STORM Manual

Release 2024.3.1

OTRS AG

22.04.2024

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 das Thema ändern.

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*.

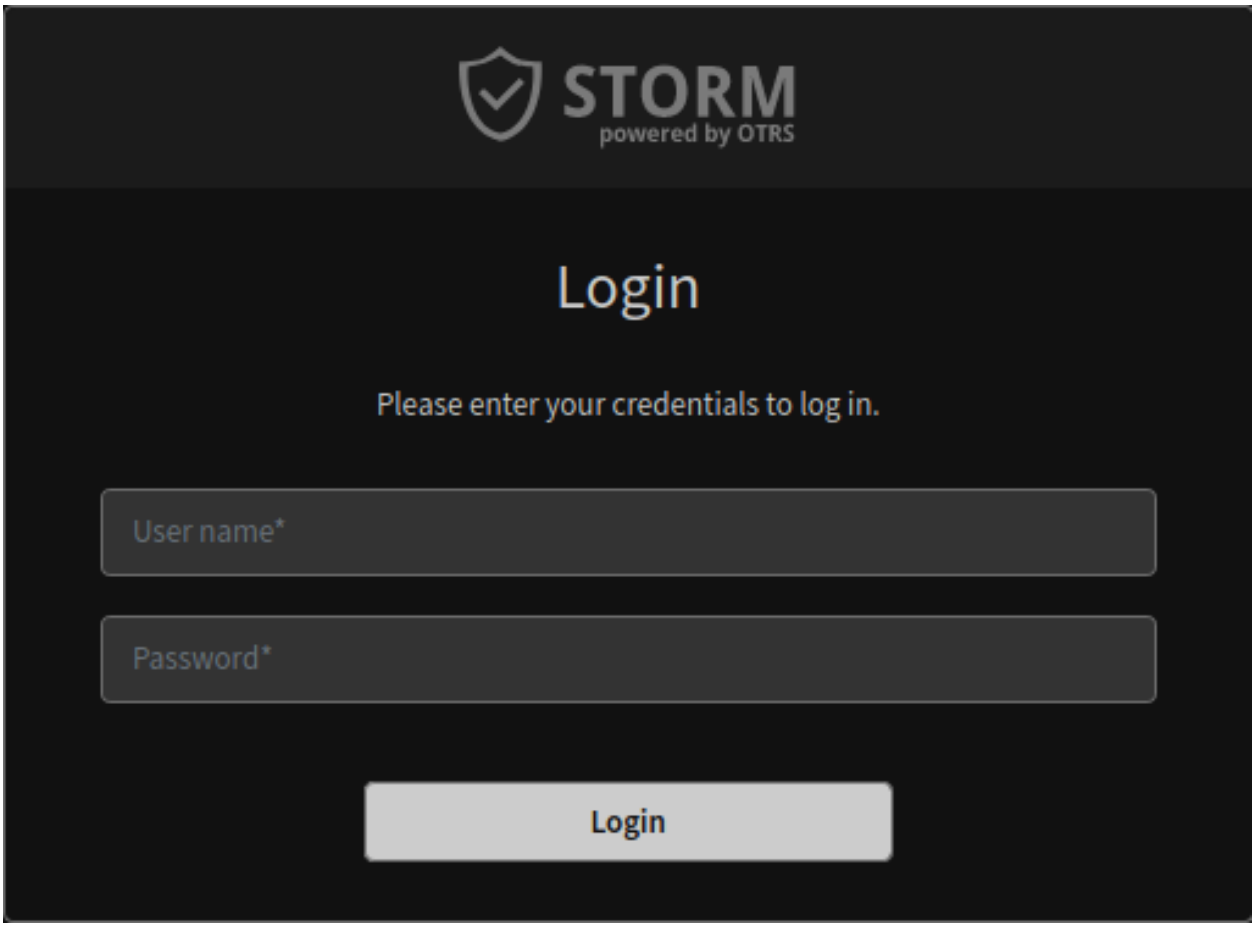

Abb. 1: Anmeldebox mit „Dark Theme “

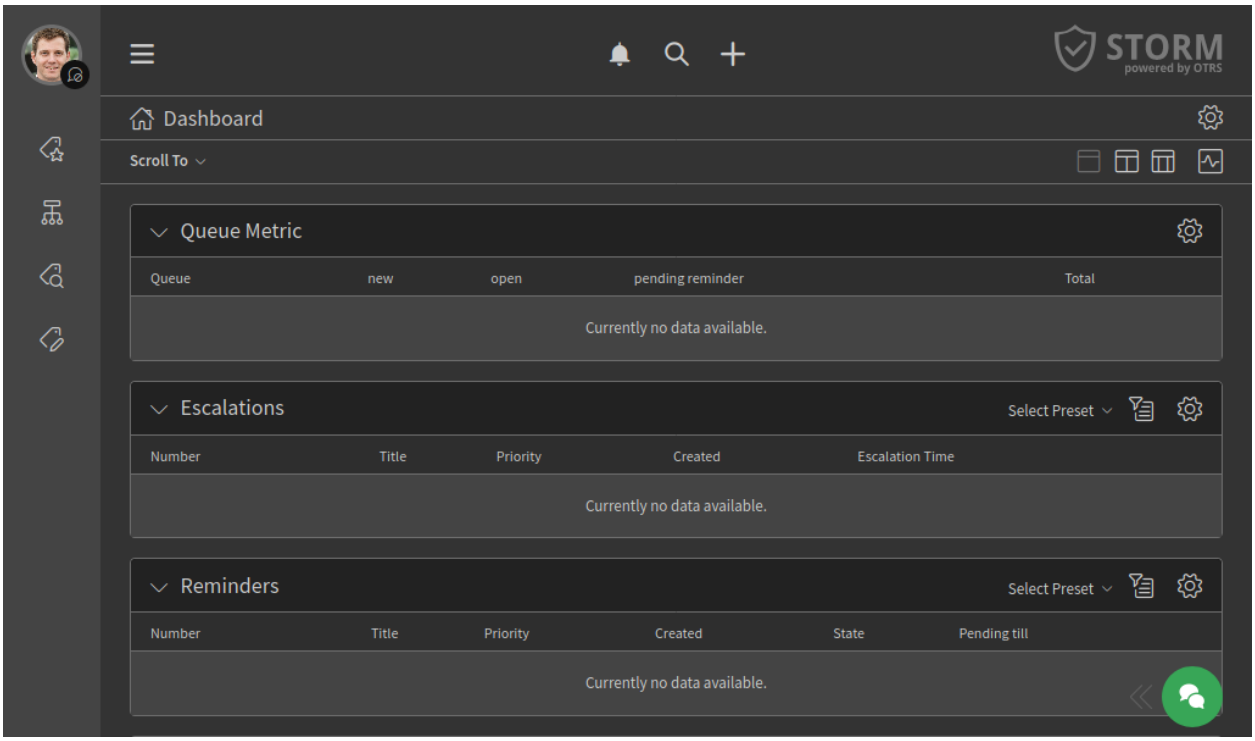

Abb. 2: Agenten-Interface mit „Dark Theme “

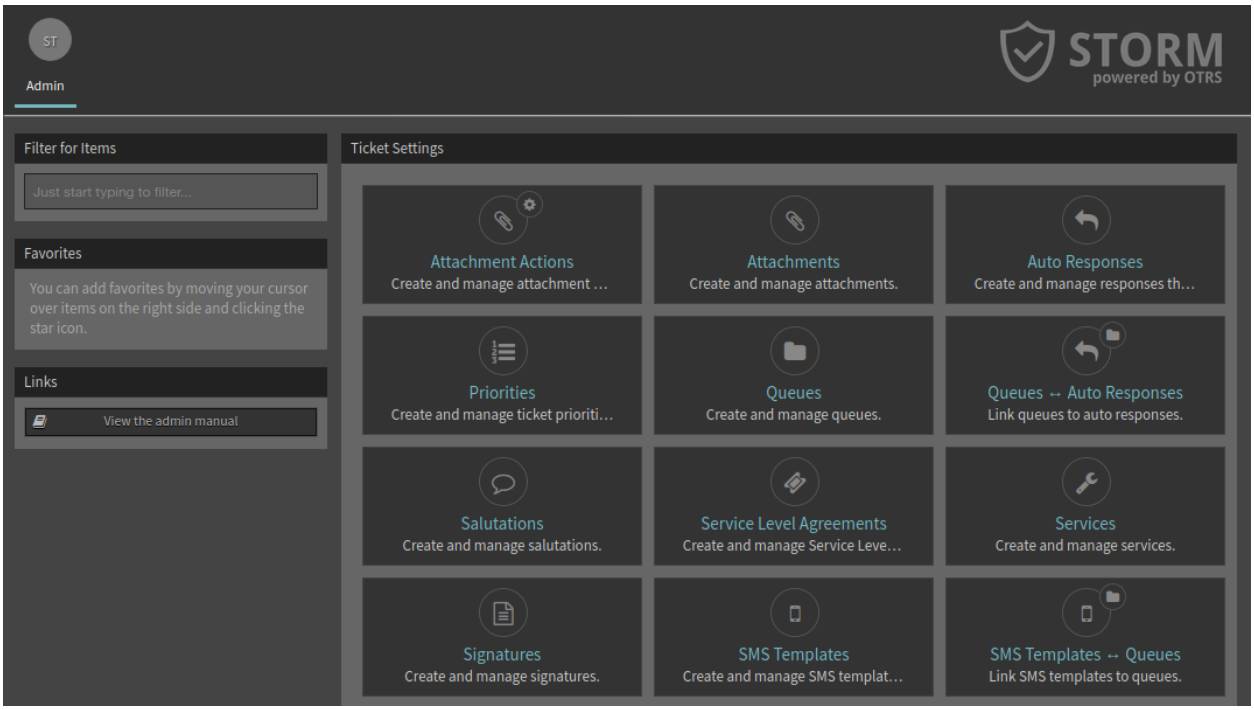

Abb. 3: Administrator-Interface mit „Dark Syle “

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.

Deaktivierter Gravatar
Gravatar ist ein Drittanbieter-Service, um Benutzer-Avatare als Profilbild in den Benutzerkarten und im Widget „Kommunikationsfluss "einzubinden. Die gehashte E-Mail-Adresse des jeweiligen Benutzers würde an einen externen Service übertragen werden und ist daher standardmäßig deaktiviert. Stattdessen werden die Initialen der Benutzer angezeigt.

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.

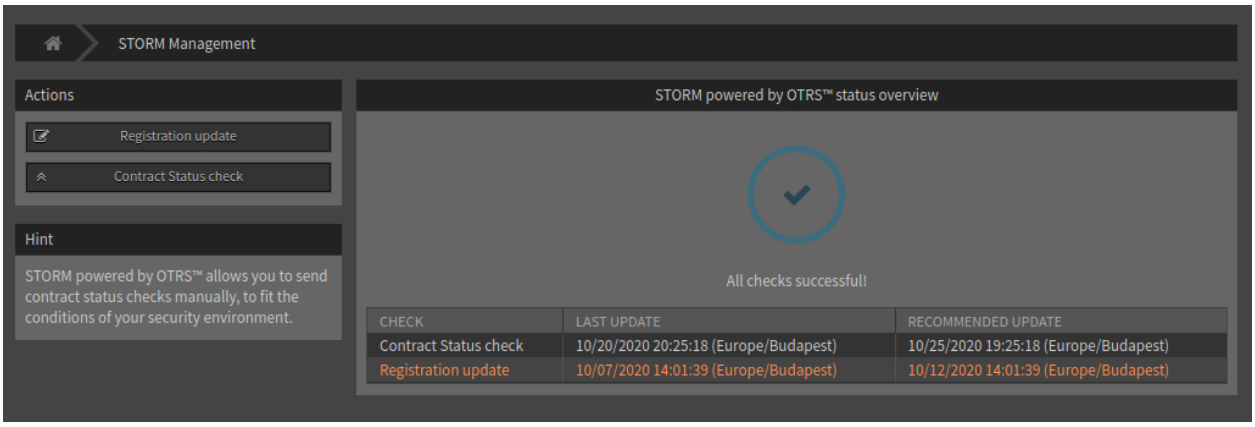

Abb. 1: STORM Verwaltungsansicht

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*.

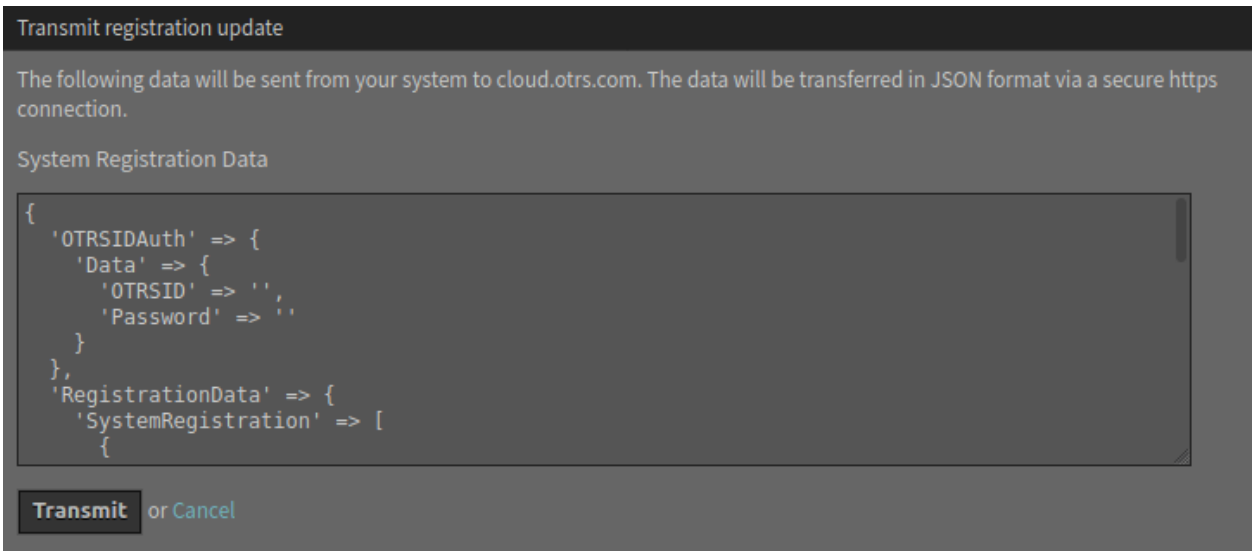

Abb. 2: Update-Aktualisierungsansicht

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*.

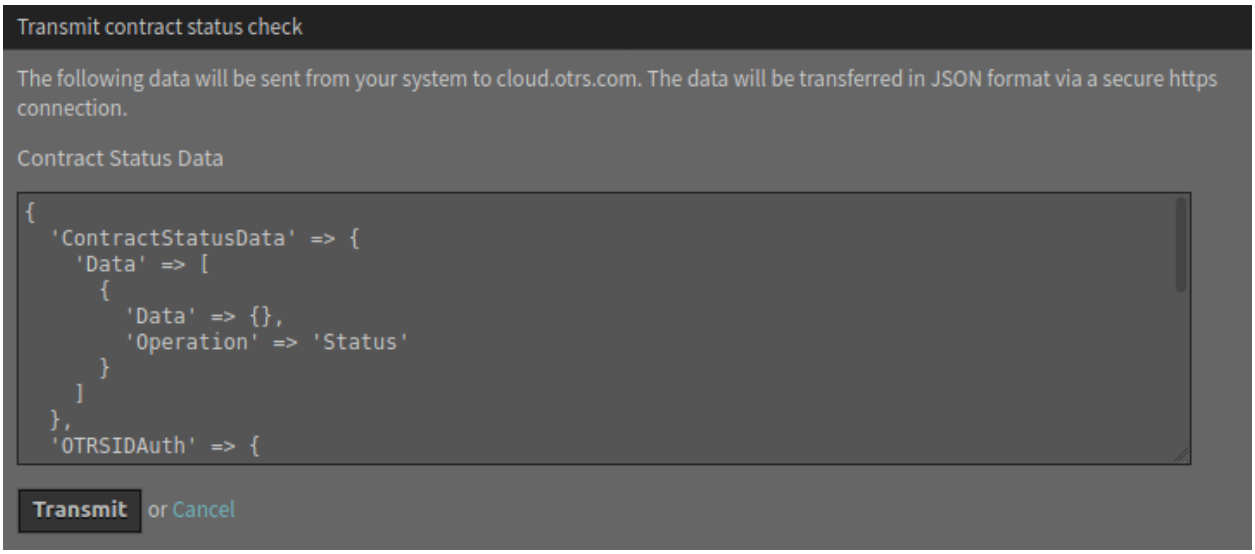

Abb. 3: Vertragsstatus-Überprüfung

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.

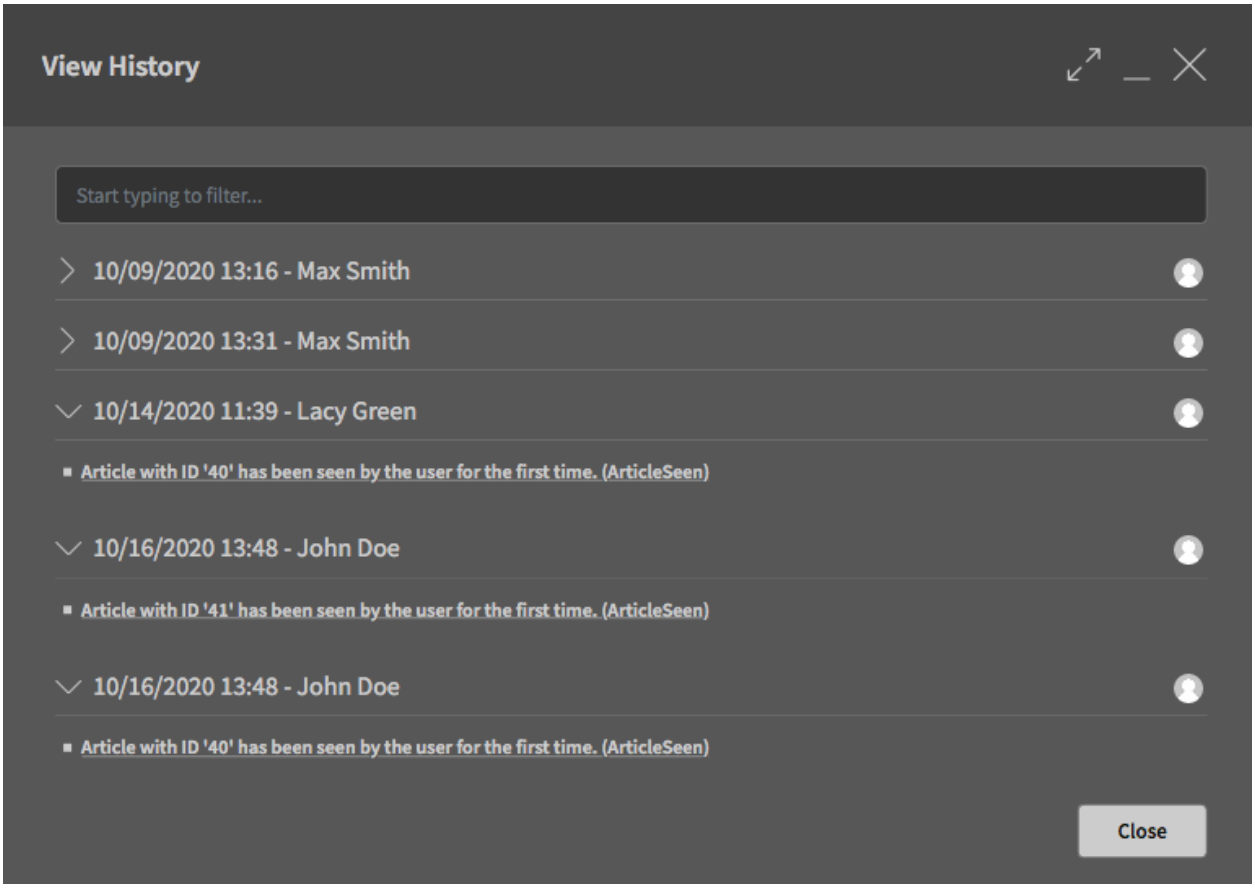

Abb. 1: Beispiel für Historie - Gesehene Artikel

KAPITEL 5

Article Raw Source for Web Service

Wenn Artikel in Web-Services nur mit ihrem Body gesendet werden, enthalten sie in der Regel zu wenig Details für eine tiefere und sicherere Analyse. Sicherheitsanalysten profitieren davon, wenn ein E-Mail-Artikel mit all seinen Rohdaten, einschließlich aller Kopfzeilen, zur tieferen Analyse an Remote-Systeme gesendet wird.

Zu diesem Zweck verfügt STORM über eine Funktion zum Senden der E-Mail-Rohdaten mit den generischen Schnittstellenoperationen und Invokern an ein Remote-System.

Wenn OTRS als Provider arbeitet, werden diese Daten automatisch beim Einrichten des Web-Services gesendet. Dies ist nur für die Operation `TicketGet` möglich.

Wenn OTRS als Requester arbeitet, muss das Feld beim Einrichten der Invoker-Einstellungen durch Auswahl des Wertes `ArticlePlain` ausgewählt werden.

Das Feld „article plain “kann für die Invoker `TicketCreate` und `TicketUpdate` verwendet werden.

Die Rohdaten des Artikels sind bei der Wiedergabe der Kommunikation des Web-Services zu sehen. Zu Testzwecken können diese Informationen auch im Debugger gefunden werden.

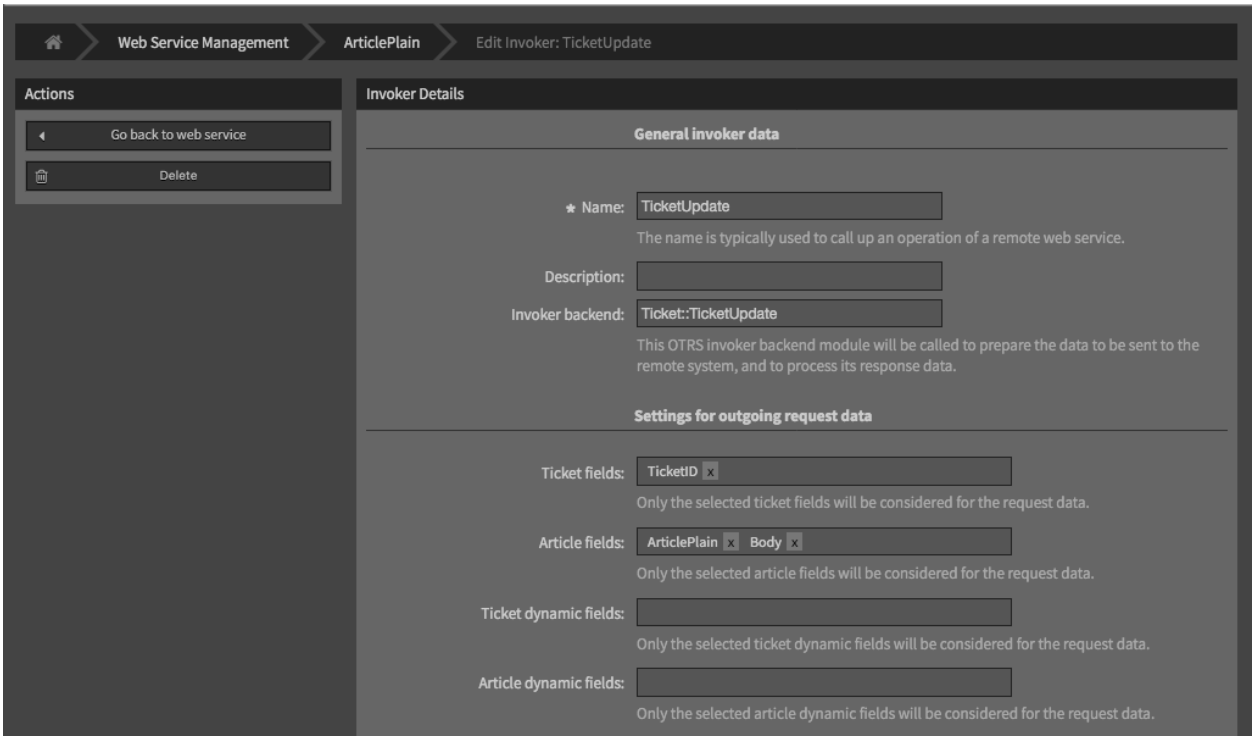

Abb. 1: Web Services Invoker-Einstellungen

KAPITEL 6

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.

6.1 Einrichten des VirusTotal-Moduls

Das System verfügt bereits über ein Modul zum Senden von Anhängen, die von *VirusTotal* per Upload des Anhangs geprüft werden. Die mit diesem Modul verknüpfte Anhangsaktion 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.

6.2 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>"
```

6.3 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.

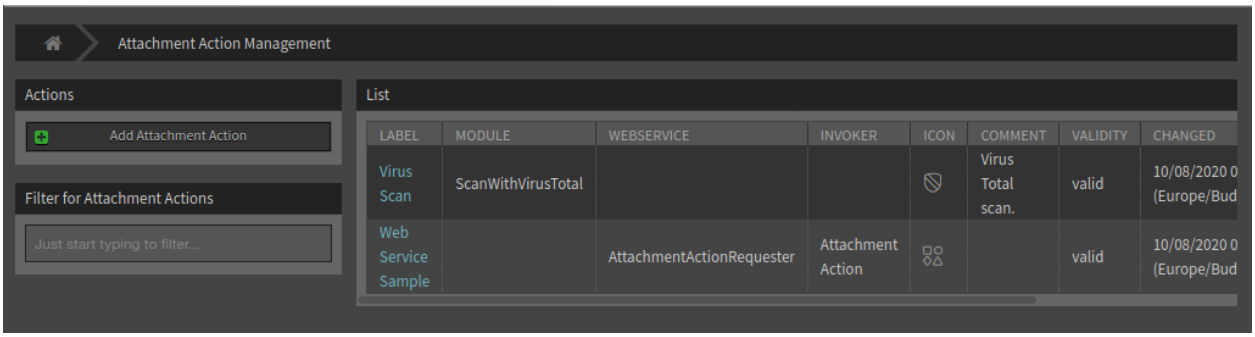

Abb. 1: Ansicht zur Verwaltung von Anhang-Aktionen

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*.

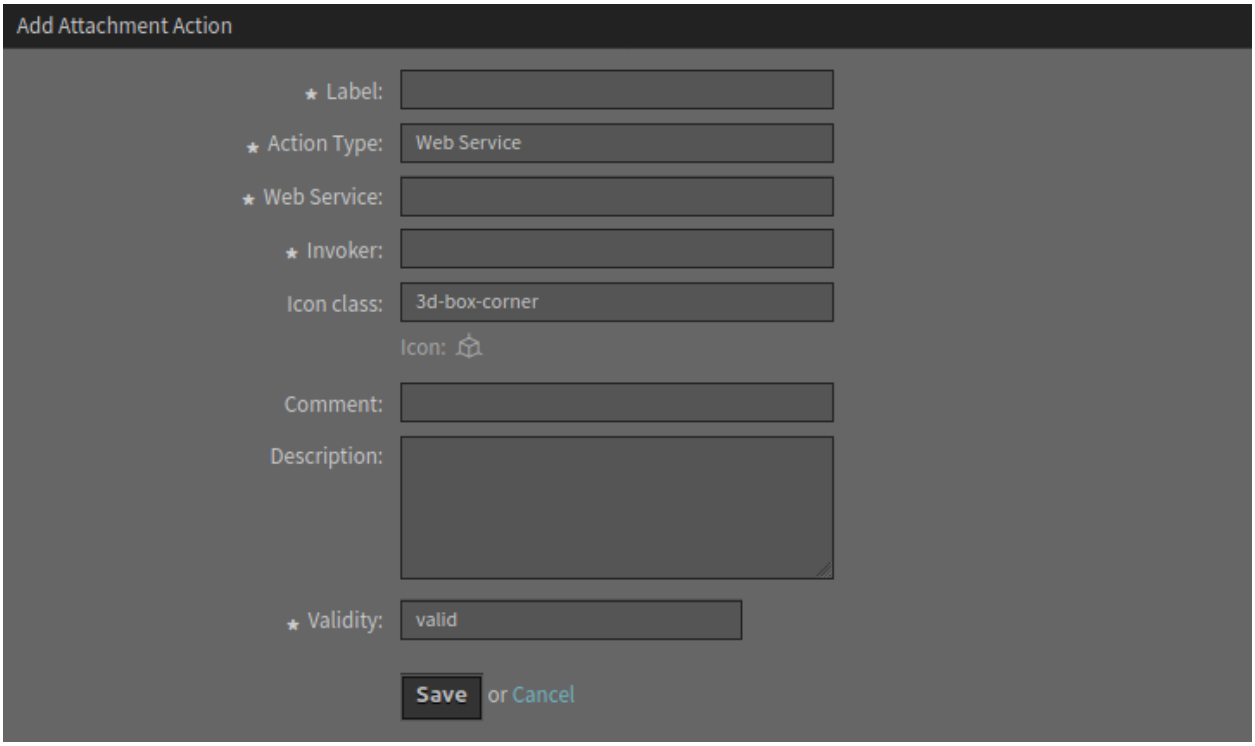

Abb. 2: Ansicht für Anhang-Aktionen

Es ist möglich, Anhang-Aktionen für Module oder Web-Services zu erstellen. Mit STORM wird das Modul `ScanWithVirusTotal` und `ReportWithVirusTotal` 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*.

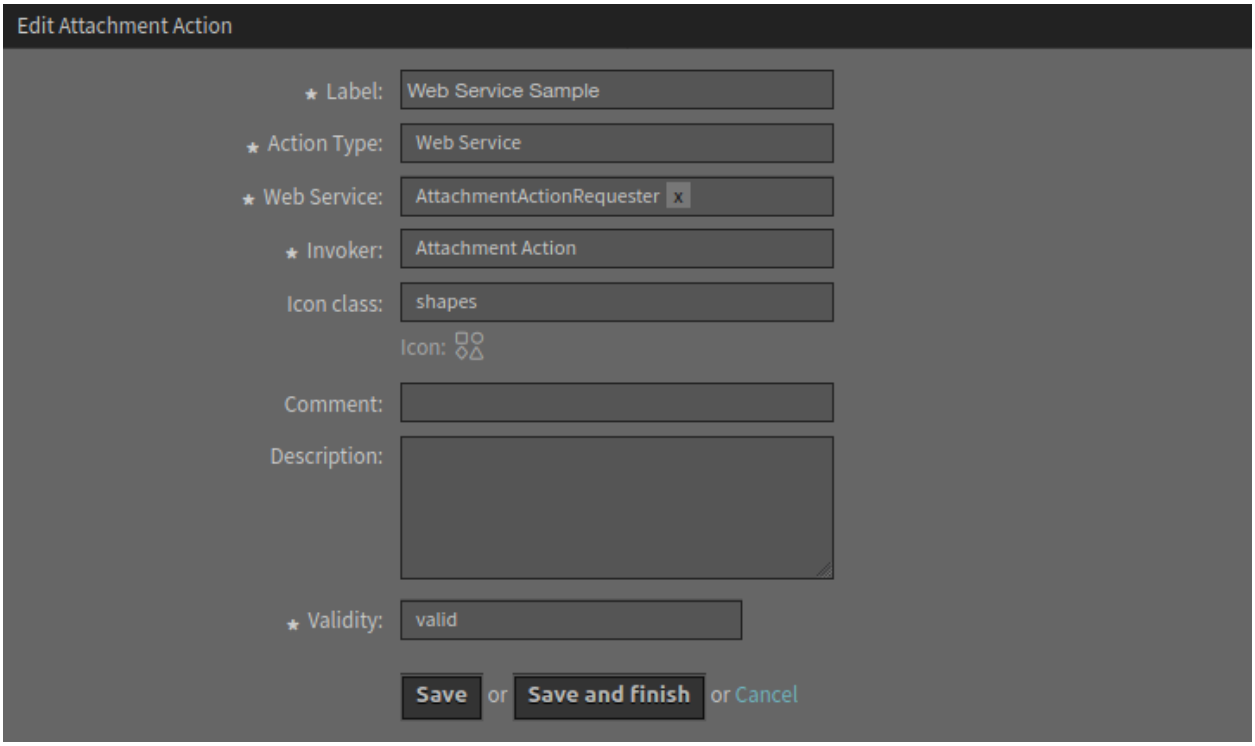

Abb. 3: Ansicht zum Bearbeiten von Anhang-Aktionen

6.4 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*.

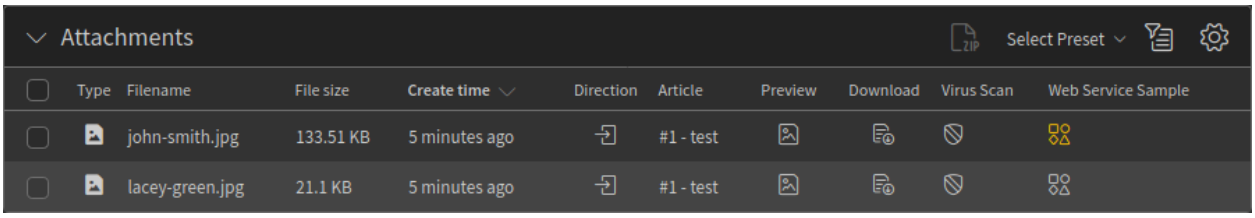

Abb. 4: Widget „Anhänge “

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

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.

6.5 Anhang Aktionen für VirusTotal

STORM bietet zwei integrierte Anhang-Aktionen, die die Webservice-API von virustotal.com verwenden. Diese Aktionen und ihre Ergebnisse werden als separate Spalten im Widget *Anhänge* angezeigt.

Abb. 5: Widget „Anhänge “

Die Symbole innerhalb der Spalten werden verwendet, um die Anfügeaktion durchzuführen und die Ergebnisse der Analyse anzuzeigen.

6.5.1 Virus Scan

Die Spalte *Virus Scan* wird verwendet, um einen Anhang zur Virenprüfung an VirusTotal zu senden. In diesem Fall wird die Datei an VirusTotal gesendet und VirusTotal gibt nach der Analyse ein Ergebnis zurück, ob diese Datei einen Virus enthält.

Die Ergebnisse dieser Analyse werden durch die Farbe des Symbols dargestellt. Die Farben haben die folgende Bedeutung:

- Grün = Kein Virus gefunden
- Gelb = Die Datei wurde analysiert, aber es liegen noch keine Ergebnisse vor
- Orange = Die Datei enthält einen Virus
- Lila = Server-Fehler

- Grau = Die Datei wurde noch nicht ausgewertet

6.5.2 Virus-Bericht

In einigen Fällen kann es erforderlich sein, statt einen Anhang direkt an Remote-Virendienst zu senden, einen Hash der Daten dieses Anhangs zu senden, der von VirusTotal als Kennung verwendet wird.

Zu diesem Zweck verfügt STORM über eine Funktion, die es erlaubt, anstelle des Anhangs selbst einen Hash zu versenden. Diese Funktion wird mit einem eigenen Symbol in der Spalte *Virus Report* dargestellt. Wenn ein Agent auf dieses Symbol klickt, wird nur der Daten-Hash dieser Datei an VirusTotal gesendet und nicht die Datei selbst.

VirusTotal durchsucht diesen Hash in seinen Datensätzen und gibt die Information zurück, ob diese Datei einen Virus enthält. Die Ergebnisse dieser Analyse werden durch die Farbe des Symbols dargestellt. Die Farben haben die folgende Bedeutung:

- Grün = Kein Virus gefunden
- Gelb = Die Datei wurde analysiert, aber es liegen noch keine Ergebnisse vor
- Orange = Die Datei enthält einen Virus
- Rot = Der Hash wurde gesendet, aber VirusTotal hat keine Datei für den Vergleich
- Lila = Server-Fehler
- Grau = Die Datei wurde nicht gesendet

KAPITEL 7

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.

7.1 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`

7.2 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 *Anhänge in dynamischen Feldern* installiert ist, werden die Downloads der Anhänge in den dynamischen Feldern ebenfalls im Systemprotokoll protokolliert.

KAPITEL 8

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.

8.1 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.

8.2 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 mehrere 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 9

Artikel Metafilter für Web-Services

Sicherheitsanalysten wollen relevante IPs und andere Daten aus Nachrichten in vorhandenen Datensätzen finden, damit sie Zeit für Untersuchungen sparen können, indem sie die Webservice-Schnittstellen des Metadatensammlers nutzen, anstatt Zeit für die manuelle Suche nach vorhandenen Übereinstimmungen von empfangenen IPs oder anderen Daten zu verschwenden, wenn Nachrichten Daten für Untersuchungen enthalten.

Das Prinzip dieser Funktion ist das gleiche wie bei anderen Artikel-Meta-Filtern. Es können einige reguläre Ausdrücke definiert werden, um einen Web Service Invoker aufzurufen. Abhängig von dem Web-Service und dem externen Server, den der Web-Service aufruft, enthält die Antwort eine Liste von Ergebnissen. Die Ergebnisliste sollte in einem bestimmten Format vorliegen, damit OTRS sie verstehen kann. Es ist sehr empfehlenswert, ein XSLT Mapping für diesen Invoker zu verwenden, so dass er die Ergebnisse des externen Providers in ein für OTRS verständliches Format umwandeln kann.

9.1 Einrichtung

Das Feature kann mit der Einstellung `AgentFrontend::TicketDetailView::ArticleMeta` aktiviert werden. Diese Einstellung wird für die im OTRS-Framework eingebauten Meta-Filter benötigt, aber auch für den Webservice-Artikel-Meta-Filter ist dies erforderlich.

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

- Der erste Meta-Filter ist nur ein Beispiel dafür, wie man mit Google nach Hostnamen sucht.
- Der zweite Meta-Filter ist nur ein Beispiel dafür, wie man mit Google nach Servern sucht.
- Der dritte Meta-Filter ist ein komplexeres Beispiel für die Suche nach IP-Adressen mit einem „Who is “-Dienst.
- Der vierte Metafilter kann Informationen über IP-Adressen liefern.
- Der fünfte Meta-Filter kann Informationen zu Schwachstellenproblemen liefern.

Es kann notwendig sein, die richtigen Werte für die Schlüssel `WebService`, `Invoker` und `Payload` in den ersten drei Beispielen zu setzen, damit sie zum aktuellen System passen. Der vierte und fünfte Meta-Filter sind Beispiele aus der Praxis, sie sollten nach der Aktivierung unverändert funktionieren.

Sie können sehen, welche regulären Ausdrücke in dem `RegExp`-Array definiert sind.

Es gibt eine weitere Einstellung `AgentFrontend::TicketDetailView::ArticleMetaFilters::WebService###00` in der die Administratoren benutzerdefinierte Metafilter definieren können.

Bemerkung: Es wird nicht empfohlen, die Beispiele zu ändern oder zu erweitern, da die eingebauten Beispiele in Zukunft geändert werden können. Verwenden Sie die benutzerdefinierte Einstellung, um eigene Meta-Filter zu definieren oder kopieren Sie den Inhalt aus dem Beispiel und erweitern Sie ihn dort.

In der Konfiguration muss angegeben werden, welcher Webservice und welcher Invoker aufgerufen wird. Der Remote-Server sollte eine Liste von Elementen zurückgeben. Diese Liste wird in einem Popup-Fenster im Artikel angezeigt, wenn der Artikel einige Schlüsselwörter enthält, die mit dem konfigurierten regulären Ausdruck übereinstimmen.

Die `Payload` ist die Information, die OTRS an den Remote-Server sendet. Diese Informationen werden vom Remote-Web-Service-Provider spezifiziert und können statische Daten oder die im `RegExp` Array spezifizierten Matches oder Matching Groups enthalten. Die `Payload` kann Referenzen auf die `TicketID`, `ArticleID` und `TicketNumber` durch die OTRS Smart Tags `<OTRS_TICKET_TicketID>`, `<OTRS_TICKET_ArticleID>` und `<OTRS_TICKET_TicketNumber>` enthalten.

Beispiel:

```
Payload:
  # ...
  TicketID: <OTRS_TICKET_TicketID>
  ArticleID: <OTRS_TICKET_ArticleID>
  TicketNumber: <OTRS_TICKET_TicketNumber>
  # ...
```

Es ist möglich, für jedes Element in der Liste eine URL zu konfigurieren, so dass der Agent die Möglichkeit hat, mit nur einem Klick direkt auf eine Website zu gehen.

STORM verfügt über einen eingebauten Invokertyp namens `Generic::ArticleMetaFilter`, der in Web-Services für diesen speziellen Zweck verwendet werden kann. Nur diese Art von Invoker kann für diese Funktionalität verwendet werden.

9.2 Verwendung

Um die Ergebnisse der Anfragen des Artikel-Meta-Filters korrekt anzuzeigen, wird dringend empfohlen, die XSLT-Eingangszuordnung zu ergänzen oder zu erweitern, um die Liste der Ergebnisse in Tags mit der Bezeichnung `Items` einzuschließen, die aus einem oder mehreren Tags bestehen.

Beispiel für ein Element:

```
<Items>Result 1</Items>
```

Beispiel für mehrere Elemente:

```
<Items>Result 1</Items>
<Items>Result 2</Items>
<Items>Result 3</Items>
```

So suchen Sie nach IP-Adressen:

1. Erstellen Sie einen Web-Service mit der obigen XSLT-Zuordnung, um einen externen Server mit den IP-Adressen aufzurufen. Der Web-Service sollte eine Liste zurückgeben, z. B. eine Liste von Host-Namen, die mit den übergebenen IP-Adressen verbunden sind.
2. Erstellen Sie ein neues Ticket.
3. Füllen Sie die Pflichtfelder aus.
4. 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*.
5. Gehen Sie zur Ticket-Detailansicht des neu erstellten Tickets.
6. Erweitern Sie den ersten Artikel im *Communication Stream* Widget, um die Schaltflächen unter dem Artikel zu sehen.

Der Web-Service sucht nach allen möglichen IP-Adressen im Artikel, die durch den regulären Ausdruck konfiguriert sind, und gibt eine Liste von Host-Namen zurück.

Die Schaltflächen verweisen auf die Suchergebnisse eines Web-Service. Dieser sollte die gleichen Suchergebnisse zurückgeben, wenn ein Agent den Web Service mit den angegebenen IP-Adressen aufruft. Der Text für die Schaltflächen (*IP-Adresse* in diesem Beispiel) stammt aus dem Schlüssel `Label` der zugrunde liegenden Systemkonfigurations-Einstellung.

Wenn die Agenten mit der Maus über eine Schaltfläche fahren, erhalten sie eine Vorschau auf die vom Web-Service zurückgegebene Ergebnisliste. Durch Anklicken der Schaltflächen kann eine mit den Ergebnissen verknüpfte URL geöffnet werden.

Diese Funktion funktioniert für alle Artikel eines Tickets.

KAPITEL 10

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.

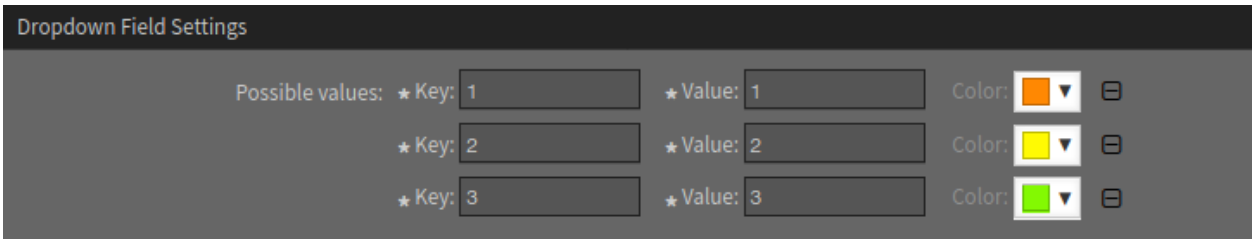

Abb. 1: Zuweisen von Farbindikatoren

Siehe auch:

Bitte lesen Sie im Administratorhandbuch nach, wie man dynamische Felder auf Bildschirmen anzeigt.

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

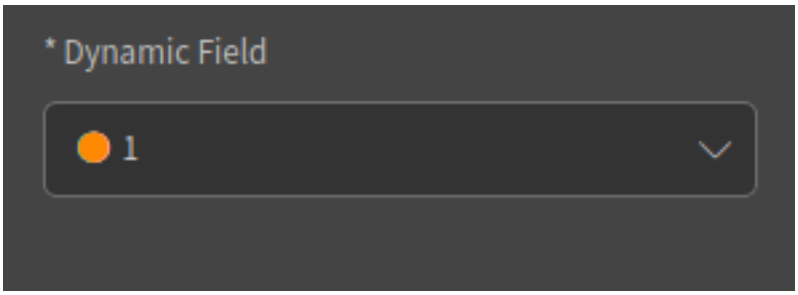

Abb. 2: Dynamisches Feld im Agenten-Interface.

KAPITEL 11

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.

11.1 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 zur Konfiguration von PGP und S/MIME finden Sie in den Kapiteln PGP-Schlüssel, S/MIME-Zertifikate und Einrichten von eingehenden E-Mails im Administrationshandbuch.

11.2 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 Artikelaktion *Antwort per E-Mail*. Abhängig von der ursprünglichen Nachricht wird das Feld *E-Mail-Sicherheit* mit der entsprechenden Methode zur Signierung und/oder Verschlüsselung vorausgefüllt.

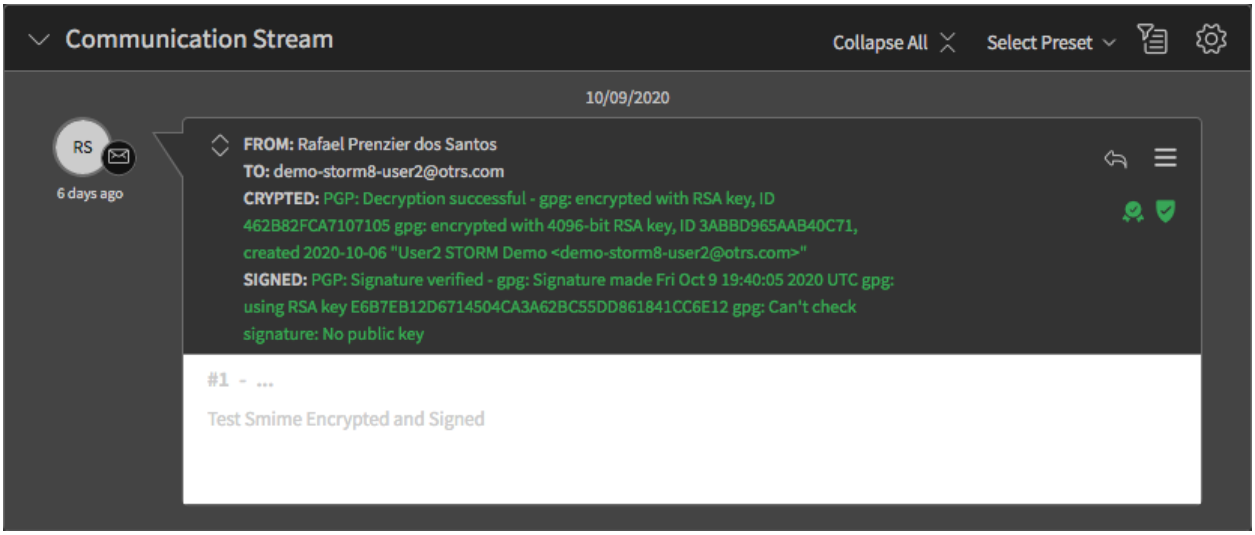

Abb. 1: PGP-signierte und verschlüsselte E-Mail

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

KAPITEL 12

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.

12.1 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 mit den als Systemadressen definierten E-Mail-Adressen übereinstimmen. 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.

12.2 Verwendung

Senden Sie eine mit PGP oder S/MIME verschlüsselte E-Mail von Ihrem persönlichen Account an die in OTRS konfigurierte E-Mail-Adresse, aber verwenden Sie nur das Blind Carbon Copy (*Bcc*)-Feld (füllen Sie weder das *To*- noch das *Cc*-Feld aus). Gehen Sie in die Ticket-Detailansicht des neuen Tickets und der Artikel sollte korrekt entschlüsselt sein.

Abb. 1: Beispiel für eine entschlüsselte Bcc-Email

KAPITEL 13

E-Mail-Sicherheit

Die Systemkonfigurationseinstellung `EnforceEmailSecurityRecipients` definiert eine Liste von E-Mail-Adressen, die immer die Verschlüsselung und/oder Signierung erzwingen. Es ist möglich, reguläre Ausdrücke zu verwenden, um mehrere Adressen zu vergleichen, z.B. `REGEX:(.*@example\.com)`.

Der Absender und alle Empfänger jeder E-Mail sollten so konfiguriert sein, dass sie die gleiche Verschlüsselungs-Engine verwenden, entweder PGP oder S/MIME. Das System ist nicht in der Lage, diese zu mischen.

Wenn die Verschlüsselung eines E-Mail-Empfängers erzwungen wird, müssen alle Empfänger dieser E-Mail einen öffentlichen Schlüssel oder ein Zertifikat im System haben. Die E-Mail muss bei allen Empfängern verschlüsselt sein, andernfalls könnte dies als Sicherheitsproblem angesehen werden.

Wenn mehr als ein Schlüssel und Zertifikat für den Absender oder einen Empfänger im System vorhanden sind (falls erzwungen), wählt diese Funktion das erste gültige Zertifikat aus. Es sei denn, es wurde zuvor ein anderes in der Benutzeroberfläche angegeben.

Bemerkung: Der E-Mail-Versand wird fehlschlagen, wenn das System nicht alle erzwungenen Schlüssel und Zertifikate finden konnte.

Wenn ein Agent einen PGP-Schlüssel oder ein S/MIME-Zertifikat verwendet, können die E-Mail zum Zurücksetzen des Passworts, die E-Mail zur Zwei-Faktor-Verifizierung, die E-Mail zur Ticket-Benachrichtigung und die E-Mail zur Terminbenachrichtigung signiert und/oder verschlüsselt gesendet werden. PGP wird gegenüber S/MIME bevorzugt.

Um diese Funktion zu aktivieren, gibt es auf den entsprechenden Verwaltungsbildschirmen ein Kontrollkästchen *Signierte und/oder verschlüsselte E-Mail senden*. Wenn dieses Kontrollkästchen aktiviert ist, wird die E-Mail in signierter und/oder verschlüsselter Form gesendet.

KAPITEL 14

Hardware Security Module (HSM) Unterstützung für private Schlüssel

Wenn der kontrollierte Zugriff auf das Dateisystem des Servers nicht als ausreichende Sicherheit angesehen wird, profitieren Sicherheitsmanager von der HSM-Unterstützung (Hardware Security Module) für private Schlüssel. Damit können sie sich gegenüber Zertifikaten und anderen Kryptographieoperationen authentifizieren, die ein HSM installiert oder angeschlossen haben. Dies gewährleistet sicherere private Schlüssel und Passwörter als die Speicherung von Zertifikaten und deren Schlüsseln und Passwörtern im Dateisystem des Servers.

14.1 Anforderungen

- Konfigurierte E-Mail-Adressen zum Senden und Empfangen von E-Mails.
- Nitrokey HSM USB-Karte für S/MIME:
  - Privater Schlüssel für die konfigurierte E-Mail, die auf der Karte gespeichert ist.
  - Zertifikat für die konfigurierte E-Mail, die auf der Karte gespeichert ist.
  - S/MIME-Unterstützung in OTRS konfiguriert.
- Nitrokey Start USB-Karte für PGP:
  - Privater Schlüssel für die konfigurierte E-Mail, die auf der Karte gespeichert ist.
  - Konfigurierte PGP-Unterstützung in OTRS.
  - Öffentlicher PGP-Schlüssel in OTRS hinzugefügt.
- Installation der OpenSC-Werkzeuge:

```
opensc-tool
opensc-explorer
pkcs11-tool
pkcs15-tool
libp11
```

14.2 S/MIME

In diesem Abschnitt wird beschrieben, wie Sie die NitroKey HSM-Karte mit S/MIME verwenden können.

14.2.1 Vorbereitung

Um die NitroKey HSM-Karte mit OTRS zu verwenden, muss zunächst OpenSSL für die Arbeit mit `libp11` konfiguriert werden. Obwohl es verschiedene Möglichkeiten gibt, dies zu tun, wird empfohlen, eine benutzerdefinierte Konfigurationsdatei zu erstellen und am Anfang die Hauptkonfigurationsdatei von OpenSSL einzubinden. Ein Beispiel für eine solche Konfigurationsdatei wird im Folgenden gezeigt:

```
openssl_conf = openssl_init

[openssl_init]
engines = engine_section

[engine_section]
pkcs11 = pkcs11_section

[pkcs11_section]
engine_id = pkcs11
dynamic_path = <libpkcs11_PATH>
MODULE_PATH = opensc-pkcs11.so
init = 0

[req]
distinguished_name = req_distinguished_name

[req_distinguished_name]
```

Dabei ist `<libpkcs11_PATH>` der Pfad zu dem von `libp11` zur Verfügung gestellten Motormodul, wie zum Beispiel:

```
/usr/lib/ssl/engines/libpkcs11.so
/usr/local/lib/engines-1.1/libpkcs11.dylib
...
```

Abhängig von der Version, dem Betriebssystem und der Art der Installation kann dies in Ihrer Situation anders sein. Bitte schauen Sie in der Dokumentation von `lib11` nach, um die richtigen Pfade für Ihre Installation zu finden.

Speichern Sie die Datei zum Beispiel in `/etc/openssl/hsm.cnf` und fügen Sie einen Link zu dieser Datei am Anfang der OpenSSL-Original-Konfigurationsdatei ein:

```
# OpenSSL example configuration file.
# This is mostly being used for generation of certificate requests.
#
# Note that you can include other files from the main configuration
# file using the .include directive.
# .include filename
.include /etc/openssl/hsm.cnf
```

14.2.2 Einstellungen

1. Setzen Sie den richtigen Pfad und aktivieren Sie `SMIME::PKCS15ToolBin`. Wenn das **pkcs15-tool** korrekt installiert ist, kann der Pfad durch die Ausführung des Befehls `which pkcs15-tool` ermittelt werden. Das Ergebnis sollte kopiert und in die Einstellung eingefügt werden.
2. Setzen Sie den richtigen Pfad und aktivieren Sie `SMIME::HSMPrivatePath`. Es wird empfohlen, ein neues Verzeichnis zu erstellen, das sich von `SMIME::PrivatePath` unterscheidet, um Verwechslungen und Überbleibsel zu vermeiden.
3. Setzen Sie die richtige Seriennummer der HSM-Karte und die Benutzer-PIN in `SMIME::HSMCard::PIN`. Die aktuelle Seriennummer der Karte kann mit dem Konsolenbefehl `Maint::SMIME::HSMCard::Check` ermittelt werden. Die aktuelle Benutzer-PIN ist diejenige, die bei der Initialisierung verwendet wurde. Die Karten-Seriennummern für Beispielkarten können entfernt werden.
4. Aktivieren Sie die Verwendung der HSM-Karte in der Einstellung `SMIME::UseHSM`.

14.2.3 Überprüfung der Umgebung

Führen Sie den Konsolenbefehl `Maint::SMIME::HSMCard::Check` aus. Die Ausgabe sollte wie folgt aussehen:

```
Reading HSM card information...
+-----------------+--------------------+
| Label | SmartCard-HSM                |
| Serial number   | DENK0100003        |
| Manufacturer ID | www.CardContact.de |
| User PIN        | Verified           |
+-----------------+--------------------+
Checking OpenSSL engines...
+-------------------------------+-------------+
| Dynamic engine loading support | Available   |
| pkcs11 engine                  | Available   |
| Intel RDRAND engine            | Available   |
+-------------------------------+-------------+
Done
```

Es ist wichtig, dass die `User-PIN` verifiziert ist und dass die `pkcs11` Engine verfügbar ist. Wenn eine andere aufgefuehrte Engine nicht verfügbar ist, bedeutet dies nicht unbedingt ein Problem.

14.2.4 Importieren von HSM-Kartenzertifikaten und -Schlüsseln

Während das Signieren und Entschlüsseln der Nachrichten auf der HSM-Karte erfolgt, muss OTRS dennoch bestimmte Informationen von der HSM-Karte importieren. Die öffentlichen Zertifikate müssen von der Karte in das Dateisystem kopiert werden. Dies kann über die übliche `SMIME::CertPath`-Einstellung erfolgen.

Es muss eine Unterdatei mit einigen Metadaten des privaten Schlüssels erzeugt und in dem Pfad abgelegt werden, der in der Einstellung `SMIME::HSMPrivatePath` festgelegt wurde. Diese Metadaten umfassen die Seriennummer der HSM-Karte, die Schlüssel-ID, das Label, den Hash, den Modulus usw.

Um diese Aufgabe zu erfüllen, wurde ein neuer `Maint::SMIME::HSMCard::Sync` Konsolenbefehl erstellt. Die Ausgabe sollte wie folgt aussehen:

```
Syncronizing certificates and private keys metadata...
  Reading HSM card information... OK
  Reading HSM card objects... OK
  Processing HSM certificates and keys...
  ID 'a1b2e3d4'... OK
  ID 'f5d6e7c8'... OK
Done.
```

14.2.5 Verwendung

Die HSM-Karte sollte nun einsatzbereit sein und die Verwendung sollte für die Benutzer transparent sein, z. B. beim Erstellen eines neuen E-Mail-Tickets.

Stellen Sie sicher, dass Sie eine Queue verwenden, bei der die Systemadresse über ein Zertifikat und einen privaten Schlüssel im HSM-Modul verfügt, und wählen Sie im Feld Sicherheitsoptionen die Option, die E-Mail mit S/MIME zu signieren. Das Absenden des Formulars kann etwas langsamer sein, da die HSM-Karte entsperrt werden muss und der Vorgang durchgeführt werden muss.

14.3 PGP

In diesem Abschnitt wird beschrieben, wie Sie die NitroKey HSM-Karte mit PGP verwenden können.

14.3.1 Einstellungen

Es ist erforderlich, die Kartenbenutzer-PIN als das gespeicherte Schlüsselpasswort in der Einstellung `PGP::Key::Password` festzulegen. Wenn z. B. die Schlüssel-ID *11223344* und die Kartenbenutzer-PIN *123456* ist, erstellen Sie einen neuen Eintrag in der Einstellung und geben Sie im ersten Teil *11223344* und dann *123456* als Wert ein.

So erhalten Sie die Schlüssel-ID:

1. Öffnen Sie das Modul *PGP-Schlüssel* im Administrator-Interface.
2. Überprüfen Sie die ID des Schlüssels in der Spalte *Schlüssel*.

Bemerkung: Wenn das System bereits konfiguriert ist und mit diesem bestehenden Schlüssel arbeitet, sollte die Einstellung bereits einen Eintrag für die ID enthalten. In diesem Fall sollte das Schlüsselpasswort bereits festgelegt sein, muss aber noch ausgetauscht werden, damit die Kartenbenutzer-PIN korrekt funktioniert.

14.3.2 Verwendung

Die Verwendung sollte nun für die Benutzer transparent sein, z. B. beim Erstellen eines neuen E-Mail-Tickets. Stellen Sie sicher, dass Sie eine Queue verwenden, bei der die Systemadresse ein öffentliches und privates Schlüsselpaar in der verschlüsselten Karte hat, und wählen Sie im Feld „Sicherheitsoptionen “, dass die E-Mail mit PGP signiert werden soll.

KAPITEL 15

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.

15.1 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`

15.2 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 16

Dynamische Empfänger für Vorlagen

Service-Agenten können E-Mails und Notizen an mehrere wiederkehrende Empfänger senden. Sie können durch vordefinierte Empfänger in Vorlagen Zeit bei der Kommunikation sparen, anstatt immer wieder neue Empfänger hinzuzufügen, wenn Nachrichten an eine bestimmte Liste von Empfängern gesendet werden müssen.

Diese Funktion bietet die Möglichkeit, beliebige Ticket-Attribute in den Feldern *An* und *Cc* einer Vorlage über OTRS Smart Tags zu verwenden. Mit dieser Funktion kann der Administrator dynamische Empfänger für Vorlagen hinzufügen.

Die Empfängerfelder sind bereits im *Categories For Text Modules* Feature enthalten. Was STORM hinzugefügt wird, ist die Verwendung von OTRS Smart Tags in den Empfängerfeldern.

Bemerkung: Diese Funktion erfordert das Feature *Kategorien für Textbausteine*.

16.1 Verwendung

Beispiel für die Verwendung von dynamischen Empfängern:

```
<OTRS_TICKET_State>@example.com
<OTRS_TICKET_DynamicField_ArchiveEmail>
support@<OTRS_TICKET_DynamicField_Company>.com
```

Je nach Ticket-Status wird `<OTRS_TICKET_State>@example.com` durch *open@example.com*, *closed-successful@example.com* usw. ersetzt.

Wenn ein dynamisches Ticket-Feld eine vollständige E-Mail-Adresse enthält, kann das dynamische Feld als E-Mail-Adresse in den Empfängerfeldern verwendet werden.

Um die Support-Anfrage an das entsprechende Unternehmen zu senden, kann `support@<OTRS_TICKET_DynamicField_Company>.com` verwendet werden, wenn das dynamische Feld den Namen dieses Unternehmens enthält.

Dynamische Dropdown- und Mehrfachauswahlfelder werden ebenfalls unterstützt.

Bemerkung: Der Ticket-Typ OTRS Smart Tags werden nur unterstützt wie `<OTRS_TICKET_...>`.

KAPITEL 17

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 könnte dies für die Benachrichtigungen verwendet werden, die per E-Mail gesendet werden. Zu diesem Zweck wurden neue Vorlagen hinzugefügt, die verschiedene Layouts mit Farben enthalten, die den Status gemäß dem Ampelprotokoll anzeigen.

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 18

Notification Plain Text Email Options

Diese Funktion bietet die Möglichkeit, E-Mails zu Termin- und Ticketbenachrichtigungen im Klartext zu versenden. Dies kann nützlich sein, wenn ein entferntes System keine Rich-Text-E-Mails lesen kann.

18.1 Verwendung

So senden Sie die E-Mail-Benachrichtigung als reinen Text:

1. Öffnen Sie im Administrator-Interface die *Terminbenachrichtigungen* oder die *Ticket-Benachrichtigungen*.
2. Fügen Sie eine neue Benachrichtigung hinzu oder wählen Sie eine vorhandene Benachrichtigung aus der Liste der Benachrichtigungen aus.
3. Markieren Sie das Feld *E-Mail als reinen Text senden*.

Wenn das Kontrollkästchen aktiviert ist, wird der Rich-Text-Editor im Abschnitt *Benachrichtigungstext* in einen normalen Textbereich umgewandelt. In den Textbereich für den Inhalt der E-Mail kann nur einfacher Text eingegeben werden.

Außerdem ist das Feld *E-Mail-Vorlage* auf *Unformatiert* und auf schreibgeschützt eingestellt. Alle E-Mails, die von einer so konfigurierten Benachrichtigung gesendet werden, sind im reinen Textformat.

OTRS Tags werden weiterhin im reinen Textformat unterstützt.

Notification Methods

These are the possible methods that can be used to send this notification to each of the recipients. Please select at least one method below.

Email

Enable this notification method: ☑

Additional recipient email addresses:
Use comma or semicolon to separate email addresses.
You can use OTRS-tags like <OTRS_TICKET_DynamicField_...> to insert values from the current ticket.

Article visible to customer: ☐
An article will be created if the notification is sent to the customer or an additional email address.

Create multiple articles: ☐
An article will be created for each additional recipient address of the notification.

Separator for recipients:
Use this setting to define a needed splitting symbol (e.g. ';' or ',').
This symbol is used as a separator for the addresses in the additional recipient addresses field.

Email template: Unformatted
Use this template to generate the complete email (only for HTML emails).

Enable email security: ☐

Email security level:

If signing key/certificate is missing: Skip notification delivery

If encryption key/certificate is missing: Skip notification delivery

Send email as plaintext: ☑
Email will be sent as plaintext

Web View

Enable this notification method: ☐

SMS (Short Message Service)

Please activate this transport in order to use it.

Abb. 1: Abschnitt Benachrichtigungsmethoden

KAPITEL 19

PDF-Bildvorschau

Diese Funktion ermöglicht es, bei Anhängen für Tickets und Wissensdatenbank-Artikel eine Bildvorschau einer PDF-Datei anzuzeigen. Dies ist hilfreich, um den Inhalt eines PDFs anzuzeigen, ohne die Datei herunterzuladen.

Zusätzlich bietet das Paket die Möglichkeit für eine Bildvorschau in dynamischen Feldern vom Typ „Anhang “(für PDF-Dateien).

Bemerkung: Um diese Funktion zu nutzen, sollte ImageMagick auf dem Server installiert sein, auf dem STORM läuft.

19.1 Einrichtung

1. Laden Sie ImageMagick herunter und installieren Sie es. In den neuesten Versionen von *ImageMagick* ist die Verwendung von PDF-Dateien eingeschränkt. Um die Verwendung von PDF zu ermöglichen, müssen Sie die *ImageMagick*-Konfiguration manuell aktualisieren.
2. Suchen Sie nach der Datei `/usr/local/etc/ImageMagick-7/policy.xml` (der Dateipfad kann je nach *ImageMagick*-Version variieren).
3. Prüfen Sie, ob die Datei einen `PDF`-Eintrag enthält und ob dieser Eintrag nicht als Kommentar markiert ist.
4. Prüfen Sie, ob der Eintrag mindestens ein `read`-Recht enthält.

```
<policy domain="coder" rights="read" pattern="PDF" />
```

5. Gehen Sie zur Systemkonfiguration und suchen Sie die Einstellung `Magick::Bin`.
6. Aktivieren Sie die Einstellung und geben Sie den Dateipfad zum *ImageMagick*-Binary an.
7. Öffnen Sie die Datei `$OTRS_HOME/Kernel/Config.pm` und fügen Sie die Programme in die Liste der erlaubten Programme ein.

```
$Self->{'SystemConfiguration::ValueType::SystemCommand::BinaryWhiteList'}->{'001-
↪OTRSSTORM'} = [
    'magick',
    'pkcs15-tool',
];
```

8. Bauen Sie die Systemkonfiguration neu auf.

19.2 Verwendung

Nach der Installation des Pakets zeigt das Widget *Anhänge* nun in der Spalte *Vorschau* zusätzlich zu den regulären Symbolen für Bilder, Audio- und Videodateien ein Symbol für die PDF-Dateien an.

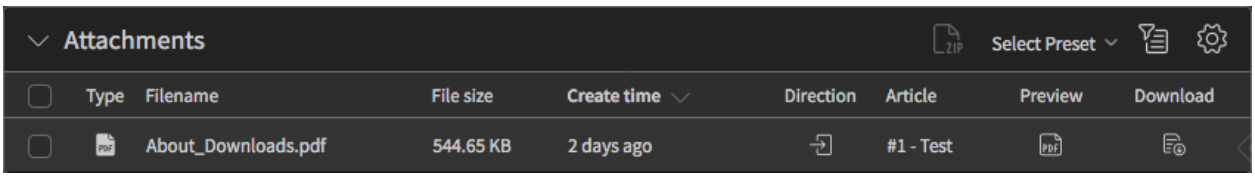

Abb. 1: Vorschauspalte im Widget „Anhänge “

So zeigen Sie eine Bildvorschau des PDFs an:

1. Öffnen Sie die Ticket-Detailansicht oder die Detailansicht des Wissensdatenbank-Artikels.
2. Klicken Sie auf das Vorschausymbol für eine PDF-Datei im Widget *Anhänge*.

Das PDF wird nun als Bild in einem kleinen Vorschaufenster angezeigt. Für den Fall, dass es sich bei der Datei nicht wirklich um ein PDF handelt, wird im Vorschaufenster nichts angezeigt. In diesem Fall ist es empfehlenswert, das PDF nicht herunterzuladen.

Bemerkung: Das angezeigte Bild des PDFs enthält nur die erste Seite des PDFs.

19.2.1 Dynamische Felder vom Typ „Anhang “

Wenn das Feature *Dynamic Field Attachment* installiert ist und ein dynamisches Feld zu einer Eigenschaftskarte hinzugefügt wurde, enthält das dynamische Feld ein zusätzliches Vorschau-Symbol neben dem Download-Symbol.

Die PDF-Bildvorschau kann mit diesem Feature überall dort verwendet werden, wo ein dynamisches Feld vom Typ „Anhang “zum System hinzugefügt wird.

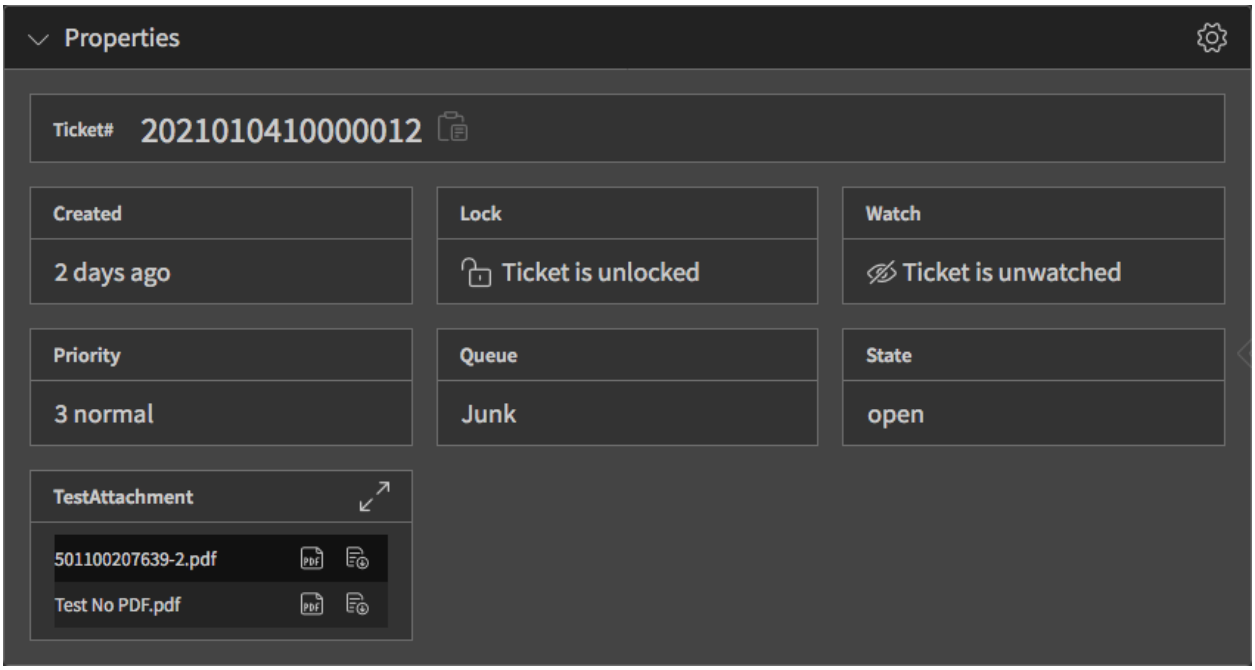

Abb. 2: Eigenschaftskarte mit dynamischem Feld vom Typ „Anhang “

KAPITEL 20

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.

20.1 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 User-Task-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.

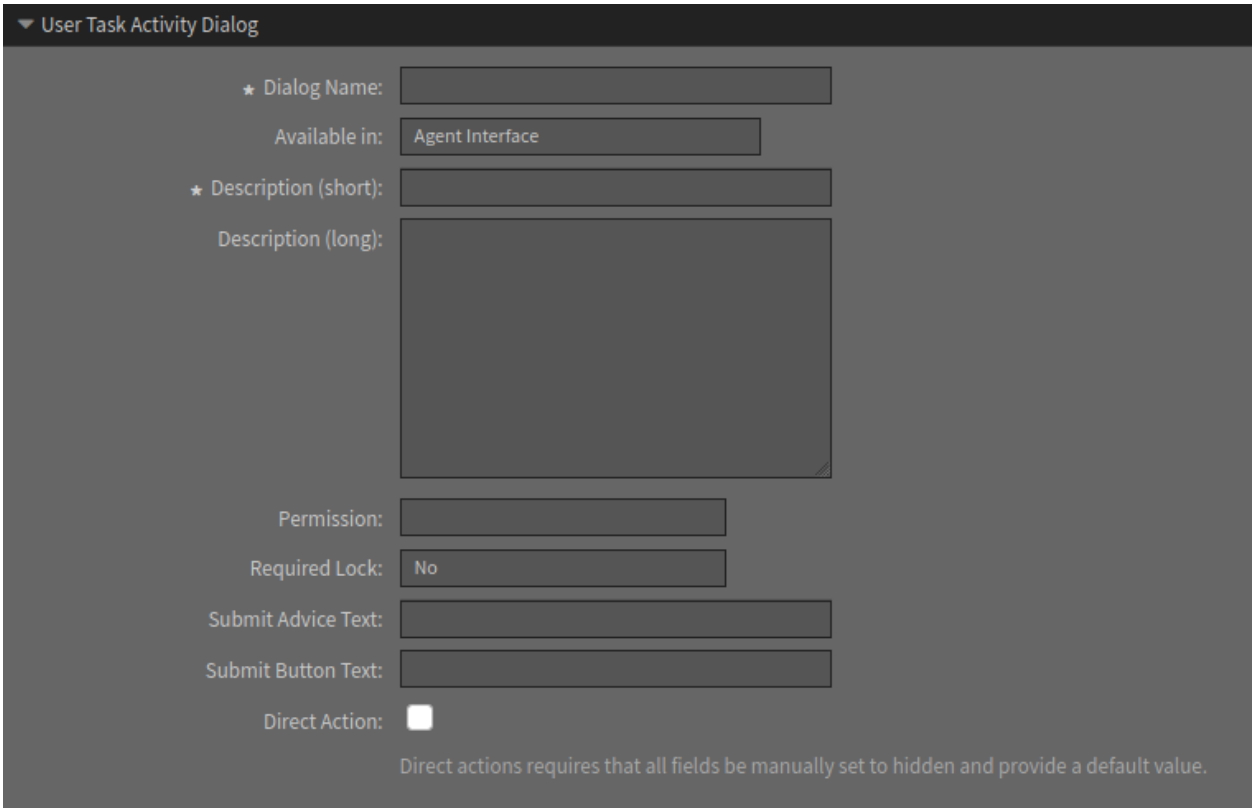

Abb. 1: User-Task-Aktivitätsdialog bearbeiten

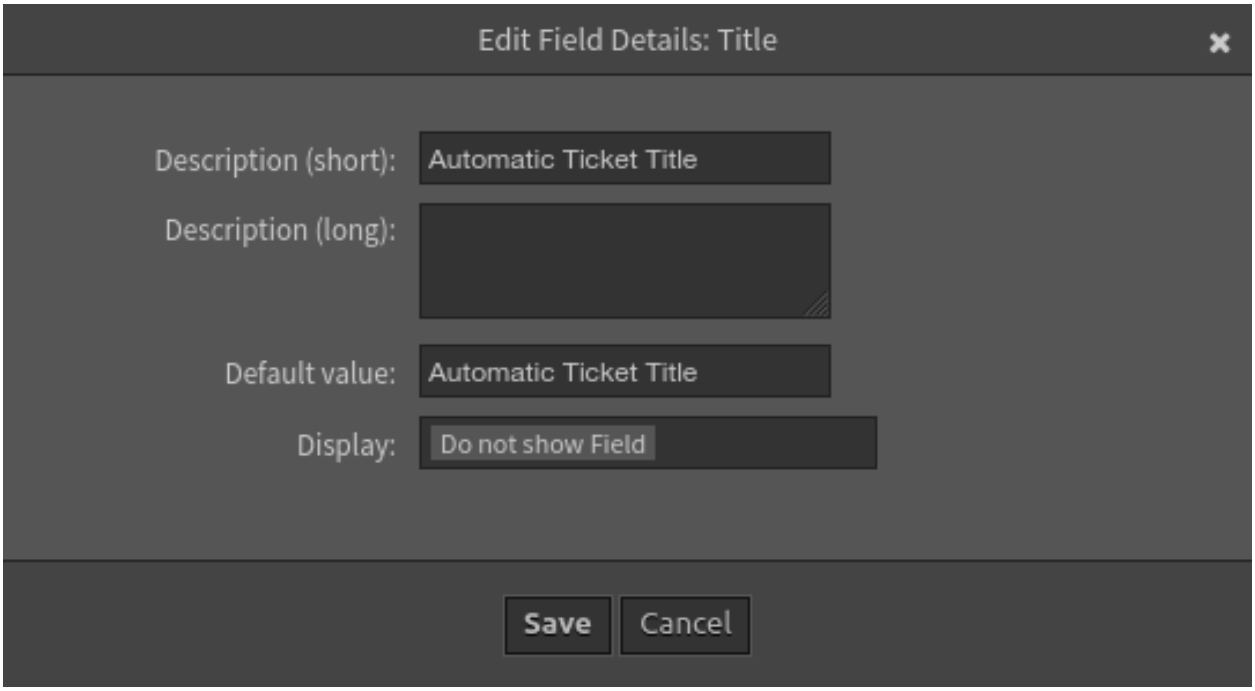

Abb. 2: Dialog Felddetails bearbeiten

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.

Der Prozess kann einige Auslöser enthalten, um von einer Aktivität zu einer anderen zu wechseln, indem ein beliebiges Ticket-Feld wie Status, Queue oder ein beliebiges dynamisches Feld gesetzt wird, indem die vordefinierten direkten Aktionen verwendet werden. Die Benutzer müssen keine Werte einstellen, um zu einer anderen Aktivität zu springen. Mit dieser Funktion ist es möglich, *Vorherige-* oder *Nächste-* Schaltflächen zu den Dialogen des Prozesses hinzuzufügen, um von einer Benutzeraktivität vorwärts oder rückwärts zu springen.

KAPITEL 21

Process Task Activities Encryption and Signing

Mit dieser Funktion ist es möglich, ausgehende E-Mails aus Prozessaufgaben-Aktivitäten so zu konfigurieren, dass sie über S/MIME oder PGP signiert und/oder verschlüsselt werden. Dies kann hilfreich sein, wenn die Empfänger eines Geschäftsprozesses eine verschlüsselte Kommunikation benötigen.

21.1 Verwendung für Skript-Task-Aktivitäten

So richten Sie eine Script-Task-Aktivität mit Signierung und/oder Verschlüsselung ein:

1. Gehen Sie im Administrator-Interface auf die Ansicht *Prozessverwaltung*.
2. Erstellen oder bearbeiten Sie einen bestehenden Prozess.
3. Erstellen oder wählen Sie eine Skript-Task-Aktivität und gehen Sie zum Konfigurationsfenster.
4. Wählen Sie das Modul *TicketSendEmail* und speichern Sie.
5. Klicken Sie auf die Schaltfläche *Konfigurieren* neben dem ausgewählten Modul.
6. Wählen Sie eine der Signier- und Verschlüsselungsmethoden im Abschnitt *E-Mail-Sicherheit*.

Alle gesendeten E-Mails aus solchen konfigurierten Script-Task-Aktivitäten folgen nun den ausgewählten Sicherheitsoptionen mit den entsprechenden Ausnahmen.

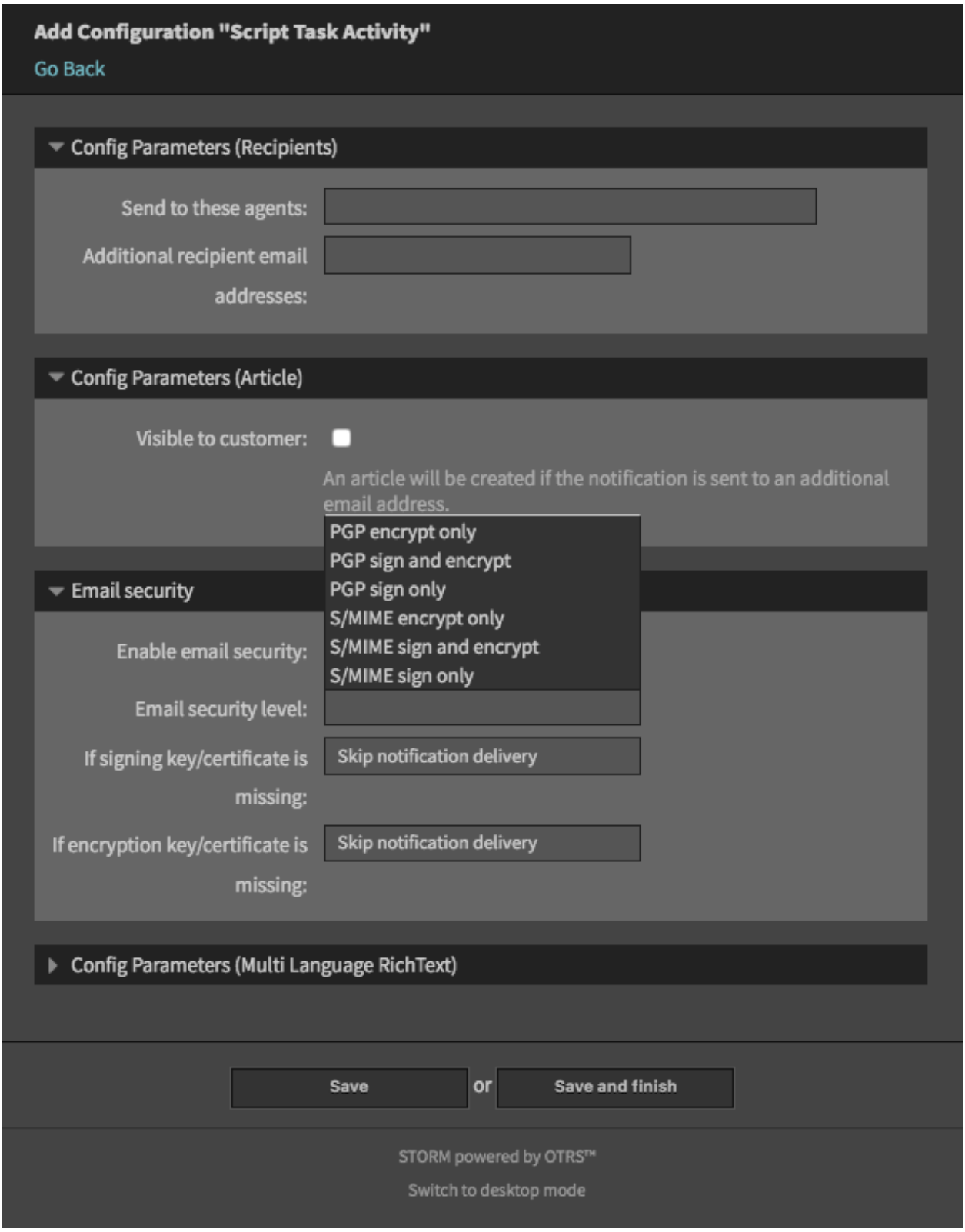

Abb. 1: Fenster zur Konfiguration der Script-Task-Aktivität

21.2 Verwendung für Benutzeraufabe-Aktivitäten

Bemerkung: Diese Funktion erfordert das Feature *Process Management Article Email*.

So richten Sie eine Benutzeraufabe-Aktivität mit Signierung und/oder Verschlüsselung ein:

1. Gehen Sie im Administrator-Interface auf die Ansicht *Prozessverwaltung*.
2. Wählen Sie einen User-Task-Aktivitätsdialog und gehen Sie zum Konfigurationsfenster.
3. Wählen Sie das Feld *Artikel* im Abschnitt *Verfügbare Felder* und verschieben Sie es in den Abschnitt *Zugeordnete Felder*.
4. Wählen Sie im Feld *Kommunikationskanal* den Wert *E-Mail*.
5. Prozess speichern und in Betrieb nehmen.
6. Gehen Sie zum Agenten-Interface und erstellen Sie ein neues Prozess-Ticket.
7. Im Abschnitt *Artikel* des Prozess-Tickets wurde ein neues Feld *E-Mail-Sicherheit* hinzugefügt, in dem die Möglichkeiten zum Signieren und/oder Verschlüsseln der E-Mail ausgewählt werden können.

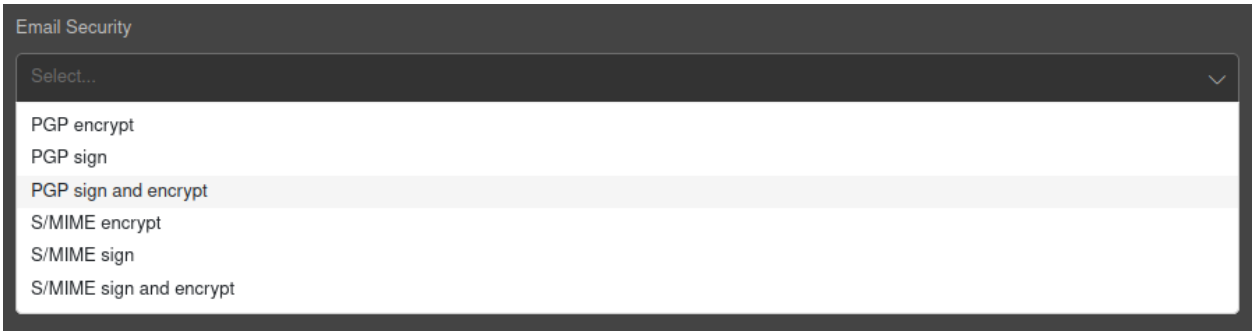

Abb. 2: E-Mail-Sicherheitsfeld im Prozessticket

KAPITEL 22

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 Systemaufrufmodul erfordert die Verwendung von XSLT-Mappings. Das Outbound-Mapping wird verwendet, um den aufzurufenden Systembefehl zu definieren, und das Inbound-Mapping wird verwendet, um die Ergebnisse des Systemaufrufs zu konvertieren, um das aktuelle Ticket zu aktualisieren.

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>
    </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 zugegriffen werden von:

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

<Output>
Beliebiger Text, der auf der Standardausgabe ausgegeben wird.

<ErrorOutput>
Beliebiger Text, der auf der Standardfehlerausgabe ausgegeben wird.

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>
            </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.

22.1 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>
                <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.

KAPITEL 23

Shared Ticket Watchlists

Diese Funktion ermöglicht es, Tickets mit Kennzeichnungen zu versehen, so dass Service-Agenten viel Zeit bei der Suche nach bereits analysierten Incidents oder Service-Anfragen sparen können, anstatt Zeit für die Analyse von Anfragen zu verschwenden, ohne sie entsprechend der Analyseergebnisse zu kennzeichnen, wenn Tickets klassifiziert werden müssen.

Bemerkung: Diese Funktion erfordert das Feature *Ticket Watchlist*.

23.1 Verwendung

Dies ist eine Erweiterung für das Feature *Ticket Watchlist* und ermöglicht die Freigabe der Beobachtungslisten nicht nur für die Stellvertreter, sondern für jeden im System.

Siehe auch:

Siehe die Ticket Watchlist Dokumentation im *Features Manual* für die Basisfunktionalität.

Die Übersicht der Ticket-Überwachungsliste kann über das Brillensymbol in der Seitenleiste des Organizers aufgerufen werden.

Das obige Beispiel zeigt zwei freigegebene Beobachtungslisten und eine persönliche Beobachtungsliste. Das dritte Symbol in der Spalte *Aktionen* ermöglicht die Freigabe einer persönlichen Beobachtungsliste.

Die gemeinsamen Beobachtungslisten haben keine Benachrichtigungen für andere Agenten und sie können die Stellvertreter der gemeinsamen Beobachtungslisten nicht sehen. Andere Agenten können die Ticketliste nur exportieren und über die Ticket-Detailansicht Tickets hinzufügen oder entfernen.

Wenn der Agent zum Stellvertreter der Beobachtungsliste befördert wird, wird dies durch ein Symbol einer Polizeimarke angezeigt. Der Stellvertreter hat einige weitere Privilegien für die Überwachungsliste.

Siehe auch:

Die Stellvertreterfunktion wird in der Dokumentation *Ticket Watchlist* beschrieben.

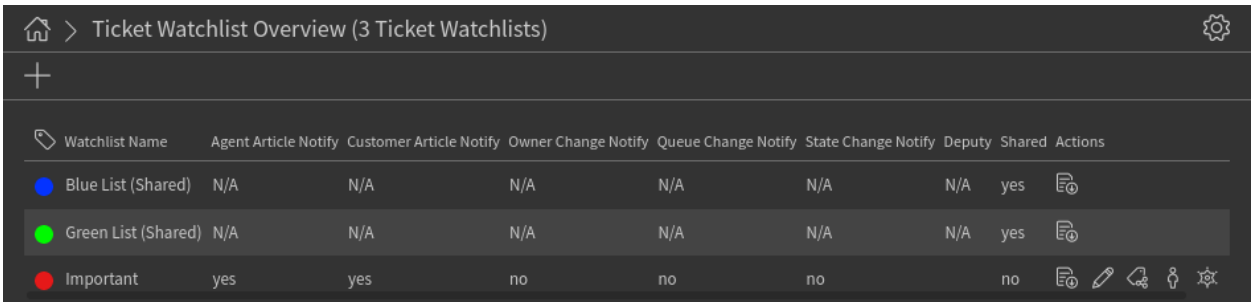

Abb. 1: Ticket-Überwachungsliste Übersicht

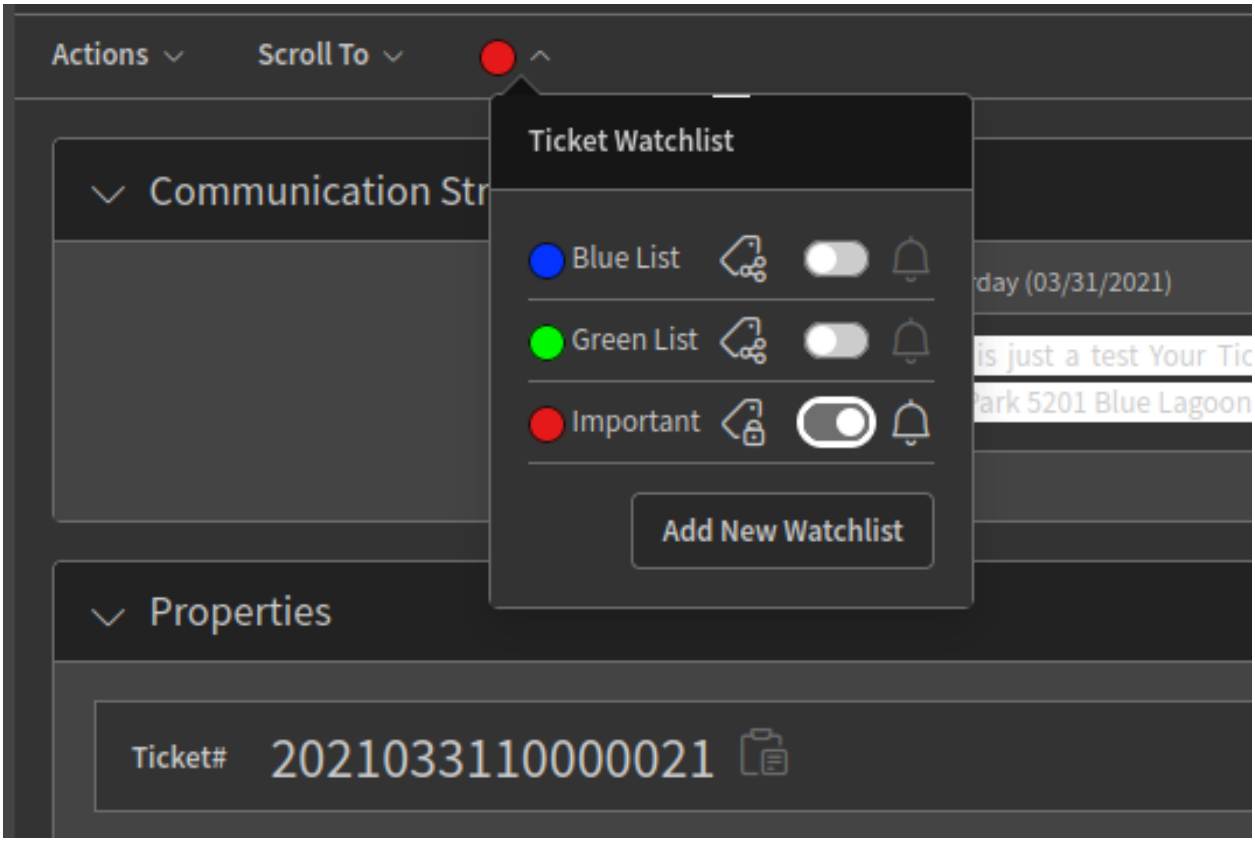

Abb. 2: Ticket-Beobachtungsliste in der Ticket-Detailansicht

Das Schloss-Symbol in der unteren rechten Ecke des Tag-Symbols zeigt an, dass die Beobachtungsliste persönlich ist. Wenn das Symbol aus drei Kreisen besteht, bedeutet dies, dass die Beobachtungsliste freigegeben ist.

Andere Agenten haben grundsätzlich nur Leserechte für gemeinsame Beobachtungslisten, können aber je nach Ticket-Berechtigung (standardmäßig *rw*) Tickets zu den gemeinsamen Beobachtungslisten hinzufügen oder entfernen. Dies bedeutet, dass sie Lese- und Schreibrechte für die jeweilige Anfrage haben. Andernfalls kann ein Agent, der nur über eine Leseberechtigung für ein Ticket verfügt, dieses nicht aus der gemeinsamen Beobachtungsliste entfernen.

Die Berechtigungsstufe zum Hinzufügen oder Entfernen von Tickets zu einer gemeinsamen Beobachtungsliste kann in der Einstellung `AgentFrontend::SharedTags::Ticket::PermissionType` definiert werden.

KAPITEL 24

Beschriftungen für Anhänge

Diese Funktion ermöglicht es, Anhänge mit Tags zu versehen, so dass Sicherheitsanalysten viel Zeit bei der Suche nach bereits analysierten Anhängen sparen können, anstatt Zeit für die Analyse von Anhängen zu verschwenden, ohne sie entsprechend der Analyseergebnisse zu kennzeichnen, wenn Anhänge klassifiziert werden müssen.

24.1 Verwendung

Diese Funktion hat eine ähnliche Funktionalität wie *Shared Ticket Watchlists*, aber für Anhänge.

Die Anhang-Tag-Übersicht kann über das Anhang-Symbol in der Seitenleiste des Organizers aufgerufen werden.

Abb. 1: Attachment-Tag-Übersicht

Es ist möglich, ein Anhangs-Tag zu bearbeiten, freizugeben und zu löschen sowie den Besitzer zu ändern. Wenn das Anhangs-Tag freigegeben ist, ist es für alle Agenten im System sichtbar.

Wenn ein Agent ein Anhangs-Tag erstellt, kann das Tag den Anhängen in einem beliebigen *Anhänge*-Widget in einer Business-Objekt-Detailansicht hinzugefügt werden.

Die Berechtigungsstufe für das Hinzufügen oder Entfernen von Anhängen zu einem gemeinsamen Tag kann in der Einstellung `AgentFrontend::SharedTags::Attachment::PermissionType` definiert werden.

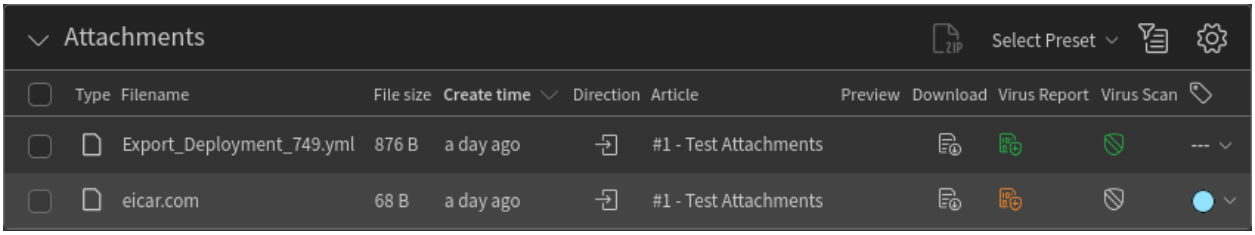

Abb. 2: Widget „Anhänge “

24.2 Anhangs-Tags als Ticket-Filter verwenden

Die Anhang-Tags können auch als Ticket-Filter verwendet werden. Sie funktionieren wie jeder andere Filter in einer Ticket-Liste. Wenn Sie den Filter verwenden, können Sie einen oder mehrere Anhangs-Tag-Namen auswählen (auf die Sie Zugriff haben).

Wenn ein Ticket mindestens einen Artikelanhang hat, der zu einem der ausgewählten Anhangstags gehört, wird dieses Ticket in der gefilterten Liste angezeigt.

KAPITEL 25

Taxonomie

25.1 Hintergrund

STORM bietet vordefinierte Felder für Enisa-, KRITIS- und TLP-Taxonomien und Ereignisklassifizierung.

- Enisa - *European Union Agency for Cybersecurity*
- KRITIS - *Kritische Infrastrukturen*
- TLP - *Traffic Light Protocol*

Neue dynamische Felder werden hinzugefügt, um Tickets mit standardisierten Informationen und Daten zu erweitern:

```
- EnisaSecurityIncidentClassification
- EventClassification
- KRITISSituationAssessment
- KRITISTaxonomy
- TLP
```

Bei einigen dieser dynamischen Felder handelt es sich um Dropdown-Felder, bei anderen um dynamische Felder vom Typ Web Service. Die dynamischen Felder sind als intern gekennzeichnet, können also nicht aus dem System gelöscht werden.

Um ihre Werte einfach aktualisieren zu können, verwenden einige dieser Felder intern Web Services, die standardmäßig eine Loop-Back-Anfrage an eine bestimmte statische Datei stellen, die auf dem lokalen System installiert ist. Die Web Services können so modifiziert werden, dass sie auf einen anderen Server verweisen, der eine aktualisierte Datei bereitstellt, die von Dritten gepflegt werden könnte.

STORM stellt nicht nur die dynamischen Felder bereit, sondern auch die zugrundeliegenden Web Services und die benötigten statischen Dateien, die die Quelle der Informationen für einige dieser dynamischen Felder sind. Die Web-Services verweisen auf den lokalen Server `localhost:8080` und die zugehörigen dynamischen Felder haben eine Standard-Caching-Konfiguration ihrer Werte für 1 Tag (86400 Sekunden) eingestellt.

Bitte stellen Sie sicher, dass die Konfiguration der Web Services mit dem OTRS-Webserver synchronisiert ist. Bei jeder Änderung muss der Cache mit dem OTRS-Konsolenbefehl `Maint::Cache::Delete` bereinigt werden.

Die statischen Dateien werden in `<OTRSHOME>/httpd/htdocs/STORM` gespeichert. Eine direkte Änderung der Datei ist nicht möglich. Zum Ändern müssen Sie die Datei kopieren und unter einem anderen Namen speichern. Die neue Datei kann dann angepasst werden. Bitte achten Sie darauf, den betroffenen Web-Service zu aktualisieren, damit er auf die richtige Datei verweist.

Bemerkung: Diese Funktion erfordert das Feature *Dynamic Field Web Service*.

Wenn die Standardeinstellungen für das aktuelle System nicht anwendbar sind, können sie in der Systemkonfiguration und/oder in den Web Service Management-Ansichten geändert werden.

25.2 Verwendung

Alle dynamischen Felder werden zur Aktion *Freie Felder ändern* der Ticketdetailansicht hinzugefügt.

Außerdem wird das TLP-Feld dem Widget *Eigenschaften* der Ticket-Detailansicht hinzugefügt und als Spalte in Ticket-Listen und Organizer-Elementen angezeigt. Das TLP-Feld wird für die Inline-Bearbeitung eingestellt, wenn es als Spalte angezeigt wird.

Die Einstellungen können so geändert werden, dass je nach Bedarf für ein bestimmtes System mehr oder weniger Felder angezeigt werden.

Siehe auch:

Die Taxonomien sind in der OTRS-Statistik verfügbar.

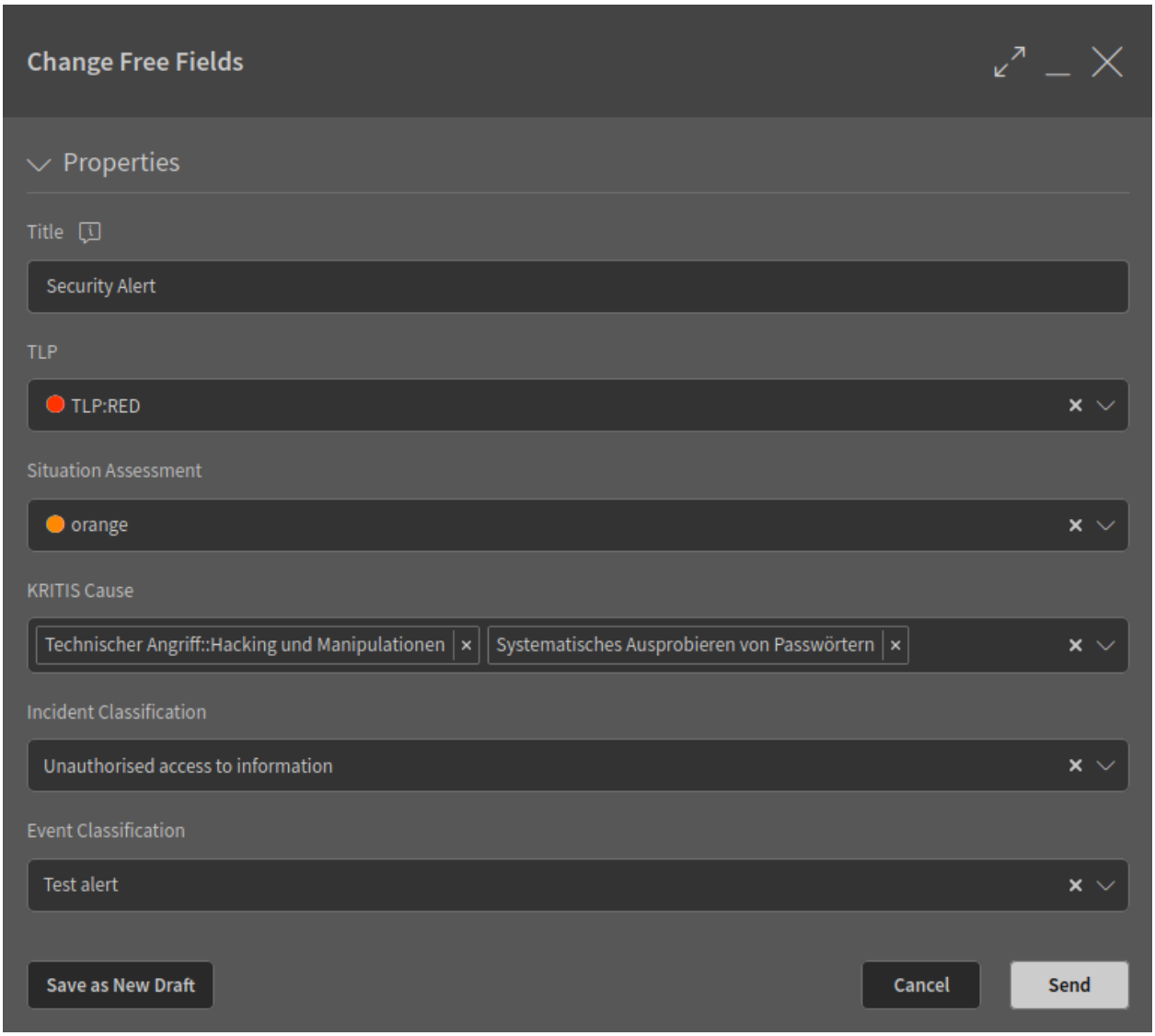

Abb. 1: Dynamische Felder bei der Aktion „Freie Felder ändern “

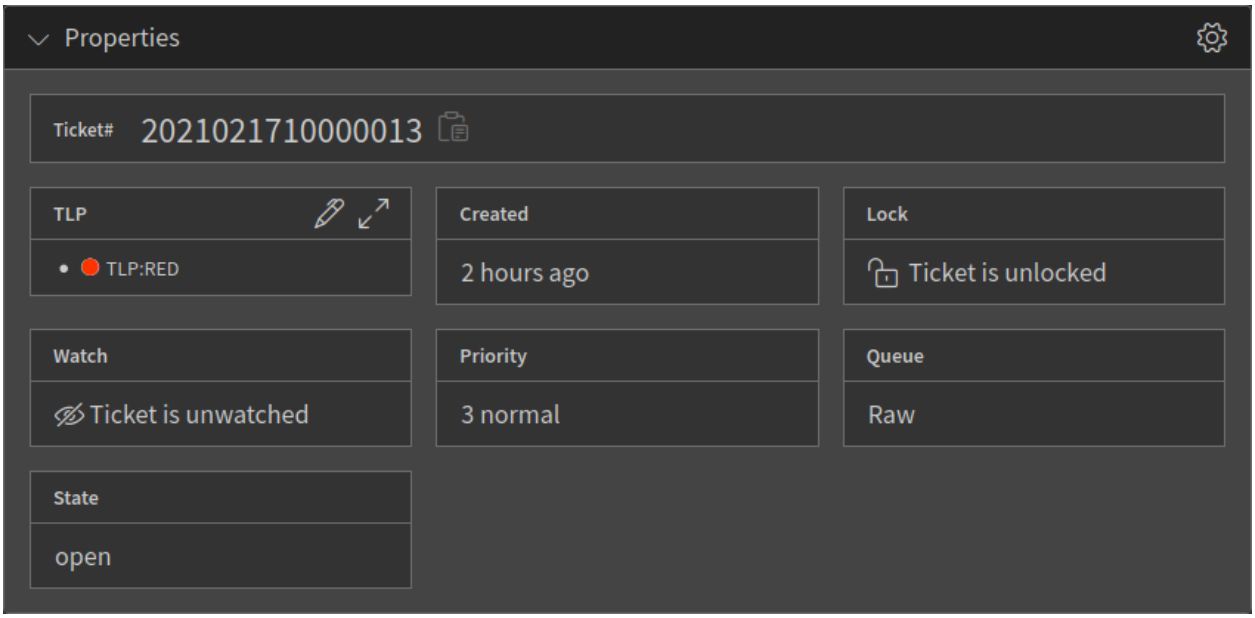

Abb. 2: Dynamisches TLP-Feld in den Ticket-Eigenschaften

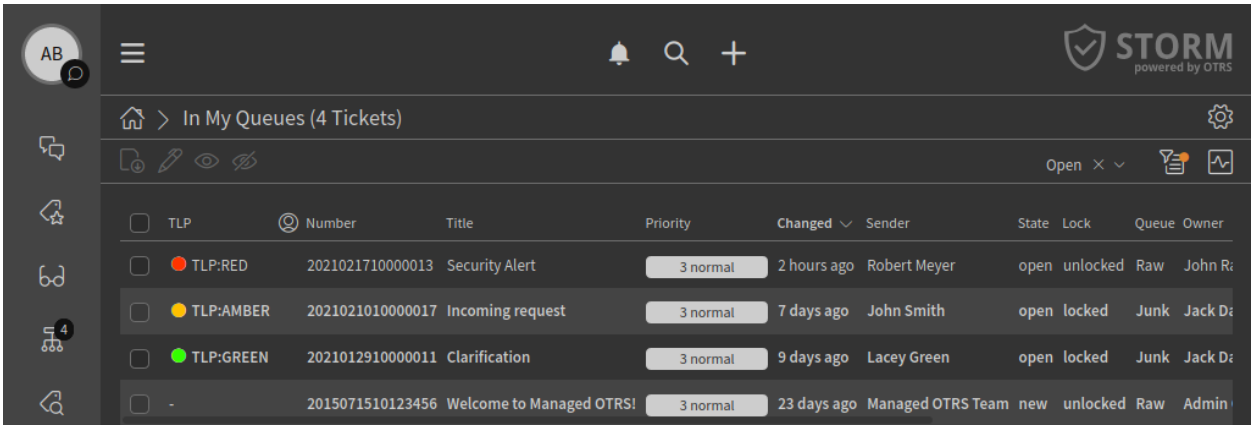

Abb. 3: Dynamisches TLP-Feld in der Ticket-Liste

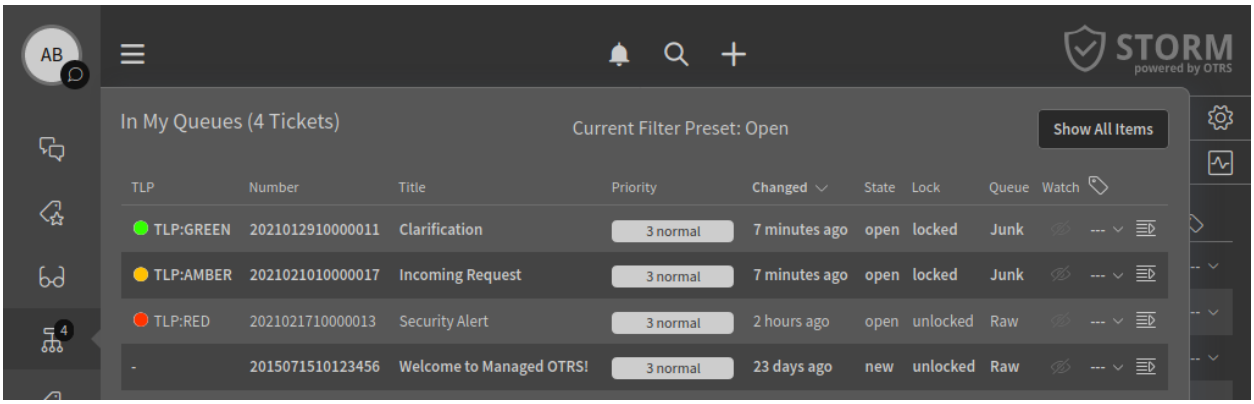

Abb. 4: Dynamisches TLP-Feld im Organizer-Element

KAPITEL 26

Prozesse

STORM verfügt über eingebaute Prozesse für die Sichtung von Ereignissen (Event Triage), die Behandlung von Incidents (Incident Handling) und die Bearbeitung von Aufgaben (Task Handling). Alle Prozesse sind standardmäßig ungültig und müssen erst von einem Administrator aktiviert werden. Jeder Prozess hat jedoch Abhängigkeiten wie ACLs, dynamische Felder, Abfragen, Ticket-Benachrichtigungen, Ticket-Typen, die aktiviert werden müssen, bevor der Prozess selbst aktiviert wird.

In diesem Kapitel wird erläutert, wie die Prozesse funktionieren.

26.1 Einrichtung

Die Prozesse können auf dem Bildschirm *Prozessverwaltung* der Administratoroberfläche aktiviert werden. Standardmäßig sind alle Prozesse *inaktiv*.

Zur Aktivierung des *Event Triage* Prozesses:

1. Gehen Sie im Administrator-Interface zum Modul *Queues*.
2. Setzen Sie die `Incidents`-Queue auf *gültig*.
3. Gehen Sie im Administrator-Interface zum Modul *Dynamische Felder*.
4. Setzen Sie die folgenden dynamischen Felder auf *gültig*.
   - `Ereignis-Klassifizierung`
   - `IncidentTicket`
   - `ProcessHelper`
5. Gehen Sie zum Modul *Access Control Lists (ACL)* des Administrator-Interface.
6. Setzen Sie die folgenden ACLs auf *gültig*.
   - `Event 001 - Forbid Actions`
   - `Event 001 - Forbid ActionsLimit DF Event Classification`

7. Alle ACLs in Betrieb nehmen.
8. Gehen Sie im Administrator-Interface zur Ansicht *Prozessverwaltung*.
9. Setzen Sie den Prozess `Event Triage` auf *gültig*.
10. Nehmen Sie alle Prozesse in Betrieb.

Zur Aktivierung des *Incident Handling* Prozesses:

1. Gehen Sie im Administrator-Interface zum Modul *Typen*.
2. Setzen Sie die folgenden Typen auf *gültig*.
   - `Ereignis`
   - `Incident`
   - `Aufgabe`
3. Gehen Sie im Administrator-Interface zum Modul *Dynamische Felder*.
4. Setzen Sie die folgenden dynamischen Felder auf *gültig*.
   - `Analyseergebnis`
   - `EnisaSecurityIncidentClassification`
   - `ISO`
   - `KRITISSituationAssessment`
   - `KRITISTaxonomie`
   - `LessonsLearned`
   - `ProcessHelper`
   - `RemediationAdvice`
   - `SendAdvice`
   - `TaskBody`
   - `TaskName`
   - `TaskRecipient`
   - `TaskResult`
   - `TaskSubject`
   - `TechContact`
   - `TLP`
5. Gehen Sie im Administrator-Interface zur Ansicht *Ticket-Benachrichtigungen*.
6. Setzen Sie die folgenden Ticket-Benachrichtigungen auf *gültig*.
   - `Incident: Hinweise zur Schadensbegrenzung und -beseitigung senden - TLP Amber`
   - `Incident: Mitigation & Remediation Advice senden - TLP Amber`
   - `Incident: Mitigation & Remediation Advice senden - TLP Red`
   - `Incident: Mitigation & Remediation Advice senden - TLP White`
7. Gehen Sie zum Modul *Access Control Lists (ACL)* des Administrator-Interface.

8. Setzen Sie die folgenden ACLs auf *gültig*.
   - `Incident 001 - Hide Actions and Dialogues`
   - ``Incident 002a - Nächste Schaltfläche in Analysephase Schritt 1 anzeigen ``
   - ``Incident 002b - Nächste Schaltfläche in Analysephase Schritt 2 anzeigen ``
   - ``Incident 003a - Nächste Schaltfläche in Mitigation-Phase Schritt 1 anzeigen ``
   - ``Incident 003b - Nächste Schaltfläche in Mitigation-Phase Schritt 2 anzeigen ``
   - ``Incident 004 - Schließen-Button anzeigen ``
   - ``Incident 005 - Kritis-Taxonomie ausblenden ``
   - ``Incident 005 - Kritis-Taxonomie anzeigen ``
9. Alle ACLs in Betrieb nehmen.
10. Gehen Sie im Administrator-Interface zur Ansicht *Prozessverwaltung*.
11. Setzen Sie den Prozess `Incident Handling` auf *gültig*.
12. Nehmen Sie alle Prozesse in Betrieb.

Zur Aktivierung des *Task Handling* Prozesses:

1. Gehen Sie im Administrator-Interface zum Modul *Typen*.
2. Setzen Sie die folgenden Typen auf *gültig*.
   - `Incident`
3. Gehen Sie im Administrator-Interface zum Modul *Dynamische Felder*.
4. Setzen Sie die folgenden dynamischen Felder auf *gültig*.
   - `TaskName`
   - `TaskResult`
5. Gehen Sie zum Modul *Access Control Lists (ACL)* des Administrator-Interface.
6. Setzen Sie die folgenden ACLs auf *gültig*.
   - `Task 001 - Aktionen ausblenden`
7. Alle ACLs in Betrieb nehmen.
8. Gehen Sie im Administrator-Interface zur Ansicht *Prozessverwaltung*.
9. Setzen Sie den Prozess `Task Handling` auf *gültig*.
10. Nehmen Sie alle Prozesse in Betrieb.

26.1.1 Konsolenbefehl

Es gibt einen Konsolenbefehl zum Auflisten, Aktivieren und Deaktivieren der Prozessgruppen. Führen Sie den Befehl mit der Option `--help` aus, um detaillierte Anweisungen zur Funktionsweise zu erhalten.

```
$ bin/otrs.Console.pl Maint::STORM::ProcessGroups::Toggle --help

Enable/Disable a process group and its dependencies

Usage:
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
 otrs.Console.pl Maint::STORM::ProcessGroups::Toggle [--name ...] [--list] [--enable]␣
↪[--disable]

Options:
 [--name ...]                   - Name of the process group (all if omitted).
 [--list]                       - List all process groups.
 [--enable]                     - Enable the process group.
 [--disable]                    - Disable the process group.
 [--help]                       - Display help for this command.
 [--no-ansi]                    - Do not perform ANSI terminal output coloring.
 [--quiet]                      - Suppress informative output, only retain error␣
↪messages.
```

26.2 Verwendung

Wir haben die Prozesse auf der Grundlage bewährter Verfahren entwickelt. Wir wissen aber auch, dass jeder Kunde andere Arbeitsabläufe hat. Daher kann es sein, dass die Prozesse angepasst werden müssen, bevor sie in der Produktion eingesetzt werden können. Bitte wenden Sie sich an unsere Experten, bevor Sie einen Prozess aktivieren.

Die allgemeine Verwendung von Prozessen wird im *Administratorhandbuch* erläutert. Für eine detaillierte Nutzung des obigen Prozesses wenden Sie sich bitte an das *Customer Solutions Team*.

KAPITEL 27

Offline-Registrierung

Diese Funktion wird durch ein zusätzliches Paket bereitgestellt. Es ermöglicht die Registrierung des Systems in einer Offline-Umgebung.

Bemerkung: Dieses Paket ist nicht Teil der Standardinstallation von STORM. Wenden Sie sich an die OTRS-Gruppe, um einen speziellen Vertrag zur Nutzung dieses Features zu erhalten.

Die folgenden Systemkonfigurationseinstellungen müssen aktiviert und richtig eingestellt sein:

- `SMIME`
- `SMIME::Bin`
- `SMIME::CertPath`
- `SMIME::PrivatePath`

Für die Offline-Registrierung wird eine von der OTRS-Gruppe bereitgestellte Registrierungsschlüsseldatei benötigt.

27.1 Verwendung

Die Offline-Registrierung kann entweder über die Administratorschnittstelle im Browser oder durch Ausführen eines Befehls im Terminal erfolgen.

So registrieren Sie das System über die Administratorschnittstelle:

1. Gehen Sie im Administrator-Interface zur Ansicht *Systemregistrierung*.
2. Laden Sie die von der OTRS-Gruppe bereitgestellte Registrierungsschlüsseldatei hoch.
3. Klicken Sie auf die Schaltfläche *Registrieren*, um den Registrierungsvorgang abzuschließen.

So registrieren Sie das System über die Befehlszeile:

1. Speichern Sie die von der OTRS Gruppe bereitgestellte Registrierungsschlüsseldatei irgendwo im System, wo der ``otrs `` -Benutzer Lesezugriff hat.
2. Öffnen Sie als `` otrs `` -Benutzer das Terminal und navigieren Sie zum Home-Ordner von STORM.
3. Führen Sie den folgenden Befehl aus:

```
otrs> bin/otrs.Console.pl Admin::OfflineRegistration::LoadKey --key-path PATH_TO_
↪KEY_FILE
```

Der Registrierungsschlüsseldatei ist ein Vertrag beigefügt. Dieser Vertrag kann ein Verfallsdatum enthalten. Einige Tage vor Ablauf des Vertrages zeigt das System Warnmeldungen an (gleicher Mechanismus wie bei einer Online-Registrierung). Um das System weiterhin ohne Unterbrechung nutzen zu können, ist es notwendig, die OTRS-Gruppe zu kontaktieren, um den Vertrag zu erneuern und einen neuen Registrierungsschlüssel zu erhalten.

Jeder neue Registrierungsschlüssel kann jederzeit innerhalb der aktuellen Vertragslaufzeit mit einer der oben beschriebenen Methoden in das System geladen werden.

Bemerkung: Wenn ein Vertrag abgelaufen ist, wird die grafische Benutzeroberfläche von STORM eingeschränkt und kann nicht mehr verwendet werden. In diesem Fall muss die Kommandozeilenmethode verwendet werden, um die neue Registrierungsschlüsseldatei zu laden und den Vertrag zu erneuern.