STORM Manual

Release 8.0

OTRS AG

20.01.2021

Inhalt

KAPITEL 1

Dark Theme

STORM führt ein eigenes „Dark Theme “für die Anmeldeseiten, das Agenten-Interface und für das Administrator-Interface ein. Das „Dark Theme “ist standardmäßig aktiviert.

Die Agenten können das Standardthema von OTRS wiederherstellen und sie können jedes andere Thema auswählen, das aus dem OTRS-Framework bekannt ist.

Siehe auch:

Bitte lesen Sie im Benutzerhandbuch nach, wie Sie change the theme.

Die Administratoren können das Thema im Agenten-Interface ändern.

So wechseln Sie ein Thema:

1. Gehen Sie im Administrator-Interface zum Modul *Agenten*.
2. Wählen Sie den Agenten aus der Liste der Agenten aus.
3. Klicken Sie in der linken Seitenleiste auf die Schaltfläche *Persönliche Einstellungen für diesen Agenten bearbeiten*.
4. Wählen Sie die Gruppe *Verschiedenes*.
5. Ändern Sie das Thema im Abschnitt *Administrator-Interface Thema*.

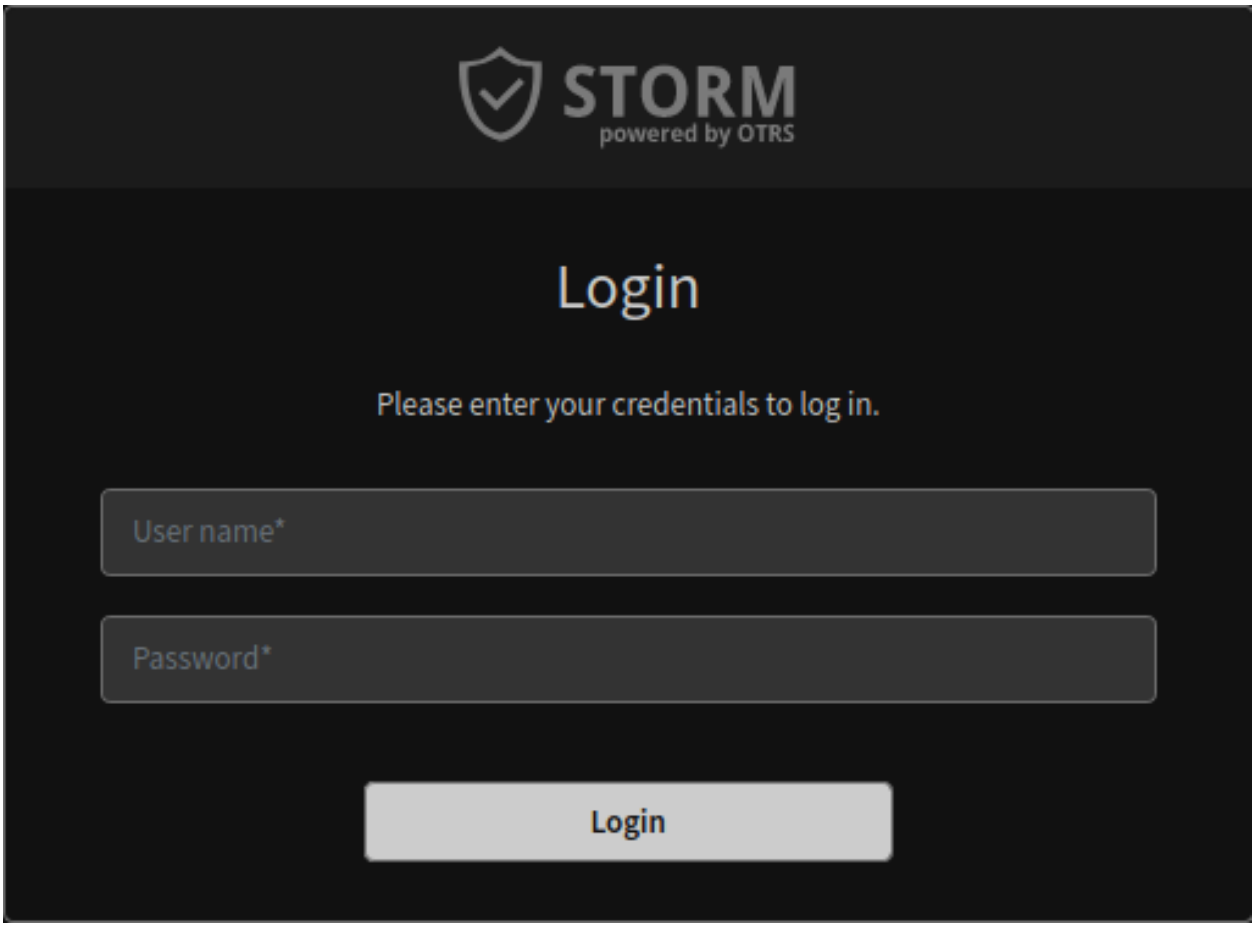


Abb. 1: Anmeldebox mit „Dark Theme “

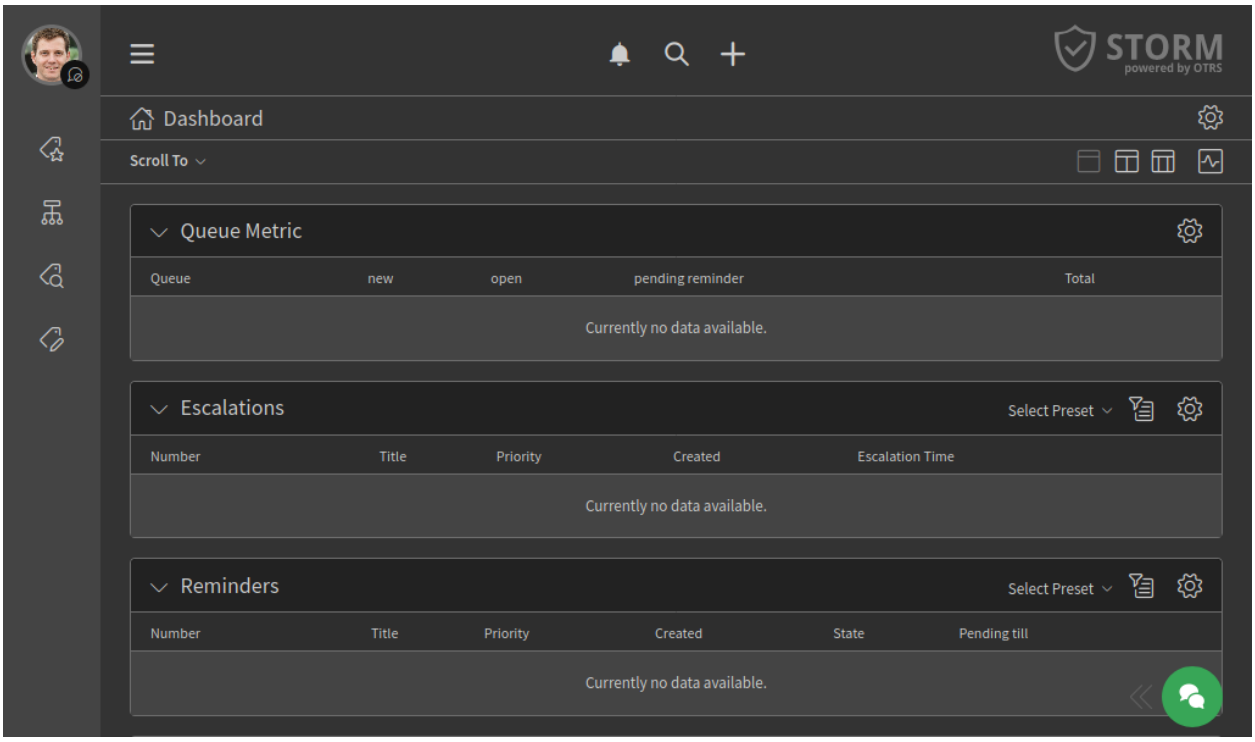


Abb. 2: Agenten-Interface mit „Dark Theme “

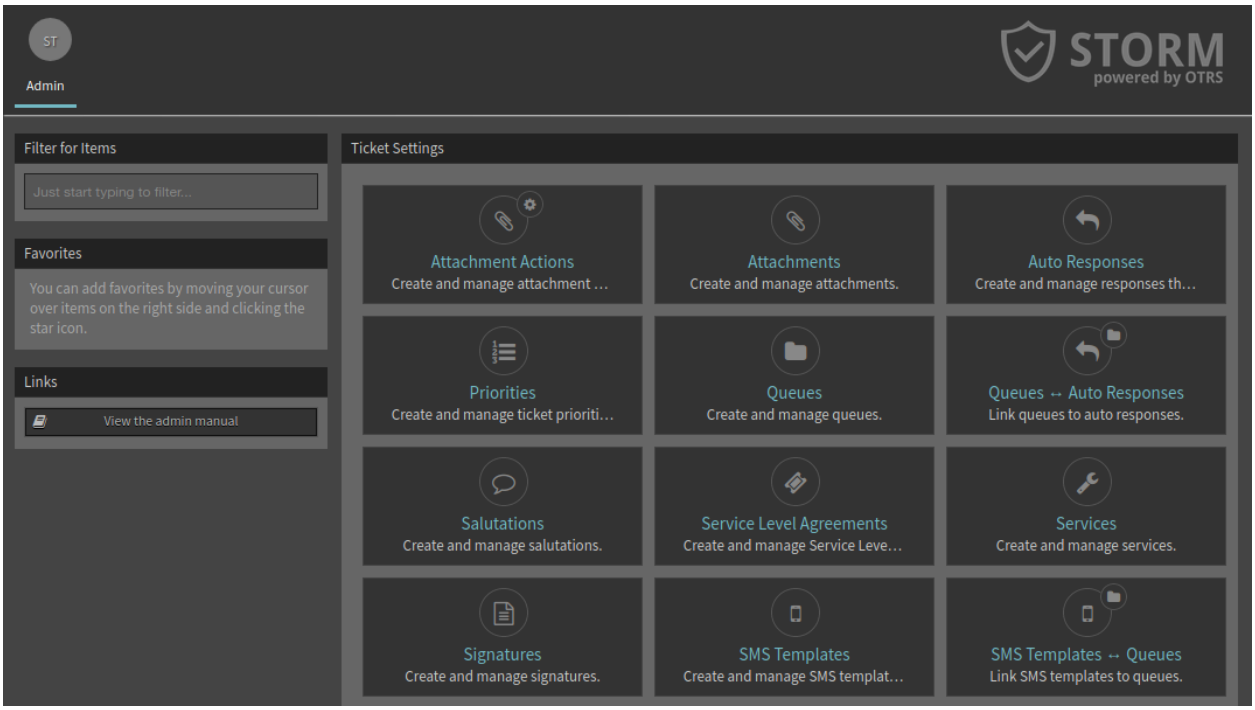


Abb. 3: Administrator-Interface mit „Dark Syle “

KAPITEL 2

Einschränkung der Kommunikation

Ausgehende Kommunikation aus der Anwendung ist standardmäßig eingeschränkt. Die Einschränkungen können über die Systemkonfiguration aufgehoben werden. Die Einschränkungen begrenzen die folgenden Funktionen:

Widget „Neuigkeiten “ Die Standardkonfiguration des Widgets *Neuigkeiten* würde einen Webservice-Aufruf an cloud.otrs.com erfordern und ist daher standardmäßig deaktiviert.

Paketverwaltung Der Paketmanager hat zwei Möglichkeiten der Bedienung. Der Administrator kann das Paket manuell hochladen und installieren oder es kann ein Online-Repository verwendet werden. Dieses Repository ist standardmäßig deaktiviert. Auch der Verifizierungsmechanismus für Pakete ist deaktiviert. Daher wird *OTRSVerify* nicht funktionieren und es kann eine Warnung in der Weboberfläche auftreten.

Cloud-Services Automatische Cloud-Service-Verbindungen zur OTRS-Gruppe sind standardmäßig deaktiviert. Dies schränkt die Nutzung von SMS, automatischer Lizenzprüfung und Registrierungs-Update ein. Um die erforderliche Lizenzprüfung durchzuführen, muss ein Administrator diese manuell über das *STORM Management Module* ausführen.

KAPITEL 3

STORM Management Module

Es gibt eine Änderung in der Systemkonfiguration, die die normale Kommunikation zwischen der STORM-Instanz und der OTRS-Gruppe einschränkt.

Aufgrund der Kommunikationsbeschränkung ist es nicht möglich, die Registrierungsinformationen regelmäßig zu versenden. Im OTRS-Framework wird dies vom Daemon erledigt, in STORM geschieht dies jedoch nicht automatisch. Es gibt jedoch ein separates Modul *STORM* in der Gruppe *OTRS Group Services* im Administrator-Interface. Verwenden Sie diese Ansicht, um Registrierungs-Updates und Vertragsstatus-Prüfungen manuell zu versenden, um sie an die Bedingungen Ihrer Sicherheitsumgebung anzupassen.

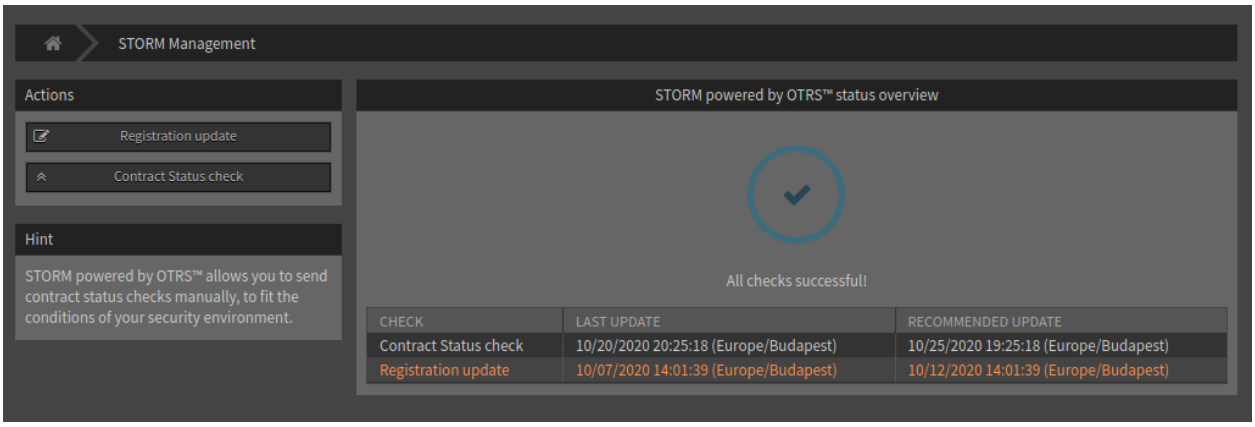


Abb. 1: STORM Verwaltungsansicht

Die Vorschau der zu versendenden Daten kann vor dem Versenden überprüft werden. Diese Methode stellt sicher, dass keine sensiblen Daten an die OTRS Group gesendet werden.

So senden Sie eine Aktualisierung der Registrierung:

1. Klicken Sie in der linken Seitenleiste auf die Schaltfläche *Registrierung aktualisieren*.
2. Überprüfen Sie die Systemregistrierungsdaten, die an die OTRS Group gesendet werden sollen.
3. Stellen Sie sicher, dass die Kommunikation mit der OTRS Group nicht blockiert wird.

4. Klicken Sie auf die Schaltfläche *Übermitteln*.

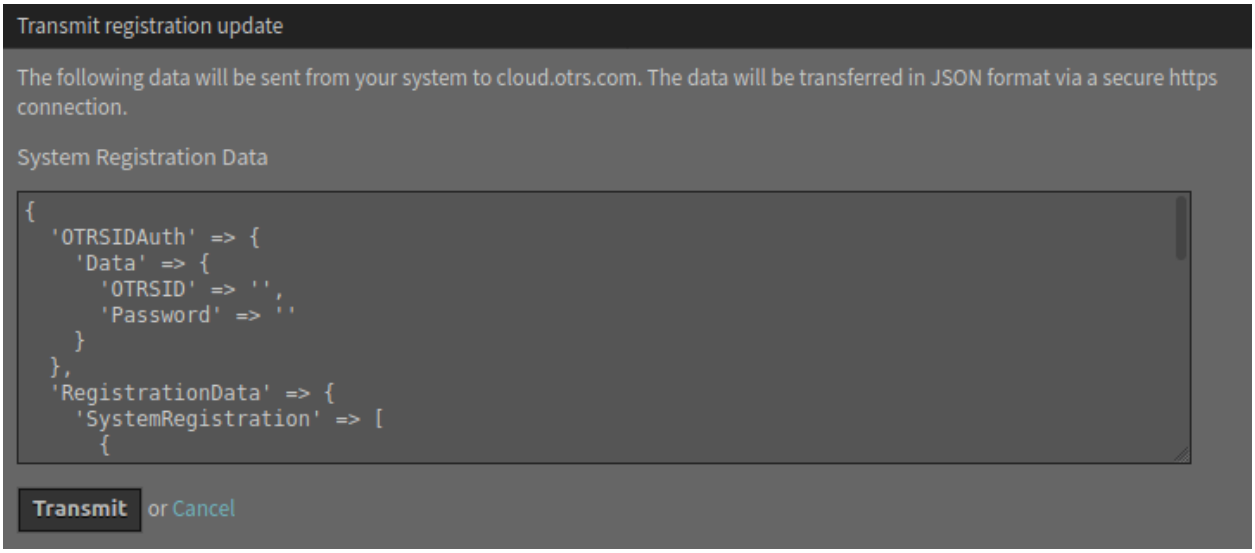


Abb. 2: Update-Aktualisierungsansicht

So überprüfen Sie den Vertragsstatus:

1. Klicken Sie in der linken Seitenleiste auf die Schaltfläche *Vertragsstatus prüfen*.
2. Überprüfen Sie die Vertragsdaten, die an die OTRS Group gesendet werden sollen.
3. Stellen Sie sicher, dass die Kommunikation mit der OTRS Group nicht blockiert wird.
4. Klicken Sie auf die Schaltfläche *Übermitteln*.

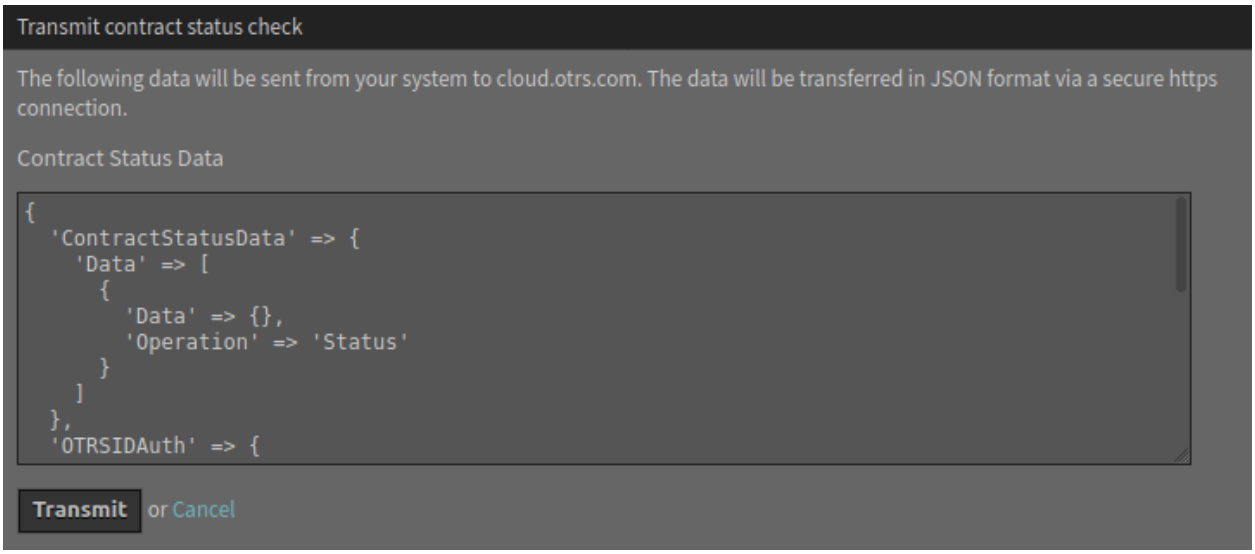


Abb. 3: Vertragsstatus-Überprüfung

KAPITEL 4

Historie - Gesehene Artikel

Diese Funktion dient dazu, die Revisionssicherheit des Systems für kritische Informationen zu gewährleisten. Mit dieser Funktion können Artikel in der Historie so angezeigt werden, dass ersichtlich ist, wer den Artikel gelesen hat.

4.1 Anforderungen

Die Systemkonfigurations-Einstellung `UserArticleSeenHistory` muss aktiviert werden.

4.2 Verwendung

Die Funktion fügt der Historie einen Eintrag hinzu, wenn ein Agent einen Artikel liest.

So rufen sie die Historie für gesehene Artikel auf:

1. Öffnen Sie ein Ticket in der Ticket-Detailansicht.
2. Wählen Sie *Historie anzeigen* im Menü *Aktionen*.

Die Einträge für die Benachrichtigungen darüber, dass eine Person den Artikel gelesen hat, werden in der Historie angezeigt:

Lesen bedeutet in diesem Fall, dass der Agent die Artikeldetailansicht geöffnet hat. In diesem Fall wird das `IsSeen` Flag auf `1` gesetzt und in der Ticket-Historie wird ein Eintrag mit der Information erstellt, welche Person den Artikel gelesen hat.

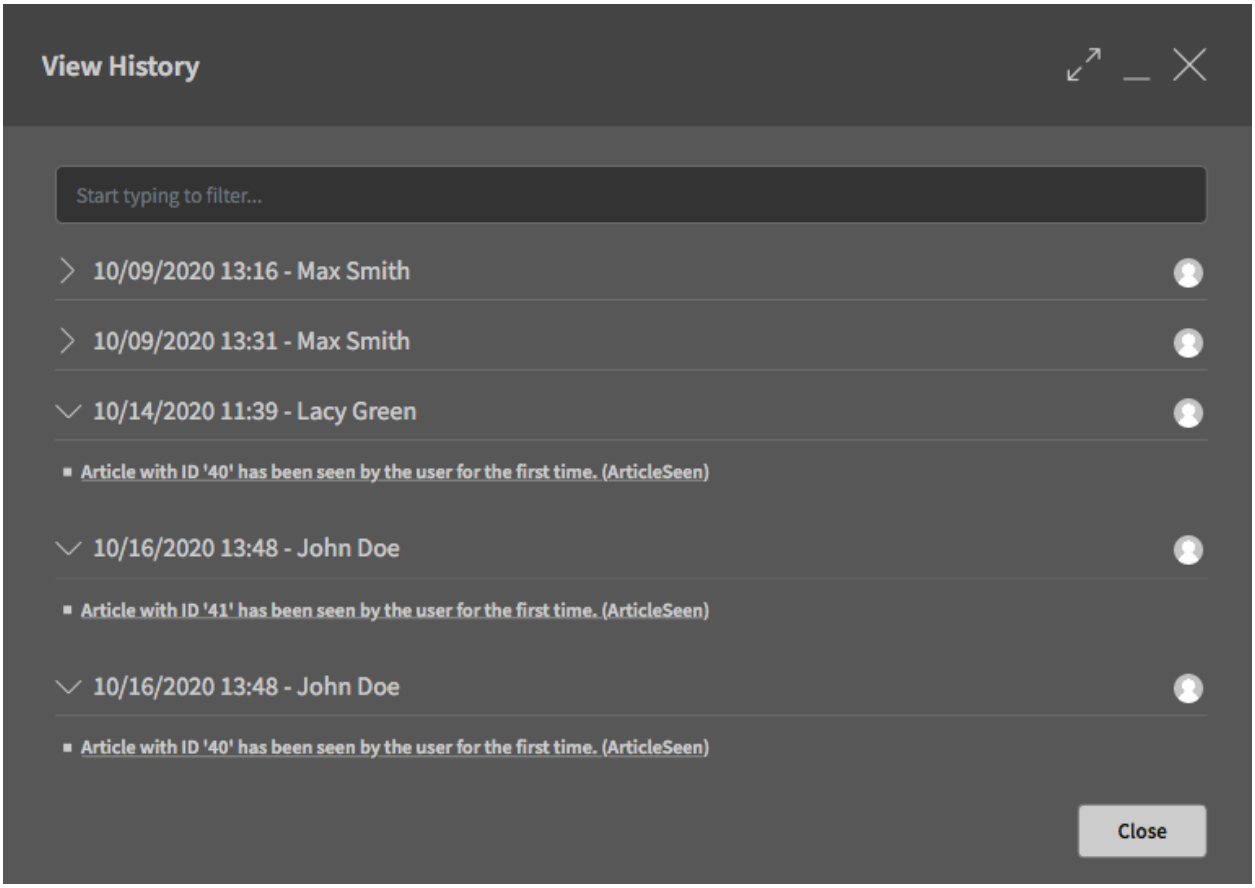


Abb. 1: Beispiel für Historie - Gesehene Artikel

KAPITEL 5

Anhang-Aktionen

Diese Funktion ermöglicht die Ausführung verschiedener benutzerdefinierter Aktionen an Ticket-Anhängen. Diese Aktionen können von Modulen wie beispielsweise dem Modul `ScanWithVirusTotal` oder von anderen Webdiensten kommen, die der Administrator definieren kann, um Informationen über Anhänge zur Analyse, Verarbeitung, Zählung usw. an ein Drittsystem zu senden.

Um die Informationen aus Anhängen an einen Server eines Drittanbieters zu senden, müssen sie möglicherweise aus dem OTRS-Format extrahiert oder in ein Format transformiert werden, das das andere System verstehen kann. Auch die Antwort des anderen Systems muss in ein spezielles Format konvertiert werden, damit sie von den Anhang-Aktionen verarbeitet und aufgezeichnet werden kann. Diese Veränderung oder Transformation des Datenformats kann durch die Verwendung der Mapping-Module in der generischen Schnittstelle von OTRS erfolgen. insbesondere das XSLT-Mapping-Modul sollte in der Lage sein, diese Aufgabe zu erfüllen.

5.1 Einrichten des VirusTotal-Moduls

Das System verfügt bereits über ein Modul zum Senden von Anhängen, die von *Virus Total* per Upload des Anhangs geprüft werden. Die mit diesem Modul verknüpfte Aktion ist standardmäßig nicht aktiviert.

So aktivieren Sie das Virenscan-Modul:

1. Gehen Sie auf die Website VirusTotal und erstellen Sie ein Konto.
2. Suchen und kopieren Sie den von VirusTotal bereitgestellten API-Schlüssel, um die Webdienste von VirusTotal zu nutzen.
3. Fügen Sie den API-Schlüssel zu der Einstellung `AttachmentAction::ScanWithVirusTotal::APIKey` hinzu.
4. Aktivieren Sie die „Virus Total “-Aktion in der Ansicht *Anhang-Aktionsverwaltung* (siehe unten).

Bemerkung: Weitere modulbasierte Anhängeaktionen werden in weiteren Versionen zu STORM hinzugefügt.

5.2 Web-Services erstellen

Anhang-Aktionen können auch Web-Services anstelle von vordefinierten Modulen verwenden. Auf diese Weise kann der Administrator seine Aktionen bei Bedarf mit Remote-Servern integrieren, indem er XSLT-Mappings verwendet, um ausgehende und eingehende Daten zu transformieren.

Aktionen mit Anhängen sollten den Aufrufer `Ticket::AttachmentAction` verwenden, der mit STORM geliefert wird. Er verhindert, dass andere Anhänge in der Anfrage versendet werden und er und er sorgt für die richtige Behandlung der Ergebnisse.

Nach dem Eingangs-Mapping sollte der Aufrufer den Schlüssel `<AttachmentActionResult>` mit den folgenden Unterschlüsseln bereitstellen:

<Status> Eine Zahl von 1 bis 6. Die Liste der Statuscodes und der vorgeschlagenen Verwendung lautet wie folgt:

- `1` (Alarm): Zur Zeit nicht in Gebrauch (Farbe violett).
- `2` (kritisch): Wird für interne Serverfehler verwendet (Farbe violett).
- `3` (Fehler): Ausführungsfehler (Farbe rot).
- `4` (Warnung): Die Ausführung war korrekt, aber es wurden externe Fehler gemeldet (Farbe orange).
- `5` (Mitteilung): Die Ausführung war korrekt, aber Ergebnisse liegen nicht vor oder stellen kleinere Probleme dar (Farbe gelb).
- `6` (Info): Alles in Ordnung (Farbe grün).

<Result> Eine Zeichenfolge, die als Tooltip angezeigt werden soll.

<Details> Vollständige Ergebnisdetails im reinen Textformat.

Die Web-Services können im Modul *Web Services* des Administrator-Interfaces erstellt werden. Die Verwendung dieser Ansicht ist identisch mit der Ansicht zur Verwaltung der Web-Services des OTRS-Frameworks.

Hier ist ein Beispiel für XSLT-Mapping:

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform
↪">
    <xsl:template match="/">
        <xsl:copy>
            <RootElement>
                <AttachmentActionResult>
                    <Status>5</Status>
                    <Result>Web service sampple result</Result>
                    <Details>This is an example</Details>
                </AttachmentActionResult>\r\n
            </RootElement>
        </xsl:copy>
    </xsl:template>
</xsl:stylesheet>"
```

5.3 Anhänge-Aktionen verwalten

Nachdem der Web-Service vom Administrator erstellt wurde, ist es notwendig, eine neue Anhangsaktion zu erstellen, bei der der Name des Web-Service festgelegt und der Aufrufer aus der Dropdown-Liste ausgewählt

werden muss. Es gibt ein neues Modul zur Verwaltung der Anhangsaktionen. Die Ansicht für die Verwaltung der Anhänge-Aktionen ist im Modul *Anhänge-Aktionen* der Gruppe *Ticket-Einstellungen* in der Administrator-Oberfläche verfügbar.

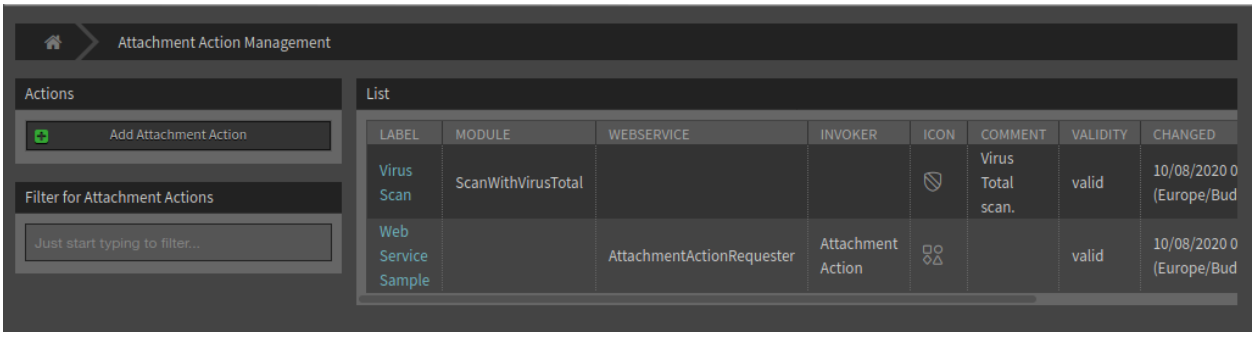


Abb. 1: Ansicht zur Verwaltung von Anhang-Aktionen

So fügen Sie einen Web-Service als Anhang-Aktion hinzu:

1. Klicken Sie in der linken Seitenleiste auf die Schaltfläche *Anhang-Aktion hinzufügen*.
2. Füllen Sie die Pflichtfelder aus.
3. Klicken Sie auf die Schaltfläche *Speichern*.

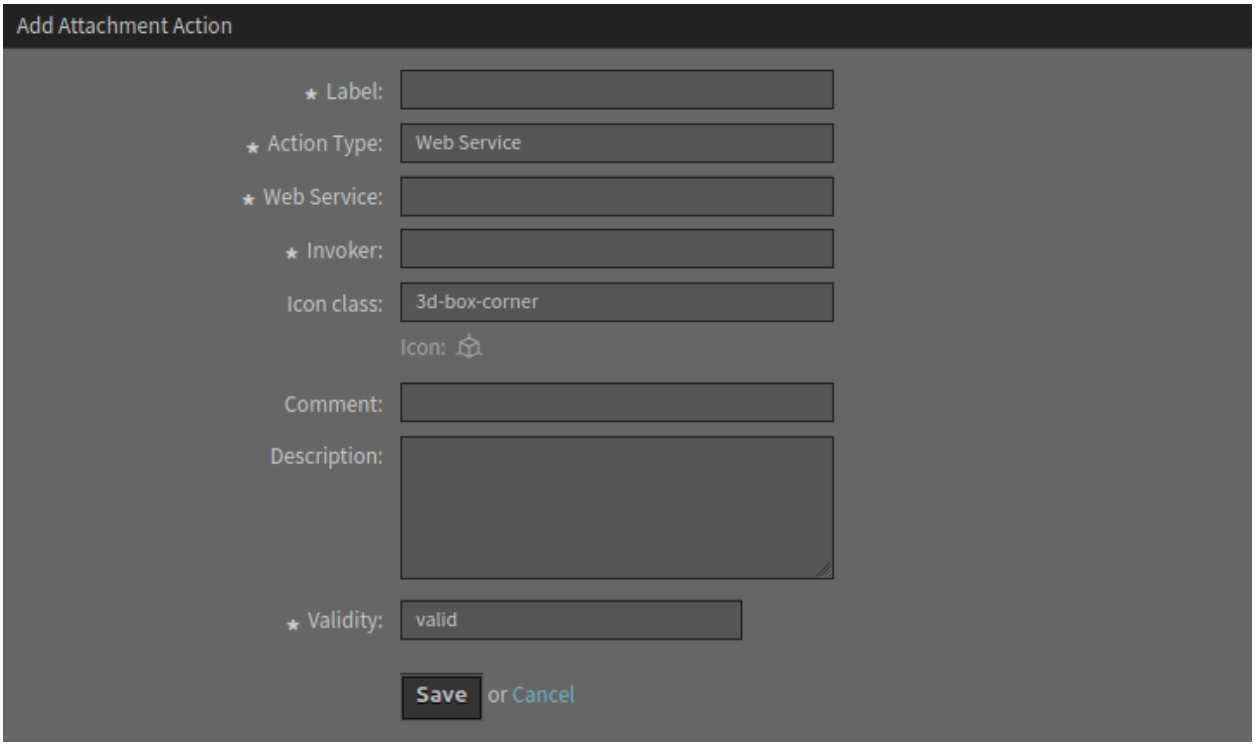


Abb. 2: Ansicht für Anhang-Aktionen

Es ist möglich, Anhang-Aktionen für Module oder Web-Services zu erstellen. Mit STORM wird das Modul `ScanWithVirusTotal` mit STORM ausgeliefert. Weitere Web-Services können von den Administratoren definiert werden.

Warnung: Anhang-Aktionen können nicht aus dem System gelöscht werden. Sie können nur deaktiviert werden, indem die Option *Gültigkeit* auf *ungültig* oder *vorübergehend ungültig* gesetzt wird.

So bearbeiten Sie eine Anhang-Aktion:

1. Klicken Sie in der Liste der Anhang-Aktionen auf eine Anhang-Aktion.
2. Ändern Sie die Felder.
3. Klicken Sie auf die Schaltfläche *Speichern* oder *Speichern und abschließen*.

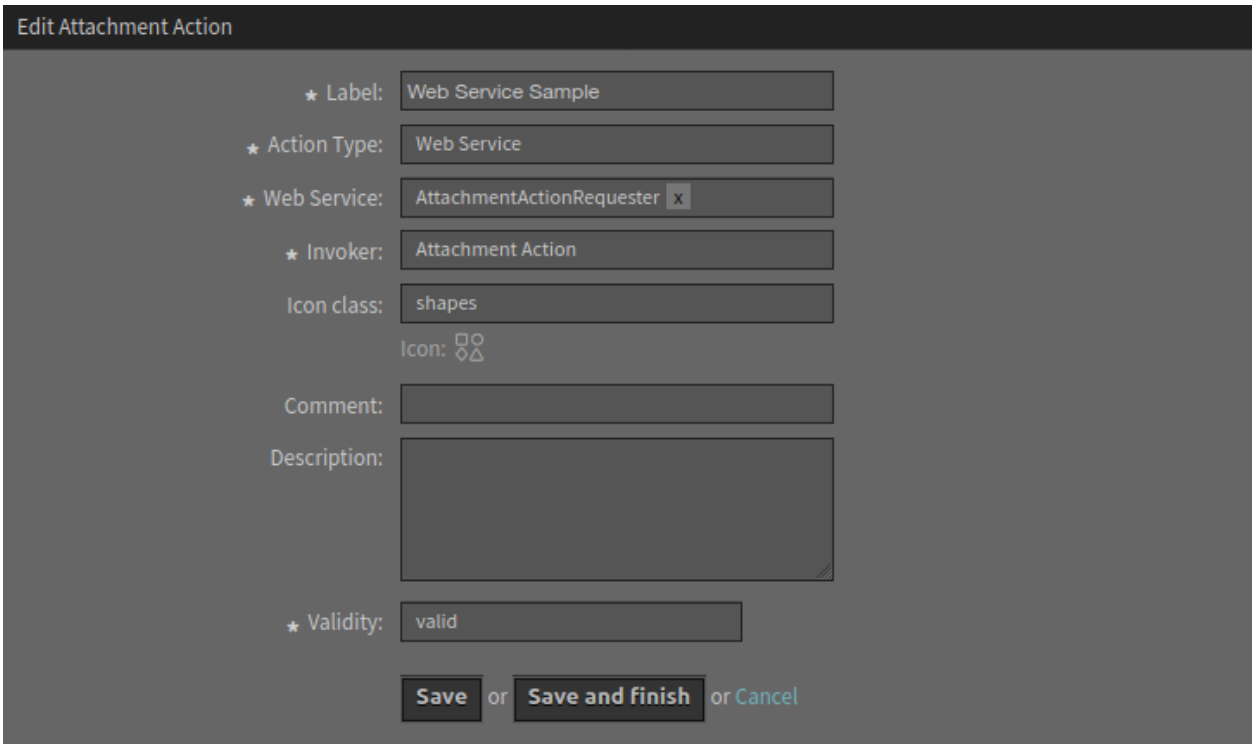


Abb. 3: Ansicht zum Bearbeiten von Anhang-Aktionen

5.4 Verwendung

Die Anhang-Aktionen können in jedem Anhangs-Widget der Detailansichten verwendet werden.

So benutzen Sie eine Anhang-Aktion:

1. Erstellen Sie ein neues Ticket.
2. Füllen Sie die Pflichtfelder aus.
3. Fügen Sie einige Anhänge hinzu.
4. Gehen Sie zur Ticket-Detailansicht und suchen Sie das Widget *Attachments*.
5. Jede Anhang-Aktion hat eine eigene Spalte im Widget *Anhänge*.

Die im Widget angezeigten Symbole sind die gleichen, die für die Aktion im Administrator-Interface eingerichtet wurden. Die Farbe der Symbole wurde oben erläutert.

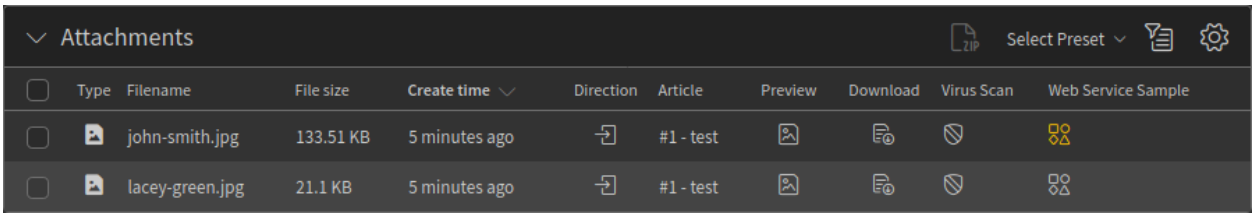


Abb. 4: Widget „Anhänge “

Bemerkung: Für jede Anhang-Aktion wird eine Spalte hinzugefügt. Versuchen Sie, so viele Anhang-Aktion zu definieren, wie wirklich nötig sind, sonst passt das Widget möglicherweise nicht in kleine Ansichten.

KAPITEL 6

Download-Protokoll für Anhänge

Wenn Anhänge sensible Daten und Informationen enthalten, profitieren Sicherheitsmanager von der Protokollierung der Downloads von Anhängen. Genauer gesagt können sie überprüfen, wer einen Anhang heruntergeladen hat und welche Details dazu vorliegen. Auf diese Weise können sie Sicherheitsaudits stressfrei bestehen. Mit Hilfe von STORM ist es möglich, im Systemprotokoll die Benutzer anzuzeigen, die einen Anhang heruntergeladen haben.

Diese Funktion hat kein Benutzer-Interface, sie protokolliert nur die Aktivitäten im Systemprotokoll. Das Modul *Systemprotokoll* der Gruppe *Verwaltung* in der Administrator-Oberfläche kann jedoch zur Überprüfung der Protokolleinträge verwendet werden.

6.1 Einrichtung

Die folgenden Systemkonfigurations-Einstellungen müssen geändert werden, um die Funktion zu aktivieren.

- `MinimumLogLevel` → *info*
- `UserAttachmentDownloadLog` → aktiviert

Die folgende Systemkonfigurations-Einstellung definiert ein optionales Präfix für die Protokolleinträge. Dies erleichtert das Parsen der Protokolldatei.

- `UserAttachmentDownloadLog::MessagePrefix`

6.2 Verwendung

Gehen Sie als Agent zur Ticket-Detailansicht eines Tickets, die einige Anhänge enthält, und laden Sie alle Anhänge herunter. Überprüfen Sie als Administrator das Systemprotokoll.

Die Daten der Anlagen-Downloads werden als Log-Einträge angezeigt. Wenn das Präfix für den Anlagen-Download definiert ist, enthalten die Einträge dieses Präfix.

```
Thu Oct 22 15:16:52 2020 (Europe/Berlin)   info   WebApp-10   ATTACHMENT -␣
↪Download of 'Inquiry.pdf' (ticket '2020102210000033') by 'John Smith'.
```

Bemerkung: Wenn das Feature Add-on *Anhänge in dynamischen Feldern* installiert ist, werden die Downloads der Anhänge in den dynamischen Feldern ebenfalls im Systemprotokoll protokolliert.

KAPITEL 7

Artikel-Meta-Filter für die Dokumentensuche

Mit den Artikel-Metafiltern können Sie eine Konfiguration mit regulären Ausdrücken von Suchkriterien definieren, nach denen Sie in einem Artikel suchen möchten. Die Funktion kann Links bereitstellen, die diese Suchkriterien verwenden, nach denen Sie in einem Artikel gesucht haben. Dies ist ähnlich wie der Meta-Filter für CVE-Nummern, der im OTRS-Framework integriert ist.

Die Idee dieses Features ist es, eine sehr ähnliche Funktion bereitzustellen, wie sie bereits im OTRS-Framework vorhanden ist, aber anstatt nach bestimmten Kriterien im Internet zu suchen oder etwas aus dem Internet anzuzeigen, möchten wir, dass dieser Meta-Filter die Dokumentensuchmaschine nutzt, um nach allem zu suchen, was man in einem Artikel und in anderen Objekten von OTRS wie Tickets, Wissensdatenbank-Artikeln, Terminen oder anderen Business-Objekten suchen möchte.

Standardmäßig gibt es einige Artikel-Meta-Filter, die mit STORM ausgeliefert werden. Wenn Sie nach Hostnamen, Servern oder IP-Adressen suchen, werden Schaltflächen mit Links zur Dokumentensuche erstellt.

7.1 Einrichtung

Die Funktion kann mit der Einstellung `AgentFrontend::TicketDetailView::ArticleMeta` aktiviert werden. Diese Einstellung ist für die Meta-Filter des OTRS-Frameworks erforderlich, aber auch für den Meta-Filter der Dokumentensuche für Artikel.

Es gibt drei Beispiele in der Einstellung `AgentFrontend::TicketDetailView::ArticleMetaFilters::DocumentS` aber alle sind standardmäßig inaktiv. Um einen von ihnen zu aktivieren, ändern Sie einfach den Wert des Schlüssels `Aktiv` auf *1*.

Im ersten Beispiel wird nach Host-Namen, im zweiten Beispiel nach Servern und im dritten Beispiel nach IP-Adressen gesucht. Sie können sehen, welche regulären Ausdrücke im Array `RegExps` definiert sind.

Es gibt eine weitere Einstellung `AgentFrontend::TicketDetailView::ArticleMetaFilters::DocumentSearch#` in der Administratoren benutzerdefinierte Metafilter definieren können.

Bemerkung: Es wird nicht empfohlen, die Beispiele zu ändern oder zu erweitern, da die eingebauten Beispiele in der Zukunft geändert werden können. Bitte verwenden Sie die benutzerdefinierte Einstellung,

um die eigenen Meta-Filter zu definieren.

Die Vorschaufunktion erfordert eine zusätzliche Einstellung. Der vollqualifizierte Domänenname (FQDN) der STORM-Instanz muss dem Schlüssel `frame-src` in der Einstellung `WebApp::Server::AdditionalOrigins` hinzugefügt werden. Andernfalls wird die Vorschau-Funktion nicht funktionieren.

7.2 Verwendung

Dieses Beispiel zeigt, wie diese Funktion zur Suche nach IP-Adressen verwendet werden kann. Dazu wird eines der eingebauten Beispiele verwendet. Wir gingen davon aus, dass dieser Beispiel-Meta-Filter wie oben beschrieben aktiviert ist.

Um alle Möglichkeiten des Features zu sehen, werden Termine, Wissensdatenbank-Artikel und Tickets benötigt, die in ihren Textfeldern eine IP-Adresse (*192.168.0.1* und *255.255.255.0*) haben. Für dieses Beispiel:

1. Erstellen Sie einen Termin mit einer IP-Adresse in der Beschreibung.
2. Erstellen Sie einen Wissensdatenbank-Artikel mit der gleichen IP-Adresse in den Feldern *Symptom* oder *Problem*.
3. Erstellen Sie ein paar Tickets mit Artikeln, die die gleiche IP-Adresse enthalten.

So suchen Sie nach IP-Adressen:

1. Erstellen Sie ein neues Ticket.
2. Füllen Sie die Pflichtfelder aus.
3. Geben Sie den folgenden Text in den Textkörper ein: *Ihre IP-Adresse ist 192.168.0.1 und Ihre Subnetzmaske ist 255.255.255.0*.
4. Gehen Sie zur Ticket-Detailansicht des neu erstellten Tickets.
5. Erweitern Sie den ersten Artikel im *Communication Stream* Widget, um die Schaltflächen unter dem Artikel zu sehen.

Die Suchmaschine sucht nach allen möglichen IP-Adressen im Artikel, wie durch den regulären Ausdruck konfiguriert.

Die Schaltflächen verweisen auf die Suchergebnisse einer Dokumentensuche. Es sollten die gleichen Suchergebnisse zurückgegeben werden, wenn ein Agent eine Suche nach den angegebenen IP-Adressen startet. Der Text für die Schaltflächen (*IP-Adresse* in diesem Beispiel) stammt aus dem Schlüssel `Bezeichnungl` der zugrunde liegenden Systemkonfigurations-Einstellung.

Wenn die Agenten mit der Maus über eine Schaltfläche fahren, erhalten sie eine Vorschau auf die Ansicht der Suchergebnisse. Wenn sie auf die Schaltflächen klicken, öffnet sich die Ansicht der Suchergebnisse.

Diese Funktion funktioniert für alle Artikel eines Tickets.

KAPITEL 8

Farbindikatoren für Werte dynamischer Felder

Wenn einige Feldwerte sehr wichtig sind und sofort bemerkt werden müssen, profitieren Sicherheitsanalysten von Farbdefinitionen für jeden der möglichen Werte in Einfach- und Mehrfachauswahlen bei dynamischen Feldern. So können sich die Benutzer mit einem Blick auf kritische oder dringende Aufgaben konzentrieren.

Mit dieser Funktion ist es möglich, den Werten von dynamischen Feldern Farbindikatoren hinzuzufügen. Dies kann den Benutzern helfen, die Auswirkungen oder die Kritikalität des Wertes zu verstehen.

So definieren Sie Farbindikatoren für ein dynamisches Feld:

1. Gehen Sie zum Modul *Dynamische Felder* im Administrator-Interface.
2. Ein dynamisches Feld vom Typ *Dropdown* oder *Multiselect* hinzufügen oder bearbeiten.
3. Definieren Sie die Werte und weisen Sie jedem Wert eine Farbe zu.

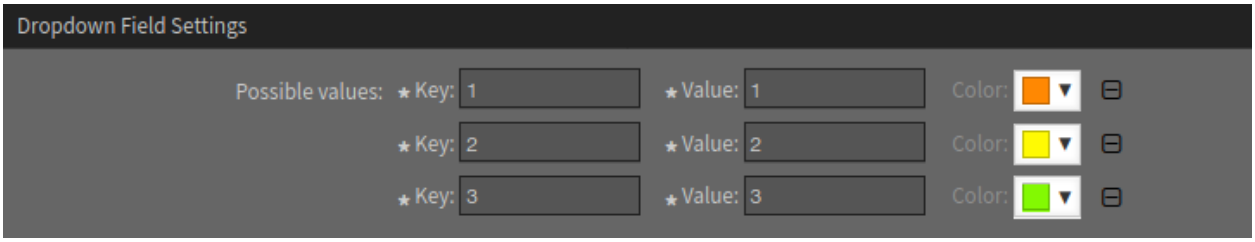


Abb. 1: Zuweisen von Farbindikatoren

Siehe auch:

Bitte lesen Sie im Administrator-Handbuch nach, wie Sie dynamische Felder auf Ansichten anzeigen.

Die Farbindikatoren werden für das konfigurierte dynamische Feld in jeder Ansicht angezeigt.

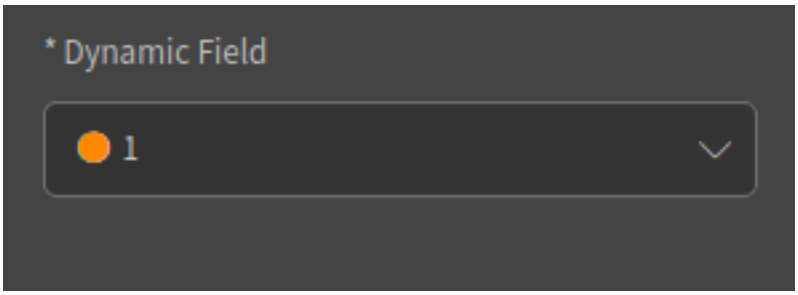


Abb. 2: Dynamisches Feld im Agenten-Interface.

KAPITEL 9

Encryption Auto Select

Mit dieser Funktion ist es möglich, auf E-Mails mit einer automatischen Auswahl der Signier- und Verschlüsselungsmethode zu antworten. Die Signierung und Verschlüsselung der Antwort wird automatisch ausgewählt, indem die gleiche Signierungs- und Verschlüsselungsmethode wie bei der eingehenden E-Mail verwendet wird.

9.1 Anforderungen

Zur Nutzung der Funktion sind die folgenden Voraussetzungen erforderlich:

- Konfigurierte PGP- und/oder S/MIME-Unterstützung.
- Es sind öffentliche und private PGP-Schlüssel und/oder Zertifikate und private Schlüssel für S/MIME hinzugefügt worden.
- Konfigurierte E-Mail-Adresse zum Abrufen von E-Mails.

Siehe auch:

Informationen über die Konfiguration von PGP und S/MIME finden Sie in den Kapiteln PGP-Schlüssel, S/MIME-Zertifikate und Einrichten eingehender E-Mails.

9.2 Verwendung

Das Feature funktioniert für verschlüsselte, signierte oder verschlüsselte und signierte Artikel.

So verschlüsseln Sie die Antwort eines Artikels:

1. Öffnen Sie die Detailansicht eines Tickets und erweitern Sie den verschlüsselten Artikel.
2. Klicken Sie auf die Artikel-Aktion *Antworten*. Abhängig von der ursprünglichen Nachricht wird das Feld *Sicherheitsoptionen* mit der entsprechenden Methode zum Signieren und/oder Verschlüsseln vorausgefüllt.

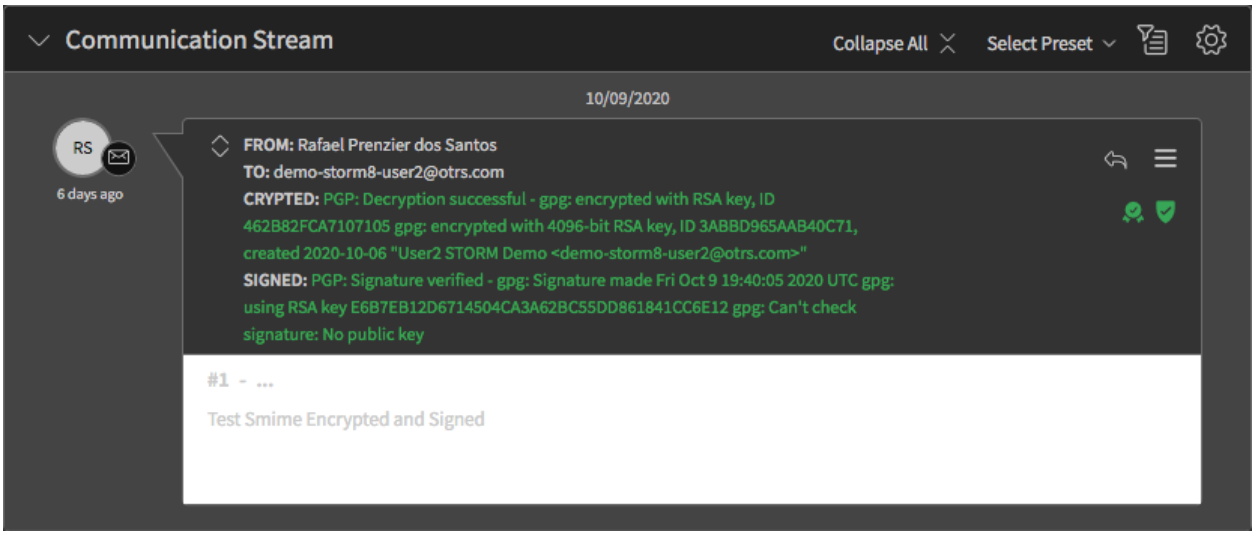


Abb. 1: PGP-signierte und verschlüsselte E-Mail

Die vorgewählten Optionen sollten nicht zurückgesetzt werden, wenn sie vom Benutzer geändert werden, nachdem andere Felder geändert wurden.

KAPITEL 10

Bcc-E-Mails entschlüsseln

Sicherheitsanalysten profitieren von der Entschlüsselung eingehender E-Mails, auch wenn die Empfängeradresse im Blindkopie-Feld (*Bcc*) steht, denn so können sie E-Mails entschlüsseln, die eine STORM-E-Mail-Adresse als Empfänger im Bcc-Feld enthalten.

10.1 Einrichtung

Die folgende Einrichtung ist für die Verwendung mit **S/MIME** erforderlich:

- Die Einstellung `SMIME::Decrypt::Methods#####Email` sucht nach Zertifikaten, die mit E-Mail-Adressen innerhalb der Mail übereinstimmen. Diese Einstellung ist standardmäßig aktiviert.
- Die Einstellung `SMIME::Decrypt::Methods####System` sucht nach Zertifikaten, die E-Mail-Adressen entsprechen, die als Systemadressen definiert sind. Diese Einstellung ist ebenfalls standardmäßig aktiviert.
- Die Einstellung `SMIME::Decrypt::Methods#####All` sucht nach allen verfügbaren S/MIME-Zertifikaten, um zu versuchen, diese zu entschlüsseln (Brute-Force, standardmäßig deaktiviert). Sie kann zum Testen aktiviert werden. In Produktivsystemen, wenn das System über mehrere Zertifikate verfügt, wird dies aus Performance-Gründen nicht empfohlen.

Für **PGP** sind keine zusätzlichen Einstellungen erforderlich.

10.2 Verwendung

Senden Sie verschlüsselt eine mit PGP oder S/MIME verschlüsselte E-Mail von Ihrem persönlichen Account an die in OTRS konfigurierte E-Mail-Adresse, aber nur unter Verwendung des Blind Carbon Copy (*Bcc*)-Feldes (füllen Sie nicht das *An*- oder das *Cc*-Feld aus). Gehen Sie in die Ticket-Detailansicht des neuen Tickets und die Artikel sollten korrekt entschlüsselt sein.

Abb. 1: Beispiel für eine entschlüsselte Bcc-Email

KAPITEL 11

Login-Logout Log

In einigen Situationen ist es notwendig, Kenntnisse über die An- und Abmeldeaktivitäten der Benutzer zu haben. Mit dieser Funktion ist es möglich, im Systemprotokoll zu sehen, welche Benutzer an- und abgemeldet wurden.

Diese Funktion hat kein Benutzer-Interface, sie protokolliert nur die Aktivitäten im Systemprotokoll. Das Modul *Systemprotokoll* der Gruppe *Verwaltung* in der Administrator-Oberfläche kann jedoch zur Überprüfung der Protokolleinträge verwendet werden.

11.1 Einrichtung

Die folgenden Systemkonfigurations-Einstellungen müssen geändert werden, um die Funktion zu aktivieren.

- `MinimumLogLevel` → *info*
- `UserLoginLogoutLog` → aktiviert

Die folgenden Systemkonfigurations-Einstellungen definieren ein optionales Präfix für die Protokolleinträge. Dies erleichtert das Parsen der Protokolldatei.

- `UserLoginLogoutLog::LoginMessagePrefix`
- `UserLoginLogoutLog::LogoutMessagePrefix`

11.2 Verwendung

Melden Sie sich als Agent beim System an und melden Sie sich dann ab. Prüfen Sie als Administrator das Systemprotokoll.

Die An- und Abmeldedaten werden als Log-Einträge angezeigt. Wenn die Präfixe für An- und Abmeldung definiert sind, enthalten die Einträge dieses Präfix.

```
Thu Oct 22 14:51:53 2020 (Europe/Berlin)   info   WebApp-10   LOGOUT_EVENT -␣
↪Logout by 'John Smith'.
Thu Oct 22 14:51:26 2020 (Europe/Berlin)   info   WebApp-10   LOGIN_EVENT -␣
↪Login by 'John Smith'.
```

KAPITEL 12

Benachrichtigungs-Vorlagen

Mit dem Traffic Light Protocol (TLP) gekennzeichnete E-Mail-Korrespondenz sollte die TLP-Farbe der Informationen neben dem TLP-Level im Hauptteil der E-Mail vor den gekennzeichneten Informationen selbst angeben.

In STORM this could be used for the notifications that are sent via email. For this purpose new templates have been added containing different layouts with colors indicating the status according to the traffic light protocol.

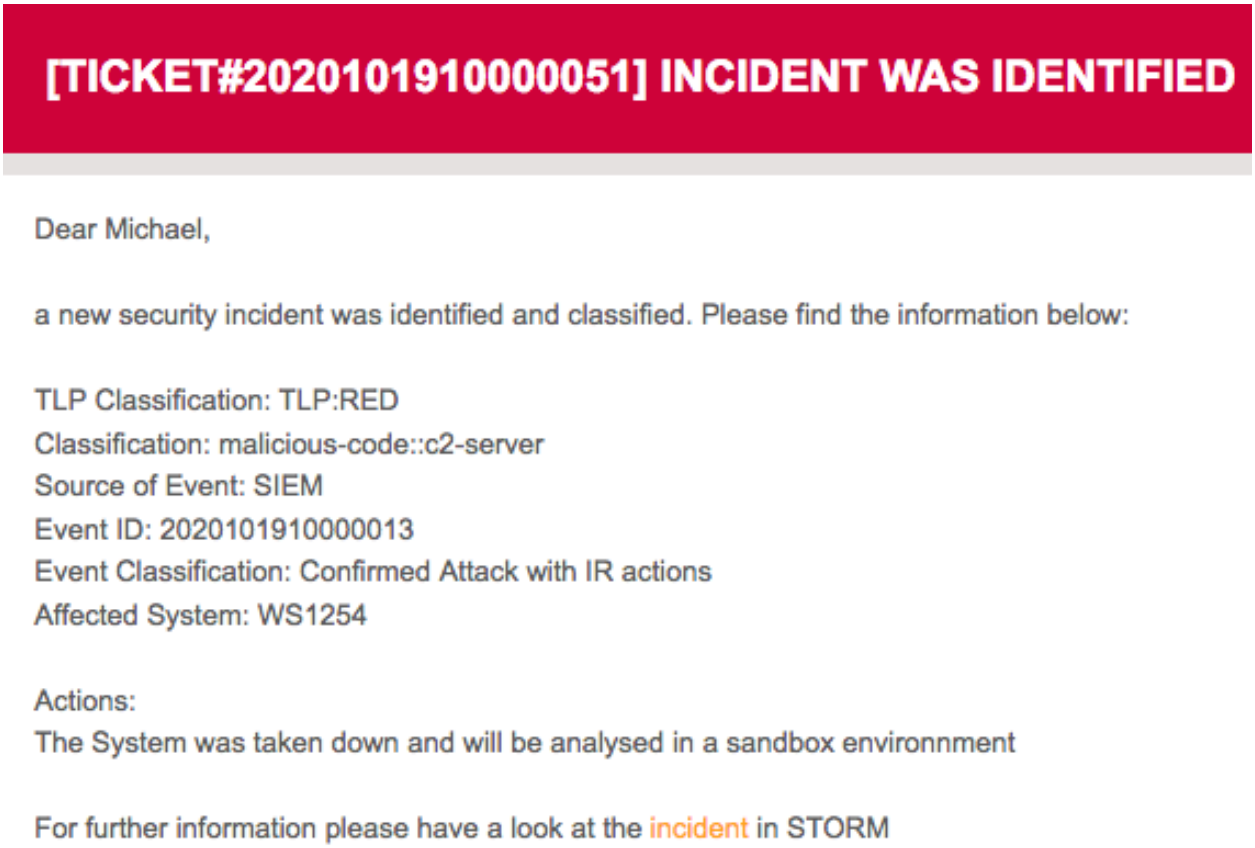
STORM wird mit vier vorgefertigten Vorlagen geliefert:

- `TLP-Red`
- `TLP-Amber`
- `TLP-Green`
- `TLP-White`

So legen Sie eine TLP-Vorlage für die Ticket-Benachrichtigung fest:

1. Gehen Sie im Administrator-Interface zur Ansicht *Ticket-Benachrichtigungen*.
2. Wählen Sie eine Benachrichtigung aus der Liste der Benachrichtigungen aus.
3. Wählen Sie im Abschnitt *Benachrichtigungsmethoden* eine TLP-Vorlage für die E-Mail-Benachrichtigung .
4. Klicken Sie auf die Schaltfläche *Speichern* oder *Speichern und abschließen*.

Je nachdem, was in der Benachrichtigung definiert ist und welche Vorlage zugeordnet wurde, enthält das Layout der Benachrichtigungs-E-Mail die gewählte Vorlage.



[TICKET#2020101910000051] INCIDENT WAS IDENTIFIED

Dear Michael,

a new security incident was identified and classified. Please find the information below:

TLP Classification: TLP:RED
Classification: malicious-code::c2-server
Source of Event: SIEM
Event ID: 2020101910000013
Event Classification: Confirmed Attack with IR actions
Affected System: WS1254

Actions:
The System was taken down and will be analysed in a sandbox environnment

For further information please have a look at the incident in STORM

Abb. 1: Beispiel für eine nach TLP gekennzeichnete E-Mail

KAPITEL 13

Process Management Direct Actions

Jeder Prozess hat einen Aktivitätsdialog, und es gibt einige Felder in diesem Aktivitätsdialog. Die Idee der direkten Aktionen besteht darin, unnötige Aktionen zu vermeiden. Wenn der Prozess ein Feld mit einem vordefinierten Wert hat und der Agent nichts weiter tun muss, als auf eine Schaltfläche zu klicken, um das Formular abzuschicken, kann diese Aktion automatisch ausgeführt werden.

Direkte Aktionen funktionieren bei allen Prozessen, die einen Aktivitätsdialog als direkte Aktion verwenden. Es gibt jedoch einige Anforderungen:

- Alle Felder im Aktivitätsdialog müssen ausgeblendet werden.
- Alle Felder im Aktivitätsdialog müssen einen Standardwert haben.

Es gibt einige Felder wie *Queue*, *Priorität* oder *Status*, die bereits vordefinierte Werte in der Konfiguration des Prozessmanagements haben. Wenn die Administratoren einen anderen Wert angeben möchten, dann müssen sie einen Standardwert haben.

13.1 Beispielverwendung

In diesem Beispiel werden wir einen sehr einfachen Prozess mit einer Aktivität und zwei Aktivitätsdialogen definieren. Der erste Aktivitätsdialog erlaubt es, den Titel des Tickets auf einen beliebigen Text zu setzen, der zweite Aktivitätsdialog setzt einen vordefinierten Text auf den Titel des Tickets. Dies wird *direkte Aktion* genannt.

Der Benutzeraufgaben-Aktivitätsdialog wurde um ein neues Feld *Direkte Aktion* erweitert. Wenn dieses Feld markiert ist, wird der Aktivitätsdialog automatisch übermittelt.

Direkte Aktionen erfordern, dass alle Felder manuell auf ausgeblendet gesetzt werden und einen Standardwert angeben.

Vergessen Sie nach dem Bearbeiten nicht, den Prozess in Betrieb zu nehmen.

Gehen Sie nun zum Agenten-Interface und erstellen Sie ein Prozess-Ticket. Wählen Sie den neu erstellten Prozess aus. Die beiden Schaltflächen, die wir in diesem sehr einfachen Prozess definiert haben, werden nun in der Ticket-Detailansicht angezeigt.

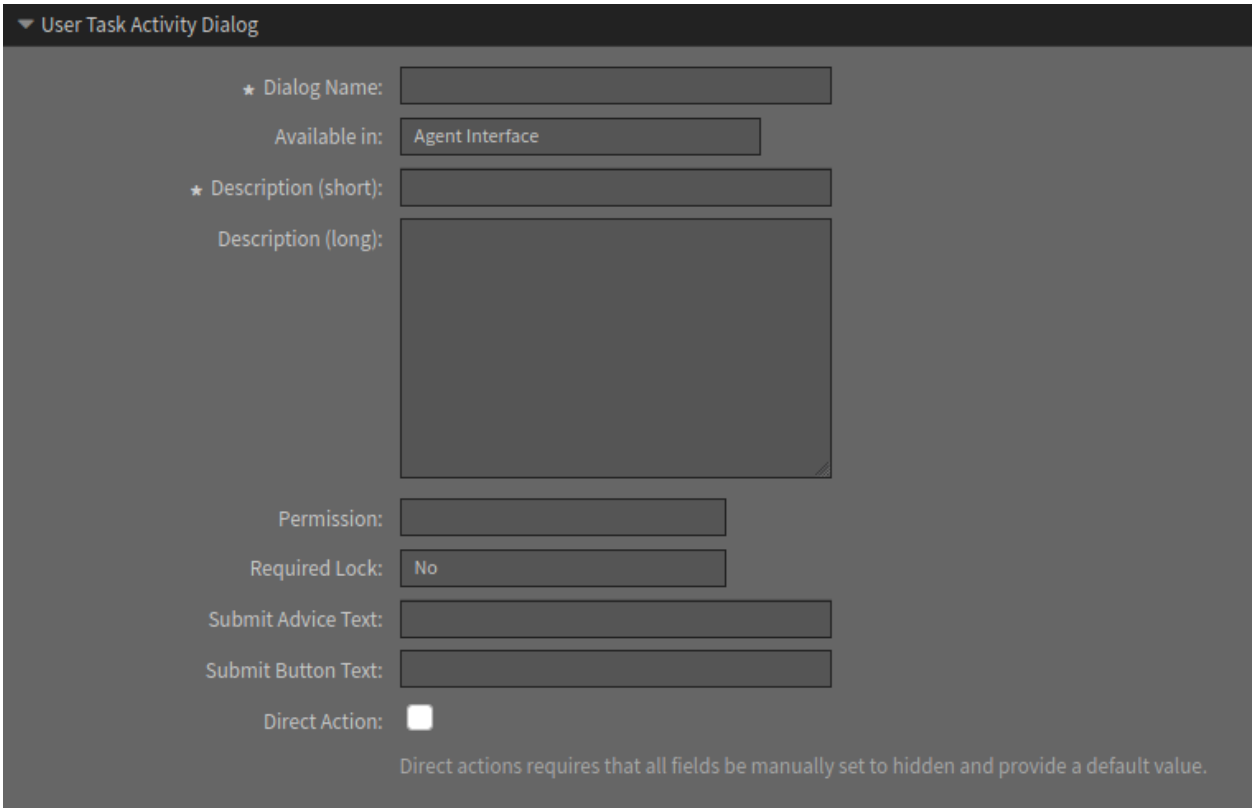


Abb. 1: Benutzeraufgabe-Aktivitätsdialog bearbeiten

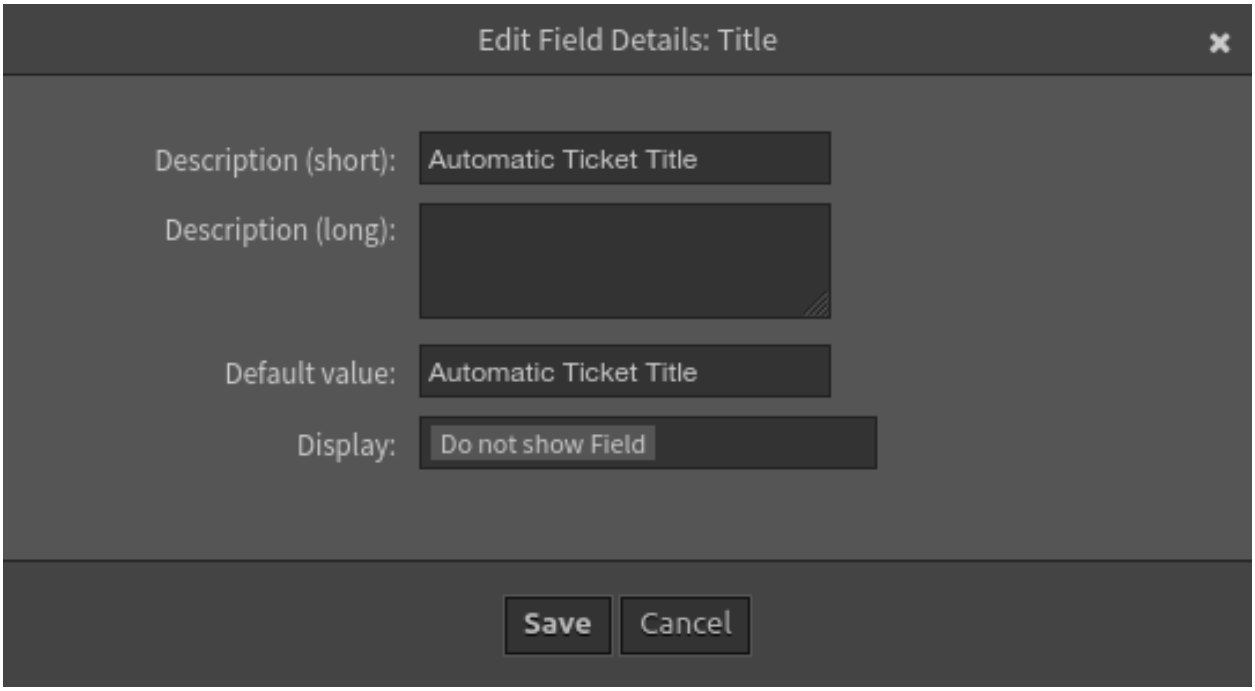


Abb. 2: Dialog Felddetails bearbeiten

Abb. 3: Dialog Felddetails bearbeiten

Die erste Schaltfläche öffnet eine Aktion, um den Titel des Tickets auf einen beliebigen Text zu setzen. Dies funktioniert genauso wie die Funktion im OTRS-Framework. Der Agent muss den Titel des Tickets manuell ändern und dann das Formular mit der Schaltfläche *Übermitteln* abschicken.

Die zweite Schaltfläche hat ein Blitzsymbol, was bedeutet, dass es sich um eine *direkte Aktion* handelt. Wenn der Agent auf diese Schaltfläche klickt, wird der Titel des Tickets auf den im Prozess definierten Text gesetzt und die Aktion wird automatisch übermittelt. Es ist keine weitere Aktion durch den Agenten manuell erforderlich.

The process can contain some triggers to go to one activity to another by setting any ticket field like state, queue or any dynamic field, by using the predefined direct actions. The users do not need to set any values to jump to another activity. With this feature, it is possible to add *Previous* or *Next* buttons to the dialogs of the process to jump forward or backward from one user activity.

KAPITEL 14

Process Management Module System Call

Wenn ein Prozess von einer Aktivität zu einer anderen Aktivität wechselt, kann dem Sequenzfluss eine Aktion angehängt werden. Diese Aktionen werden als Module definiert, um bestimmte Aufgaben auszuführen, wie z.B. Ticket-Attribute ändern, Artikel erstellen, dynamische Felder festlegen usw. Die Module können auch an bestimmte Aktivitäten der Prozessverwaltung angehängt werden, die als Aktivitäten vom Typ *Skript* bezeichnet werden und das angehängte Modul ausführen, wenn sie aufgerufen werden.

Das Systemaufruf-Modul ermöglicht es den Agenten, jedes Programm, Skript, Binär- oder Exe-Datei aufzurufen, das im Betriebssystem des Servers, auf dem OTRS läuft, verfügbar ist. Das Ergebnis des Systemaufrufs kann zur Aktualisierung der Ticket-Informationen verwendet werden.

Das Systemaufruf-Modul erfordert die Verwendung von XSLT-Mappings. Das ausgehende Mapping wird verwendet, um den aufzurufenden Systembefehl zu definieren, und das eingehende Mapping wird verwendet, um die Ergebnisse aus dem Systemaufruf in Informationen zur Aktualisierung des aktuellen Tickets umzuwandeln.

Im ausgehenden Mapping ist es notwendig, den Schlüssel `<Command>` und bei Bedarf einen oder mehrere Schlüssel `<Argument>` zu haben. Die zu setzenden Werte können aus dem Prozess-Ticket unter dem Schlüssel `<Ticket>` und dann den normalen Ticket-Attributen als Unterschlüssel wie z.B. `<Priorität>`, `<QueueID>`, `<Titel>` usw. transformiert werden. Oder sie könnten als feste Werte definiert werden.

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform
↪">
    <xsl:template match="/">
        <xsl:copy>
            <RootElement>
                <Command>command</Command>
                <Arguments>argument1</Arguments>
                <Arguments>argument2</Arguments>
                <Arguments>argumentN</Arguments>
                <Arguments><xsl:value-of select="//Ticket/Priority"/></
↪Arguments>
            </RootElement>
        </xsl:copy>
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
    </xsl:template>
</xsl:stylesheet>
```

Aus Sicherheitsgründen können dem Schlüssel `<Command>` nur solche Befehle hinzugefügt werden, die der Einstellung `ProcessManagement::Modules::SystemCall::CommandWhiteList` als erlaubte Befehle hinzugefügt werden. Dadurch wird verhindert, dass Benutzer nicht erlaubte Befehle auf dem Server ausführen.

Das eingehende Mapping wird verwendet, um die Ergebnisse aus dem Systemaufruf in Informationen zur Aktualisierung des aktuellen Tickets umzuwandeln. Alle Unterschlüssel müssen sich innerhalb des Schlüssels `<Ticket> befinden. Hier ist die mögliche Liste von Unterschlüsseln:

```
<CustomerUser>
<DynamicField>
<Lock>
<LockID>
<Owner>
<OwnerID>
<Pending>
<Priority>
<PriorityID>
<Queue>
<QueueID>
<Responsible>
<ResponsibleID>
<Service>
<ServiceID>
<SLA>
<SLAID>
<State>
<StateID>
<Title>
<Type>
<TypeID>
```

Auf die Ergebniswerte kann von dort aus zugegriffen werden:

<ReturnCode> Der numerische Wert, der von einer Ausführung eines Systemprozesses zurückgegeben wird.

<Output> Jeder für die Standardausgabe erstellte Text.

<ErrorOutput> Jeder Text wird in die Standardfehlerausgabe ausgegeben.

Hier ist ein Beispiel für ein eingehendes Mapping, das die Ausgabe des Systemaufrufs als Ticket-Titel festlegt:

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform
↪">
    <xsl:template match="/">
        <xsl:copy>
            <RootElement>
                <Ticket>
                    <Title><xsl:value-of select="//Output" /></Title>
                </Ticket>
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
            </RootElement>
        </xsl:copy>
    </xsl:template>
</xsl:stylesheet>
```

Siehe auch:

Es gibt einen Abschnitt *Erläuterung zur Handhabung des Mappings* in der Ansicht der Konfiguration. Diese Erklärung kann als Referenz verwendet werden.

Die Systemaufrufe werden durch den OTRS-Daemon im Hintergrund mit den entsprechenden Berechtigungen asynchron ausgeführt. Wenn ein Systemaufruf einige Zeit dauert, wartet das Prozessmanagement, bis der Systemaufruf beendet ist und die Ergebnisse des Systemaufrufs vorliegen. Während dieser Zeit kann der Prozess nicht in den nächsten Zustand versetzt werden, aber der andere Teil der Agentenschnittstelle kann weiterhin verwendet werden.

14.1 Beispielverwendung

In diesem Beispiel werden wir einen sehr einfachen Prozess mit einer Skript-Task-Aktivität definieren. Der Prozess ist so konfiguriert, dass der Titel des Tickets in das Ergebnis des Systembefehls `uname -s` geändert wird. Das Ergebnis könnte je nach Betriebssystem *Darwin*, *Linux*, *GNU* usw. sein.

So definieren Sie einen Beispielprozess:

1. Gehen Sie zur Ansicht „Prozessmanagement “und legen Sie einen neuen Prozess an.
2. Fügen Sie dem Prozess eine neue Skript-Task-Aktivität hinzu.
3. Wählen Sie im Feld *Script* im Abschnitt *Script-Einstellungen* den Wert `SystemCall` . Klicken Sie auf die Schaltfläche *Speichern*.
4. Klicken Sie neben dem Feld *Script* auf die Schaltfläche *Konfigurieren*.
5. Fügen Sie die folgenden Zeilen zur Vorlage *Ausgehend: XSLT-Mapping* hinzu.

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/
↪Transform">
    <xsl:template match="/">
        <xsl:copy>
            <RootElement>
                <Command>uname</Command>
                <Arguments>-s</Arguments>
            </RootElement>
        </xsl:copy>
    </xsl:template>
</xsl:stylesheet>
```

6. Fügen Sie die folgenden Zeilen zur Vorlage *Eingehend: XSLT-Mapping* hinzu.

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/
↪Transform">
    <xsl:template match="/">
        <xsl:copy>
            <RootElement>
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
                <Ticket>
                    <Title><xsl:value-of select="//Output" /></Title>
                </Ticket>
            </RootElement>
        </xsl:copy>
    </xsl:template>
</xsl:stylesheet>
```

7. Klicken Sie auf die Schaltfläche *Speichern und beenden*.
8. Nehmen Sie den Prozess in Betrieb.
9. Erstellen Sie ein neues Prozess-Ticket im Agent-Interface und klicken Sie dann auf die Aktivität *Start*.
10. Warten Sie, bis der Daemon den Systemaufruf ausführt.
11. Der Ticket-Titel wird in das Ergebnis von `uname -s` geändert.