# STRY0022334 - Asset Mgmt-Dc0512 Audit. Automation to create ServiceNow tickets to manage Unknown asset process.

Request Details (original):

We need a new ticket on the service request screen called Unknown Asset that will be limited to IT partners. We need workflow around this as there will be tasks necessary. Assets with no hardware inventory scan (and for future, no heartbeat), the asset moves to Unknown status.

As assets (CIs) are moved to Unknown status, we need tickets to be automatically created for the unknown assets. Individual tasks to be used are: Verify, Return, Receive, Update. The ticket assignment should be based on the location of the asset, which can be determined by the machine name.

If the ticket is not resolved within 60 days of original Unknown ticket due date, the ticket should automatically escalate to the manager of the assignment group. The support group manager will then be required to determine if the asset is truly unknown and all methods have been used to locate the asset. Once determined the DAM team will move the asset to 'Lost Internal' status. If the asset comes back on the wire with a scan, it should move back to In Service, with a report that identifies this change.

Solution:

~~Create a daily batch job to query for CI’s that went to Unknown on the previous day. For each CI found by the query, create a ServiceNow Incident with four Incident Tasks.~~

Create a business rule that will execute when the Status of the CI changes to ‘Unknown’. The business rule will create a new Incident with four Incident Tasks.

The Incident will be assigned based on location information derived from fields on the CI record in ServiceNow (*Deployed to User* and *Last discovered user)*. If no location information can be derived from the CI, the assignment will default to an assignment group specified in a ServiceNow system property (initially to be set to ‘Desktop Asset Management’). The Priority of the Incidents will be set to Medium with the exception of the scenario were the lost device has an unencrypted drive – which poses risk to the bank.

Four Incident Tasks will be created for each Incident created. The summaries of the four tasks will be “Verify”, “Receive”, “Return” and “Update Status”. The assignment groups for these tasks will be the same as the parent INC – except for the “Update Status” task which will always be assigned to the group specified in a ServiceNow system property (initially to be set to ‘Desktop Asset Management’).

Current standard Incident escalation process will apply to these INCs. Escalation emails are sent to assignment group managers when tickets remain unassigned to indviduals.

< more detail needed here to describe escalation and SLA >

Technical details

**~~QUERY~~**

~~Query cmdb\_ci\_computer where:~~

~~Class (sys\_class\_name) = cmdb\_ci\_computer or “Computer” Which is it? And~~

~~Sub class (u\_sub\_class) != “Virtual” and~~

~~Status (install\_status) = Unknown (7) and~~

~~Status hist unknown date (u\_stat\_hist\_unknown\_date) = yesterday~~

**NEW BUSINESS RULE on table cmdb\_ci\_computer**

**Business Rule Condition**: Execute when Status (install\_status) changes to Unknown (7)

* Sub class (u\_sub\_class) != “Virtual” and

**Business Rule Script:**

Create a new INC with the following fields populated:

**Requestor** (u\_user\_id) = “SN JOB (system-job)”

**Short Description (**short\_description): “ Unknown Desktop Asset detected”

**Status** (incident\_state): Assigned (1)

**Assignment Group** (assignment\_group): create a function to assign. See function requirements below.

**Operational Tier 1** (u\_op\_tier\_1)**: “**Malfunction”

**Operational Tier 2** (u\_op\_tier\_2): **“**Data Issue”

**Product tier 1** (u\_product\_tier\_1)**: “**Hardware”

**Product tier 2** (u\_product\_tier\_2)**: “**u\_sub\_class”

**Product tier 3** (u\_product\_tier\_3)**: “**Unknown Process”

**Product Name** (u\_product\_name)**: “**Unknown Process”

**Affected CI** (u\_requester\_ci) **:** sys\_id

**Affected CI override** (u\_asset\_override): true

**Single Service Outage** (u\_impindpartner): true

**High Deadline Risk (**u\_urg\_hideadlinerisk): true -> If u\_encryption\_state != “Protection On”

**Medium Deadline Risk** (u\_urg\_meddeadlinerisk): true -> If u\_encryption\_state == “Protection On”

**Details** (u\_details):

Unknown Device Details:

Class: (u\_class)

Sub-class: (u\_sub\_class)

Name: (name)

Serial Number: (serial\_number)

Two Letter Functional Extention: (u\_2\_letter\_functional\_extensio)

Deployed to: (u\_deployed\_to)

Deployed to cable box: (u\_cable\_box)

Discover User: (u\_discovered\_user)

Discovered User string: (u\_discovered\_user\_string)

IP Address: (ip\_address)

Encryption state: (u\_encryption\_state)

Encryption state date: (u\_encryption\_state\_date)

Create 4 Incident Tasks:

For each Incident created, create 4 child Incident Tasks (u\_incident\_task) with the following field assignments:

**Requestor** (u\_user\_id) = “SN JOB (system-job)” (current user for batch jobs)

**Short Description (**short\_description):

* Verify
* Return
* Receive
* Update Status

**Status** (incident\_state): Assigned (1)

**Assignment Group** (assignment\_group):

* Verify – Same as parent INC
* Return – Same as parent INC
* Receive – Same as parent INC
* Update Status – Group specified in system property **ntrs.unknown.default.group**

**Operational Tier 1** (u\_op\_tier\_1)**: “**Malfunction”

**Operational Tier 2** (u\_op\_tier\_2): **“**Data Issue”

**Product tier 1** (u\_product\_tier\_1)**: “**Hardware”

**Product tier 2** (u\_product\_tier\_2)**: “**u\_sub\_class”

**Product tier 3** (u\_product\_tier\_3)**: “**Unknown Process”

**Product Name** (u\_product\_name)**: “**Unknown Process”

**Affected CI** (u\_requester\_ci) **:** sys\_id

**Priority (**u\_priority) -> If u\_encryption\_state != “Protection On” then ‘2 – High’ (20) else ‘3 – Medium’ (30)

**Details** (u\_details):

Unknown Device Details:

Class: (u\_class)

Sub-class: (u\_sub\_class)

Name: (name)

Serial Number: (serial\_number)

Two Letter Functional Extention: (u\_2\_letter\_functional\_extensio)

Deployed to: (u\_deployed\_to)

Deployed to cable box: (u\_cable\_box)

Discover User: (u\_discovered\_user)

Discovered User string: (u\_discovered\_user\_string)

IP Address: (ip\_address)

Encryption state: (u\_encryption\_state)

Encryption state date: (u\_encryption\_state\_date)

**Assignment Group Function:**

This function will return the proper assignment group based on the location of a user determined from the CI. There are 2 different fields on the CI that reference sys\_user – **Deployed To (**u\_deployed\_to) and **Discovered User** (u\_discovered\_user). You need to pull location information from sys\_user table. Check the Deployed to user first. If there is no value specified for Deployed to then get the location for Discovered user. If neither of the user fields have a value, assignment group cannot be determined from a sys\_user record. It will need to be defaulted to the group specified in system property **ntrs.unknown.default.group**:

// determine location bundle (aka region)

var LocationBundle

If (u\_deployed\_to != “”) {

LocationBundle = u\_deployed\_to.location.u\_region

} else if(u\_discovered\_user != “”) {

LocationBundle = u\_discovered\_user.location.u\_region

} else {

LocationBundle = “unknown”;

}

// determine assignment group for the location bundle

If LocationBUndle = “unknown” then return the value found in property ntrs.unknonw.default.group

// determine assignment from the assignment routing table.

Query table u\_assignment\_routing where:

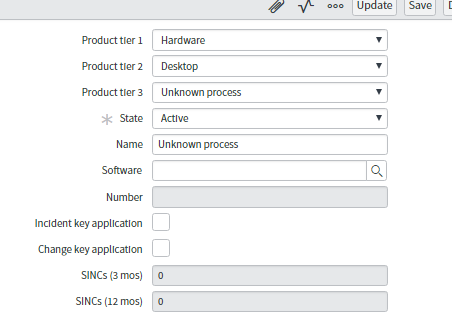
U\_region = LocationBundle and

U\_product = “Unknown Process”

If the query returns a record from the Assignment Routing table, return u\_assignment\_group

Else return the value found in property ntrs.unknonw.default.group

Configuration:

1. New property to drive default Unknown INC assignment – **ntrs.unknown.default.group**
2. New Entry in Product table (cmdb\_ci\_model)
3. 
4. New entries in Assignment Routing table for Hardware/Desktop/Unknown, Hardware/Laptop/Unknown and Hardware/Tablet/Unknown x One per location bundle (18) = 54 new records - groups TBD. ???? would we every distinguish routing by Laptop vs. tablet vs. desktop? Maybe we don’t need 54? Maybe just one per location bundle (18) ?