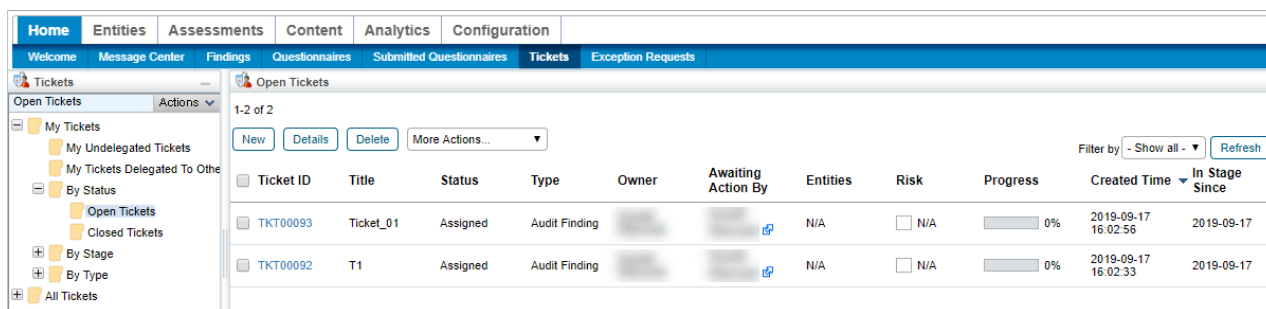


Understanding Ticket Flow

Tickets are used to track efforts to review, analyze, and deploy remediation and prevention steps associated with specific vulnerability instances. The **Tickets** section of a vulnerability lists the tickets associated with the instance.

Tickets have an associated workflow. Vulnerability resolution tickets are related to their vulnerability instance. The status of the ticket corresponds to the current stage of the workflow. The workflow and its stages can be customized to suit specific requirements, but typical ticket workflow stages include:

- New
- In Progress
- Review
- Closed
- Closed via Exception



Ticket ID	Title	Status	Type	Owner	Awaiting Action By	Entities	Risk	Progress	Created Time	In Stage Since
TKT00093	Ticket_01	Assigned	Audit Finding			N/A	N/A	0%	2019-09-17 16:02:56	2019-09-17
TKT00092	T1	Assigned	Audit Finding			N/A	N/A	0%	2019-09-17 16:02:33	2019-09-17

The Tickets page.

The disposition field affects the workflow while editing a ticket. Set the disposition to **Escalate** or **Exception** or customize the set of disposition choices.

Ticket updates can change the ticket disposition. You can also select a disposition that will not generate escalations. However, changing the ticket disposition does not automatically close the ticket or prevent a closed ticket from being reopened.

Tickets also have an **Exception Expiration** field. If you specify a date in this field, the system will send an email to ticket stakeholders when the ticket is overdue. The email template used for this notification is specified in the property `ticket.exception.expired.notification.template`.

Ticket escalation templates can be specified by priority using the system property: `com.agilance.ticket.escalation.template` with a value such as "high, Default Ticket Escalation Template; medium, Default Ticket Escalation Template".

Relevant system properties include:

- `vulnerability.status.exception`: Names the exception status for all vulnerabilities; and
- `vulnerability.status.cannot.override`: Names the exception status that cannot be further modified by a scanner or other source reporting the same vulnerability instance again.

Vulnerability: CVE-1999-0594

Tickets

1-1 of 1

Details More Actions... Filter by - Show all - Refresh

<input type="checkbox"/>	Ticket ID	Title	Status	Type	Owner	Entities	Risk	Progress	Description	Created Time
<input type="checkbox"/>	TKT00040	CVE-1999-0594	New	Vulnerability Resolution		2	High	0%	N/A	2016-02-25

The Tickets tab of a vulnerability.

Tickets are associated with a vulnerability instance. Ticket email templates can contain the vulnerability title and description. To append vulnerability information in the notification that you send to stakeholders, use the object `getAttachmentVulnerabilities()` to specify the following html code in the email template.

```
#set($vulnerabilities= $ticket.getAttachedVulnerabilities())
#foreach($v in $vulnerabilities)
Vulnerabilities: $v.getCaption()
#end
$ticket.getAttachedVulnerabilities()
```