification	WindowsPhone	
Push Notification	Litom	
Push Notification	Android	
Push Notification	iPhone	
Push Notification	BlackBerry	
Push Notification	Windows Phone	
IP Phone Push	Cisco IP Phone	
Instant Message	SIP Address	derdack_test@freenet.de
MMS	(same as SMS mobile number)	
Pager Message	Pager Number	
Fax	Fax Number	
Add...	New Contact Address Name...	Enter Contact Address...

See 5.3 *Active Directory Integration* for more information about Enterprise Alert® Active Directory Integration.

5.4.5 Setting up SMS text messaging

Enterprise Alert® supports three possible scenarios for enabling SMS text messaging.

- Direct IP connection to the mobile operator (SMSC)
- MultiTech iSMS modem
- Directly connected (RS232) or virtualized (using DigiPortServer® TS) GSM/GPRS/LTE modem
- GSM/GPRS/LTE modems connected using IP technology and Telnet protocol

SMSC

To set up a SMSC connection, open [System > Notification Channels](#) in the Enterprise Alert® Web Portal. Then create a New Channel, and select SMS/MMS as the Media type. Then for the type of SMS select SMSC(SMPP).

You should only need to configure the following configuration settings; for everything else the default values should be sufficient.

- Connection name: A unique name identifying the connection in Enterprise Alert®
- Network Address and Port: IP Address and port of the SMSC
- SMSC password: Password for authentication with the SMSC.

Change the other values only if the defaults do not work or if your SMSC provider explicitly provided you with different configuration settings.

iSMS Modem

To set up a connection to an iSMS Modem, open [System > Notification Channels](#) in the Enterprise Alert® Web portal. Then select SMS/MMS as the Media Type, and MultiModem® iSMS as the SMS type.

New Channel

Media *
SMS / MMS

Type *
MultiModem® iSMS

Activated

Name *
New Connection

Username *
Username

Password

iSMS IP Address *
iSMS IP Address

iSMS Port *
iSMS Port

Receiving Activated

Replace Destination Prefix(es)

Message Status Refresh Interval (ms)
10000

The following configuration settings are required for a valid iSMS connection:

- **Connection name:** A unique name identifying the connection in Enterprise Alert®
- **User Credentials:** Username and SMSC password of an account allowed to connect to the iSMS modem
- **iSMS IP Address and Port:** IP Address and port of the iSMS modem
- **Receiving Activated/Deactivated:** If enabled an IP Listener Address and Port is required.
- **Local Listener Address and Port:** IP address of the Enterprise Alert® host and the port where the connection will listen for incoming SMS's. If the default port is in use, you can change it here.

If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.

Serial/USB/Telnet based Modem Connection

Open [System > Notification Channels](#) in the Web portal of Enterprise Alert® to configure a GSM/GPRS modem connection. Then for the Media type, select SMS/MMS, and for the MMS type select SMS-MMS Modem.

New Channel

<p>Media *</p> <p>SMS / MMS</p> <p>Type *</p> <p>SMS-MMS Modem</p> <p><input checked="" type="checkbox"/> Activated</p> <p>Name *</p> <p>New Modem Connection</p> <p>Validity period in minutes</p> <p>1440 - One Day</p> <p>Connection Type *</p> <p>1 - COM Port</p> <p>COM Port *</p> <p>AutoDetect</p> <p>MSN *</p> <p></p> <p>SMSC number *</p> <p></p> <p>SIM card PIN</p> <p></p> <p>Device initialization</p> <p>Falcom - AT+CMGF=0</p> <p>Connection speed *</p> <p>9600</p> <p>Data bits *</p> <p>8</p> <p>Parity *</p> <p>None</p>	<p>Stop bits *</p> <p>1</p> <p><input checked="" type="checkbox"/> Encode SMSC number in PDU</p> <p>Number of resend attempts</p> <p>0</p> <p><input type="checkbox"/> Auto recovery</p> <p>Interval to check for incoming messages in seconds *</p> <p>10</p> <p><input type="checkbox"/> MMS enabled</p>
---	--

The following settings are required to establish a proper connection to a GSM/GPRS modem:

- **Connection name:** A unique name identifying the connection in Enterprise Alert®
- **Connection Type:** Select **COM port** or **Telnet** depending on how you have connected your modem
- **COM Port:** The **COM port** that the device is connected to e.g. "COM2", only if connection type is COM port
- **SIM card PIN:** The PIN number of the SIM card in the GSM/GPRS device.

- **MSN:** Represents the mobile phone number of the SIM card. The number will be used internally as recipient number for incoming messages.
- **Connection speed:** Select the supported speed of your modem in the dropdown menu

Once you have entered the information, select the correct device initialization for your modem. This is important for sending messages and receiving message statuses. With an incorrect value, you cannot send messages or receive delivery reports. The message status will always be buffered in this case. The other values can be left unchanged.

After saving, Enterprise Alert® will try to connect to the device. If all values and settings are correct, you will automatically switch to the SMS-MMS connection overview and the signal quality is displayed. If the status shows an error, recheck your settings.

In case the GSM/GPRS device could not be activated, please check the following:

- Have you connected the GSM device to the computer?
- Has the COM port that the GSM device is connected to been activated?
- Has the GSM device been switched on?
- Is there a SIM card in the GSM device?
- Have you entered the correct PIN for the SIM card in the GSM device?

5.5 Integration in 3rd party Systems

5.5.1 Integration in System Center Operations Manager (SCOM)

Enterprise Alert® provides a smart connector for System Center Operations Manager (SCOM).

This connector supports the following versions:

- System Center Operations Manager 2007 R2
- System Center Operations Manager 2012 R2
- System Center Operations Manager 2016
- System Center Operations Manager 1801

The connector's integration into System Center is based on the System Center SDK (SCOM 2012) and the SCOM Web Service (SCOM 2007).

The bidirectional integration the connector provides allows Enterprise Alert® to retrieve and also update alerts, including owner, status and history. Additionally, all SCOM alert parameters are available in Enterprise Alert®.

The connector supports multiple connections, even to different SCOM server versions.



Depending on which server version you want to connect to, the configuration steps will vary. Below, we will guide you through the setup of a connection for each SCOM version.

System Center Operations Manager 2007 R2

The basic SCOM 2007 integration setup workflow is:

- Ensure that the OMCF Web service is installed on the System Center server
- Add the run-as account of the SCOM Connector Windows service to the "Operations Manager Admins" group in the SCOM Admin Console
- Configure a SCOM connection in Enterprise Alert®
- Set up a subscription for the connector in SCOM
- Create Alert Policies in Enterprise Alert® for events received from SCOM

The following steps will guide you through the initial setup process.

By default, the OMCF Web service is installed with System Center Operations Manager 2007 R2. If the Web service was not installed during your SCOM setup, you can install it manually using the "System Center Operations Manager 2007 R2 Connectors" redistributable package, which can be downloaded here:

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=592e4143-c5c8-4270-9a7a-cd0a31ab3189&displaylang=en>

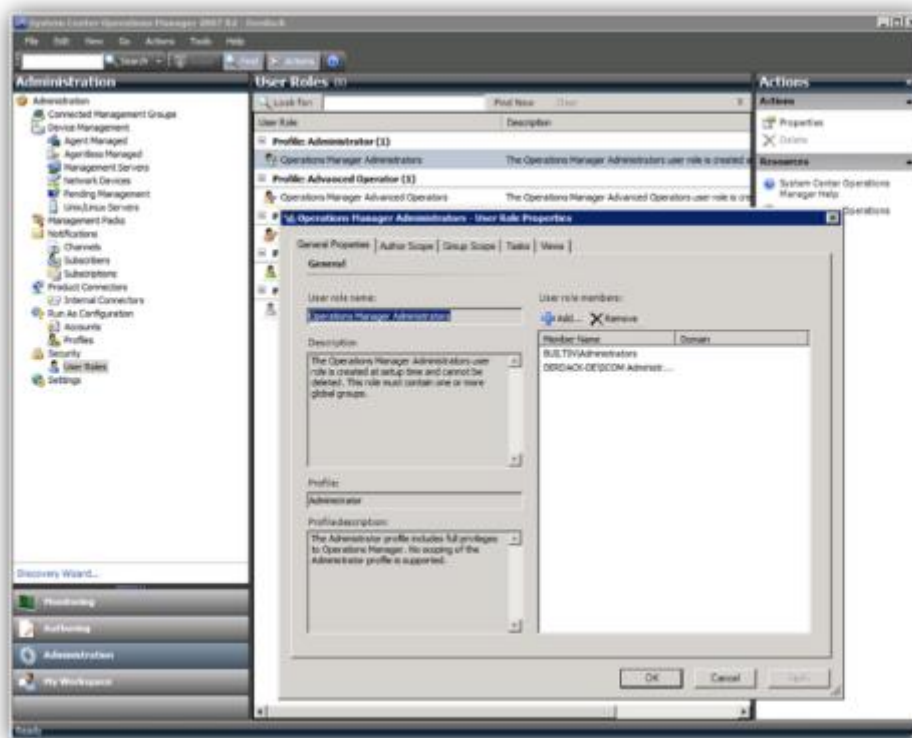
Once you have downloaded it, run the Universal Connector setup to install the OMCF Web service.



The SCOM connector Windows service runs under the Enterprise Alert® server's LOCAL_SYSTEM account by default. Changing this is not recommended. However, if you wish to use a different account, you will need to grant this account full access to the following:

- Enterprise Alert® installation folder
- Enterprise Alert® database
- *mmmomconnector* message queues in MSMQ

In the System Center Operations Manager Admin Console, add the account the connector is using to the "Operations Manager Administrators" group.



Open [System > Event Sources](#) in the Web portal of Enterprise Alert® to configure the connection to SCOM. Select "New Source" at the bottom of the screen, and select System Center Operations Manager as the Source Type. Enterprise Alert® ships with preconfigured connections. You can either modify one of these or create a new one from scratch.

New Source

Source Type *

System Center Operations Manager ▼

Activated

Name *

orvax

Product Connector Name *

Enterprise Alert®

Operations Manager Version *

2 - SCOM 2007, 2007 R2 ▼

Connector Framework URL *

http://orvax:51905/ConnectorFramework

System Center Data Access Service Run-As Account *

2 - Domain Account ▼

Connector Framework UPN *

bormann@derdack-de.local

Alert polling interval in ms.

2000

Language Code *

ENU

Alert update tolerance in ms.

110

The following connection properties must be set for a valid SCOM connection:

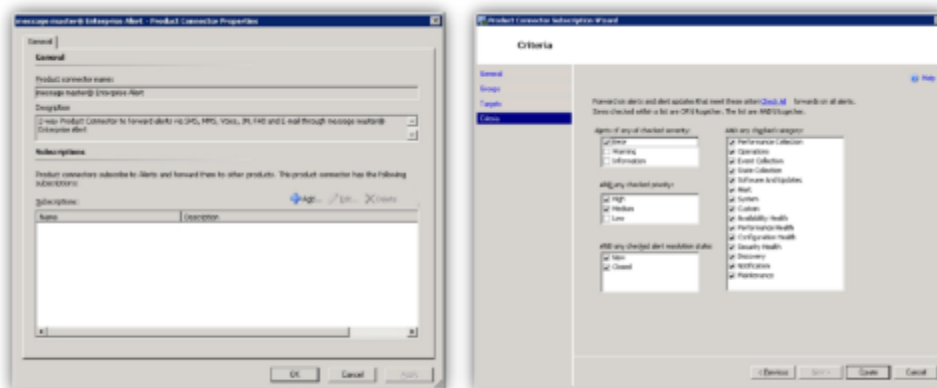
- **Connection name:** A unique name identifying the connection in Enterprise Alert®
- **Connector Framework URL:** The URL where the OMCF Web service listens; by default <http://scomhost:51905/ConnectorFramework>
- **System Center SDK Service Account Type:** The type of account the *OpsMgrSDKService* is running under
- **Language Code:** ENU for United States English
- **UPN/SPN:** Depending on the previous selection, either UPN or SPN must be configured.
For SPN enter *host/scomhost.domain.local*
For UPN enter the UPN of the domain account used i.e. scomuser@domain.local

After saving the configuration, the connector will attempt to connect to the OMFC and register itself in SCOM. If this is successful, a Product Connector GUID will be returned and displayed in the configuration settings. The connector will then also be listed in the SCOM Operations Console.



If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.

Set up a subscription for the created connector in the SCOM Operations Console and select which alerts should be forwarded to Enterprise Alert®.



You now have successfully configured Enterprise Alert® integration into System Center Operations Manager 2007 R2. You should now create Alert Policies to set up alerting for events received from SCOM.

System Center Operations Manager 2012, 2012R2, 2016 and 1801

The basic integration setup workflow is:

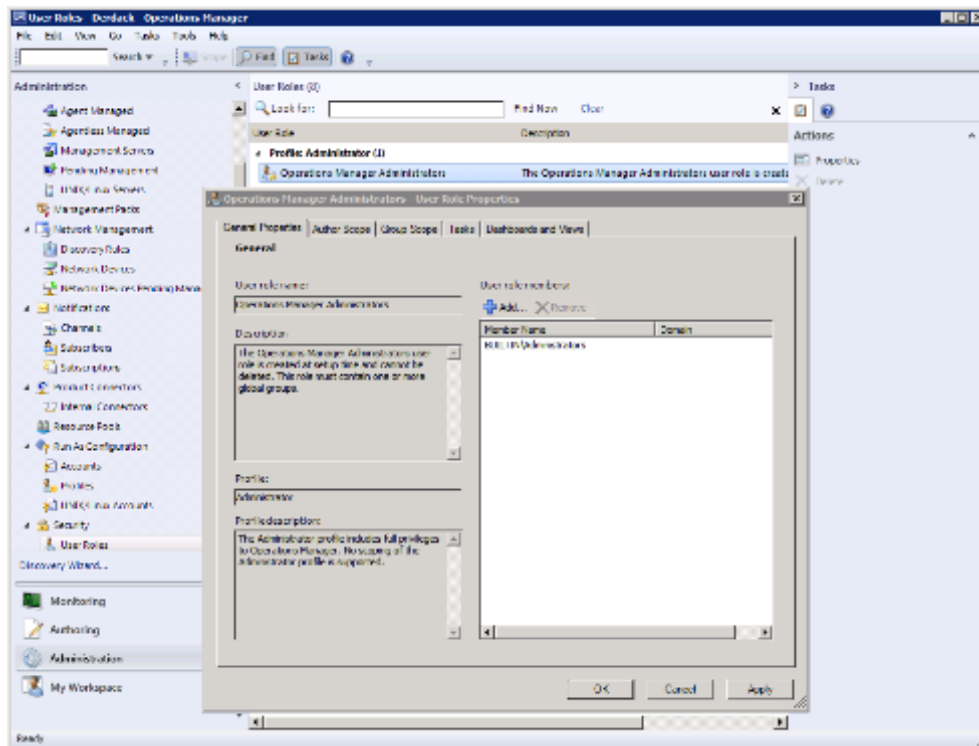
- Ensure that the SCOM Console is installed on the Enterprise Alert® server
- Configure a domain account for Enterprise Alert® to access SCOM
- Configure a SCOM connection in Enterprise Alert®
- Create Alert Policies in Enterprise Alert® for events received from SCOM

The following steps will guide you through the initial setup process.

Since the System Center SDK is only shipped by Microsoft as part of the System Center console and cannot be redistributed, you have to manually install the console on the Enterprise Alert® server.

Restart the SCOM connector Windows service after the console installation for it to load the SDK.

You need to either create a dedicated domain account or use an existing account to enable Enterprise Alert® to access System Center Operations Manager. You will also need to make this account an Administrator in SCOM.



Open [System > Event Sources](#) in the Web portal of Enterprise Alert® to configure the connection to SCOM. Enterprise Alert® ships with preconfigured connections. You can either modify one of these or create a new one from scratch. To create a new, one simply select New Source from the action bar, and choose System Center Operations Manager as the Source Type.

New Source

Activated

Name *

Product Connector Name *

Operations Manager Version *

Operations Manager Server *

Operations Manager Access Credentials *

Domain *

Username *

Password *

Alert polling interval in ms.

Change Resolution State on Acknowledgement
 Resolution State for Acknowledged Alerts

Change Resolution State on Closure
 Resolution State for Closed Alerts

Page Size

The following connection properties must be set for a valid SCOM connection:

- **Name:** A unique name identifying the connection in Enterprise Alert®
- **Product Connector Name:** This is the connector name used for the connection in SCOM itself. If the connector name already exists in SCOM, it will be reused, otherwise a new product connector will be installed

- **Operations Manager Version:** This configuration property defines the version of Operations Manager in which to integrate Enterprise Alert®.
- **Operations Manager Server:** Hostname of the Management Server
- **Operations Manager Access Credentials:** Select which credentials this source should use when accessing System Center Operations Manager.
- **Domain:** Enter the domain of the account used to access System Center Operations Manager.
- **Username/Password:** Enter the account credentials of the configured domain account here. The password provided here is encrypted when saved.

After saving the configuration of the product connector, a default subscription forwarding ALL alerts to Enterprise Alert® will be installed in SCOM, if one does not exist already.

If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.

You now have successfully configured Enterprise Alert® integration into System Center Operations Manager 2012. You should now create Alert Policies to set up alerting for events received from SCOM.

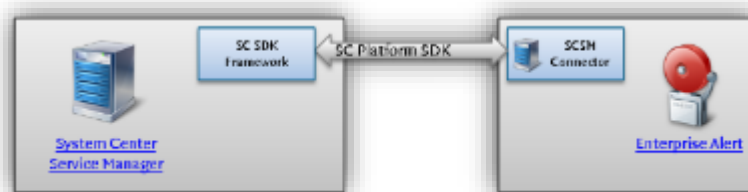
5.5.2 Integration in System Center Service Manager (SCSM)

The Enterprise Alert® integration for System Center Service Manager 2012 provides support for incident related alerting scenarios, from SLO warnings and end user notifications to analyst assignments.

Enterprise Alert's Remote Actions also enable you to log incidents through UC channels (Voice-Calls, Emails and SMS) or even more conveniently by means of your smartphone.

Enterprise Alert® integration consists of two different components:

- A SCSM smart connector
- A Management Pack for SCSM – which contains activities to forward incidents to Enterprise Alert®



The basic SCSM integration setup workflow is:

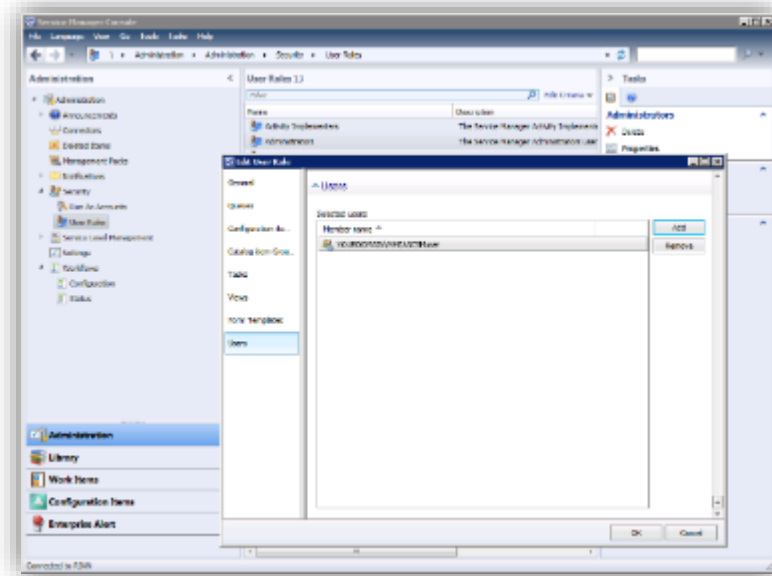
- Ensure that the SCSM Console is installed on the Enterprise Alert® server
- Configure a domain account for Enterprise Alert® to access SCSM
- Configure a SCSM connection in Enterprise Alert®
- Create Alert Policies and Remote Action Policies in Enterprise Alert® covering your SCSM scenarios

The following steps will guide you through the initial setup process.

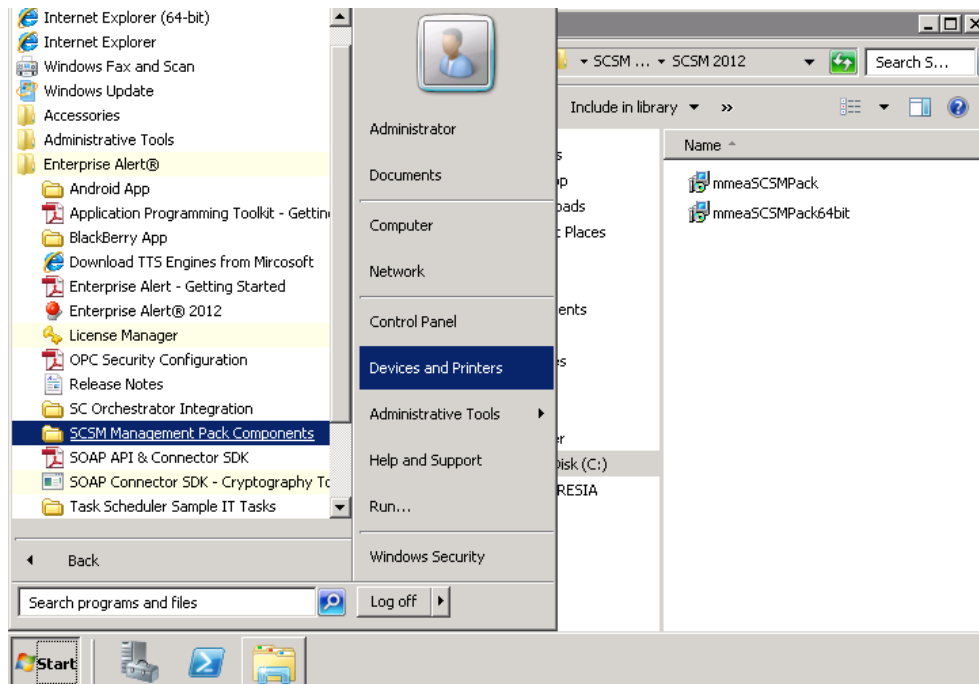
Since the System Center SDK is only shipped by Microsoft as part of the System Center console and cannot be redistributed, you have to manually install the console on the Enterprise Alert® server.

Restart the SCSM connector Windows service after the console installation for it to load the SDK.

You need to either create a dedicated domain account or use an existing account to enable Enterprise Alert® to access System Center Service Manager. You also need to make this account an Administrator in SCSM.



Install the Enterprise Alert® SCSM Management Pack on the System Center Service Manager host. The Installation packages can be found in the associated folder in the Enterprise Alert® host Start menu.



Open [System > Event Sources](#) in the Web portal of Enterprise Alert® to configure the connection to SCSM. Select 'New Source' on the action bar, then select System Center Service Manager as the Source Type.

New Source

Activated

Name *

Connector Name *

Service Manager Server *

Service Manager Version *

Service Manager Access Credentials *

Domain *

Username *

Password *

Enterprise Alert® Portal Url *

Resolution Classification

Incident Status on Alert Acknowledgement

Incident Status on Alert Resolution

Polling Interval (ms)

The following connection properties must be set for a valid SCSM connection:

- **Name:** A unique name identifying the connection in Enterprise Alert®
- **Product Connector Name:** This will be the connector name under which the connection will be visible in SCSM.
- **Service Manager Server:** Hostname of the Management Server

- **Service Manager Version:** This configuration property defines the version of Service Manager in which to integrate Enterprise Alert®.
- **Enterprise Alert® Portal Url:** Enter the URL under which the Enterprise Alert® portal can be accessed. By default this would be <http://eahost/EAPortal>

Other optional configuration settings allow you to change the way the smart connector modifies incidents when the alert status changes or how the Enterprise Alert® portal is displayed in SCSM.

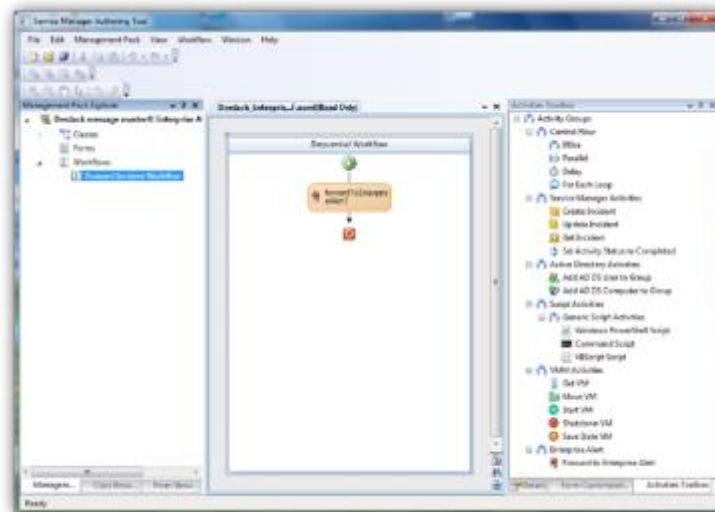
If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.

You now have successfully configured Enterprise Alert® integration into System Center Service Manager 2012.

There are two ways to forward incidents to Enterprise Alert®:

- Manually clicking an Enterprise Alert® action in the System Center console
- Setting up a workflow to automatically forward incidents using the Enterprise Alert® workflow actions

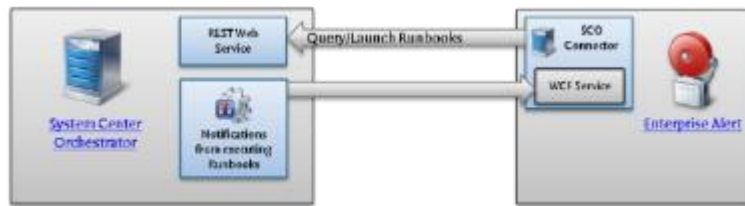
Events received from SCSM will have an *EANotificationWorkflow* parameter, allowing you to trigger the correct notification workflow in your Alert Policies.



5.5.3 Integration in System Center Orchestrator (SCO)

Enterprise Alert® provides integration with System Center Orchestrator. This integration enables you to send notifications from of Orchestrator Runbooks and to remotely initiate Runbooks through UC channels and the Enterprise Alert® smartphone apps.

This integration uses the SCO REST Web service and a custom Enterprise Alert® Integration Pack (IP).

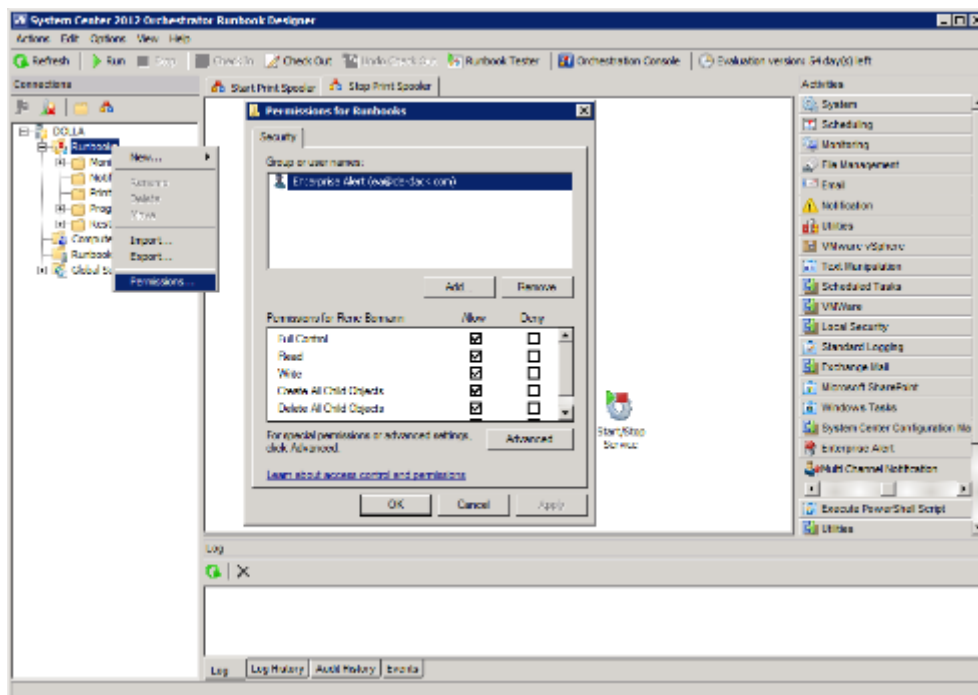


The basic SCO integration setup workflow is:

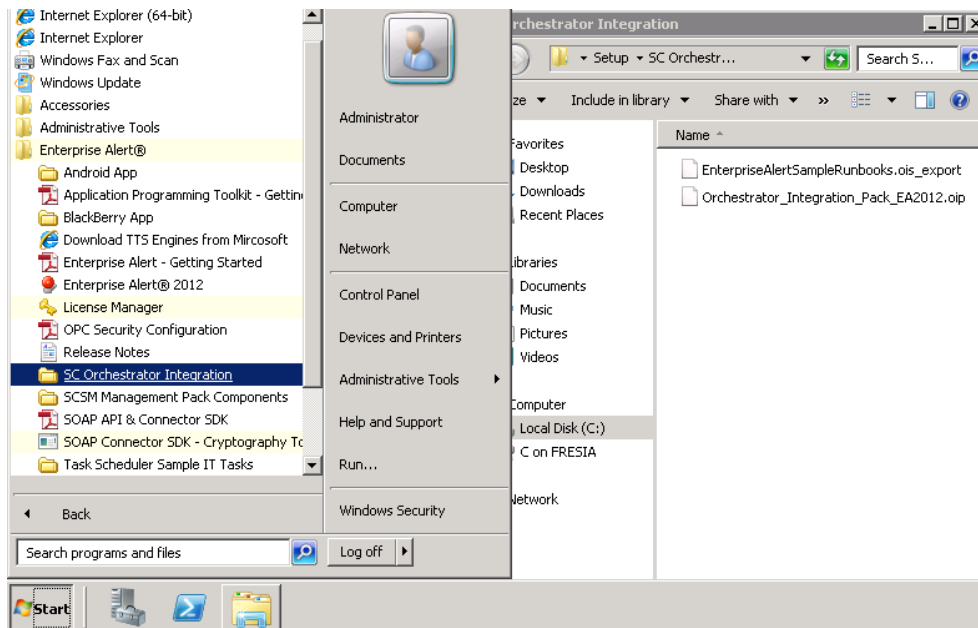
- Configure a domain account for Enterprise Alert® to access SCO
- Deploy the Enterprise Alert® IP on the SCO host
- Configure a SCO connection in Enterprise Alert®
- Configure the Enterprise Alert® IP in SCO
- Create Alert Policies and Remote Action Policies in Enterprise Alert® covering your SCO scenarios

The following steps will guide you through the initial setup process.

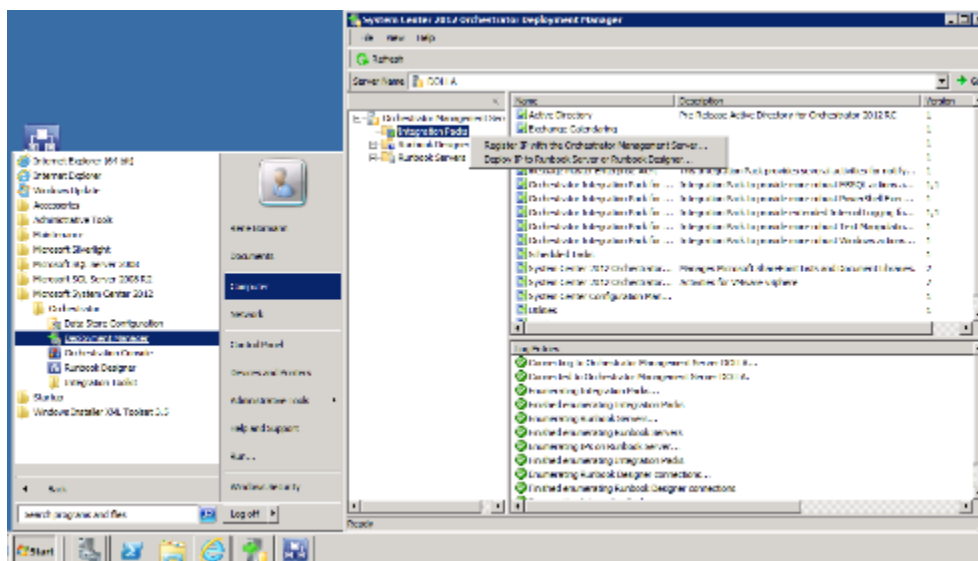
You need to either create a dedicated domain account or use an existing account to enable Enterprise Alert® to access System Center Orchestrator. Grant the account permissions to read and execute SCO Runbooks by adding the account to the *OrchestratorUsersGroup* on the SCO host.



Deploy the Enterprise Alert® SCO Integration Pack on the System Center Orchestrator host. The file can be found in the associated folder in the Enterprise Alert® host Start menu.



Using the Deployment Manager of SCO, register and deploy the Enterprise Alert® IP with the Management Server and make it available to all SCO Runbook Designers you need to use it with.



Open [System > IT Automation](#) in the Web portal of Enterprise Alert® to configure the connection to SCO. Then select New Connection from the action bar at the bottom of the screen, and choose System Center Orchestrator as the Connection Type.

New Connection

Connection Type *
System Center Orchestrator

Activated

Name *
SCO 2012 Connector

Orchestrator WebService URL *
<http://host:81/Orchestrator2012/Orchestrator.svc>

Local Listening Port *
59672

Orchestrator Access Credentials *
1 - Enter Access Credentials

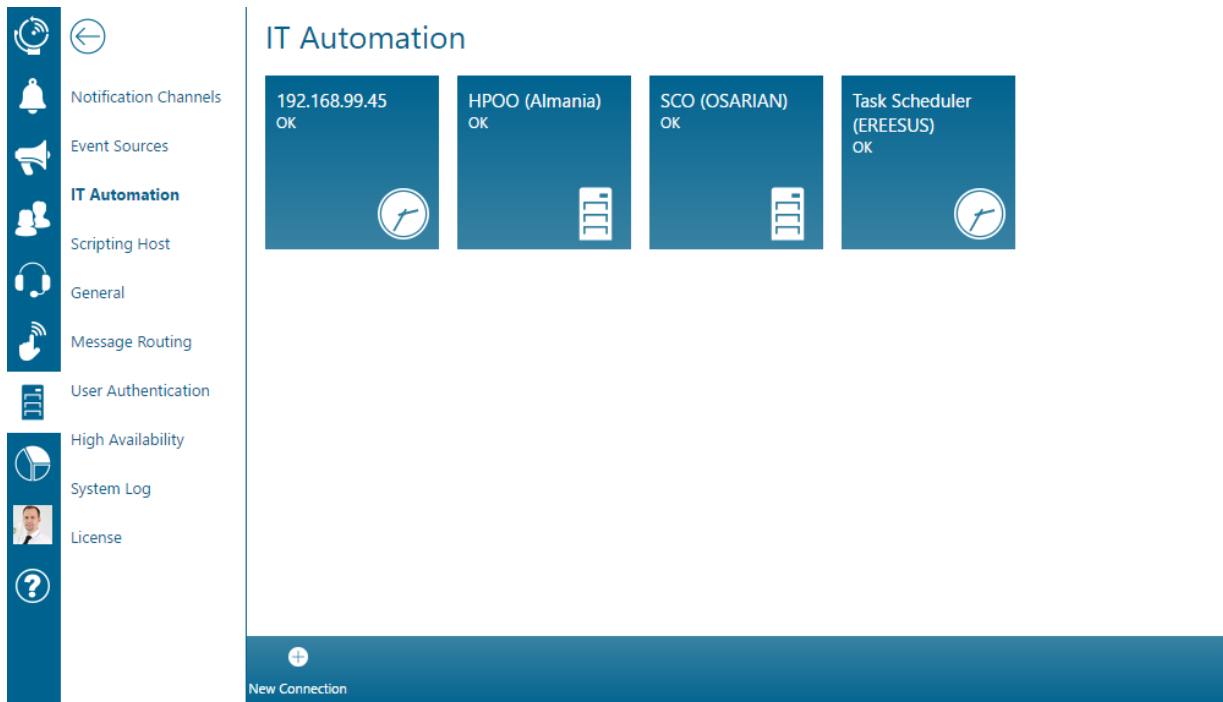
Domain *
derdack-de

Username *
bormann

Password *

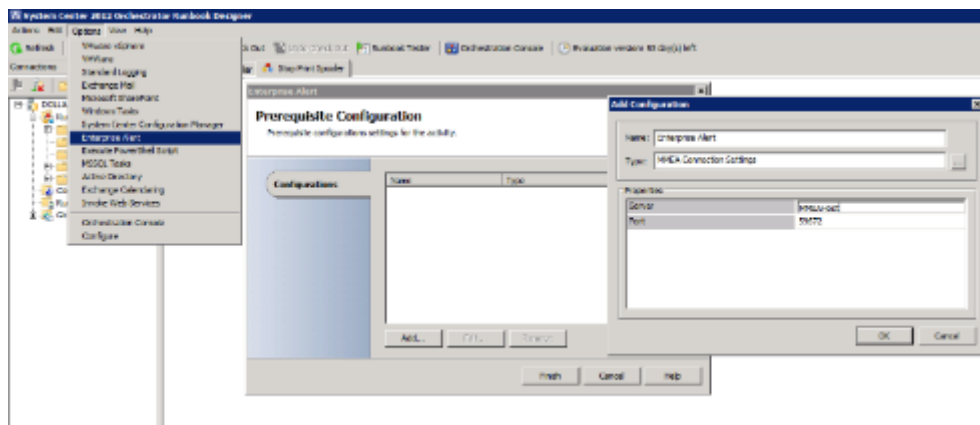
The following connection properties must be set for a valid SCO connection:

- **Name:** A unique name identifying the connection in Enterprise Alert®
- **Orchestrator Web Service URL:** The URL of the Orchestrator Web service; by default <http://<host>:81/Orchestrator2012/Orchestrator.svc>
- **Local Listening Port:** This port is used by the Enterprise alert® SCO smart connector to listen for events initiated from SCO IP activities. Please ensure that this port is not already in use or blocked by a firewall.
- **Orchestrator Access Credentials:** Select which credentials this source should use when accessing Orchestrator.
- **Domain:** Enter the domain name of the user account you configure below.
- **Username/Password:** Enter the account credentials of the configured domain account here. The password provided here is encrypted when saved.



If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.

To finish the setup, add a new connection configuration for Enterprise Alert® on the SCO Management Server (Options > Enterprise Alert). Enter the name of the Enterprise Alert® host and the previously configured port here.



You have now successfully configured Enterprise Alert® integration into System Center Orchestrator 2012.

The integration will now import all Runbooks flagged with the "Flag for Mobile Execution" activity from the Enterprise Alert® IP and make them available for use in Remote Actions. You can now create your Remote Action Policies to enable the remote execution of these Runbooks.

5.5.4 Integration IBM Tivoli Monitoring (ITM)

Enterprise Alert® provides a smart connector for dedicated integration with IBM Tivoli Monitoring (ITM). The connector is SOAP-based and communicates with the ITM Web service.

The basic ITM integration setup workflow is:

- Ensure the ITM Web service is installed on the ITM Hub Server
- Configure a domain account for Enterprise Alert® to access ITM
- Configure a ITM connection in Enterprise Alert®
- Create Alert Policies in Enterprise Alert® for events received from ITM

The following steps will guide you through the initial setup process.

Ensure that this Web service is installed on the ITM Hub Server. Refer to the ITM documentation for more information on how to install this Web service.

You need to configure a dedicated domain account to enable Enterprise Alert® to access IBM Tivoli Monitoring. This account requires full access privileges to the ITM Web service.

Open [System > Event Sources](#) in the Web portal of Enterprise Alert® to configure the connection to ITM. Then click New Source on the action bar at the bottom of the page, then select IBM Tivoli Monitoring as the Source Type.

The screenshot shows the 'New Source' configuration page. The sidebar on the left contains navigation icons and labels: Notification Channels, Event Sources (highlighted), IT Automation, Scripting Host, General, Message Routing, User Authentication, High Availability, System Log, License, and a help icon. The main content area is titled 'New Source' and contains the following fields and options:

- Source Type ***: IBM Tivoli Monitoring (dropdown menu)
- Activated**: A toggle switch is turned on.
- Name ***: New ITM Connection (text input)
- Hub Server ***: http://Host:1920///cms/soap (text input)
- Remote Hub Alias**: (empty text input)
- Username ***: Username (text input)
- Password ***: Password (password input field)
- Poll Events Without Situation**: (checkbox, unchecked)
- Handle Events With Latest Status ***: 1 - Off (dropdown menu)
- Network Connection Timeout (ms)**: (empty text input)
- Save**: A button at the bottom of the form.

The following connection properties must be set for a valid ITM connection:

- **Name**: A unique name identifying the connection in Enterprise Alert®
- **Hub Server**: This URL of the Hub Monitoring Server where the SOAP Web service is running; by default <http://<host>:1920///cms/soap>
- **Remote Hub Alias**: This property sets the alias of a remote Hub that has been configured in the Hub list. All SOAP requests will be forwarded to this Hub alias e.g. for the purpose of load balancing.
- **Username/Password**: Enter the account credentials of the configured domain account here. The password provided here is encrypted when saved.

With the remaining optional configuration settings, you can fine-tune the behavior of the ITM integration for the initial connection:

- **Poll Events without Situations:** This property activates or deactivates the polling of events that are not based on a situation. Such events can be created by the SOAP method "CT_Alert" and are an optional feature for administrators who would like to use custom scripts for submitting events to IBM Tivoli Monitoring. Such events do not have a "Started" status in the Global Status History.

Please note that if this property is not selected, the Connector will only poll situation-based events of type "sampled", "pure" and "hub".

- **Valid Event Sources:** This property is used to specify a comma-separated list of sources from where an event created via CT_Alert may originate. This is necessary for differentiating such events from situation-based events, since CT_Alert has no restrictions concerning the validity of events and their origin.
- **Event Closing Time:** The time in minutes after which an event without situation will be removed from the connector cache and closed by the connector inside ITM. This is necessary, because such events are not based on real agent probes and the user cannot close it manually. To poll an occurrence of the same event in short time periods, a value greater than "0" must be set. "0" means that such events will not be closed, which has the consequence of the connector not detecting multiple occurrences of the same event.

Please note that this property is only visible when "Poll Events without Situations" has been selected. All comma-separated source names must differ from existing monitoring server names or agent names to avoid conflicts.

- **Handle Events With Latest Status:** This property specifies that only situation-based events with the specified status should be handled.
 1. *Off* refers to the handling of events with the latest status being "Raised".
 2. *Both* refers to the handling of events that have the status "Raised", "Reopened" or "Expired" within the Tivoli Monitoring Enterprise.
 3. *Expired* enables the polling of events with status "Expired". Such events have already been acknowledged by a user in the past, but where the ITM event timeout period has been reached and event status set to expired, even though the situation rule is still true. An alert triggered for such events could be used as a reminder for situations whose rules are still true.
 4. *Reopened* refers to the polling of events with status "Reopened".

Please note that this property is only visible and applied when the *Event Handling Condition* option 2 or 3 has been selected. Setting the expiration time to zero means that acknowledged ITM events will never expire.

If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.

You now have successfully configured Enterprise Alert® integration IBM Tivoli Monitoring. You should now create Alert Policies to set up alerting for events received from ITM.

5.5.5 Integration in HP Operations Manager

Enterprise Alert® provides a smart connector for dedicated integration with HP Operations Manager. The connector communicates with HP Operations Manager using the Incident Web Service. The connector supports the following versions of HP Operations Manager:

- HP Operations Manager 8.1 for Windows or higher

- HP Operations Manager 8.3 for UNIX or higher
- HP Operations Manager i 9.10 or higher

The basic HPOM integration setup workflow is:

- Ensure the Incident Web Service is installed on the HPOM Management Server
- Configure a domain account for Enterprise Alert® to access HPOM
- Configure a HPOM connection in Enterprise Alert®
- Create Alert Policies in Enterprise Alert® for events received from HPOM

The following steps will guide you through the initial setup process.

HP Operations Manager for Windows installs the Web service during the Management Server installation by default. For the UNIX version, the Web service may have to be installed separately. Please refer to your HP Operations Manager documentation on how to do this.

You will need to configure a domain account for Enterprise Alert® to access HP Operations Manager. This account must have appropriate rights to perform the operations that the connector attempts (Query, Annotate, Own and Acknowledge). Usually, membership in the *Operators* or *Administrator* groups should fulfill those needs.

If the user you specify is an operator, the connector's permissions depend on the platform:

- *HP Operations Manager for UNIX*: The Connector has the same permissions as the operator would have in the Operations Manager console. For example, it returns only incidents that the operator would see as messages in the console.
- *HP Operations Manager for Windows*: The Connector may have more permissions than the operator would have in the Operations Manager console. In particular, any restrictions for user roles do not apply. The service can enumerate all messages and change messages that are not already owned by another user.

Open [System > Event Sources](#) in the Web portal of Enterprise Alert® to configure the connection to HPOM. Then click the 'New Source' button on the action bar at the bottom of the page, then select HP Operations Manager as the Source Type.

The following connection properties must be set for a valid HPOM connection:

- **Name**: A unique name identifying the connection in Enterprise Alert®
- **Polling Interval(ms)**: The interval in milliseconds in which the source queries information from ITM.
- **HP Operations Manager Version**: This configuration property sets the version of HP Operations Manager connection will connect to.
- **Hostname or Web service URL**: Host name of the machine where the Incident Web Service of HP Operations Manager is running. Usually the Management Server. You can also add the port or enter the complete URL of the Web service if it differs from the default location. Examples of valid inputs would be *Host*, *Host:Port* or *https://Host:Port/opr-webservice/Incident.svc* (OM) or *http:// Host:Port /omi/opr-console/rest* (OMi)
- **Username/Password**: Enter the account credentials of the configured domain account here. The password provided here is encrypted when saved.
- **Domain**: The domain or machine of the account to login to the Incident Web Service.

- **Notification Filter Setting:** This configuration property flags if the Product Connector should filter the incidents when polling the Incident Web Service. When this property is set to TRUE, only Incidents that are flagged as ForwardToNotification will be received. If set to FALSE, only Incidents not flagged as ForwardToNotification will be received. To receive all incidents no matter their ForwardToNotification flag, set this property to BOTH.
- **TroubleTicket Filter Setting:** This configuration property flags if the Product Connector should filter the Incidents when polling the Incident Web Service. When this property is set to TRUE, only incidents that are flagged as ForwardToTroubleTicket will be received. If set to FALSE, only Incidents not flagged as ForwardToTroubleTicket will be received. To receive all Incidents no matter their flag, set this property to BOTH.

Please note that depending on the Operations Manager version that you integrate with not all of the above listed parameters are displayed for configuration. Each version has its own set of configuration values which are displayed depending on the version that was selected.

If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.

You now have successfully configured Enterprise Alert® integration with HP Operations Manager. You should now create Alert Policies to set up alerting for events received from HPOM.

5.5.6 Integration in HP Network Node Manager (HP NNM)

Enterprise Alert® provides a smart connector for dedicated integration with HP Network Node Manager i. The connector communicates with HP NNMi using the Incident Web Service and is compatible with the following HP NNMi versions:

- HP NNMi 9.x or higher for Windows
- HP NNMi 9.x or higher for UNIX

The steps for integrating Enterprise Alert® with HP NNMi is as follows:

- Ensure the Incident Web Service is installed on the HP NNMi server
- Configure a new user account in HP NNMi for Enterprise Alert®
- Configure a new HP NNMi connection in Enterprise Alert®
- Create Alert Policies in Enterprise Alert® for events received from HP NNMi

Ensure the availability of the Incident Web Service

The Incident Web Service of HP NNMi is usually installed with the management server by default. To check the availability of the Web Service you can enter the following URL in a browser where you replace "nmsserver.yourdomain.com" with the FQDN of your NNMi server and adjust the port if need be:

<http://nmsserver.yourdomain.com:8004/IncidentBeanService/IncidentBean?wsdl>

If the WSDL file is displayed in the browser, the Incident Web Service is available for Enterprise Alert®.

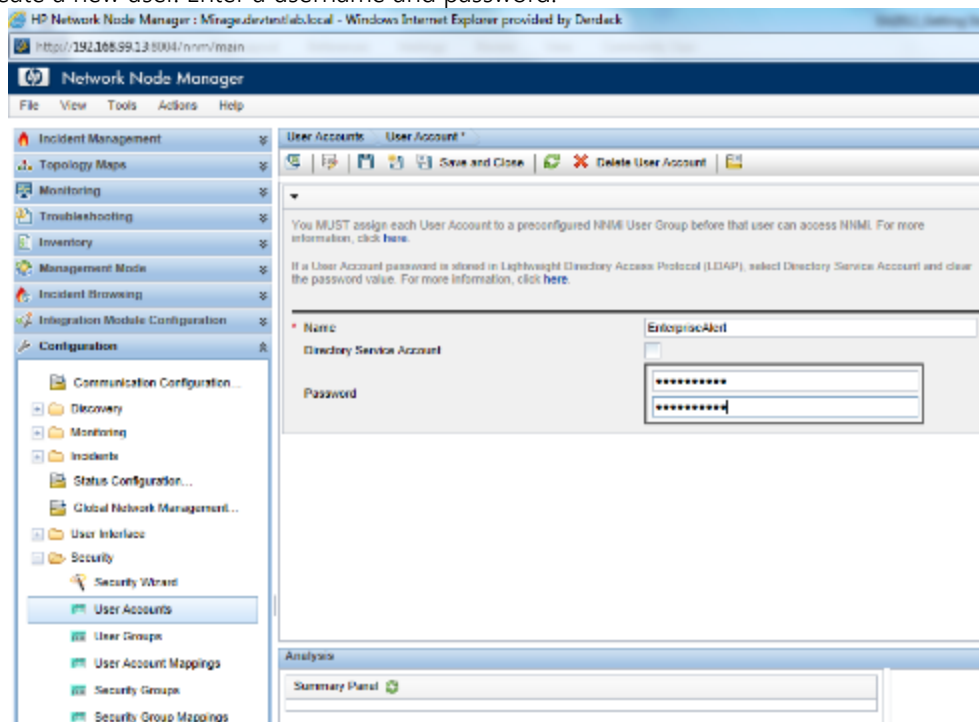
Otherwise please check your HP NNMi installation media and install the Web service on your HP NNMi server before proceeding.

```

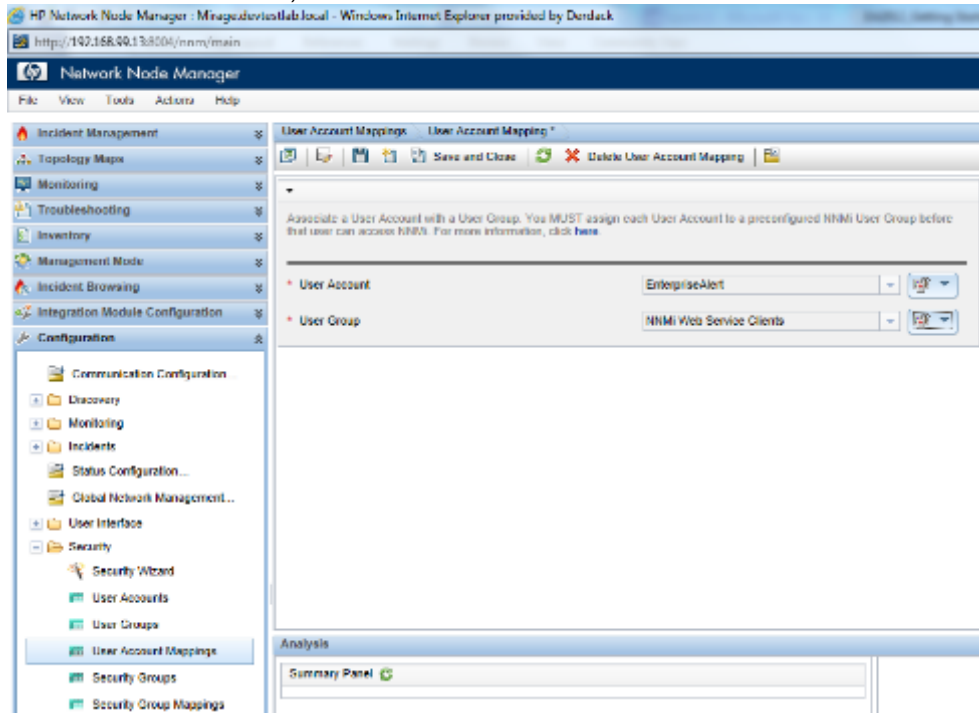
<-definitions name="IncidentBeanService" targetNamespace="http://incident.sdk.nms.ov.hp.com">
  <-types>
    <-xs:schema targetNamespace="http://incident.sdk.nms.ov.hp.com" version="1.0">
      <xs:element name="NmsIncidentFault" nillable="true" type="tns:NmsIncidentFault"/>
      <-xs:complexType name="incidentMgmtEvent">
        <-xs:sequence>
          <xs:element maxOccurs="unbounded" minOccurs="0" name="cias" nillable="true" type="tns:cia"/>
          <xs:element minOccurs="0" name="name" type="xs:string"/>
          <xs:element minOccurs="0" name="nature" type="tns:nature"/>
          <xs:element minOccurs="0" name="originOccurrenceTime" type="xs:dateTime"/>
          <xs:element minOccurs="0" name="priority" type="xs:string"/>
          <xs:element minOccurs="0" name="sourceName" type="xs:string"/>
          <xs:element minOccurs="0" name="sourceNodeName" type="xs:string"/>
          <xs:element minOccurs="0" name="sourceNodeUuid" type="xs:string"/>
          <xs:element minOccurs="0" name="sourceType" type="xs:string"/>
          <xs:element minOccurs="0" name="sourceUuid" type="xs:string"/>
          <xs:element minOccurs="0" name="uuid" type="xs:string"/>
        </xs:sequence>
      </xs:complexType>
      <-xs:complexType name="cia">
        <-xs:sequence>
          <xs:element minOccurs="0" name="name" type="xs:string"/>
          <xs:element minOccurs="0" name="type" type="xs:string"/>
          <xs:element minOccurs="0" name="value" type="xs:string"/>
        </xs:sequence>
      </xs:schema>
    </types>
  </definitions>

```

Configure a new user account in HP NNMi for Enterprise Alert®
 In this step, you add a new user account in HP NNMi that Enterprise Alert® then uses to access Network Node Manager. Open the NNMi Console and navigate to [Configuration -> Security -> User Accounts](#). Click [New](#) to create a new user. Enter a username and password:



Furthermore, the user account must become a member of the “NNMi Web Service Client” group. To create the membership open the NNMi Console and navigate to [Configuration -> Security -> User Account Mappings](#). Click on [New](#) to create a new mapping and associate the new user account with the “clients” group (“NNMi Web Service Clients”):



After you have created the user account and the user account mapping in HP NNMi, it is essential that you restart NNM. To do this, open your NNM server and run a `ovstop` followed by an `ovstart`. Only after the restart are the new credentials completely provisioned and available in NNM.

Configure a new HP NNMi connection in Enterprise Alert®

In this configuration step you create a new connection to your HP NNMi server in Enterprise Alert®.

Open [System > Event Sources](#) in the Web portal of Enterprise Alert® to configure the connection to HP NNMi.

Then click on the HPNNM tile:

The screenshot shows the configuration page for an HP NNMi connection named 'Kavado'. The connection is currently 'Activated'. The form fields are as follows:

- Name ***: HP NNMi (Kavado)
- Hostname or Webservice URL ***: http://kavado/IncidentBeanService/IncidentBean
- Username ***: EnterpriseAlert
- Password ***: [Redacted]
- Polling Interval (ms)**: 2000
- Incident Status for Closed Alerts ***: 3 - Closed

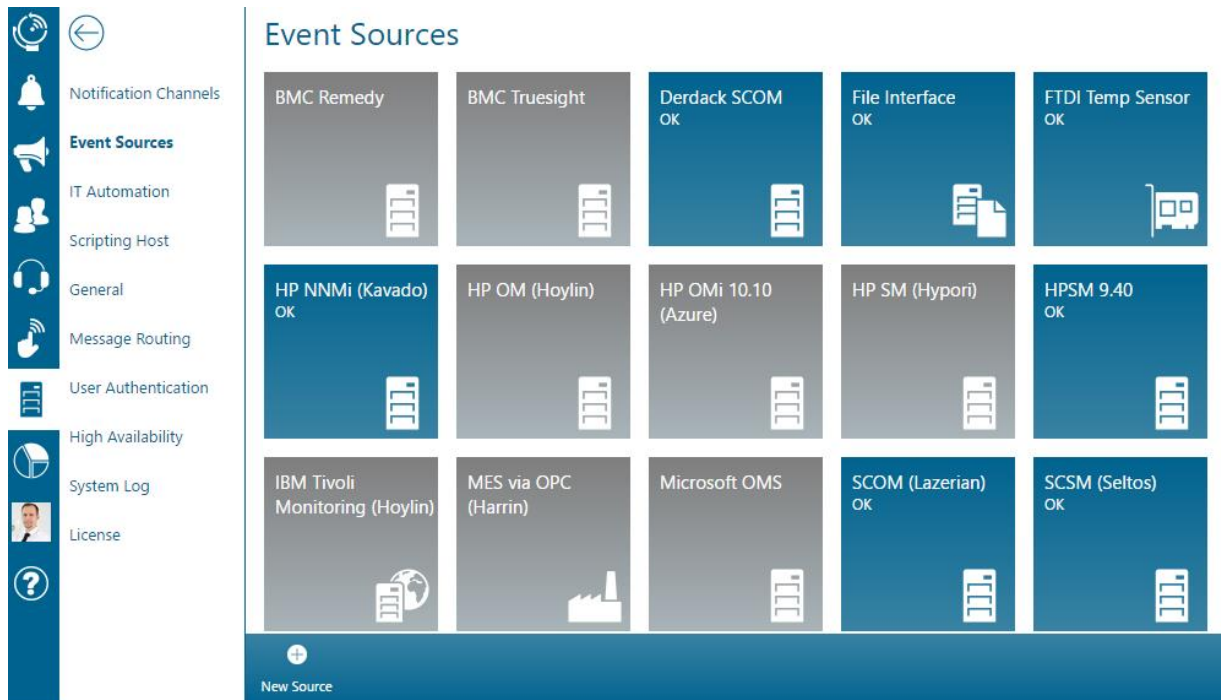
At the bottom of the form, there are 'Save' and 'Delete' buttons. A status box on the right indicates 'Status OK'.

The following connection properties must be set for a valid HP NNMi connection:

- **Activated:** Check this box in order to activate the connection.
- **Connection Name:** A unique name identifying the connection in Enterprise Alert®
- **Host:** Host name of the machine where the Incident Web Service of HP Network Node Manager is running. You can also add the port or enter the complete URL of the Web service if it differs from the default location.
- Examples of valid inputs would be *Host*, *Host:Port* or *http://Host:8004/IncidentBeanService/IncidentBean*
- **Account Credentials:** Enter the account credentials of the Enterprise Alert® user account that you created in HP NNMi. The password provided here is encrypted when saved.
- **Incident Status for Closed Alerts:** Select the status that Key Incidents in NNMi should get assigned by Enterprise Alert® when a user closes an alert. If you select "Completed", HP NNMi will not immediately raise new incidents for the underlying problem when the problem persists. However, if you select "Closed", HP NNMi will continuously recheck the incident conditions and may raise new incidents if the underlying problems still persists. Such new incidents will result in new alert notifications from Enterprise Alert®, which can be helpful in determining (remotely) whether the problem has really been fixed.

Click **Save** to create your new connection. Enterprise Alert® will afterwards attempt to connect to the Web service and query new key incidents.

If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.



You now have successfully configured Enterprise Alert® integration with HP Network Node Manager. You should now create Alert Policies to set up automated alerting for events received from HP NNMi.

Please refer to section 3.4 and 4.1.4 for further details about Alert Policies.

5.5.7 Integration in HP Service Manager (HPSM)

Enterprise Alert® provides a smart connector for dedicated integration with HP Service Manager. The connector communicates with HP NNMi using the Incident Web Service and is compatible with the following HPSM versions:

- HPSM 9.x or higher for Windows
- HPSM 9.x or higher for UNIX

The steps for integrating Enterprise Alert® with HPSM are as follows:

- Ensure the Incident Web Service is installed on the HPSM server
- Configure a new user account in HPSM for Enterprise Alert®
- Configure a new HPSM connection in Enterprise Alert®
- Create Alert Policies in Enterprise Alert® for events received from HPSM

Ensure the availability of the Incident Web Service

The Incident Web Service of HPSM is usually installed with the management server by default. To check the availability of the Web Service you can enter one of the following URLs in a browser where you replace "smserver.yourdomain.com" with the FQDN of your HPSM server and adjust the port if need be:

<http://smserver.yourdomain.com:13080/SM/7/IncidentManagement?wsdl>

<http://smserver.yourdomain.com:13080/sc62server/PWS/IncidentManagement?wsdl>

If either one or the other WSDL file is displayed in the browser, the Incident Web Service is available for Enterprise Alert®. Otherwise please check your HPSM installation media and install the Web service on your HPSM server before proceeding. You may also check your firewall configuration on the Enterprise Alert Server and the HPSM server to ensure that there are no ports blocked.

```

- <definitions targetNamespace="http://schemas.hp.com/SM/7" xsi:schemaLocation="http://schemas.xmlsoap.org/wsdl/ http://schemas.xmlsoap.org/wsdl/">
- <types>
- <xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
targetNamespace="http://schemas.hp.com/SM/7" version="2013-04-05 Rev 2">
  <xs:import namespace="http://www.w3.org/2005/05/xmlmime" schemaLocation="http://www.w3.org/2005/05/xmlmime"/>
  <xs:import namespace="http://schemas.hp.com/SM/7/Common"
schemaLocation="http://Mirage.devtestlab.local:13080/SM/7/Common.xsd"/>
- <xs:complexType name="IncidentKeysType">
- <xs:sequence>
  <xs:element minOccurs="0" name="IncidentID" nillable="true" type="cmn:StringType"/>
</xs:sequence>
  <xs:attribute name="query" type="xs:string" use="optional"/>
  <xs:attribute name="updatecounter" type="xs:long" use="optional"/>
</xs:complexType>
- <xs:complexType name="IncidentInstanceType">
- <xs:sequence>
  <xs:element minOccurs="0" name="IncidentID" nillable="true" type="cmn:StringType"/>
  <xs:element minOccurs="0" name="Category" nillable="true" type="cmn:StringType"/>
  <xs:element minOccurs="0" name="OpenTime" nillable="true" type="cmn:DateTimeType"/>
  <xs:element minOccurs="0" name="OpenedBy" nillable="true" type="cmn:StringType"/>

```

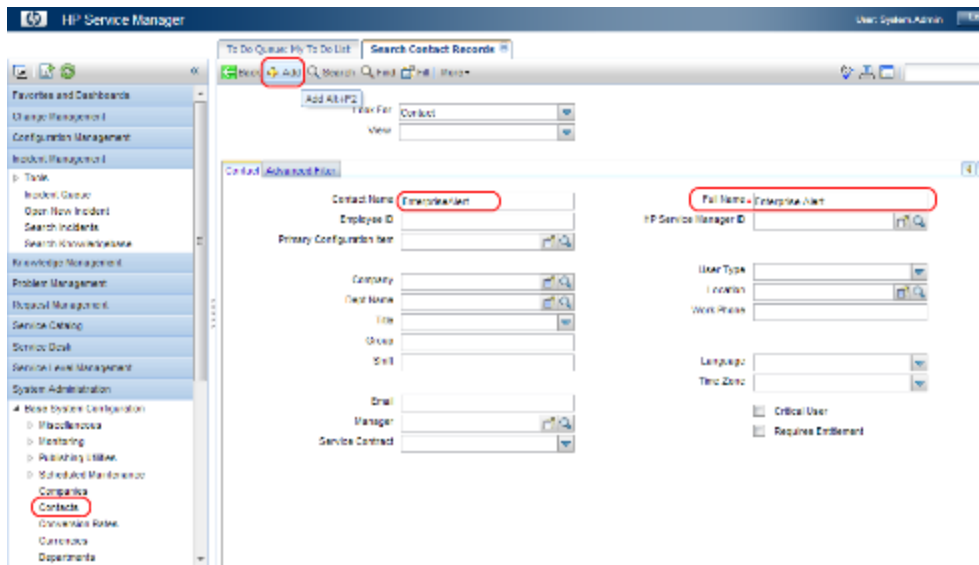
Configure a new user account in HPSM for Enterprise Alert®

In this step you add a new user account in HPSM that Enterprise Alert® then uses to access Service Manager.

In order to create the account you must first create a new *Contact* and afterwards a new *Operator* for that Contact.

To create a contact open the SM portal and navigate to [System Administration -> Base System Configuration -> Contacts](#). Enter "EnterpriseAlert" as contact name and "Enterprise Alert" as Full Name for the contact.

Afterwards click [Add](#):

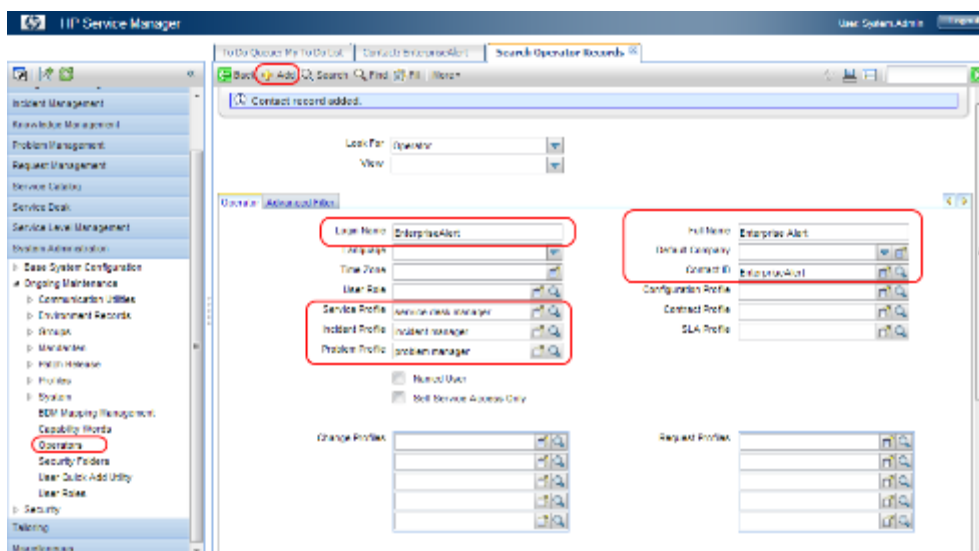


In order to create an *Operator* now, open the SM portal and navigate to [System Administration -> Ongoing Maintenance -> Operators](#). Enter "EnterpriseAlert" as login name and "Enterprise Alert" as Full Name for the Operator. Furthermore please make sure to set the following profiles for the new *Operator*:

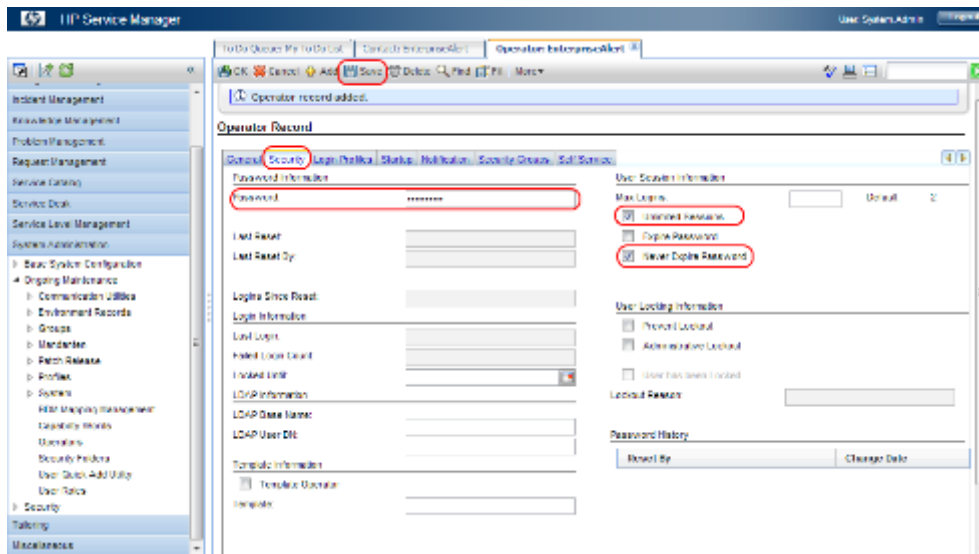
- Service Profile: "service desk manager"
- Incident Profile: "incident manager"
- Problem Profile: "problem manager"

Finally, please select "EnterpriseAlert" as contact ID for this new Operator.

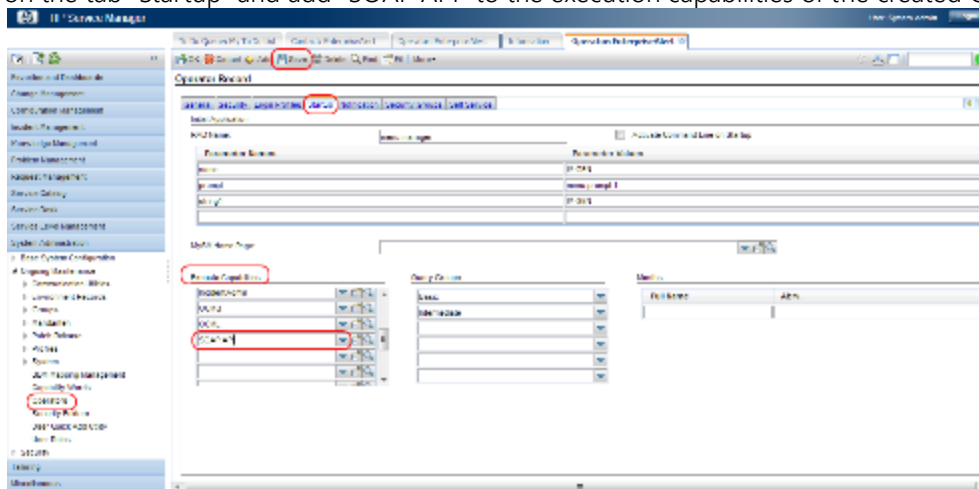
Afterwards click [Add](#) to create the new *Operator*:



After the new Operator has been created, click on its security tab and type in a password for the EnterpriseAlert account. Also ensure that you allow unlimited sessions for this account and that the password never expires:



Now click on the tab "Startup" and add "SOAP API" to the execution capabilities of the created Operator:



Afterwards click [Save](#) in order to save the new Operator account for Enterprise Alert.

Configure a new HPSM connection in Enterprise Alert®

In this configuration step, you create a new connection to your HPSM server in Enterprise Alert®.

Open [System > Event Sources](#) in the Web portal of Enterprise Alert® to configure the connection to HPSM.

[Edit](#) the default connection or click on [New Source](#) to configure a connection to HPSM, then select HP Service Manager as the Source Type:

Please enter the following configuration values and click Save to connect Enterprise Alert® to HPSM:

- **Activated:** Check this box in order to activate the connection.
- **Name:** A unique name identifying the connection in Enterprise Alert®
- **Hostname or Web service URL:** Enter the FQDN of the machine where the Incident Web Service of HP Service Manager is running. You can also add the port or enter the complete URL of the Web service if it differs from the default location.
Examples of valid inputs would be *Host*, *Host:Port* or *http://smsserver.yourdomain.com:13080/SM/7/IncidentManagement*
- **Username/Password:** Enter the account credentials of the Enterprise Alert® user account that you created in HPSM. Enter the login name and password of the Operator that you have created in the previous section.
- **Service Manager Date Format:** Please select or enter the Date Time format that your HPSM instance is working with. You can find out the active Date Time format in HPSM under [System Administration -> Base System Configuration -> Miscellaneous -> System Information Record -> Date Info](#).
- **Incident Status for Acknowledged Alerts:** Select the status that incidents in HPSM should get assigned by Enterprise Alert® when a user acknowledges an alert.
- **Incident Status for Closed Alerts:** Select the status that incidents in HPSM should get assigned by Enterprise Alert® when a user closes an alert.
- **Close Incident on Alert Closure:** Select whether the incident in HPSM should be closed when the corresponding alert in Enterprise Alert® is closed.

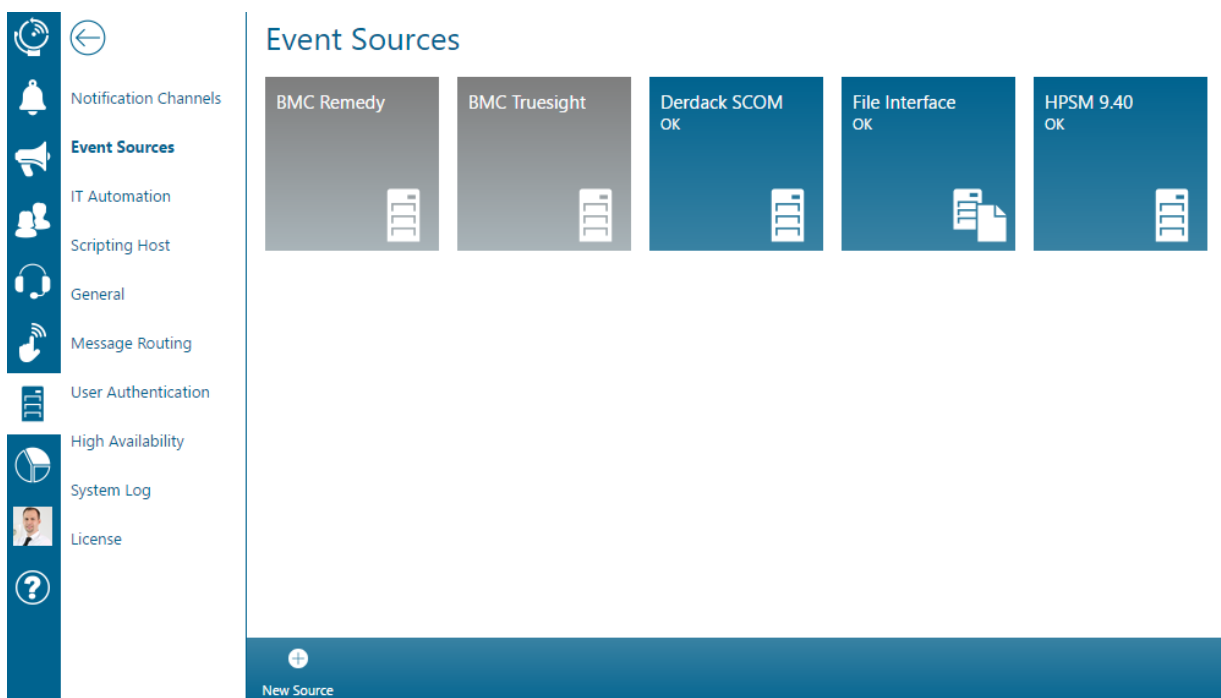
Please note that there is a difference between simply setting the status of the incident to *Closed* and closing the incident itself.

Once an incident is closed, no more changes may be made. Simply changing the status of the incident to *Closed* allows for further changes.

- **Incident Closure Code:** Select the closure code that should be set for an incident in HP Service Manager by Enterprise Alert® when a user closes an alert. If you leave this property blank, the closure code will not be set.
- **Polling Interval(ms):** The interval in milliseconds in which the Connector queries information from HP Service Manager.

Click **Save** to create your new connection. Enterprise Alert® will afterwards attempt to connect to the Web service and query new incidents.

If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.



You now have successfully configured Enterprise Alert® integration with HP Service Manager. You should now create Alert Policies to set up automated alerting for events received from HPSM.

Please refer to section 3.4 and 4.1.4 for further details about Alert Policies.

5.5.8 Integration in Windows Task Scheduler

Enterprise Alert® supports the Windows Task Scheduler as a provider for Remote Actions, enabling a wide range of possible actions. The Task Scheduler integration can connect to multiple remote hosts providing access to Task Schedulers beyond the server Enterprise Alert® is running on.

The basic Task Scheduler integration setup workflow is:

- Configure a domain account for Enterprise Alert® to access the Task Scheduler hosts

- Configure a Task Scheduler connection in Enterprise Alert®
- Create Remote Action Policies in Enterprise Alert®

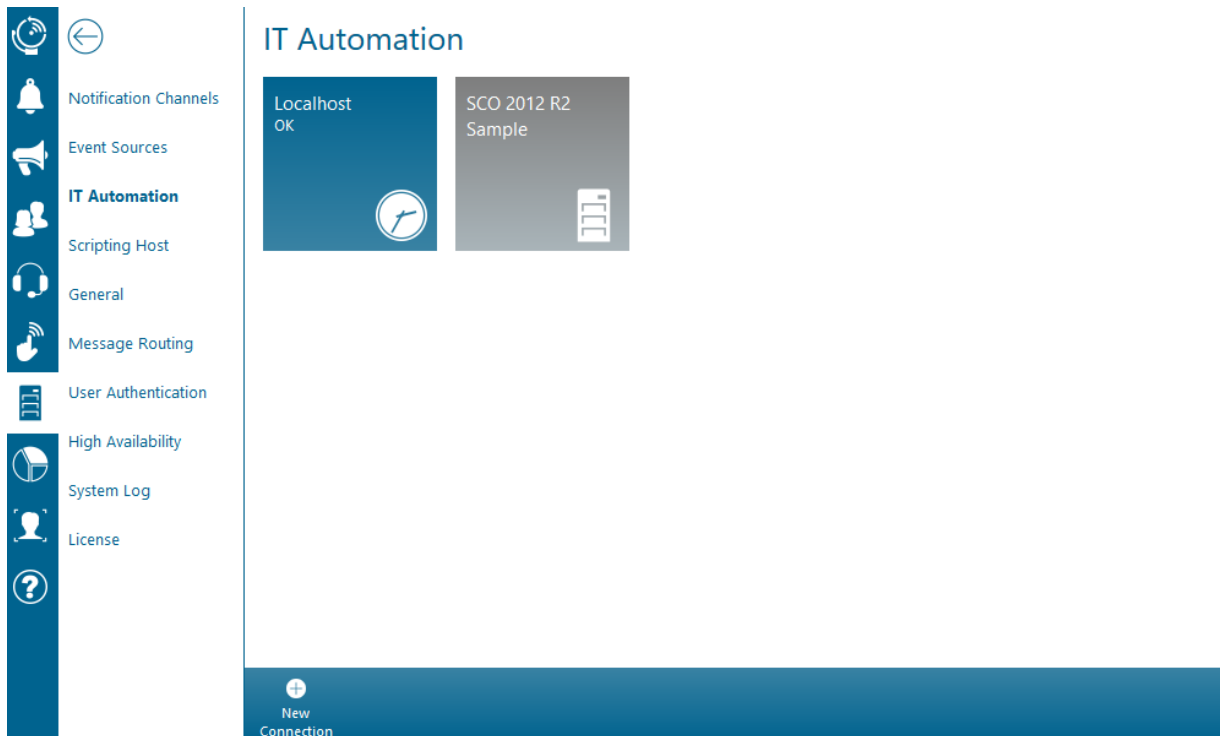
The following steps will guide you through the initial setup process.

You need to either create a dedicated domain account or use an existing account to enable Enterprise Alert® to access the Task Scheduler hosts. This account needs to be a local Administrator on the Enterprise Alert® host and also needs permissions to log in to all desired remote hosts.

Open [System > IT Automation](#) in the Web portal of Enterprise Alert® to configure the connection. Then either select an existing, or Create New at the bottom of the page. For the connection type select Windows Task Scheduler.

The following connection properties must be set for a valid Task Scheduler connection:

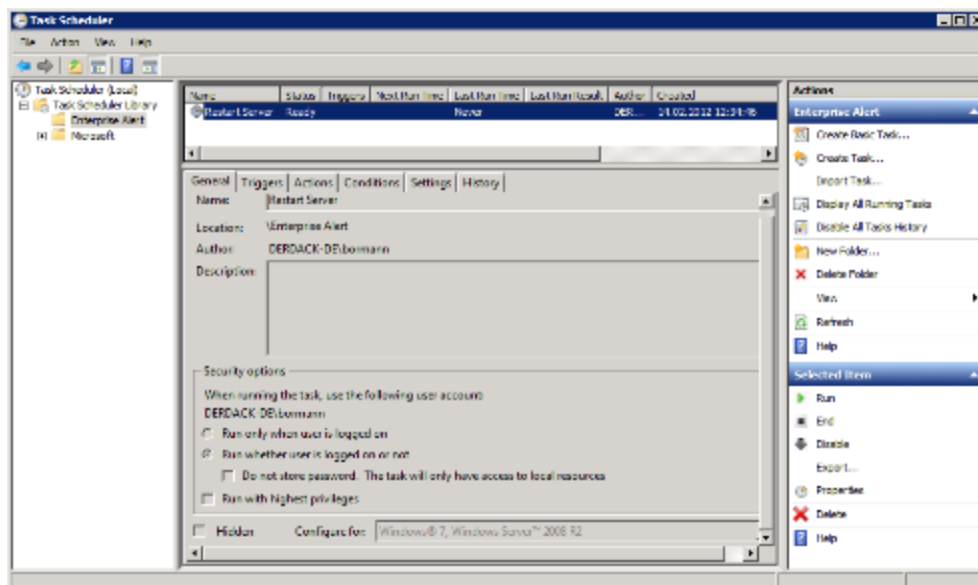
- **Computer:** Name or IP address of the Task Scheduler host you want to connect to
- **Name:** Name for the Task Scheduler Connection
- **Task Scheduler Version:** Which version of Windows Task Scheduler is being used?
- **Task Scheduler Access Credentials:** Choose which account to use for the service.
- **Root Folder in Task Scheduler:** Name of a folder in the Task Scheduler where Enterprise Alert® will import tasks from. If the folder does not yet exist, the connector will create it



If the connection has been configured correctly, the connection status will show 'OK'. Otherwise, a short error description will indicate the type of connection problem.

You now have successfully configured Enterprise Alert® integration into the Windows Task Scheduler. You should now create Remote Action Policies to trigger the tasks on the connected host.

Please note that the Enterprise Alert® connector will not actually log on to the host to start the tasks, so please ensure that the "Run whether user is logged on or not" option is checked for the tasks you want to execute.



5.5.9 Standard Interfaces

For 3rd party products where no dedicated smart connector is provided or where you would like to implement specialized custom scenarios, Enterprise Alert® also provides various Standard Interfaces.

The Standard Interfaces of Enterprise Alert® are:

- Command Line Interface (CLI)
- File Interface
- REST API
- SOAP API (Web Service)
- Serial Connector
- SMTP Server

Command Line Interface (CLI)

The Enterprise Alert® Command Line Interface (CLI) can be used to submit simple raw events (plain text) as well as parameterized events, which can then be evaluated in Alert Policies. It enables you to integrate custom systems into Enterprise Alert® that are able to execute a shell command to forward their events.

There are two versions of the CLI.

- The standard CLI which communicates directly with the Enterprise Alert® kernel and thus can only be used directly on the Enterprise Alert® server
- The remote CLI which communicates with Enterprise Alert® using the SOAP Web Service and can therefore be used from other systems to remotely generate events.

Both interfaces can be found here: %Program Files%/Enterprise Alert/CommandLine/

For more information on how to use the CLIs, you can use the '-?' parameter.

File Interface

Enterprise Alert® monitors a configurable folder in the file system. Files in this folder will be read and sent to the Enterprise Alert® kernel. The folder can either be on the local disks or on an UNC share.

Using the Enterprise Alert® XML schema in these files allows you to create incoming messages and events which can be evaluated in Alert Policies.

Sample files can be found in the Enterprise Alert® folder.

To configure the File Interface, open [System > Event Sources > File Interface](#) in the Enterprise Alert® Web portal.

The screenshot shows the 'File Interface' configuration page. On the left is a sidebar with navigation icons and labels: Notification Channels, Event Sources (highlighted), IT Automation, Scripting Host, General, Message Routing, User Authentication, High Availability, System Log, License, and a help icon. The main content area is titled 'File Interface' and contains the following settings:

- Activated:** A toggle switch that is currently turned on.
- Directory *:** A text input field containing the value 'FileInterface'.
- Polling interval in seconds *:** A text input field containing the value '10'.

At the bottom of the configuration area, there is a 'Save' button.

The following configuration settings are available:

- **Directory:** Path to the folder to be monitored
- **Polling Interval:** Interval in which Enterprise Alert® will check the folder for new files
- **Username/Password required:** When this option is set, Enterprise Alert® will ignore XML files without valid Enterprise Alert® user credentials

REST API

The REST API can be used to submit events to Enterprise Alert® via HTTP REST requests. The API provides a fully flexible interface with support for request contents in JSON format, XML format or Plain/Text.

The default URL of the REST API is <http://<host>/EAWebService/Rest/events>

Before you can send events through the REST API, you need to register a new Event Source of type "REST API Client" in Enterprise Alert®. To register such REST API Client, open [System > Event Sources](#) in the Enterprise Alert® Web Portal, click "Create New" from the action bar and select "REST API Client" as "Source Type". Now specify a name for your provider, copy the generated API key to the clipboard and press "Save".

(The API key is later used to authenticate your client requests and to assign the requests to your provider.)

New Source

Source Type *
REST API Client

Activated

Name *
My Rest Provider

API Key *
q401ohr8t3lnzbida2w2xztqpac8xuto Generate New Copy

Detailed documentation of the REST API can be found here:
[REST API Documentation](#)

Name	Path	Value of Last Event	External ID
There are currently no items.			

+

Save

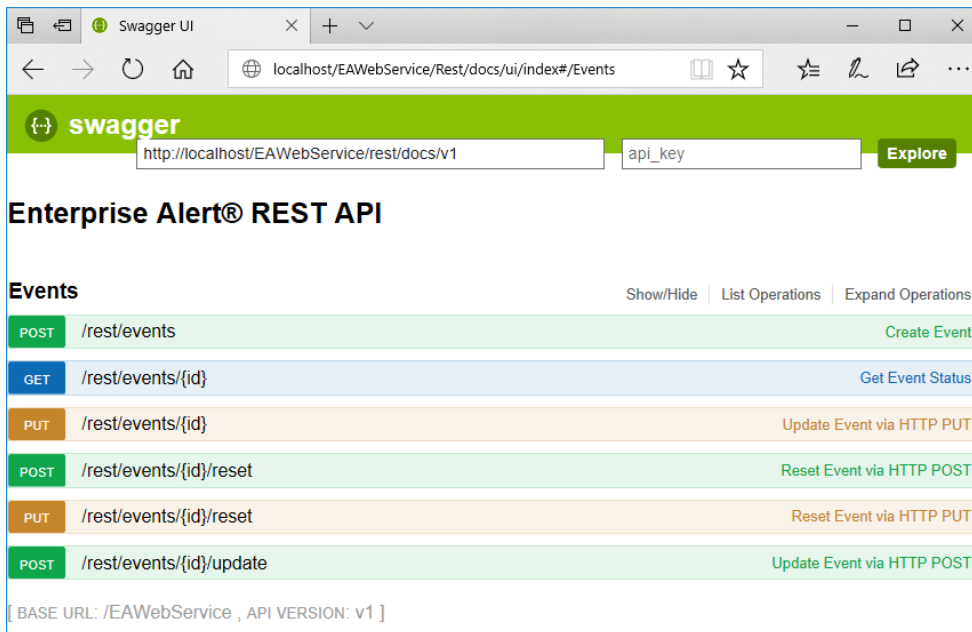
In the next step configure the target URL <http://<host>/EAWebService/Rest/events> in your client application and enable it to use one of the following supported mechanisms for providing the API Key:

1. HTTP Basic Authentication: If your REST client supports HTTP Basic Authentication, then use "ApiKey" as username and as password the value of your Api Key.
E.g.: *q401ohr8t3lnzbida2w2xztqpac8xuto*
2. Api Key Authorization: By this option your client requests need to contain an HTTP header named "Authorization" followed by the scheme "APIKey" and the value of your Api Key.
E.g.: *Authorization: APIKey q401ohr8t3lnzbida2w2xztqpac8xuto*
3. Api Key HTTP Header: By this option your client requests need to contain an HTTP header named "ApiKey" with the value of your Api Key. E.g.: *ApiKey: q401ohr8t3lnzbida2w2xztqpac8xuto*
4. URL Parameter: As fourth option you can provide the API key in your requests as URL Parameter named "ApiKey".
E.g.: <http://<host>/EAWebService/Rest/events?ApiKey=q401ohr8t3lnzbida2w2xztqpac8xuto>

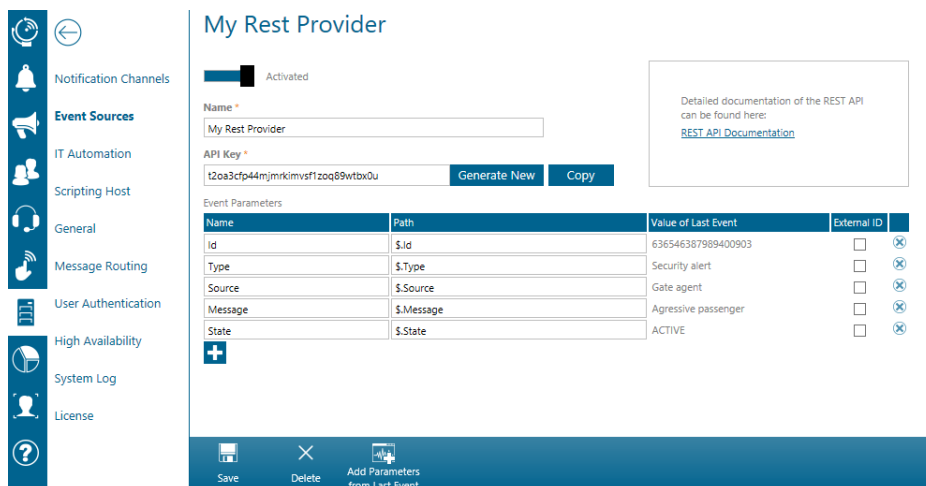
If you have configured your client application, send a test event to Enterprise Alert®.

Alternatively, to a REST Client application you can test the REST API by using the API documentation in the Browser. Open the documentation <http://<host>/EAWebService/Rest/docs/ui/index>, expand the operation "Create Event", press the red exclamation mark, enter the API Key in one of the Authentication fields and press "Authenticate". Put the "Example Value" into the event field and press "Try it out!".

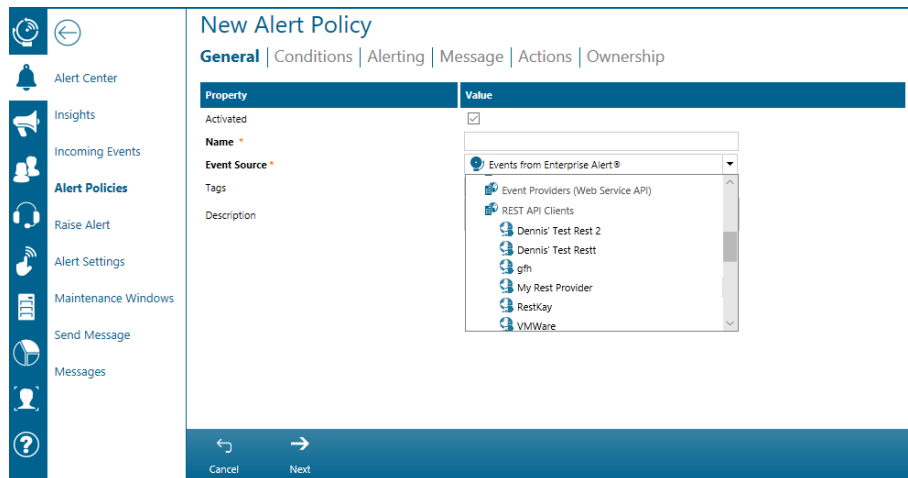
REST API Documentation: <http://<host>/EAWebService/Rest/docs/ui/index>



After you have submitted your first event to the REST API, all parameters of your event will be automatically detected and registered. If you now re-open the configuration of your REST API Client in Enterprise Alert® you can see and edit the parameter names and JSON paths. Please, select one parameter which should be used as External ID. This is helpful if you want to submit update or reset events via additional REST calls.



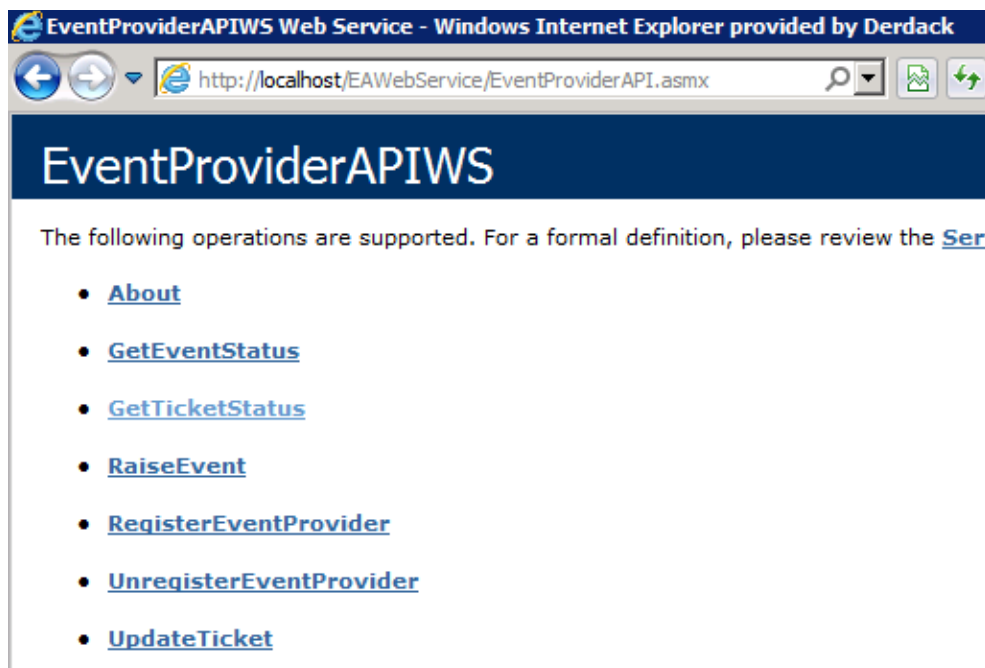
Your registered REST API Client provider will be available for use in the creation of Alert Policies. Events coming from clients using the REST API can thereby be evaluated and processed. To create a new Alert Policy, navigate to [Alerts->Alert Policies](#) then select "Create New" from the action bar at the bottom of the page. Then for the Event Source option, select [Event Sources->REST API Clients->Your Client](#):



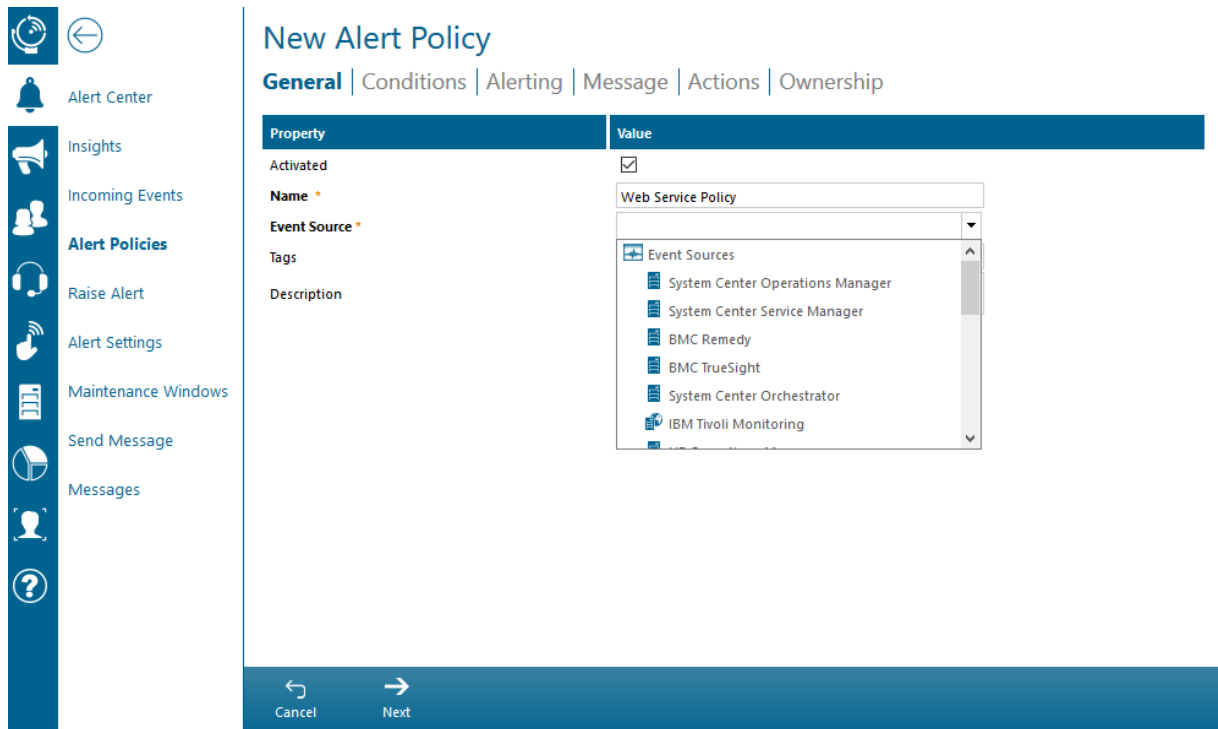
SOAP API (Web Service)

Enterprise Alert® also provides a Web service interface to submit events. This Web service supports HTTP POST/GET as well as SOAP calls.

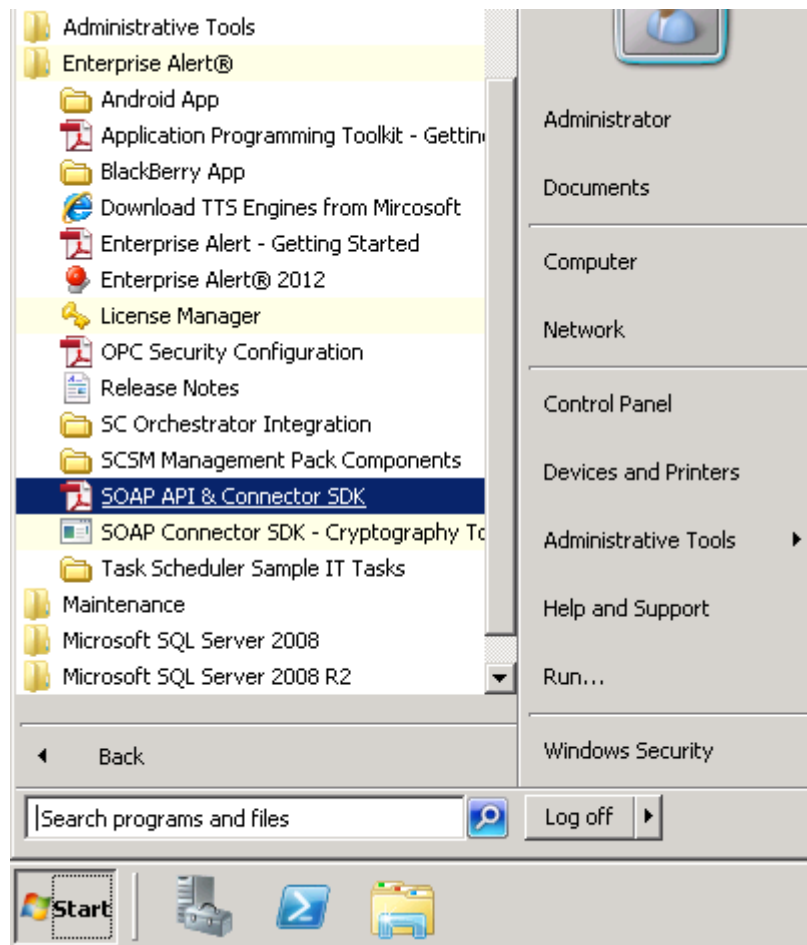
The default URL of the Web service interface is <http://<host>/EAWebService>



Before you can send events through the Web service, you need to register a custom event provider and event parameters by calling the corresponding Web service methods. This registered provider will then be available for use in the creation of Alert Policies. Events coming from various components using the Web service can thereby be evaluated and processed. To create a new Alert Policy, navigate to [Alerts->Alert Policies](#) then select "Create New" from the action bar at the bottom of the page. Then for the Event Source option, select [Event Sources->Event Providers\(Web Service API\)](#):



After the registration of the event provider, you can create events using the Web service methods. For more advanced scenarios, you can even create custom code for evaluation of events before event processing in the Enterprise Alert® kernel. For more information on the Web service interface, see the Web Service Documentation in the Enterprise Alert® Start menu folder.



Serial (RS232)

Enterprise Alert® provides a Serial Connector to communicate with RS232 serial interfaces. The primary use for these interfaces is in facility management scenarios. The connector will continuously read data from RS232 ports.

The connector can forward the read data to the Enterprise Alert® kernel and even raise events when no data has been received (missing heartbeat) in a configurable timeframe. Enterprise Alert® itself can also send heartbeats through the serial port.

To configure the File Interface, open [System > Event Sources](#) in the Enterprise Alert® Web portal. Select Create New from the action bar. As the Source Type select RS232/Serial.

The screenshot shows the 'New Source' configuration page. The sidebar on the left contains the following navigation items: Notification Channels, Event Sources (highlighted), IT Automation, Scripting Host, General, Message Routing, User Authentication, High Availability, System Log, and License. The main configuration area is titled 'New Source' and includes the following fields and options:

- Source Type ***: RS232 / Serial
- Activated**: A toggle switch is currently turned on.
- Name ***: New Serial Connection
- Serial Port ***: (Empty dropdown menu)
- Connection Speed ***: 9600
- Data Bits ***: 8
- Stop Bits ***: 1
- Parity ***: None
- Flow Control ***: 0 - None
- Data Terminal Ready (DTR) Signal activated**: A checked checkbox.
- Save**: A button at the bottom of the form.

The following configuration settings are available:

- **Name:** The name for the serial connection.
- **Serial Port:** This property specifies the serial computer port that should be used with this connection.
- **Connection Speed:** This property defines the connection speed for the data transmission in bits per second. In most cases, 9600 is defined here.
- **Data Bits:** This property defines the data bits for the data connection. 8 is suitable in most cases.
- **Stop Bits:** This property defines the stop bits for the data connection. 1 is suitable in most cases.
- **Parity:** This property specifies the parity for the data connection. In most serial protocols, None is defined here.
- **Flow Control:** This property specifies the control protocol used in establishing serial port communication. Possible values: None, Hardware, Xon/Xoff, Hardware&Xon/Xoff.
- **Data Terminal Ready(DTR) Signal Activate:** This property defines, whether the control line should be active or not.
- **Heartbeat:** Enable the sending of heartbeat signals by Enterprise Alert®

SMTP Server

To configure the SMTP server, open [System > Event Sources > SMTP](#) in the Web portal of Enterprise Alert®.

Configuring the SMTP server is basically only about activating the server with the default settings. Please ensure that the field SMTP server address is left empty or contains the IP address of the host where Enterprise Alert® is running. To activate the server, check SMTP server activated.

Once the SMTP server is configured and active, Enterprise Alert® is able to receive emails.

To send emails to the server, the destination address must include the server name or its IP address as domain e.g. the address *test@yourhost.com*, where *yourhost* is the DNS name or IP address of the server Enterprise Alert® is running on.

5.5.10 Integration in other ITSM Products

For integration of other products where no dedicated smart connector exists, you can use the Standard Interfaces of Enterprise Alert®. Below are a couple of Standard Interface implementation solutions for common 3rd party systems.

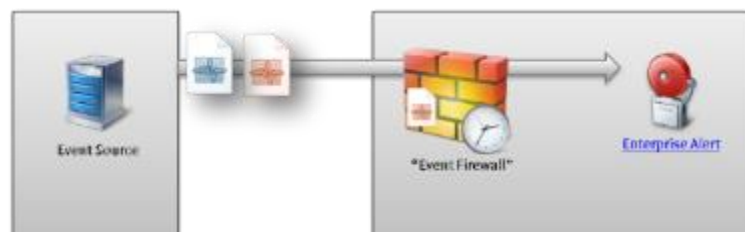
- *Nagios*
You can configure Nagios to send email notifications to the SMTP Server of Enterprise Alert®. You can then create alert policies that trigger on these emails.
- *HP Service Manager*
You can create a database trigger in the HPSM database to send email notifications to the SMTP Server of Enterprise Alert® when new incidents are logged. You can then create alert policies that trigger on these emails. Furthermore, you can create a trigger on the Enterprise Alert® database to submit alert changes back to the HPSM database.

For detailed integration information please contact the Derdack Support Team.

5.6 Advanced Notifications

5.6.1 Duplicate Event Suppression

Duplicate Event Suppression is a feature allowing you to suppress the creation of multiple alerts for duplicate or similar events.



When an event is received and *Duplicate Event Suppression* is enabled, Enterprise Alert® checks to see if an identical or similar event has already been received and thereby prevents triggering a new alert if this is the case.

You can configure how far back in time Enterprise Alert® will look for duplicate events and also define which event parameters must have changed for the event to *not* be considered a duplicate.

This allows you to define conditions like *"Do not alert me again if the affected server and the severity is the same as before"*. In which case you would only be notified if, for example, the severity of the events the server is reporting turned from *major* to *critical* or the previous event occurred too long ago.

Duplicate Event Suppression can be configured for each Alert Policy individually.

Check Duplicate Event Suppression on the Alert Policy's Conditions tab. This will display a selection of event parameters available for the policy's event source. Here you can check the parameters that must change for a new alert to be created (*Affected Server* and *Severity* would have been checked in the previous example).

5.6.2 Multiple Event Occurrences

Especially in after-hours you typically only want to notify people if the incident is critical. The criticality is often determined by the number of system monitoring failures that occur in a row. If your monitoring system does not have a correlation mechanism for these multiple failures you can configure such intelligence in Enterprise Alert. In the Alert Policy details on the condition tab you can enable a checkbox in order to specify the amount of events matching your conditions within a given amount of time in order to trigger the notifications. If the number of events that is received in that timeframe is less than the configured threshold, no notifications will be sent as the underlying problem does not seem to be critical enough.

5.6.3 Team Broadcast Alerts

Team Broadcast is a notification procedure in Enterprise Alert® for alerting all team members at the same time. By configuring *Team Broadcast* to not require acknowledgement, *Team Broadcast* can be used to inform teams of non-critical incidents or status information. In such a scenario, you can configure the percentage of notifications that must be successfully delivered for the alert not to fail. This enables you to ensure that at the very least, a certain percentage of your team members were successfully notified.

When combining the *Team Broadcast* and acknowledgement requirement options, the notified team members must acknowledge the alert. You can define the percentage of team members which are required to acknowledge the alert, before it is automatically closed.

5.6.4 Team Escalation Alerts

The *Team Escalation* notification procedure in Enterprise Alert® is a mechanism for finding a person within a team, who is in a position to resolve the problem, without having to disturb the whole team. When an alert is triggered, *Team Escalation* will start notifying the team members in the configured order. If the first notified user declines the alert or cannot be reached, Enterprise Alert® escalates to the next team member until:

- A team member acknowledges the alert
- No team members are left to escalate to (in which case the alert fails)
- The team manager cancels the alert

To prevent the same team members(s) from being notified first all the time, Enterprise Alert® ships with a custom script that you can activate to rotate team members in a configurable interval. This script moves the first team member to the end of the list and everybody else one position down.

5.6.5 Acknowledgement and Closure Workflows

Enterprise Alert® offers three different workflows for the acknowledgement and closure of alerts.

- *Alert must be manually acknowledged*
This is the default alert option. Alerted users have to manually reply to acknowledge the alert to avoid further escalation and confirm that they are now responsible for the alert. They are also required to manually close the alert once they have resolved the underlying problem.
- *Automatic acknowledgement on notification delivery*
The user who first receives a notification successfully will automatically have the alert acknowledged and assigned to them. They will also have to manually close the alert once the underlying problem has been resolved.
- *Automatic closure on notification delivery*
The alert is automatically closed once a successful notification delivery has been received. This option should be used for non-critical informational alerts only.

5.6.6 Acknowledgement Time Limit

Setting an *Acknowledgement Time Limit* grants each user the same amount of time to acknowledge the alert. This improves the alerting process and ensures that each user has the same opportunity to respond to the alert. In previous versions, the more channels you had in your notification profile, the longer your acknowledgement timeout would have been.

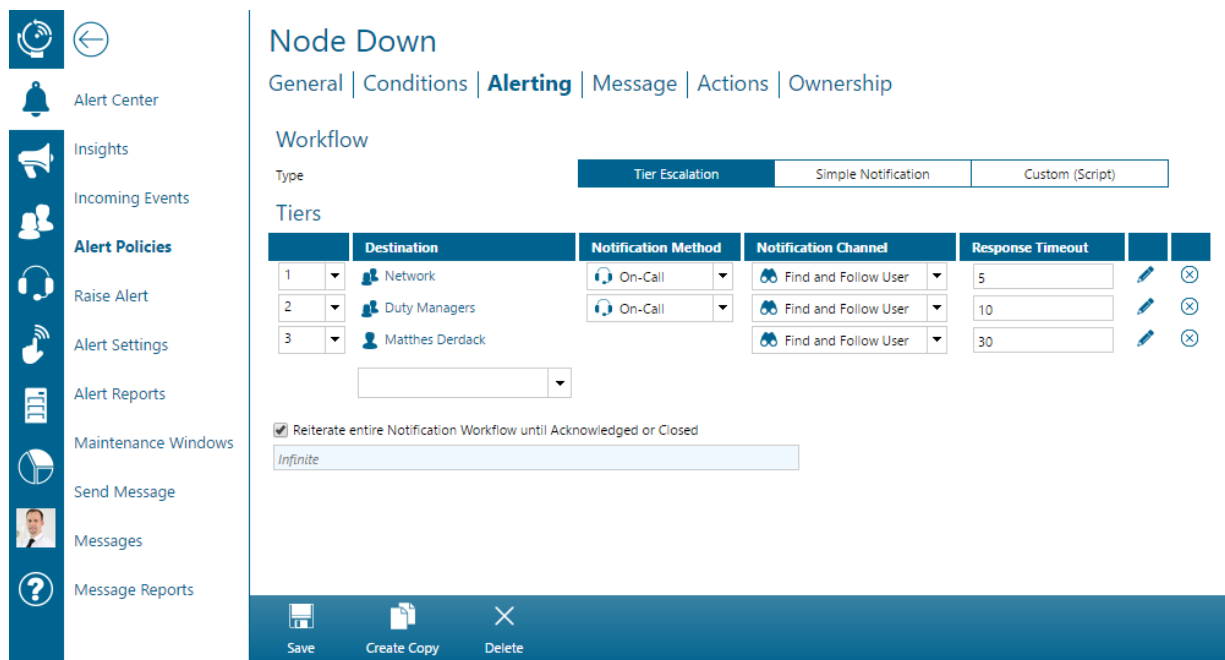
Enterprise Alert® notifies the user on all configured channels, depending on the notification procedure (either broadcast or escalation) and then waits for a response from the user until the acknowledgement time limit has expired. If the user has a number of channels configured and the acknowledgement time limit expires before all the channels can be made use of, Enterprise Alert® nonetheless still escalates to the next user, skipping the remaining channels in the process.

You can set a default value for the acknowledgement time limit ([Alerts > Alert Settings](#)) and then configure each alert policy individually to either use the default global value or a custom value.

Please note that Enterprise Alert® will not send notifications if there is not enough time left realistically for the user to receive and respond to the notification. If a previous notification has been successful, the system will rather wait another 30 seconds for a reply than send out another notification.

5.6.7 Tier Escalation

It is possible to escalate through multiple tiers when the workflow type is set to "Tier Escalation". In this case you can assign multiple targets to which the alert will be sent until someone (or enough people) in that tier has responded or received the notification. The latter depends on the alerting settings of each tier. In each tier, you can add individual users, teams or a multi-team schedule. This allows you to setup an escalation where you route all alerts to the on-duty person from the responsible operational team (e.g. "Network Team"). In case no one from that expert team finally responded you can escalate to a general manager on duty (e.g. "Duty Managers"). Should that person also finally miss the alert, it can be escalated to the IT director.

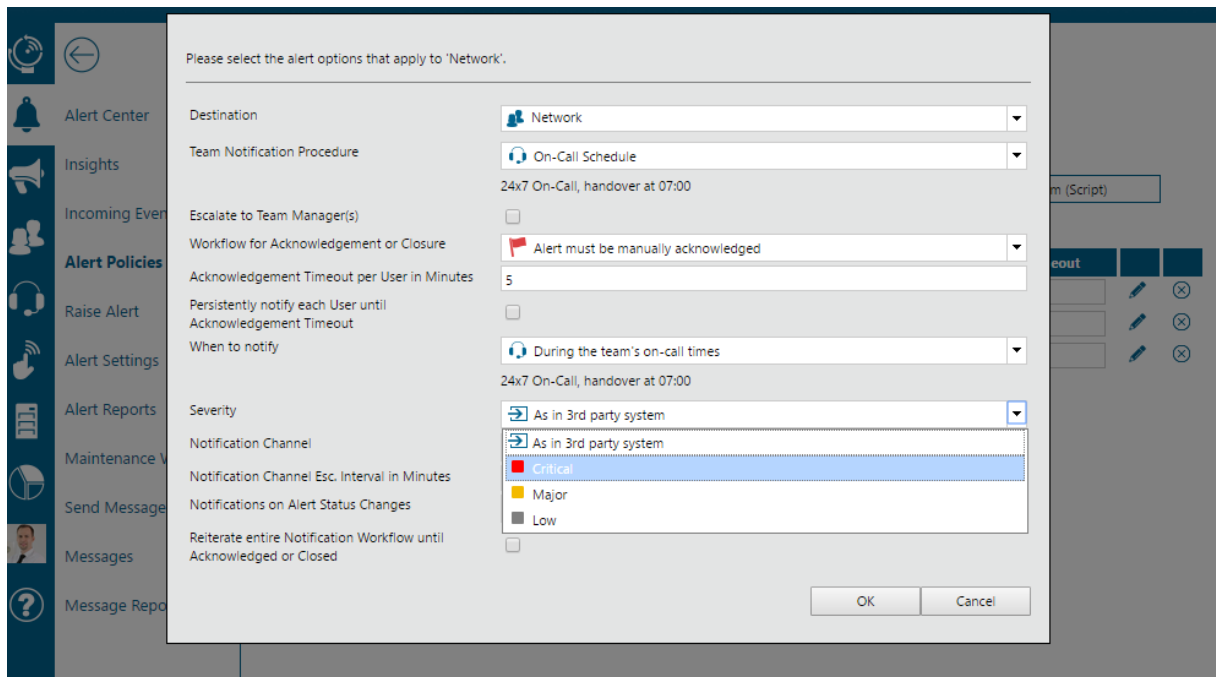


5.6.8 Alert Severity

Enterprise Alert® supports the following alert severities for alert classification:

- Critical
- Major
- Low

In the Alert Center alerts are displayed based on their severity which can be assigned statically or automatically adopted from a 3rd party system. To modify the severity of an alert, go into [Alerts>Alert Policies](#) then select the [Alerting tab](#). Here, click the edit button of the alert to the desired tier which will open the following dialog:



The following table displays the severity mapping that has been implemented in case a policy has been configured to automatically adopted the severity from the 3rd party system:

EA Event Severity	HP NNM	HPOM	HP SM*	SCOM	SCSM*	ITM
Critical	Critical	Critical	Critical	CriticalError Error	High	Fatal Critical
Major	Major	Major	High	Warning SecurityIssue ServiceUnavailable	Medium	Warning
Low	Minor Normal Warning	Minor Normal Warning Informational	Average Low	Information MatchMonitorHealth Success	Low	Minor Harmless Informational

5.6.9 Find me, follow me Notifications

The *Find Me, Follow Me* channel option notifies the user one notification channel at a time in the order configured in their currently active notification profile.

Once a notification has been successfully sent, the Enterprise Alert® kernel waits a configurable amount of time (*Notification Channel Escalation Interval*) for the alerted user to respond. If this time runs out, or the notification fails, the next available notification channel will be used.

This process will be repeated until either one of these conditions is met:

- All configured notification channels in the user's notification profile have been used
- The alert is acknowledged, declined or canceled
- The acknowledgement timeout expires

5.6.10 First Channel Notifications

The *First Channel* option notifies the user on the first notification channel configured in their currently active notification profile. This corresponds to the user's currently preferred channel.

Please note that selecting *First Channel* works in the same way as selecting a single notification channel directly. Enterprise Alert® will send out one notification using this channel and if this fails or the user cannot be reached, no other channel will be attempted.

5.6.11 Channel Broadcast Notifications

The *Channel Broadcast* option notifies the user on all available channels at the same time.

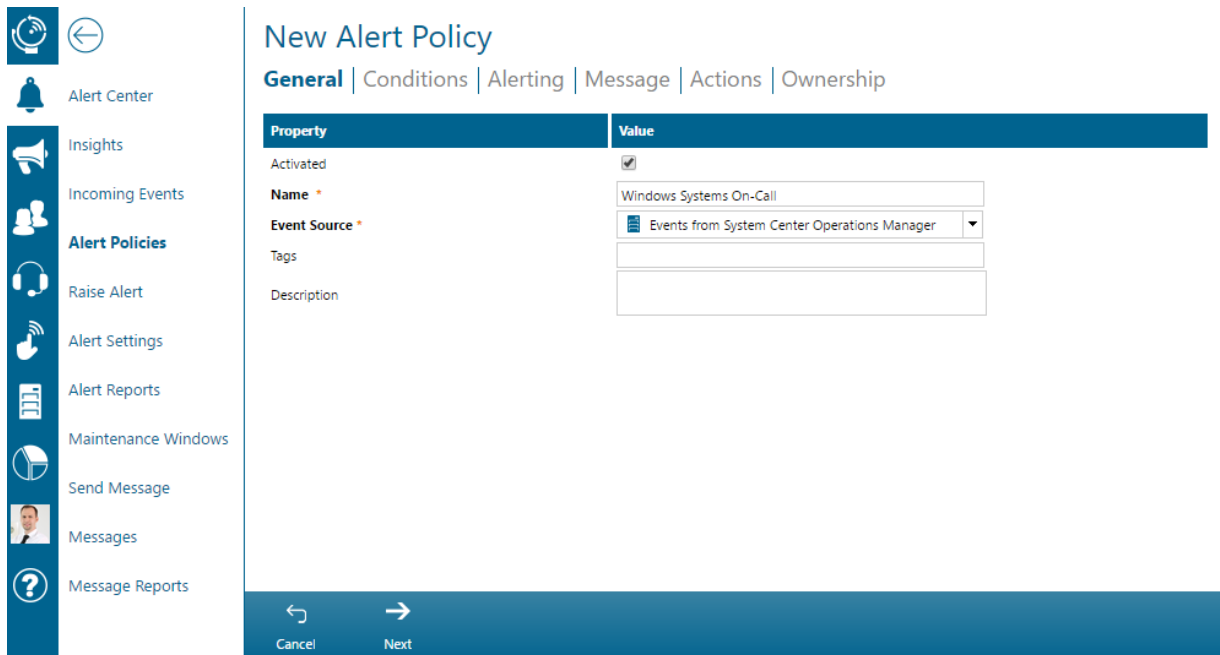
This gives the user the maximum amount of time to respond to the alert, especially in scenarios where users have lots of notification channels configured in their notification profile, but can only be reached on one of the channels at the time of the alert.

5.6.12 On-Call Notifications

One major use case of EnterpriseAlert® is sending automated and reliable notifications requiring manual acknowledgement to on-call persons.

The people who are on call can be automatically notified about relevant incidents through *Alert Policies*. They are created for events which are received through a selected *Event Source*. In addition, the event itself must match specific criteria in order for it to result in a new alert notification. If such an alert has to be sent to an on-call person, the *Alert Policy* must be configured to target the corresponding *Team*, where the person is on-call. When an event is received that matches the criteria of an *Alert Policy* that targets a *Team* and which is configured to only create an alert notification during the *Team's* on-call times, the alert notification will be sent to the *Team* member who is currently on call. In this case, Enterprise Alert® then queries the current on-call member of the *Team* based on the *Team's On-Call Schedule*. More information on how to manage and maintain an *On-Call Schedule* for a *Team* can be found in section 0.

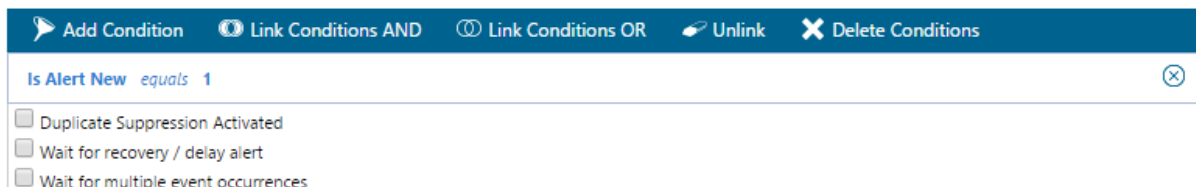
To create an *Alert Policy* that notifies an on-call person, open the *Alert Policy* overview by clicking on [Alerts>Alert Policies](#). In the overview, click [Create New](#). On the first tab, enter in a name for the new *Alert Policy*, such as "Windows Systems on-call" and select an *Event Source* through which corresponding incidents will be received. Afterwards, select the [Conditions Tab](#).



On the next tab, set up the criteria that an incoming event from the selected source must match in order to result in a new alert notification. In this example, the event will be received from System Center Operations Manager (SCOM). Once you have set up your criteria, click the [Alerting](#) tab to proceed.

New Alert Policy

General | **Conditions** | Alerting | Message | Actions | Ownership



On the next tab, select the *Team* from which the corresponding on-call person should receive the alert notification as first tier. Once the *Team* has been selected, two additional properties will be displayed.

For the property "Notification Method" select the value "On-Call". As notification channel select "Find and Follow User" (refer to section 4.6.9).

After you are done, click the [Edit Icon](#) in the table row to configure additional details of your on-call notification workflow.

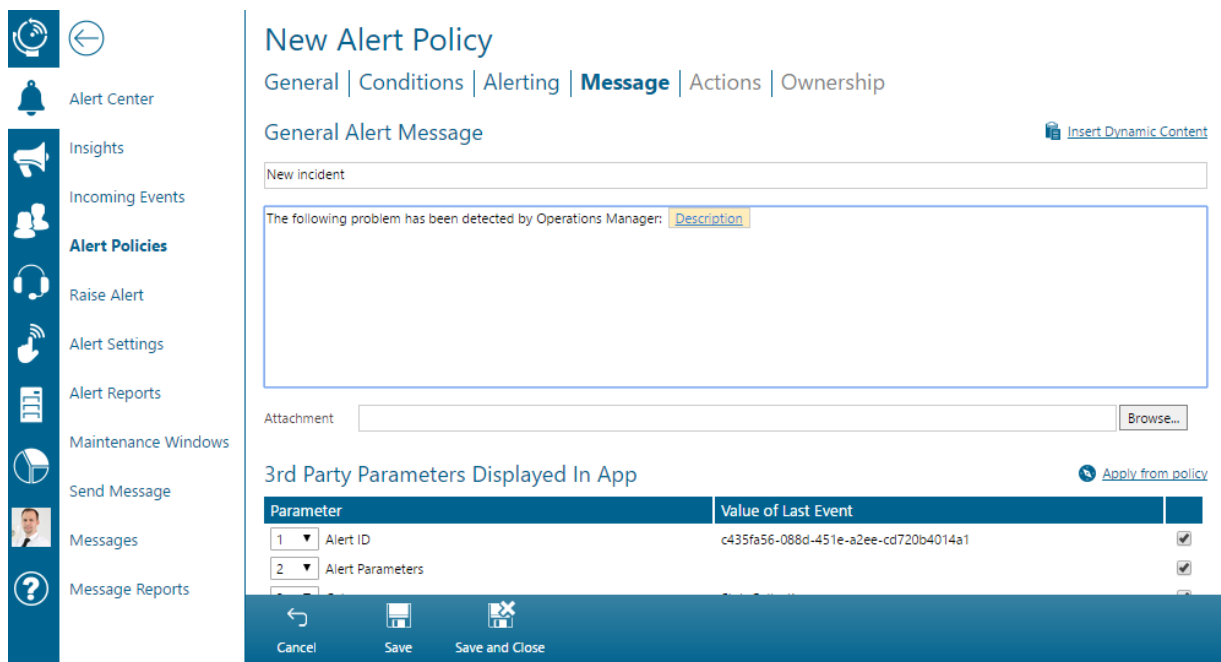
The property "Escalate to Team Manager(s)" allows selecting whether the manager(s) of the selected *Team* should receive the alert notification when the on-call users (primary and backup if applicable) either miss or do not acknowledge the alert. In this case, Enterprise Alert® will send the notification directly to the managers of the team in the order that they have added or set on the "Managers" tab in the *Team* details.

Additionally, you can select or enter details for how the alert that should be created and processed. For example, you can select whether the alert notification must be manually acknowledged by the recipient and you can enter the time limit within which the recipient must respond.

For the purpose of this example, set the alert workflow to "Alert must be manually acknowledged" and leave the remaining fields as they are.

Afterwards, click the [OK](#) to close the dialog and proceed to the [Message](#) tab.

On the next tab "Message", you can compose the notification message. You can insert properties from the original event through the "Insert Dynamic Content" button. After you have finished composing the message, click [Save](#) to proceed.



Your policy has now been created and is active. You may use the "Ownership" tab to control who may see and modify the created *Alert Policy*.

The *Alert Policy* that has been created in the above example will only trigger and create a new alert notification if the incoming event matches the policy's criteria *and* is received within the configured on-call times of the selected *Team*. Additionally, someone needs to actually be scheduled for on-call at that time, otherwise the alert notification will immediately fail.

5.6.13 Notifications to Teams on duty (e.g. "Follow the Sun" notifications)

Automated alert notifications can also be sent to *Teams* who are currently on duty. This is done in an *Alert Policy* by selecting a so-called *Multi-Team Schedule* as destination in the corresponding tier. When the event is received and the policy is triggered, the team that is currently on duty is automatically selected as destination for the alert depending on which *Team* has been scheduled for that time.

Scheduling Teams

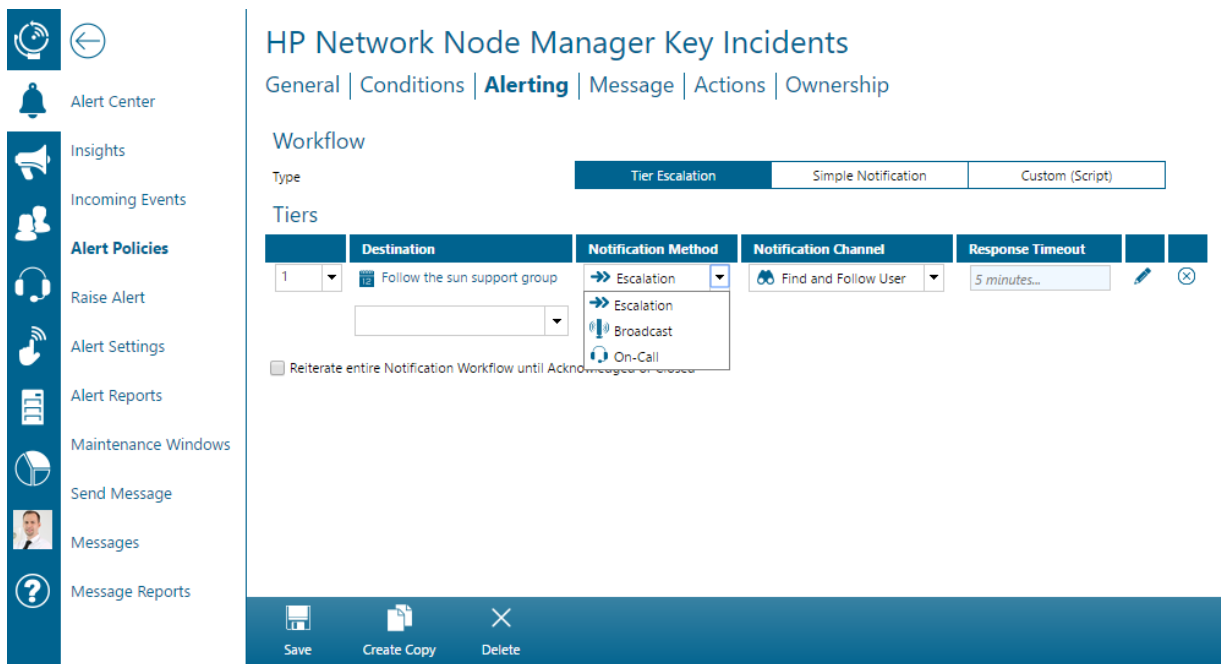
The Teams can be scheduled in so-called *Multi-Team Schedules* ([On Call > Multi-Team Schedules](#)). Then select 'Create New' from the action bar.

In the 24x7 calendar, teams can be scheduled simply by dragging and dropping them into the calendar. The coverage times of that team can be adjusted by dragging at the end of a Team's bar.

Automated notifications to the scheduled Team

Once you have created the *Multi-Team Schedule*, the schedule can be targeted as a tier destination for alerts notifications that need to be sent to the Team that is currently on duty. In an *Alert Policy*, navigate to the tab "Alerting". Instead of selecting a specific *Team* directly as tier destination, select the corresponding *Multi-Team Schedule*.

When an event is then received, that matches the criteria set up in the *Alert Policy*, the alert notification will be sent to the *Team* that is scheduled in the *Multi-Team Schedule*.



Please note that if no Team is on duty when an alert occurs that the alert addressed to the schedule will fail, except if the alert is created with the "Re-iterate" option. In this case, the alert will remain open until the next scheduled team is on-call. Please ensure therefore that your schedule is complete and covers all available times.

5.6.14 One-way Outbound Notifications

Notification Feeds are a feature of Enterprise Alert® enabling subscription based alerting for one-way outbound notifications. You can create feeds for fields of interest that external users (so-called *Subscription Users*) such as suppliers and customers can subscribe to. Internal users may subscribe to *Notification Feeds* as well. You can even create private feeds which are only available for internal users. Addressing an alert or sending a message to a *Notification Feed* will notify all subscribers to the feed.

Notification Feeds

All | Netz Berlin | App-Banking System | App-CRM | DWDM | Email | Employees | Facility
 FB_Server | feed | HD Guide | Internal IT | MPLS | Network | Private feed | Router | SiteA
 Video | VOD

10 | 20 | 50 1 to 33 of 33

	Name	Description	Subscribers	Visibility
<input type="checkbox"/>	AFEnroll Service	AFEnroll	1	Internal
<input type="checkbox"/>	Alex Smits Notification Feed		4	Public
<input type="checkbox"/>	Annual Statement		8	Public
<input type="checkbox"/>	Banking Service End Users	Banking system end user information feed. Subscribing this feed is recommended when you are using Banking v13 on a regular basis.	2	Public
<input type="checkbox"/>	Banking Service Owners	Banking system service owners.	3	Public
<input type="checkbox"/>	Building Alert		3	Public
<input type="checkbox"/>	Business Applications		1	Internal

Refresh Create New Delete

Notification Feeds

To create a *Notification Feed*, open [People > Feeds](#) in the Enterprise Alert® Web portal and click on *Create New*.








Select a name for the new *Notification Feed* e.g. a product name and an optional description. If the feed should be visible to external users such as customers and suppliers as well, please select the *Public Feed* option. Public feeds are available to internal as well as external users. You can also enter a tag to ensure that you can easily find the feed at a later stage.

On the *Managers* tab, you can enter in Team Leaders who are responsible for managing the feed's subscriptions and details. Unless a Team Leader has been added to the list of managers, they will not be able to view or modify the feed.

On the *Subscribers* tab, you can see all users that are subscribed to the feed.

CRM Business Clients

General | **Subscribers** | Ownership

	Name	Mobile	Email	Status	
10	20	50			1 to 3 of 3
	Doreen Jacobi	+4917155554	djacobi@us.derdack.com	Alerts on	
	Melanie Schultes	+4917065610	mschultes@de.derdack.com	Alerts on	
	Rene Bormann	+49151148587	rbormann@de.derdack.com	Alerts on	
<input type="text" value="Add a subscriber..."/> 					

All users that have subscribed themselves to the feed will appear here. Alternatively, you can also manually subscribe the user to the feed, if you are an Administrator or Team Leader managing the feed. Note though that once the user has been *manually* subscribed to the feed, only an Administrator or Team Leader can unsubscribe the user again i.e. the user will not be able to unsubscribe themselves from the feed.

Besides managing the subscriptions inside the feed itself, you can also manage a user's subscriptions on the *Notification Feeds* tab of the user's profile.

Subscription Users

Subscription Users that would like to receive notifications for the areas of interest can register themselves on the login page of Enterprise Alert®. All self-registered external users are created as *Subscription Users*. *Subscription Users* can only manage their own subscriptions and cannot perform any other task in Enterprise Alert®.

To manage *Subscription Users* open [People > Subscription Users](#).

Although *Subscription Users* can register themselves via the login page of Enterprise Alert®, they can also be added manually.

To create the user manually, click on 'Create New' from the action bar and provide a user name, name and password for the user. Optionally, you can enter in some general information about the user. Next, configure the contact addresses, whereby an email address is required by default.

Subscribing to Feeds

When *Subscription Users* log on to Enterprise Alert®, they can manage their personal subscriptions. This can be done on the *Notification Feeds* tab of their profile. Once logged in, *Subscription Users* are automatically taken to this tab. External *Subscription Users* may only view public feeds while internal users can see all *Notification Feeds*.

John Smith

General | Contact Addresses | **Notification Feeds**

All | _Netz Berlin | App-Banking System | App-CRM | DWDM | Email | Employees | Facility
 FB_Server | feed | HD Guide | Internal IT | MPLS | Network | Private feed | Router | SiteA
 Video | VOD

10 | 20 | 50 1 to 33 of 33

Name	Description	Last Notified	Subscribed
AFEnroll Service	AFEnroll		<input type="checkbox"/>
Alex Smits Notification Feed			<input type="checkbox"/>
Annual Statement			<input type="checkbox"/>
Banking Service End Users	Banking system end user information feed. Subscribing t...		<input type="checkbox"/>
Banking Service Owners	Banking system service owners.		<input type="checkbox"/>
Building Alert			<input type="checkbox"/>

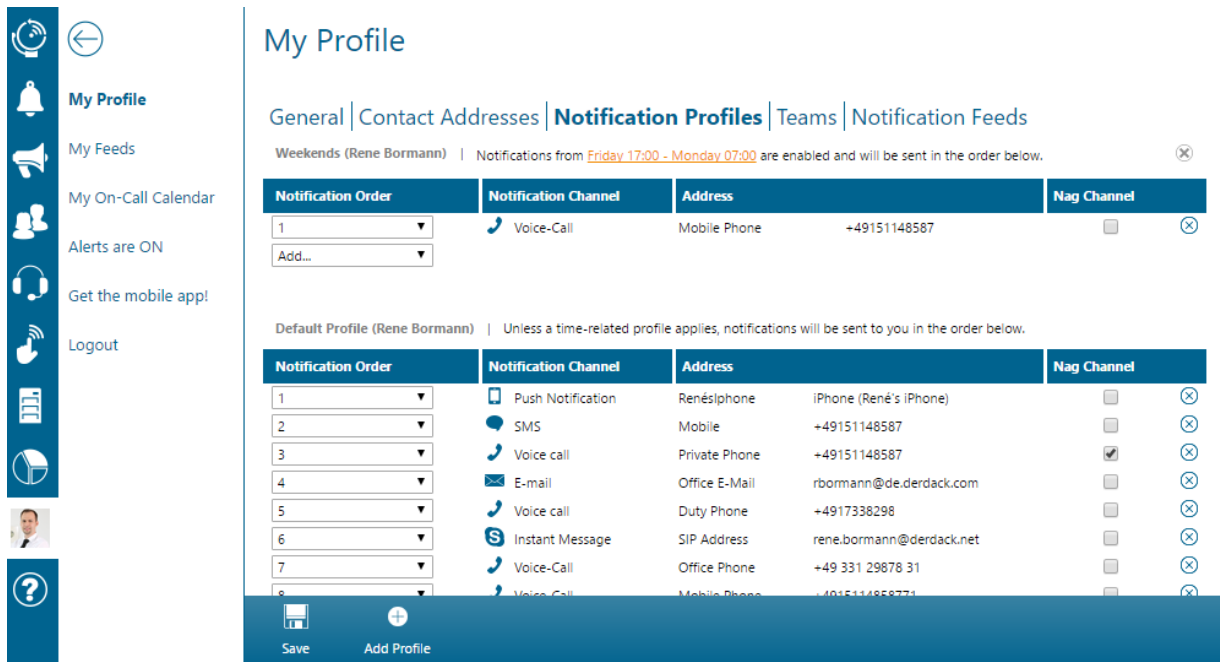
Save

Notification Feeds as Notification Destination

Alert Policies to *Notification Feeds* will always create alerts with no acknowledgement workflow and which will automatically be closed once the notifications have been submitted. You can automate notification feed messaging by selecting a feed as the destination of an *alert policy* or you can manually send messages to subscribers by selecting the feed as destination in the *Messenger*.

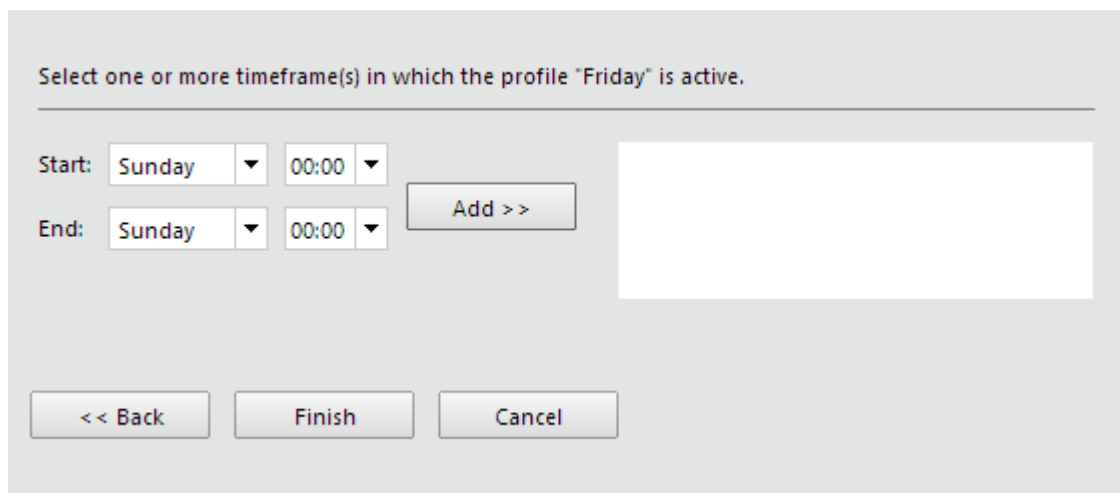
5.6.15 Time based Notification Channels

Notification Profiles define a sequential list of notification channels through which users would like to be alerted at a given time. To configure notification profiles, open the user profile (*People > Users*) select a user, and select the *Notification Profiles* tab.

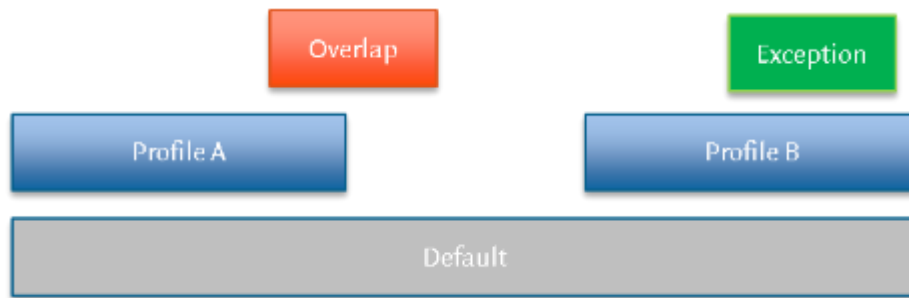


Each user has a least one default notification profile, which is used when no other notification profile is active at the time of the alert. This ensures that notifications can be sent to the user at any time.

You can add, remove and reorder the notification channels. Adding a channel to a notification profile requires that a contact address has been entered for the channel, otherwise it will not be available for selection. The notification profile is automatically updated after each change.



When adding a new notification profile, you can select multiple timeframes that specify when the profile will be active. Enterprise Alert® will check the profile's existing timeframes and automatically combine them with the new ones where appropriate.



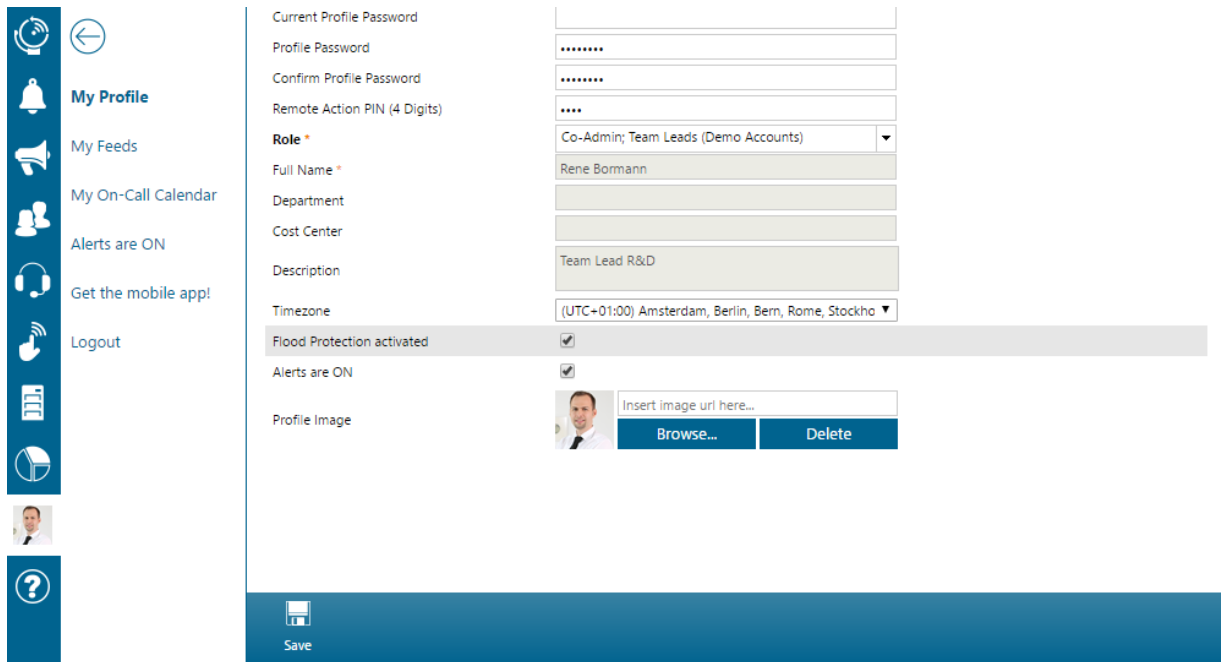
You may not create overlapping notification profiles. However, creating a profile that is enclosed within another profile's timeframe is allowed, in which case the enclosed profile will be used.

To edit the timeframes of a previously configured profile, click on the link in the header of the corresponding profile. Clicking on the delete icon in the profile's header will remove the profile from the database.

5.6.16 Anti Flood Protection

Anti Flood Protection is a feature of Enterprise Alert® that helps prevent users from handling unnecessary message storms. Anti Flood Protection is user based, meaning that every individual user can enable or disable it based off their preferences. A flood is defined by an excessive amount of incoming alerts in a very short period of time, in some cases several alerts will be received instantaneously. What Anti Flood Protection will do, is detect this mass of incoming alerts, and hold them until EA has detected that the flood is over. Once over EA will send a final alert informing you of a flood and must be acknowledged like a regular alert.

Enabling Anti Flood Protection is very easy, simply navigate to [People>Users](#) and select the user you wish to enable protection for. Once a user has been selected, click the edit icon to the right of their name and navigate to the general tab in the user options. Once there, find the selection box labeled "Flood Protection activated" and ensure it is selected:



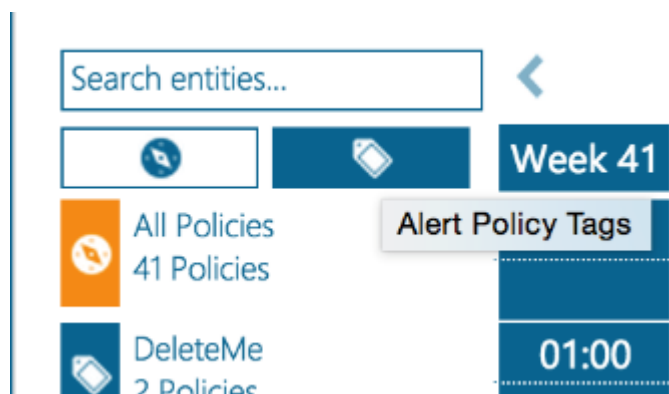
Once selected, simply save the users settings and flood protection is now enabled!

When a flood situation occurs, the designated user will receive the first few alerts, however after that an additional alert will be sent informing the user of the flood situation. They will no longer be receiving alerts for the duration of the flood. After some time, the user will be sent an additional notification informing them that the flood is over, and that alerts are once again enabled.

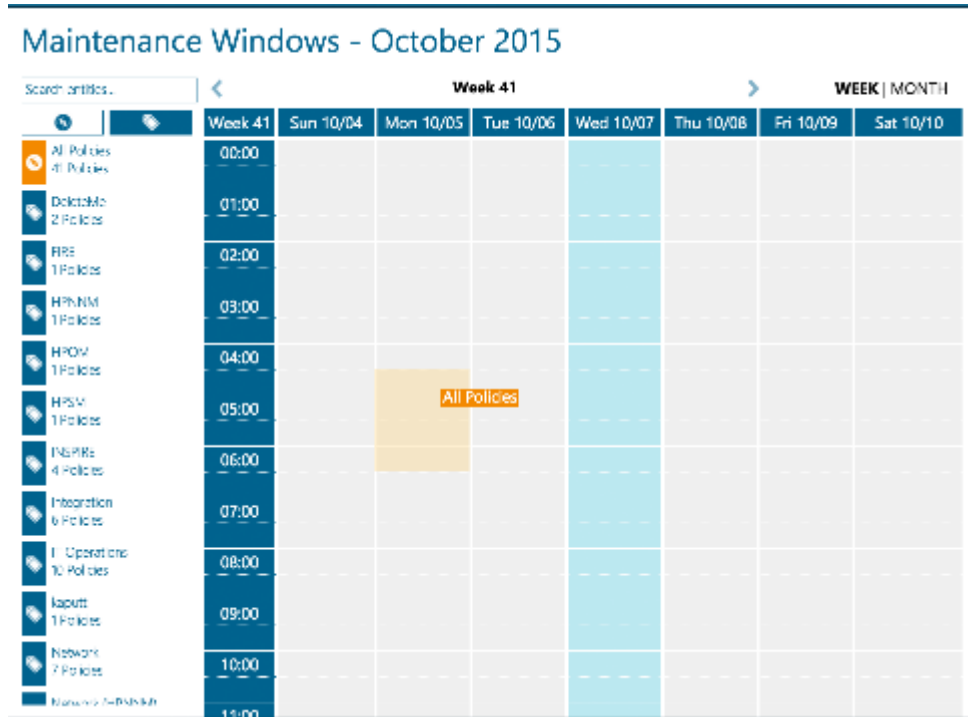
5.6.17 Maintenance Windows

As explained earlier, Maintenance Windows are a feature of Enterprise Alert® that allow you to stop all incoming alerts from a specified Alert Policy or Alert Policy Tag during a designated time period. This is useful when any maintenance is being done on a particular connection that may trigger an Alert.

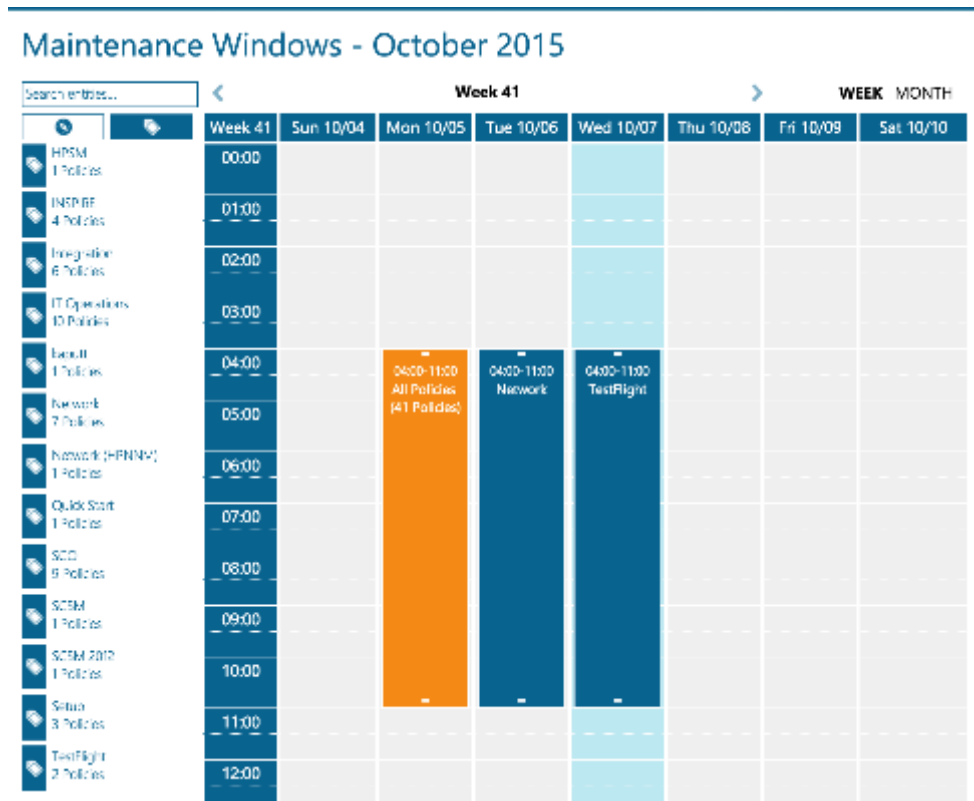
Setting up Maintenance Windows is simple, to get started navigate to [Alerts>Maintenance Windows](#).



Once on the Maintenance Windows page, creating a Window is simply drag and drop based. What you must first decide is what kind of window you want to set up. You have 3 options: either select a specific Alert Policy, an Alert Policy Tag (by notification channel type, E-mail, IM, etc..), or select 'All Policies' to disable all alerts at that time. You also have the option of searching for specific policies. Once you select an option, simply drag the desired tile onto the calendar, to the date you want to turn off the alert(s).



Once dropped, you can extend or shorten the period of time the window is active by dragging the top or bottom of the bar:



You can also click on the dropped bar, if it is an Alert Policy or Alert Policy Tag, and define them farther. The following dialog box appears upon click:

Here there are several configurable options:

- **Maintainable Entities:** Here you can see which Alert Policy or Alert Policy Tags are going to be stopped at the time of this Maintenance Window, and remove any undesired entities.
- **Name:** This options allows you to input a name that will be displayed on the calendar for this Maintenance Window.

- **Recurrence:** There are a variety of options here. You can enable recurrence for your window on a daily, weekly, or monthly basis.
 - Daily: These options are shown above, and allow you to input how often you want the window to occur.(every day, every other day, etc.) You also have the option to select when the recurrence ends, either by date or the number of occurrences.
 - Weekly: Weekly occurrence allows for input of how often you want the maintenance window to occur.(every week, every other week, etc.) You can also input on what day of the week you want the Maintenance Window to occur. Like the daily recurrence, you can also input either the date you want the weekly recurrence to end, or by the number of occurrences.

The screenshot shows the 'Recurrence' settings panel. At the top, there are four tabs: 'None', 'Daily', 'Weekly', and 'Monthly'. The 'Weekly' tab is selected. Below the tabs is a horizontal slider with a black marker positioned over the 'Weekly' tab. Underneath, there is a text input field for 'Recur every' with the value '2' and the text 'week(s) on:'. Below this are seven radio button options for the days of the week: Monday, Tuesday (checked), Wednesday, Thursday, Friday, Saturday, and Sunday. At the bottom, there are two radio button options for ending the recurrence: 'End after:' with a value of '10' occurrences, and 'End by:' with a date of '08/05/2014'.

- Monthly: There are several options to configure here. First of all, you can select which day of the month you want the Maintenance Window to occur, and how often you want it to reoccur.(every month, every other month, etc.) You can select the day either by the number of the day (e.g. the 5th), or by which day of the week and on which week. (e.g. the first Tuesday) Like the other recurrences, you can select when you want it to end either by the number of occurrences or a specific date.

The screenshot shows the 'Recurrence' settings panel. At the top, there are four tabs: 'None', 'Daily', 'Weekly', and 'Monthly'. The 'Monthly' tab is selected. Below the tabs is a horizontal slider with a black marker positioned over the 'Monthly' tab. Underneath, there are two radio button options for selecting the day of the month: 'Day 5 of every 2 month' (checked) and 'The first Tuesday of every 2 month'. At the bottom, there are two radio button options for ending the recurrence: 'End after:' with a value of '10' occurrences, and 'End by:' with a date of '08/05/2014'.

Once all settings of the new Maintenance Window are configured to your satisfaction, click 'Save' and the specified alerts will be turned off at the designated times!

5.7 On-Call Scheduling

In this section, you can find out about how to schedule your on-call service with Enterprise Alert®. The main objective here is to define which team member (engineer) is on call at which time. Furthermore, you will need to configure when the on-call service is operational, be it 24x7 or mainly afterhours. This section also explains how you can handle public holidays in your on-call service, how to export your schedule and how you can subscribe to schedule gap notifications to help you prevent incident notifications failing when no-one is available during on-call times.

5.7.1 On-Call Times

The first action to perform is entering the times your team operates the on-call service. When configured, Enterprise Alert® will only send alert notifications to an on-call engineer when an incident occurs within the operated on-call service times.

To enter the on-call service times, first open the team details. To do this, click on [People>Teams](#). Then locate the Team for which you want to plan the on-call schedule in the overview, select the edit button to the right of the interface and click on [Open On-Call Schedule](#) on the bottom action bar.

The on-call schedule for your team will be displayed. You can find the configured on-call times below the Team's name. By default, the on-call service times are 24x7. Click on the shortcut to open the on-call times dialog:

Windows Systems - June 2017

24x7 (Change) on-call times | 06/30/2017 scheduled until

Week	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Category
22	28	29	30	31	1	2	3	Primary
		Rene Bormann		Hanno Ferdinand				
23	4	5	6	7	8	9	10	Backup
		Hanno Fer...	Rene Bormann		Christian Kühne			
24	11	12	13	14	15	16	17	Stand-In
	John Doe							
25	18	19	20	21	22	23	24	
	Doreen Jacobi				Ronald Czachara			
26	25	26	27	28	29	30	1	
	Ronald Czachara							
27	2	3	4	5	6	7	8	

Auto Rotation: Rotating duty

Options | Times | Holidays | PDF Export

The dialog in which you can enter your on-call times will be displayed:

On-Call Times for team Windows Systems

based on (UTC +02) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

On-Call Times
When is your team on-call?

24x7 On-Call

Duty Handover
When do you hand over on-call?

Public Holidays
How do you handle public holidays?

No on-call service

Use regular on-call times

Custom times

Start	End
<input type="text" value="00:00"/>	<input type="text" value="24:00"/>

Exception Days
When are the on-call times on exception days?

Start	End
<input type="text" value="00:00"/>	<input type="text" value="24:00"/>

In the dialog, you can configure the following on-call options, which are clarified in more in detail below:

- On-Call Times: the times at which your team operates the on-call service
- Duty Handover: the time of day at which your team usually hands over the on-call service from one engineer to another
- Public Holidays: how to handle the on-call service during public holidays
- Exception Days: The time of day which the on-call plan does not apply to the team on exception days.

On-Call Times

On-call times allow you to specify at which times your team operates the on-call service during the week. By default it is assumed that your team operates on call on a 24x7 base. If your on-call times are different, you can customize the on-call times by moving the slider to the left, thereby enabling the entering of custom on-call times.

Use the [plus button](#) to add a new period for on-call coverage. The following screenshot displays the setup for the on-call times below. This example basically covers afterhours on weekdays as well as the entire weekend:

Monday:	00-09, 18-24
Tuesday:	00-09, 18-24
Wednesday:	00-09, 18-24
Thursday:	00-09, 18-24
Friday:	00-09, 17-24
Saturday:	00-24
Sunday:	00-24

On-Call Times
When is your team on-call?

24x7 On-Call

Start		End		
Mon ▼	18:00	Tue ▼	09:00	⊗
Tue ▼	18:00	Wed ▼	09:00	⊗
Wed ▼	18:00	Thu ▼	09:00	⊗
Thu ▼	18:00	Fri ▼	09:00	⊗
Fri ▼	17:00	Mon ▼	09:00	⊗

Duty Handover

The handover time defines when the on-call service is handed over from one engineer to another. Please note however that the custom on-call times previously entered do *not* define how long an engineer is on-call. Firstly, the on-call duration is directly defined by the number of days that the on-call duty is planned for in the scheduler. Secondly, if an on-call assignment in the scheduler ends on a Wednesday for example, and another engineer is assigned from Thursday onwards, the handover from the predecessor to the successor will be on Thursday at the handover time entered here.

Public Holidays

How you can select what should happen if your on-call service also operates on public holidays. The options are as follows:

- No on-call service
Select this option if you do not operate the on-call service on public holidays. If selected, on-call engineers will not receive alert notifications on a holiday, even if the engineer is scheduled for on-call on that particular day.
- Use regular on-call times
Select this option if you operate your on-call service on public holidays with the same times as on a regular week day. This option would be applicable for example if your on-call times are on a 24x7 basis.
- Custom times
Select this option to enter specific on-call times that are only active on public holidays. This option can be useful for example if an on-call service that usually only covers afterhours on regular week days needs to be extended to cover 24 hours on public holiday.

Exception Days

Exception days are specific days of the year or month, when the regular on call times do not apply to the entire team. This option in the on-call menu allows you to modify what times the team will be on-call during these specified days.

Section 5.7.4 explains how public holidays can be entered in to the system.

Once you have entered your on-call times, handover time, public holiday preferences, and exception day settings, click on [Save](#) to apply the changes made.

On-Call Times for team Windows Systems

based on (UTC +02) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

On-Call Times
When is your team on-call?
 24x7 On-Call

Start	End	
Mon 18:00	Tue 09:00	<input checked="" type="checkbox"/>
Tue 18:00	Wed 09:00	<input checked="" type="checkbox"/>
Wed 18:00	Thu 09:00	<input checked="" type="checkbox"/>
Thu 18:00	Fri 09:00	<input checked="" type="checkbox"/>
Fri 17:00	Mon 09:00	<input checked="" type="checkbox"/>

Duty Handover
When do you hand over on-call?
09:00

Public Holidays
How do you handle public holidays?
 No on-call service
 Use regular on-call times
 Custom times

Start	End
00:00	24:00

Exception Days
When are the on-call times on exception days?

Start	End
00:00	24:00

5.7.2 On-Call Scheduling

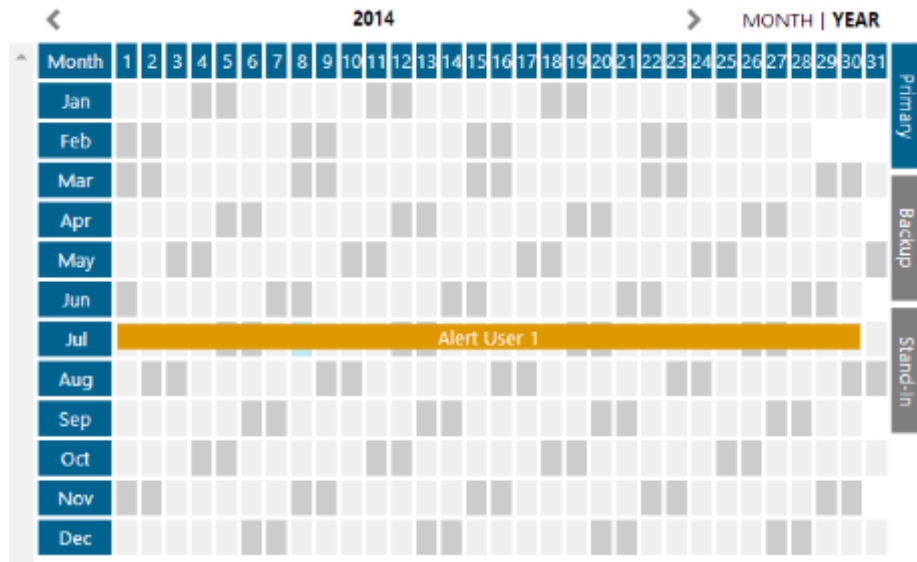
On-call scheduling has been made very easy and is based on drag & drop, which simply involves selecting a team member on the left side, dragging the member into the schedule and dropping the member on the preferred day. Once placed on the schedule, you can extend or reduce the on-call duration of the team member by dragging or beginning or end of the assignment bar to another day.



Month View and Year View

You can schedule your on-call service in either a month view or in a year view. The on-call calendar will be displayed in the month view by default. You can switch views in the top right corner by clicking either on

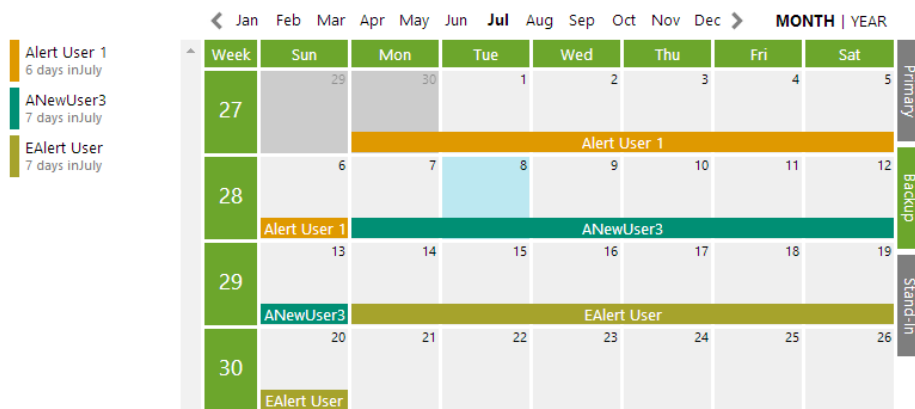
“MONTH” or on “YEAR”. The scheduling functionality is the same in both views, which means you can assign, reassign or swap on-call duties in both views.



Primary and Backup Scheduling

You can schedule primary and backup on-call engineers. If a backup on-call engineer is scheduled, the backup engineer will only receive an alert notification if the primary on-call engineer missed the alert or is “offline”. Most companies only work with a primary on-call engineer and do not have a backup level due to increased costs this model may involve.

You can only schedule a backup or primary depending on the active layer you are in. You can activate or switch between primary or backup layers by clicking on the tab on the right hand side of the schedule. In the active layer, the primary or backup assignments for the corresponding inactive layers are shown in gray.



Please note that in the above example, the on-call duty of Rene and Kay does not end on Wednesday, July 03 at 00:00. It ends instead at the configured handover time on Wednesday, July 03. An on-call assignment bar in the schedule only indicates that the person starts an on-call duty at the handover time on the day where the assignment bar begins.

Stand-Ins

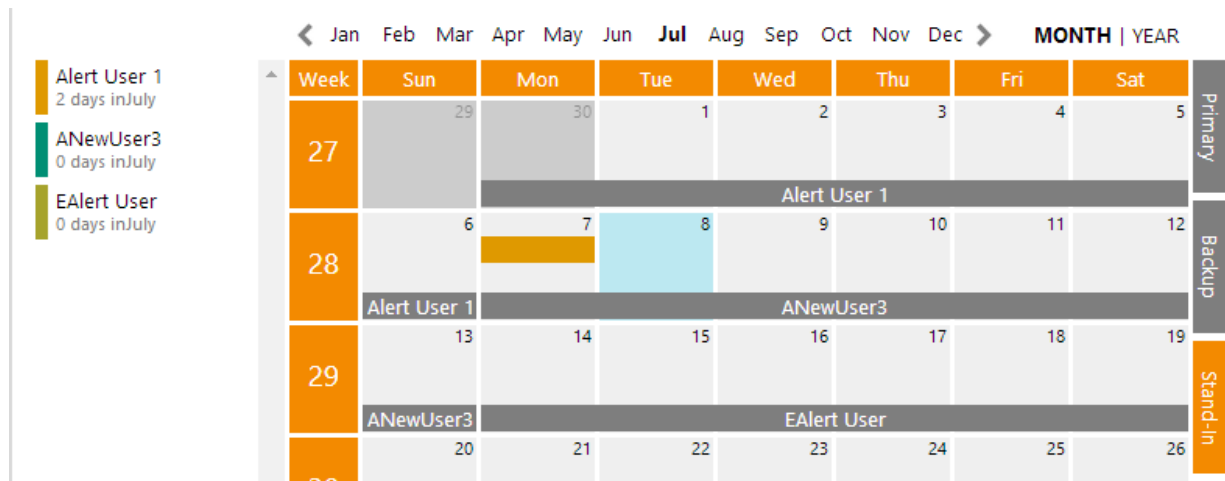
Stand-Ins are a way to reflect changes that may be necessary when unforeseen events occur. Examples are doctors appointments or other important personal circumstances for the primary on-call person. Stand-Ins can only be added for the primary on-call engineer. If the backup engineer has an appointment or becomes sick, the schedule in the backup layer must be adjusted directly.

To add a new stand-in, click on the Stand-In tab on the right. Afterwards, select a team member to become the stand-in by dragging them onto the schedule. A dialog appears which lets you enter the stand-in time on the day on which you dropped the stand-in team member.

The dialog box is titled "Stand-Ins" and contains the question "When is the stand-in?". It features a table with three columns: "Start", "End", and "Stand-In". The "Start" field contains "12:00", the "End" field contains "13:00", and the "Stand-In" field contains "Alert User 1". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Start	End	Stand-In
12:00	13:00	Alert User 1

A corresponding stand-in bar will be visible in the schedule, once you have entered the stand-in time.



Please note that stand-ins can only be added for the primary on-call person.

In order to remove a stand-in assignment, click on the stand-in bar in the stand-in layer. In the dialog that opens, click on Delete.

Stand-Ins

When is the stand-in?

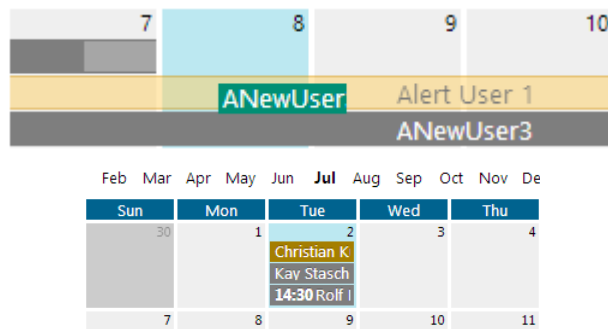
Start	End	Stand-In
12:00	13:00	Alert User 1

OK Cancel

In this dialog, it is also possible to adjust the length of an existing stand-in by changing the times and clicking on **OK** once finished.

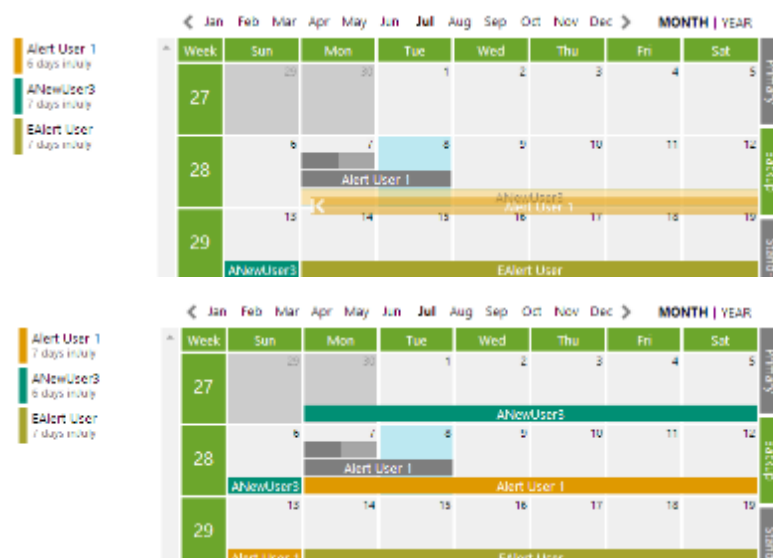
Reassigning Shifts

An on-call assignment can easily be re-assigned. To re-assign an existing on-call duty to another team member, simply drag the member from the left straight onto the bar of the existing on-call duty. Upon dropping the selected member, the existing on call member will be replaced.



Swapping Shifts

On-call assignments can also be swapped very easily. This can be done by simply dragging an existing on-call assignment bar onto the other existing on-call bar. This will swap the assignments accordingly.

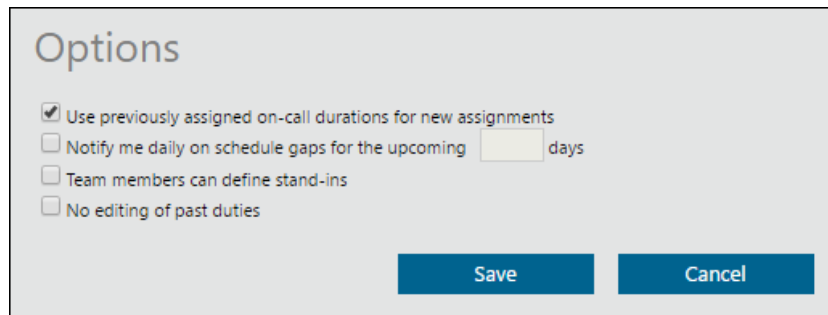


Scheduling Preferences

When a new member is dropped onto the on-call schedule, they will be scheduled for one day only by default. This behavior can be changed such that the length of each successive on-call assignment assumes the length of the preceding on-call assignment automatically.

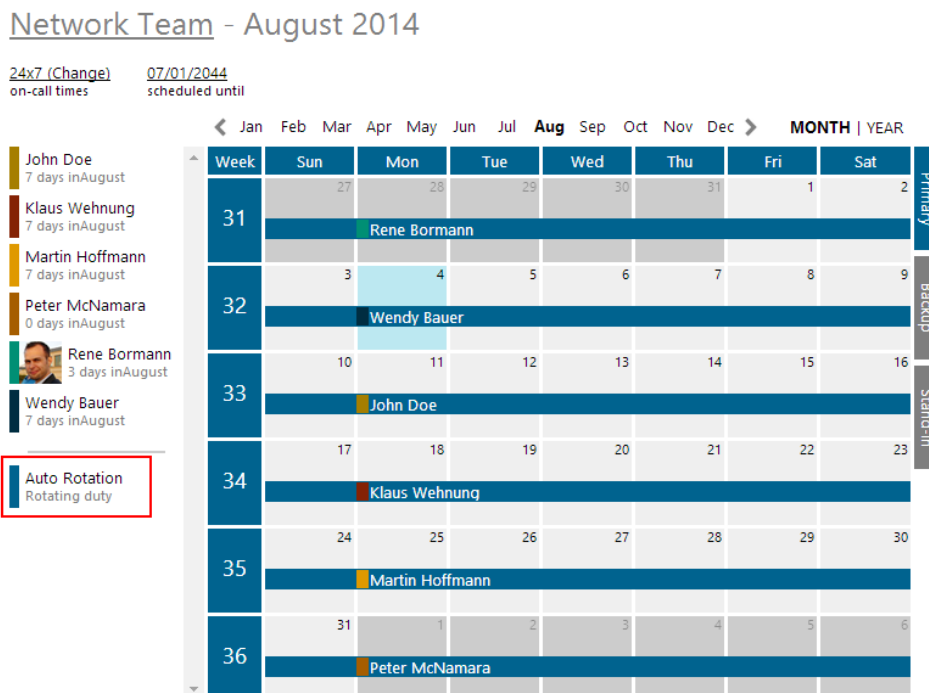
In order to use this behavior, first open the on-call schedule and then click on the [Options icon](#) on the bottom left corner.

In the dialog that appears, select the option "Use previously assigned on-call durations for new assignments" and click on [Save](#).

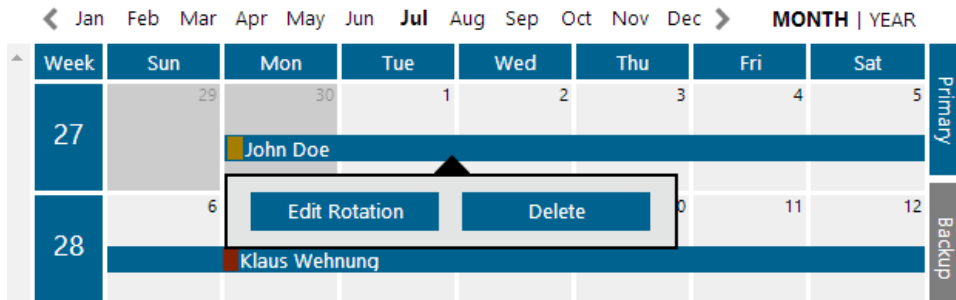


5.7.3 Auto Rotation

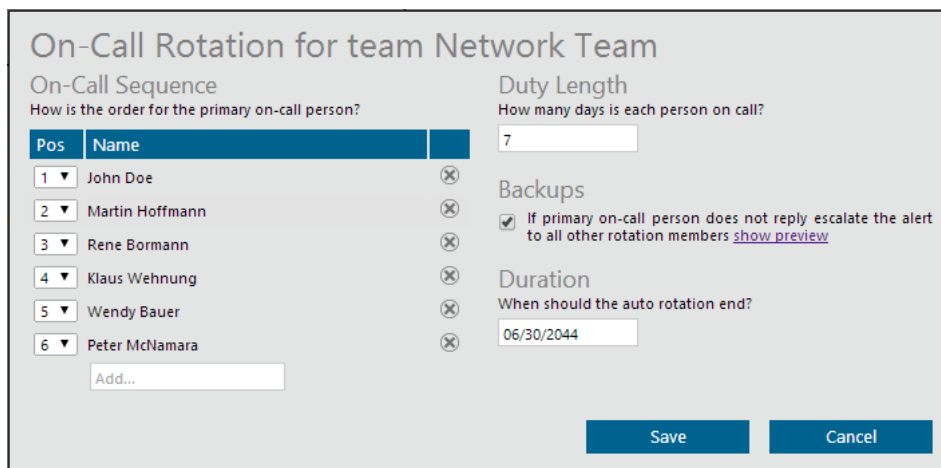
When scheduling team members for primary on-call schedules, it is also possible to setup an Auto Rotation to make long-term on-call scheduling easier. Creating an Auto Rotation for any team is very similar to regular on-call scheduling, simply drag the Auto Rotation tile from the resource menu on the left side of the On-call schedule directly onto the calendar:



Once the Auto Rotation is dropped into the calendar, simply click on the bar and select "Edit Rotation" to configure the rotation settings:




The following dialog box will appear:



In the rotation configuration you can edit the following settings:

- On-Call Sequence

Here you can add users, remove users, and define the order that the team-members will be rotated through. To add a user, type their name into the text-box at the bottom of the list; they must be a member of the current team to be added. To remove a user simply click the  to the right side of their name. To change the order, select the desired order number from the drop box to the left side of the specified user's name.

On-Call Sequence
How is the order for the primary on-call person?

Pos	Name	
1 ▼	John Doe	⊗
2 ▼	Klaus Wehning	⊗
3 ▼	Martin Hoffmann	⊗
4 ▼	Peter McNamara	⊗
5 ▼	Rene Bormann	⊗
6 ▼	Wendy Bauer	⊗

Add...

▪ **Duty Length**

This property defines how long each user in the rotation will be on-call during their designated time slot. Simply enter the number of days desired for each rotation.

Duty Length
How many days is each person on call?

▪ **Backups**

Enabling this property will allow escalation through each team-member in the Auto Rotation when the primary user on-duty fails to acknowledge an alert. When the primary user does not respond to an alert, the alert will be passed onto the team-member who is on call for the next time period. If the second user fails to respond, the escalation will continue to the person who is on-call for the third time period, and so on.

< Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec > MONTH | YEAR

Week	Sun	Mon	Tue	Wed	Thu	Fri	Sat	
27	29	30	1	2	3	4	5	Primary
		John Doe	Klaus Wehning -> Martin Hoffmann -> Peter McNamara -> Rene Bormann					
28	6	7	8	9	10	11	12	Backup
		Klaus Wehning	Martin Hoffmann -> Peter McNamara -> Rene Bormann -> Wendy Bauer ->					
	13	14	15	16	17	18	19	

▪ **Duration**

This setting defines when the entire rotation sequence will end. After this date, you must define on-call users individually, or create an additional Auto Rotation.

Duration
When should the auto rotation end?

After all settings are defined to your satisfaction, click "Save" to confirm and finalize your changes.

5.7.4 Public Holidays

You can enter in public holidays that are applicable to the corresponding Team's work location. This is useful when your on-call procedures or on-call times are different on public holidays.

All public holidays are highlighted in the on-call calendar, making it easier for Team Leaders to balance the holiday on-call assignments between team members in order to prevent the same engineer always being on call on public holidays.

Public holidays can either be entered directly in the team details or by clicking on the palm icon label 'Holidays' in the bottom left corner of the on-call schedule. The following dialog will then be displayed:

Select public holidays for team Nathan's Team

2014

Jan	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Feb	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28			
Mar	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Apr	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
May	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Jun	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Jul	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Aug	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Sep	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Oct	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Nov	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Dec	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Save Cancel

In the dialog, simply click on all days which are public holidays at the Team's work location and click [Save](#).

Select public holidays for team Nathan's Team

2014

Jan	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Feb	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28			
Mar	1	2	3	4	5	6	7	8		10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Apr	1		3	4	5	6	7	8	9	10	11	12	13	14		16	17	18	19		21	22	23	24	25	26	27	28	29	30	
May	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Jun	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Jul	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Aug	1	2	3	4	5	6	7		9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Sep	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19		21	22	23	24	25	26	27	28	29	30	
Oct	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Nov	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Dec	1	2	3	4	5	6	7	8	9	10	11	12	13	14		16	17	18	19	20	21	22	23	24			27	28	29	30	31

Save Cancel

5.7.5 PDF-Export

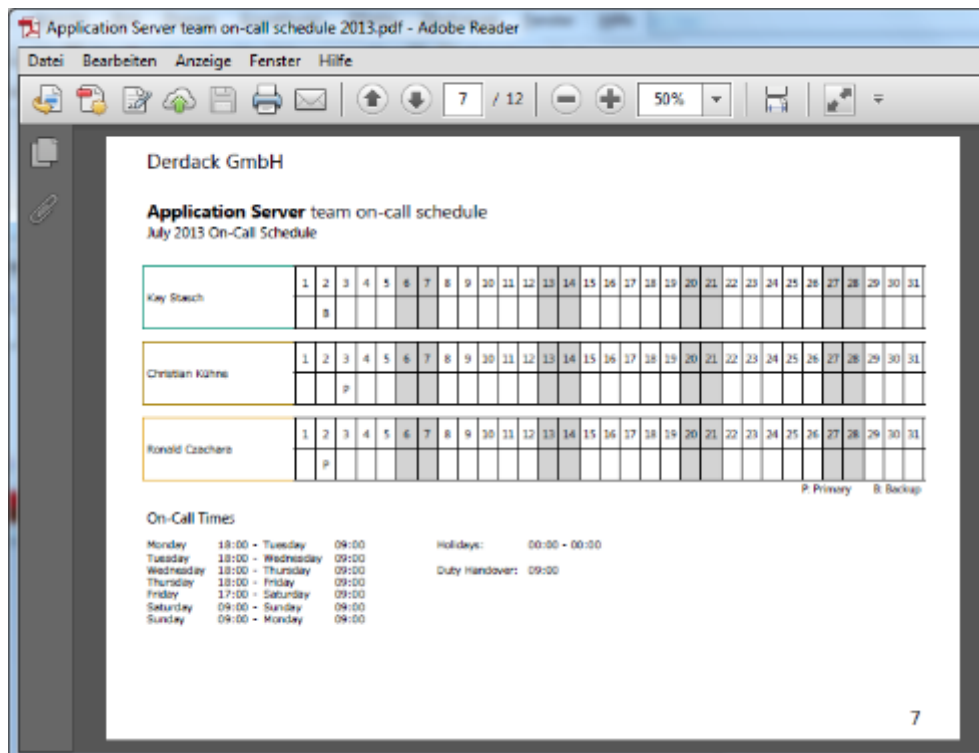
You can export your on-call schedule as a PDF document. This is useful when you need to print out the schedule e.g. if you would like to hang it out in the Team's workplace. You may also want to send the on-call schedule as PDF to all scheduled team members.

The content of the exported PDF document depends on whether you export it from the month view or from the year view. In the month view, only the currently displayed month is exported, while all the months in the currently displayed year are exported when in the year view. In this case, approximately 12 pages are exported i.e. about 1 page for each month.

To export the PDF document, click on the [PDF Export icon](#) on the bottom left. After the document has been generated, you will be prompted for the download location of the PDF file, depending on your browser configuration.



Save the file to your disk and open it in Adobe Acrobat or send it in an email to your team members.



5.7.6 Gap-Reminders

So-called gap reminders are useful for preventing gaps in your on-call schedule where nobody is scheduled for handling incidents during the operated on-call service times. Gap reminders were designed for team leaders, who along with their team members, need to regularly maintain the on-call schedule. They are sent as an email after the team leader subscribes to the notifications.

To subscribe to receiving gap reminders, open the on-call schedule for the corresponding team and click on the [Options icon](#) in the bottom left corner.



In the dialog that appears, check the option "Notify me daily on schedule gaps for the upcoming X days" and enter the number of days to check for schedule gaps in advance.

If activated, the system will check daily whether the schedule contains one or more unassigned days for the period starting from the current day and ending after the entered number of days.

Options

- Use previously assigned on-call durations for new assignments
- Notify me daily on schedule gaps for the upcoming days
- Team members can define stand-ins
- No editing of past duties

Save
Cancel

By default, the gap reminder email will then be sent daily at 10am if applicable.

5.7.7 Publishing Contact Address Information

Enterprise Alert® enables you to select which contact address information is shown for example in the exported PDF version of the on-call schedule or in the “Who’s on call” overview. This is useful for those who need to be able to quickly contact the on-call engineer in the event of an incident.

You can select which contact address information may be made public in the previous PDF and overview by first opening the Team details. Then select the contact addresses to make public in the dropdown “Public contact addresses in on-call overviews” of the General Tab and click on [Save](#).

Windows Systems

General | Managers (1) | Members (8) | Times | Notification Feeds | Ownership

Property	Value
Activated	<input checked="" type="checkbox"/>
Name *	Windows Systems
Public contact addresses in on-call overviews	Select up to four public contact addresses
Display on-call person name in Who's on Call	<input type="checkbox"/> SMS
Display team managers in Who's on Call	<input type="checkbox"/> Voice-Call (Work)
	<input type="checkbox"/> Voice-Call (Home)
	<input type="checkbox"/> Voice-Call (Mobile)
	<input type="checkbox"/> Instant Message
Description	<input type="checkbox"/> E-mail

None of the contact addresses are shown by default, so you will need to explicitly select the addresses you would like to make accessible. This is to ensure that only the contact address information that is in line with your company policy is displayed.

5.8 On-Call Management

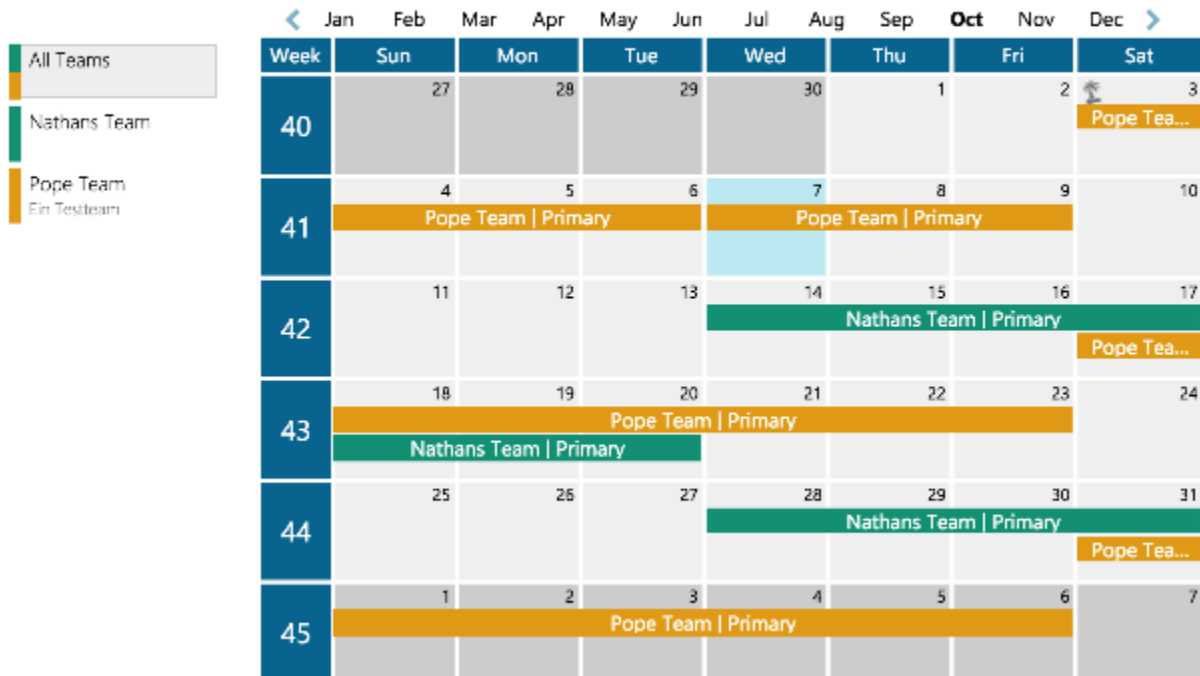
This section contains information for on-call engineers and explains how they can manage their on-call duties.

5.8.1 My On-Call Calendar

Team members with on-call assignments can identify when they are on-call in their personal on-call calendar. This calendar can be opened from the Personal tab of the Enterprise Alert Web Portal, then clicking on the “My On-Call Calendar” tile.

The screenshot shows the Enterprise Alert Web Portal interface. On the left is a navigation sidebar with icons for Home, Alerts, Callouts, People, On Call, Remote Actions, System, Analytics, and a user profile for Rene Bormann. The main content area is titled 'Welcome Rene Bormann' and features an 'Activity in Last 24h' chart showing 'Created Alerts' (orange) and 'Incoming Events' (blue). Below the chart is a 'Shortcuts' section with tiles for 'Alert Center' (0), 'Insights' (0), 'My On-Call Calendar' (highlighted with a red border), 'Enterprise Hub Edition' (183 users remaining), 'My Profile', and 'Logout'. To the right is an 'Endpoints' section listing various URLs for the Web Portal, Mobile App, and Web Services.

My On-Call Calendar - October 2015



The default view ("All Teams") displays the on-call assignments across all Teams the on-call engineer is a member of. This is useful when the engineer is on call for more than one service, which may be the case when the engineer is a member in multiple *Teams*. The "All Teams" view will only be displayed if the user has on-call assignments in more than one Team, otherwise the team-specific view below will be shown by default.

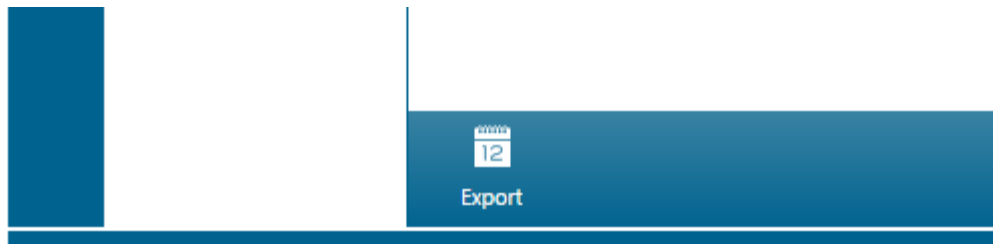
To only display the on-call assignments for a specific service or Team, simply click on the Team name on the left side. This will display the personal on-call assignments as colored bars and the on-call assignments of other team members as grey bars.

For on-call engineers this view may be useful to identify which colleagues are on call and to swap on-call duties where needed e.g. for important personal appointments.

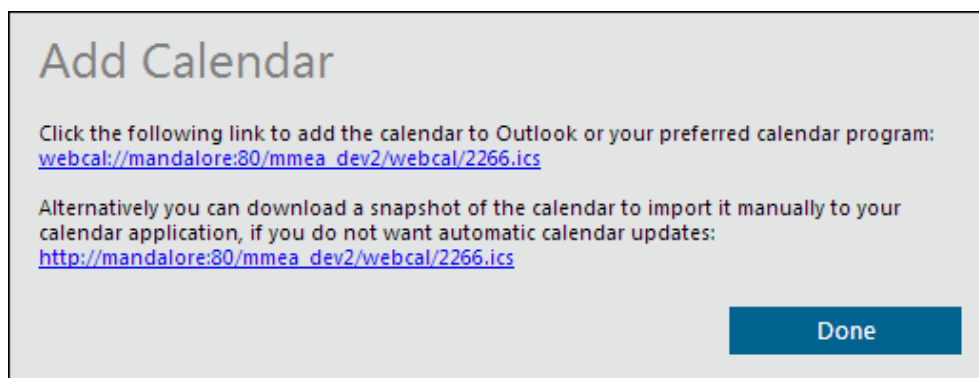
5.8.2 ics-Export to Outlook and others

On-call engineers can export their personal on-call calendar to an iCalendar(ics)-compatible calendar application such as Microsoft Outlook. The calendar export is available as webcal URI (web calendar format) or as a direct HTTP URI for download.

To export the on-call schedule in ics format, first click the [Calendar icon](#) in the bottom left corner of the on-call calendar view:



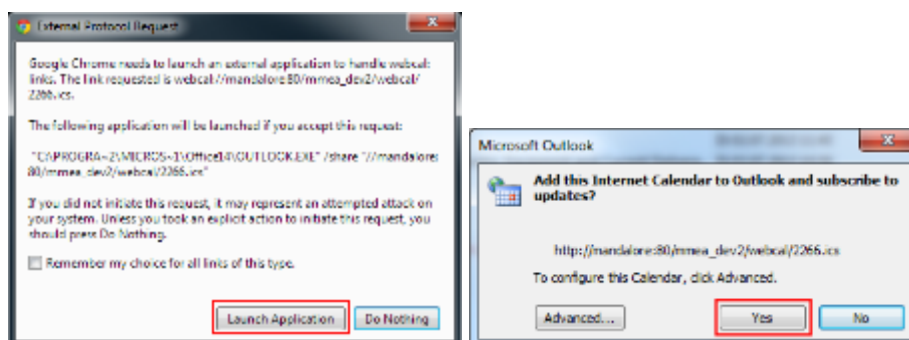
In the displayed dialog, you can now either import the calendar directly into your iCalendar-compatible application, such as Microsoft Outlook, or you can download the ics-file to your computer for later import. Both options are explained in more detail below:



Webcal URI Link

The first link in the dialog provides access to the ics calendar via a webcal URI. Webcal is a format that allows the iCalendar-compatible application to directly access the ics file over the network instead of having to download the ics file manually to your computer.

If you have a webcal compatible application such as Microsoft Outlook available when clicking on the first link, it will import the calendar and synchronize it continuously. The advantage being is that whenever you access the calendar in your application, it will always be up-to-date in case the on-call schedule in Enterprise Alert® changes.



HTTP Download Link

In contrast to the webcal export, the on-call schedule can also be downloaded as a ics-file to your computer. It can then be manually imported into an ics-compatible calendar application afterwards. However, please note that in this case only a "snapshot" of the current on-call schedule is downloaded. If the team leader changes the on-call schedule afterwards, you will have to download and reimport the ics-file.

5.8.3 Who is on call?

It may be necessary for end users or IT helpdesk personnel to quickly be able to find out who is on call when an incident occurs and to be able to contact such a person. They can do this in Enterprise Alert® by opening the “Who’s on call” page, which displays all the respective on-call engineers from all Teams that operate an on-call service.

All user roles in Enterprise Alert® except for subscription users can access the „ Who’s on call” page. It is also possible to make this page available for unauthenticated users, who otherwise have nothing else to do with Enterprise Alert®. If this scenario is relevant for you, you can contact Derdack (see section 8) for further details. The page can otherwise be opened from the dashboard by clicking on the tile “Who’s on call?”.

5.9 Remote IT Management

Especially in IT environments, some problems may be fixed through simple predefined actions, like restarting a service, a server or a VM. Other cases may merely require a confirmation of the problem or the logging of a new incident. Such simple fixes or incident logging can easily be done after receiving an alert – presuming of course that you are in the office and at your desk.

Otherwise, Enterprise Alert® provides you with Remote IT Management functionality through integrating into IT automation systems as well as with the means to initiate the actions these systems provide in a convenient and secure way.

Enterprise Alert® provides integration with the following 3rd party IT automation systems:

- System Center Orchestrator
- Windows Task Scheduler
- HP Operations Orchestration

Additionally, you can implement your remediation scripts directly with Enterprise Alert® by using the Application Programming Toolkit.

The multitude of actions these systems provide can be executed via:

- Enterprise Alert® Smartphone App
- SMS/MMS
- Email
- Voice-Call
- Instant Message

These automation systems and execution channels provide you with virtually unlimited possibilities for remote IT management in your enterprise.

5.9.1 Remote Action Policies

To enable the remote execution of an imported action from a configured IT automation system, you need to create a corresponding *Remote Action Policy*. This ensures that only the desired actions can be executed through Enterprise Alert®.

Remote Action Policies define the execution channel, provide parameter mappings and default values, allow you to add dynamic content and also manage execution permissions.

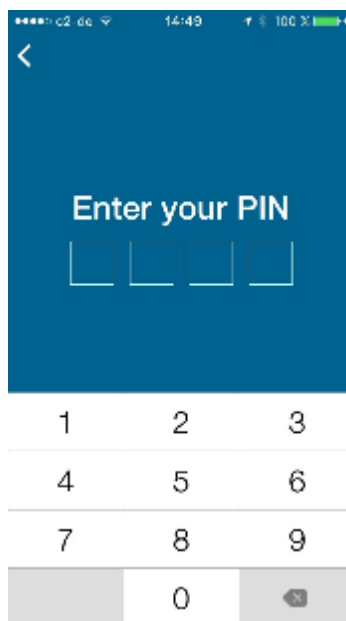
See section 4.6 Step 6 - Create a Remote Action Policy for more information on creating remote action policies and executing remote actions.

5.9.2 Security and Rights Management

Enterprise Alert® provides you with the means to significantly reduce the risk of making actions in your IT environment remotely available.

Dedicated Remote Action PIN

For remote action execution from the Smartphone App, Enterprise Alert® provides an option to request the input of a *Remote Action PIN* to confirm the identity of the user before executing the action. By default, this option is always set and should only be disabled for low risk actions.



Users need to configure their own *Remote Action PIN* on their *My Profile* page in the Enterprise Alert® Web portal. Without a *Remote Action PIN*, a user cannot execute actions which require a PIN.

Remote Action Execution Permissions

By default, all remote actions can only be executed by the user who created them. The creator must explicitly grant other users permission to execute the action. Enterprise Alert® identifies the user trying to execute the action by checking the smartphone login or contact address if the remote action has been triggered from a UC channel and verifies that the user has the required permissions to execute remote action.

To grant execution permissions to other users, add them to the permission list on the *Ownership* tab of the desired remote action. Additionally, you can also grant permissions to edit the remote action here.

The screenshot shows the 'Start Service' interface with the 'Ownership' tab selected. The table below lists the current owner and provides an input field to add a new owner.

Name	Last Executed	Times Executed
Rene Bormann		0

Below the table is an input field labeled 'Add an owner...' with a plus sign icon to its right.

The bottom bar contains three buttons: 'Save', 'Create Copy', and 'Delete'.

If the remote action requires a *Remote Action PIN* and the user does not have one configured yet, a warning will be displayed next to the user name.

5.9.3 Remote Action Parameter Values

When configuring Remote Action Policies, you can set default values for the action parameters, which the user can change before executing the action. Entering multiple default values separated by a semicolon will result in a list of possible values being made available for selection when executing the action.

Start Service

General | **Action** | Ownership

Property	Value
Action To Execute	StartService

Name	Display Name	Insert Dynamic Content	Value
Executor	Executor	<input type="checkbox"/>	Executor
Host	Host	<input type="checkbox"/>	almania
ServiceName	ServiceName	<input type="checkbox"/>	Print Spooler

Save Create Copy Delete Refresh Actions

You can also add dynamic content as a parameter value. This allows you to forward runtime execution details, like the profile name of the user executing the action, to the IT automation system. Parameters containing dynamic content will be set at the time of execution and are not visible to the user before execution.

5.10 Multi-tenancy

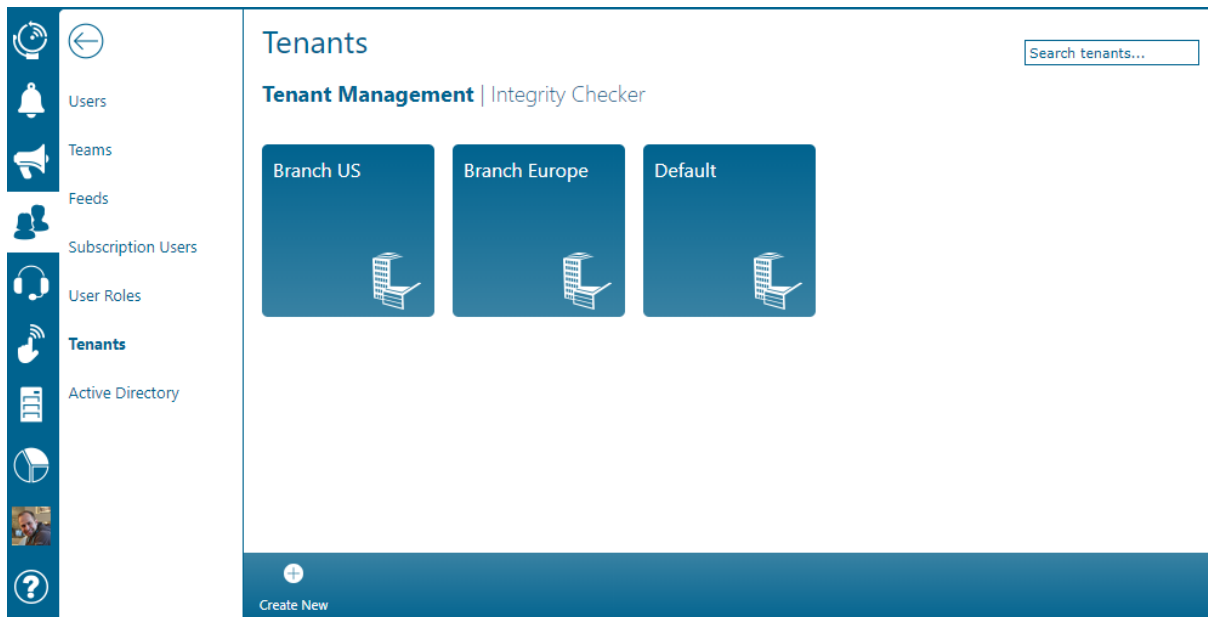
In order to segregate data on your Enterprise Alert® instance with the use of so called tenants, please make sure that your license includes the user role add-on. Otherwise you will not be able to manage tenants. In this case you may want to consider implementing data segregation with the use of the built-in ownership model which works in smaller installations fine as well.

Tenant isolation is implemented on the application layer and not on the database layer with Enterprise Alert®. All data of different tenants is still stored in one and the same database.

5.10.1 Managing tenants

Tenants can only be managed (e.g. created, updated deleted) by global system administrators in Enterprise Alert®. Other users do not see tenant related settings. Please refer to section 4.2 for further details.

The installation of Enterprise Alert® creates a default tenant for you. To create additional tenants, navigate to [People -> Tenants](#). All existing tenants will be displayed. You can right click tenants to remove them or you can click [Create New](#) to create new tenants, e.g. your branch locations that you want to provide alerting services for.



5.10.2 Entity/tenant relationships

Entities can only be assigned to tenants by global system administrators in Enterprise Alert®. Other users do not see tenant related settings. Please refer to section 4.2 for further details.

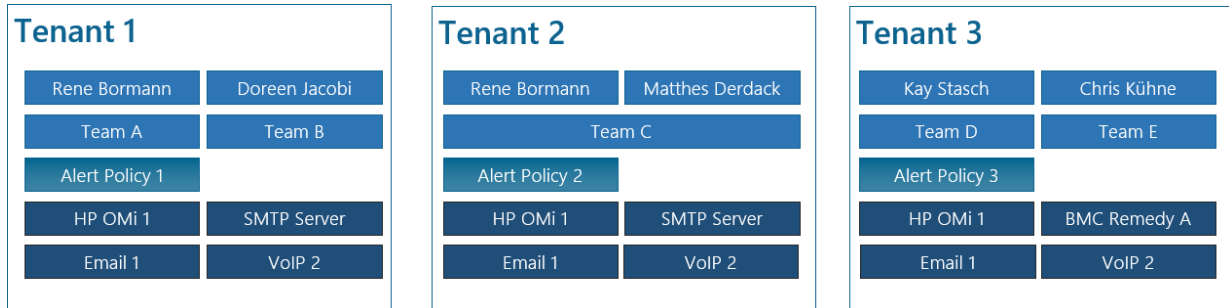
There are three relationship types between entities and tenants:

- 1:n – Indicates that the corresponding entity (e.g. a user can belong to multiple tenants)
- 1:1 – Indicates that the corresponding entity (e.g. an alert policy can only belong to one tenant at a time)
- m:n – Indicates that the entity is shared between all tenants (e.g. a notification channel)

The following table lists all entities each with their relationship type:

Relationship type	Entity type
1:n (Entity can belong to one or more tenants)	Event Source
	Event
	IT Automation System
	Remote Action Policy
	Remote Action
	Script
	User
1:1 (Entity can only belong to one tenant at a time)	Alert Policy
	Alert
	Emergency Callout
	Team
	Multi-Team Schedule
	Feed
m:n (Entity is shared across all tenants)	Notification Channel

The following illustration displays an example that includes the entity types User, Team, Alert Policy, Event Source and Notification Channel:



Assigning entities to tenants

Entities can be assigned to tenants either from the tenant details or from within the details of the entity to be assigned to a tenant. If you want to perform batch assignments, e.g. multiple policies need to be assigned to a tenant, you may want to add them in the tenant details. If you have just one entity (e.g. a user changed departments, you may want to look up that user profile and assign the tenant in the user profile details.

Tenant Details

Click on a tenant tile to open its details and select [Entities](#).

The table that is displayed shows all entities to which members of the tenant can have access to. This includes event sources or scripts that have not been assigned to a specific tenant but where assigned to all tenants and are thereby “public”. You can filter that page by entity type by clicking on the corresponding tags above the table.

To remove an entity from a tenant, it must be assigned to another tenant. In other words you cannot have tenant-less entities in Enterprise Alert®. Find the entity in the table and either deselect the current tenant in the dropdown (for entities which can belong to multiple tenants) or select the new tenant (for entities that can belong to only one tenant at a time)

The screenshot shows the 'Branch US' entities page in the Derdack Enterprise Alert interface. The page has a navigation sidebar on the left with options like Users, Teams, Feeds, Subscription Users, User Roles, Tenants, and Active Directory. The main content area is titled 'Branch US' and 'Entities'. It features a search bar, a filter menu (All, Users, Teams, Subscription Users, Feeds, Policies, Other), and a table of entities. The table has columns for Name, Description, and Assigned to. The 'Assigned to' column shows a dropdown menu with options: All Tenants (Public), Branch US, Branch Europe (selected), Default, and All Tenants (Public). At the bottom of the table, there are buttons for Save, Refresh, and Delete.

Name	Description	Assigned to
Sensor Alerts		Daimler
Android Push		All Tenants (Public)
Cil_Rene		Branch US
File Interface		Branch Europe
SMTP Server		Default
Contoso		All Tenants (Public)
CreateMessages		All Tenants (Public)
Demo Duty Reminder		All Tenants (Public)

Entity Details

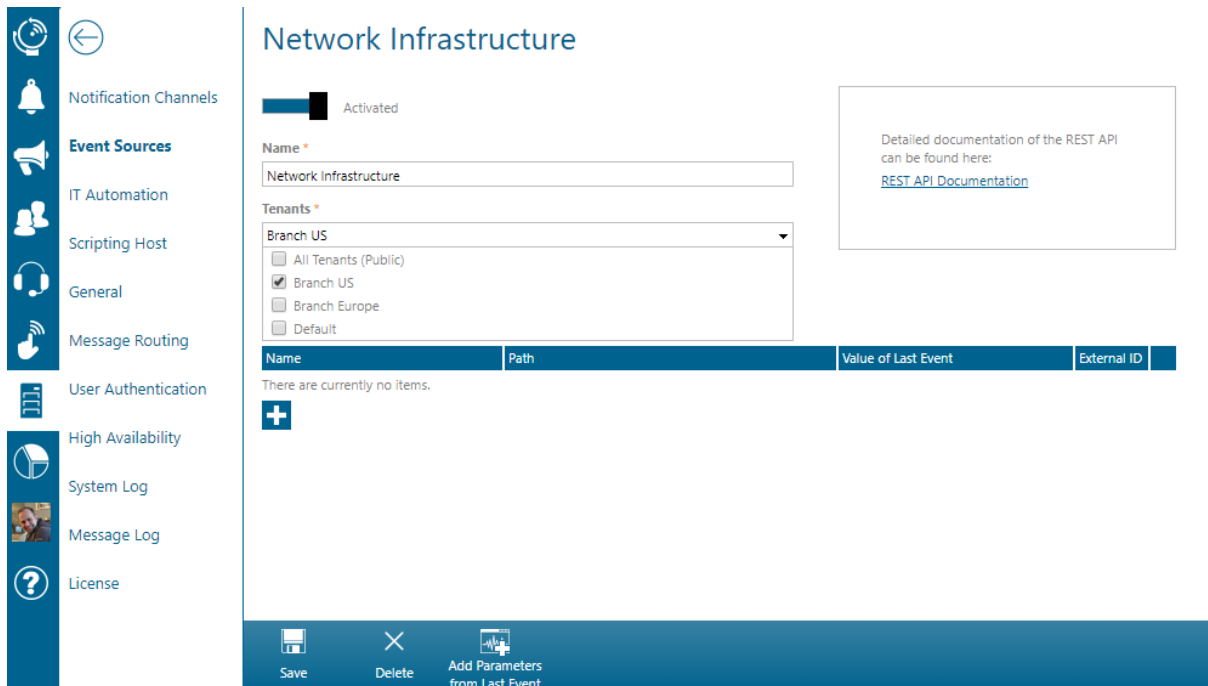
The following example discusses how to assign an individual event source of your Enterprise Alert® instance (e.g. a REST API) to a dedicated tenant. It is thereby not public and events are only visible to users who belong to that tenant and have sufficient permissions to view events. Global system administrators can still see all events (regardless of which tenant they belong to) in Enterprise Alert®.

Open [System -> Event Sources](#), find your source and open its details by clicking on it.

The displayed entity details contain a field called "Tenant" and is used to assign it to one or more tenants depending on the entity type (see 4.10.2). If the entity should be available in all tenants, select "All Tenants (Public)".

This principle is the same for all entities except for notification channels which cannot be assigned and are used to send and receive notifications from/for all tenants. They are shared.

In the details of all these entities (see right column above) you will find the tenant field that defines to which tenant(s) the corresponding entity belongs.



5.10.3 Integrity Checker

All entities in Enterprise Alert® (refer to the right column in 4.10.1) do not only have a relationship to one or more tenant(s) but they also have relationships between each other.

Lets take the following example (capital words are entities):

An EVENT received from EVENT SOURCE which triggers an ALERT POLICY that notifies a USER from a TEAM.

In this scenario the entities EVENT, EVENT SOURCE, ALERT POLICY, USER and TEAM are in a relationship.

The entity that "builds" this relationship is the ALERT POLICY.

In this example you would want each entity belonging to the same tenant. In other words, you would not want that the ALERT POLICY belongs to a tenant "Branch US" while the TEAM that is notified via the alert policy belongs to a tenant "Branch Europe".

When you setup e.g. an alert policy from scratch you can only apply it to event sources that belong to the tenant that you have chosen for the new policy as well. Likewise you can only select notification targets from within the same tenant as the alert policy belongs to.

However, you can at any time open up the the details of an individual entity (e.g. the TEAM) and (re)assign it to a different tenant. It may then no longer be in the same tenant as the alert policy that has this team set as notification target and creates a so called relationship breach.

To be able to manage this situation, Enterprise Alert® contains the so called "Integrity Checker". The integrity checker can scan your system topology and identify breaches in your entity/tenant relationships. Each breach is displayed as an inconsistency on the integrity checker page.

To open the integrity checker, nativgate to [People -> Tenants](#) and click "Integrity Checker".

Tenant	Inconsistency
Default	Policy Voice To Alert is assigned to tenant Default but destination team Kay's Team is not.
Default	Policy WebEvent is assigned to tenant Default but destination team kays is not.
Default	Remote Action Ping is assigned to tenant Default but owner Rene is not.
Default	Callout General Emergency is assigned to tenant Default but owner Rene is not.
Default	Callout Fire Alert is assigned to tenant Default but destination user Kay Connor is not.
Default	Callout Fire Alert is assigned to tenant Default but destination team kays is not.
Default	Callout Fire Alert is assigned to tenant Default but owner Kay Connor is not.
Daimler	Policy Sensor Alerts is assigned to tenant Branch US but destination team Response Team is not.

The integrity checker runs as part of your alerting workflows which means, that new inconsistencies may appear on the page automatically.

You can also manually trigger an integrity check by clicking on [Start Integrity Check](#). The check itself is an asynchronous job which means that you may have to come back later to that page in order to see new results.

If you see inconsistencies on the page, you can open the involved entities directly (follow the shortcuts) and assign them to the same tenant. Afterwards you can click the refresh icon of that inconsistency row. If you have resolved the inconsistency, it should disappear after refresh.

6 SUPPORT

Derdack delivers a portfolio of professional services to guarantee efficient and fast deployment and successful and profitable operation and maximum exploitation of its Enterprise Alert® software. Derdack offers its know-how and expertise within optional support and service agreements.

24x7 Support and Preemptive Maintenance

Derdack's Germany-based support center provides global support services via phone, email, instant messaging and remote access on a 24x7 basis, 365 days a year. All support incidents of contracted customers are rated and handled according to a defined ticket and escalation procedure with guaranteed response and resolution times. With 24x7 Premium Support Derdack also offers preemptive maintenance i.e. regular system audits for optimum runtime environments and continuity.

Deployment Consultancy and Services

To ensure the optimal integration of Enterprise Alert® software into the business processes of our customers, all software deliveries of Derdack are based on a thorough analysis of customer requirements. A dedicated deployment plan is the foundation of every single software installation by qualified Derdack engineers.

Worldwide On-site and Remote Deployments

Derdack offers global installation and deployment services – according to customer preferences either on-site or remotely. Derdack has especially trained deployment engineers who are able to conduct successful installation of even complex scenarios within a few days.

Technical Trainings

Derdack offers both mobile service design and operational support training enabling customers to self-maintain and manage Enterprise Alert® software and to develop innovative service applications on top of it. A first training session is usually part of the deployment process. Additional training can be organized in Germany or at the customer site.

Software Update Insurance

As a vendor of standard software products Derdack provides patches and fixes, service packs and updates on a regular basis and according to a software lifecycle process. Customers can sign a software update insurance contract to benefit from a continuous flow of both minor and major updates.

Please contact sales@derdack.com for further information on support and maintenance offerings.

6.1 Important Links

Technical Blog: <https://www.derdack.com/category/technical-blog/>

7 ABOUT

Derdack is an independent software vendor offering advanced enterprise notification and rapid response software. Derdack's premium products help clients to automate alert notifications and to communication-enable business processes and applications. Derdack is recognized for its intuitive yet inspiring software products and has customers in over 50 countries worldwide. Derdack was founded in 1999 and its corporate headquarters are in Berlin, Germany.

8 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>

9 CONTACT

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

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

9.1 Mailing Address

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

Derdack GmbH
Friedrich-Ebert-Straße 8
14467 Potsdam
Germany

9.2 Hours of Operation

Monday – Friday 09:00 a.m. – 06:00 p.m. Central European Time (GMT+1)

Closed Saturday and Sunday and on German and local public holidays

10 DISCLAIMER

© 2019 Derdack GmbH. All rights reserved. This document is for information purposes only. Derdack GmbH makes no warranties, express or implied, in this document. Enterprise Alert is a registered trademark of Derdack GmbH in the EU, the US and other countries. The names of actual companies and products mentioned herein may be trademarks of their respective owners.