ServiceNow

Integration Guide

Notices

Contents

Overview

Digital transformation across healthcare, manufacturing, retail, transportation, and logistics is accelerating the hyper-connectedness of enterprise systems powered by IoT and connected OT devices. The enterprise IT network is now the melting pot for a highly eclectic mix of devices that businesses must manage and protect or face immediate security risk, bad-actors are constantly attacking the long-held belief and sovereignty of application data, critical to the running of most Healthcare and Enterprise businesses.

The Ordr Systems Control Engine (SCE) allows organizations to rapidly inventory every wired or wireless connected device in your network, classify it based on the type and business function, and assess it for risk. Furthermore, SCE provides for endpoint security monitoring and enforcement without the need for running agents on end devices. SCE learns behaviors and creates device flow genomes, so you'll know what each device or group of devices should be talking to, and often more importantly what they should not be talking to.

Ordr SCE can be integrated with many widely used Enterprise software products for a better andcomplete user experience. This guide describes in detail how to configure Ordr Systems Control Engine (SCE) with ServiceNow CMDB to provideadvanced Endpoint device discovery, classification, and ultimately building the foundation for the automation of secure network access control and micro-segmentation policy to all networked users and devices.

ServiceNow is a service management platform that offers advanced automation and process workflow for the enterprise. You will be able to leverage ServiceNow's workflow and ticketing capabilities with this integration.

In some cases, customers might already be using ServiceNow for Asset management and Ticketing system. Ordr provides a way to integrate with ServiceNow for customers to see all their assets in one place and automate the ticketing process for any vulnerabilities found by the Ordr SCE platform.

Through automated alerts, ticketing, problem-solving, and validation, the integration of Ordr SCE and ServiceNow enables closed-loop incident management. Ordr SCE can push inventory and incident information to ServiceNow.

When Ordr SCE finds threats or risks within the network, it sends an alert in the form of incidents/events to ServiceNow. ServiceNow creates a ticket and provides the user the option to fix the problem automatically/manually. ServiceNow validates the resolution is successful and closes the ticket.

Integration Workflow

This section provides step-by-step instructions on how to integrate ServiceNow with the Ordr SCE application:

Step 1. Import XML Schema into ServiceNow

Step 2. Preview update set and resolve any conflicts

Step 3. Create a new user at ServiceNow

Step 4. Ordr ServiceNow Configuration

Step 5. Ordr Discovered Equipments Verification

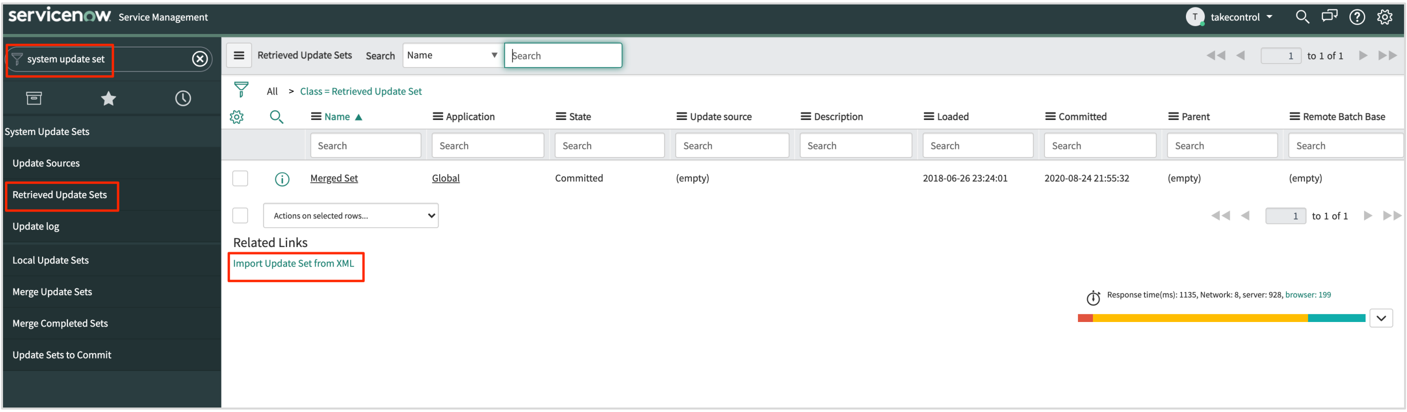
Step 1. Import XML Schema into ServiceNow

As part of the integration between Ordr SCE and SNOW CMDB, Ordr has developed an XML file that is used to ensure data sent from the SCE platform can be ingested and parsed correctly. It is important that before you begin to configure the integration between the two platforms, this file is imported as described below to ensure data consistency.

To get started with the ServiceNow integration, contact the Ordr support team to obtain the XML file for importing into ServiceNow, else the latest file should be available in the following location on our resources website. Use this link to download the XML file. <Click here for XML Import Schema file>

Ensure to save the XML file to a local location and computer you will use to log in to ServiceNow.

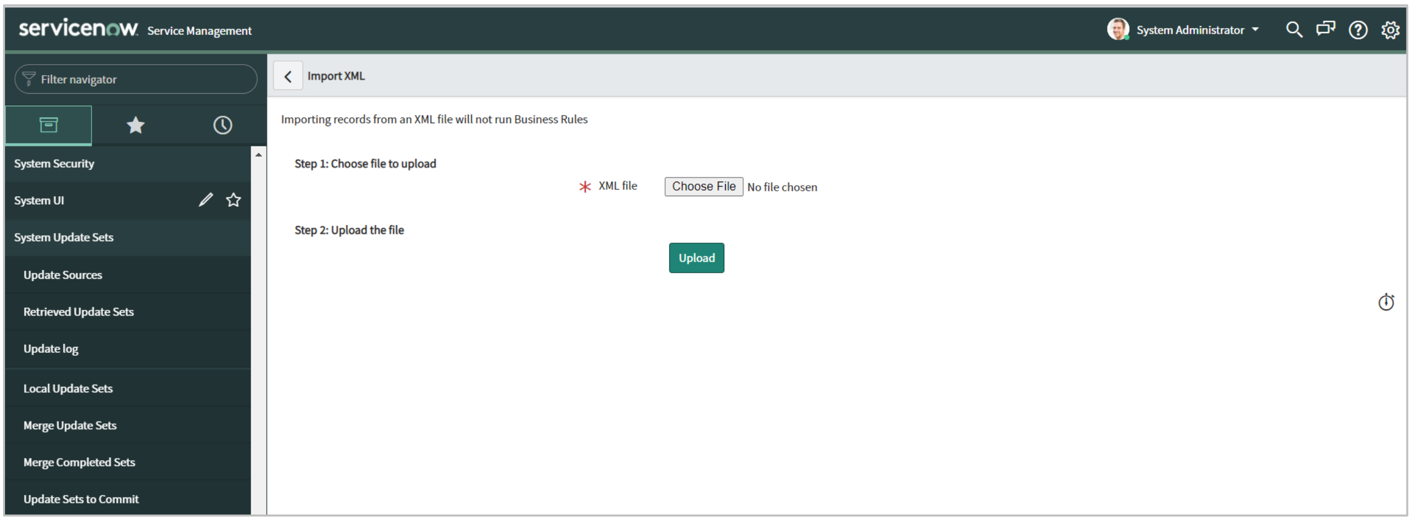
1. Log in to ServiceNow with your user credentials.
2. Within the ServiceNow homepage search for **System Update Sets**, click on **Retrieved Update Sets**, and then click **Import Update Set from XML**.



Name ▲	Application	State	Update source	Description	Loaded	Committed	Parent	Remote Batch Base
Merged Set	Global	Committed	(empty)		2018-06-26 23:24:01	2020-08-24 21:55:32	(empty)	(empty)

Response time(ms): 1135, Network: 8, server: 928, browser: 199

3. Click **Choose File** to upload the XML file that was saved in the initial step or received from the Ordr support team member.
4. Click **Upload** as shown below.



Importing records from an XML file will not run Business Rules

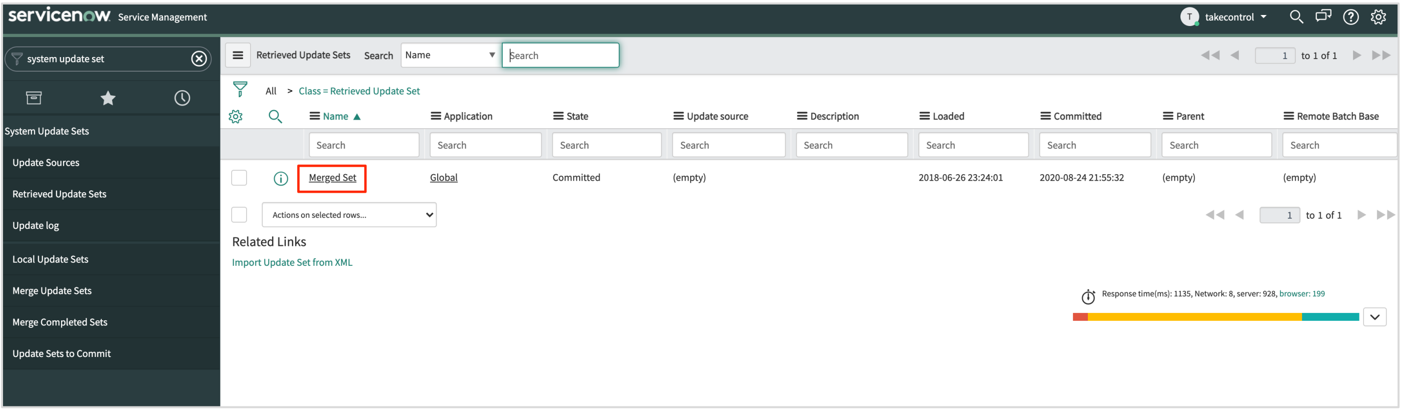
Step 1: Choose file to upload

* XML file Choose File No file chosen

Step 2: Upload the file

Upload

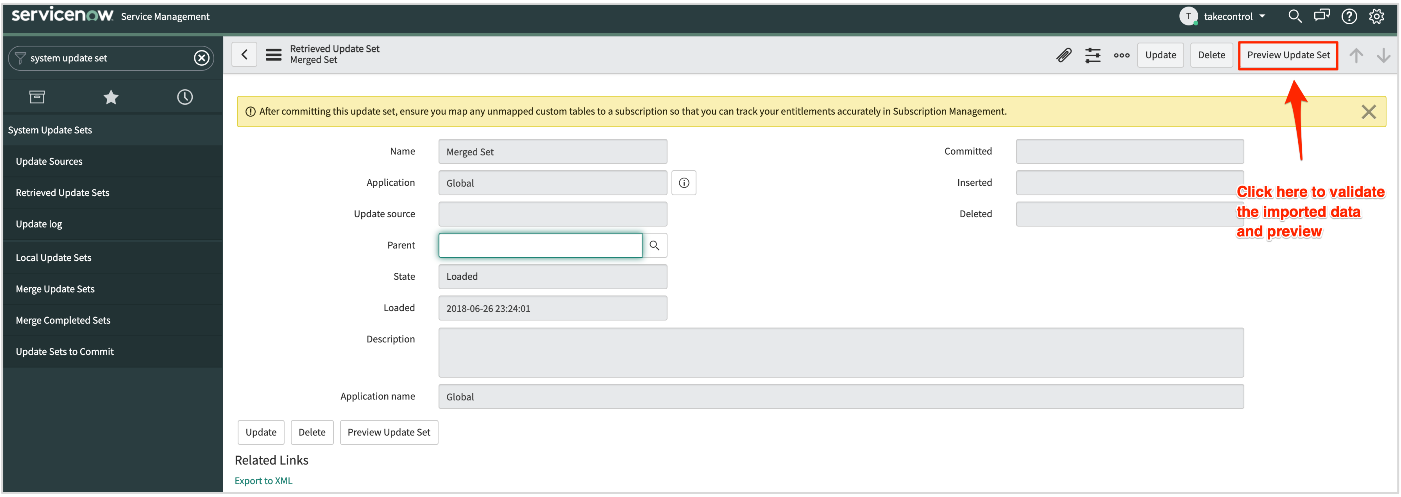
When the upload is complete, the Retrieved Update Sets screen displays a new entry '***Merged Set***'. Notice the state is set currently as **Loaded**, after the merge is completed it will show as **Committed**.



Name	Application	State	Update source	Description	Loaded	Committed	Parent	Remote Batch Base
Merged Set	Global	Committed	(empty)		2018-06-26 23:24:01	2020-08-24 21:55:32	(empty)	(empty)

Step 2. Preview update set and resolve any conflicts

1. Click the **Merged Set** entry.
2. To validate and preview the imported data, click **Preview Update Set**.



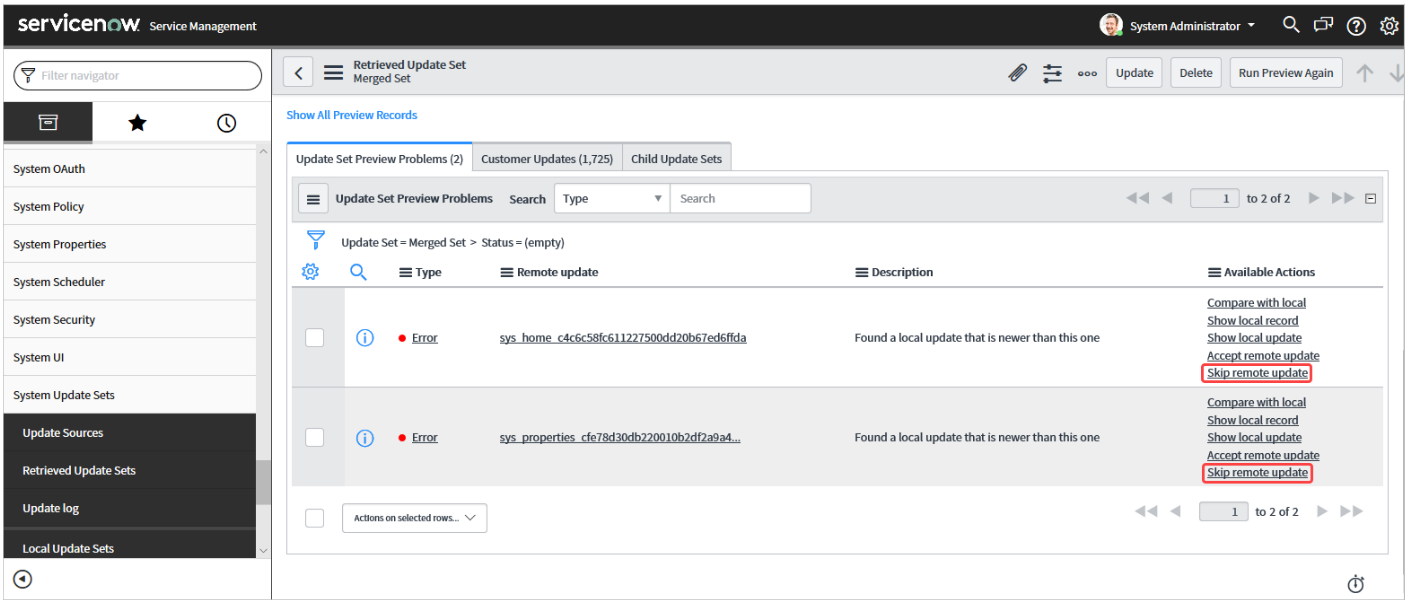
After committing this update set, ensure you map any unmapped custom tables to a subscription so that you can track your entitlements accurately in Subscription Management.

Name	Merged Set	Committed	
Application	Global	Inserted	
Update source		Deleted	
Parent			
State	Loaded		
Loaded	2018-06-26 23:24:01		
Description			
Application name	Global		

Click here to validate the imported data and preview

Once the analysis is complete, it may present you with a list of errors to validate, ignore, etc. Similar to the example below.

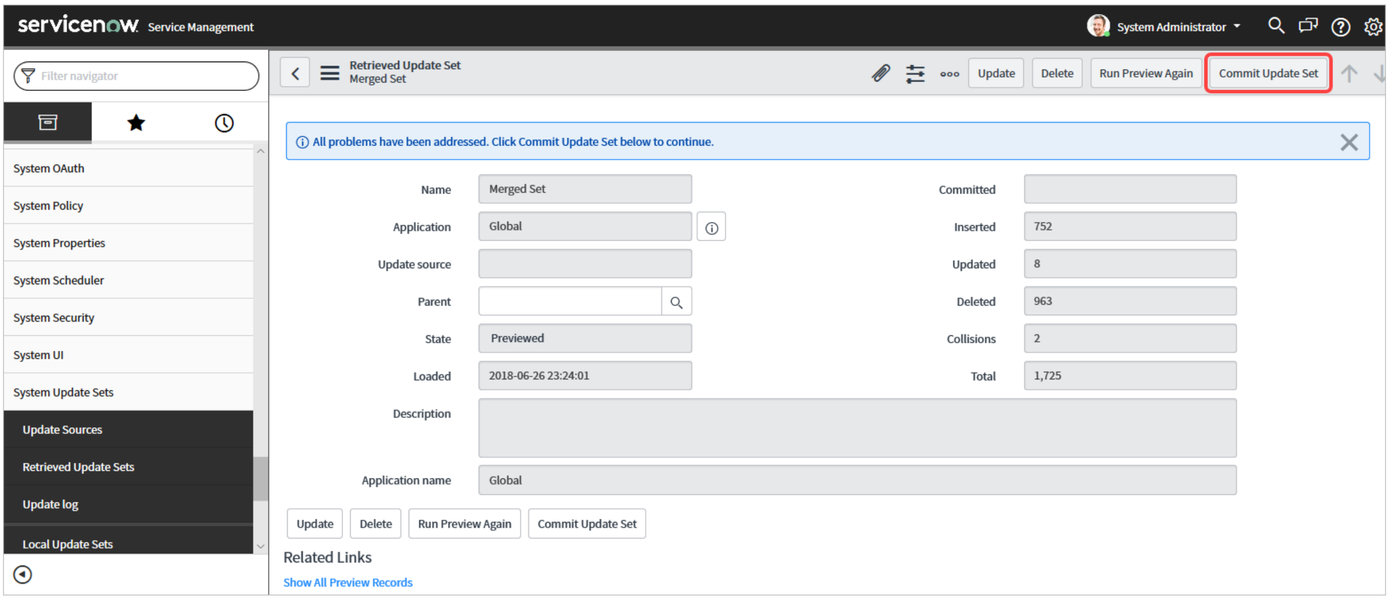
3. While validating the merged set, if the preview displays error messages, click **Skip remote update**. There will likely be two warnings as shown below.



Update Set = Merged Set > Status = (empty)

Type	Remote update	Description	Available Actions
Error	sys_home_c4c6c58fc611227500dd20b67ed6ffda	Found a local update that is newer than this one	Compare with local Show local record Show local update Accept remote update Skip remote update
Error	sys_properties_cfe78d30db220010b2df2a9a4...	Found a local update that is newer than this one	Compare with local Show local record Show local update Accept remote update Skip remote update

4. Once the warnings have been skipped, update the changes by clicking **Commit Update Set**.



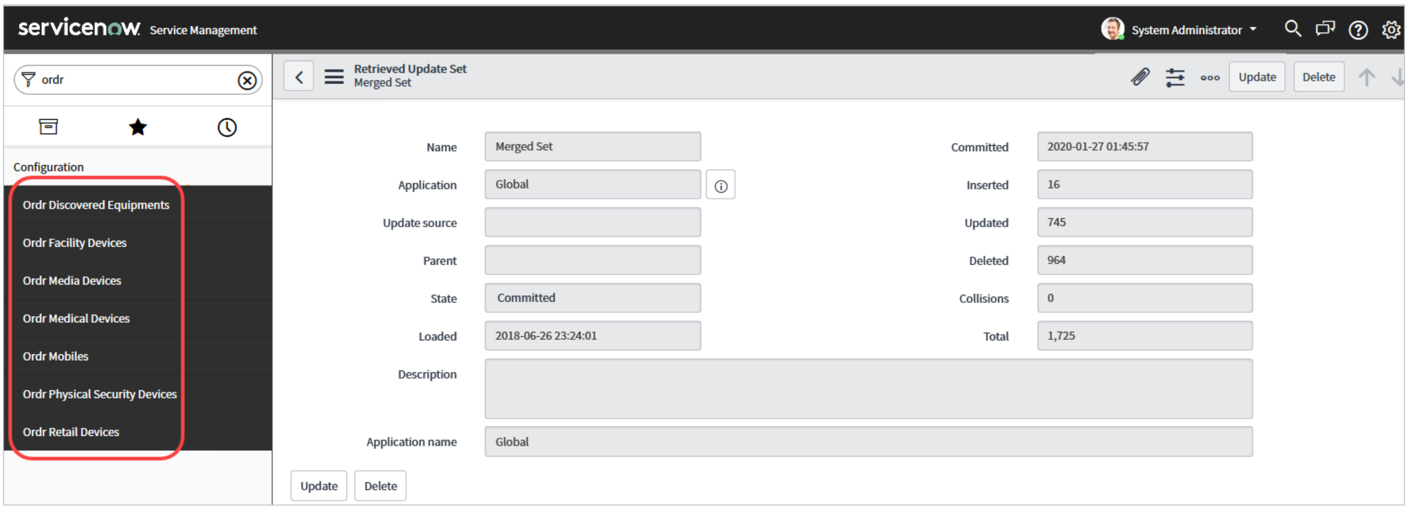
All problems have been addressed. Click Commit Update Set below to continue.

Name	Merged Set	Committed	
Application	Global	Inserted	752
Update source		Updated	8
Parent		Deleted	963
State	Previewed	Collisions	2
Loaded	2018-06-26 23:24:01	Total	1,725
Description			
Application name	Global		

5. In the ServiceNow homepage, search ‘**Ordr**’ and verify the following Configuration Items {CI’s} entries are created:

- Ordr Discovered Equipments
- Ordr Facility Devices
- Ordr Media Devices
- Ordr Medical Devices
- Ordr Mobiles
- Ordr Physical Security Devices
- Ordr Retails Devices

NOTE: ‘*Ordr Discovered Equipments*’ is the parent table and tables below its child.



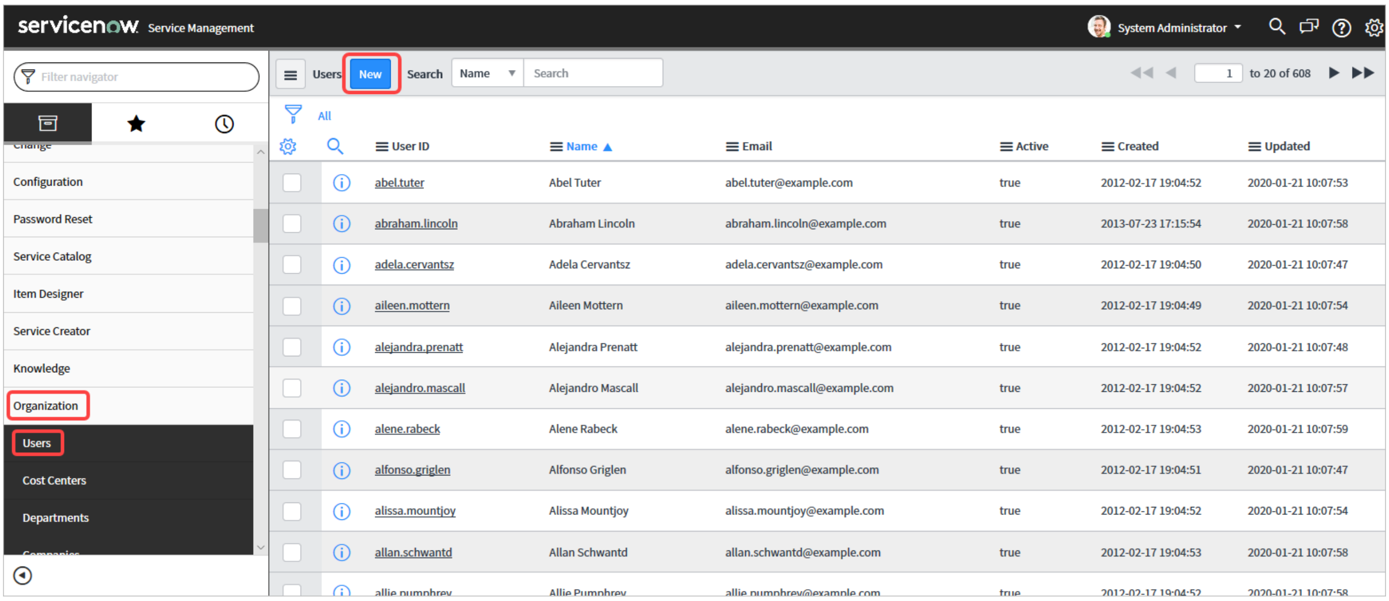
Name	Merged Set	Committed	2020-01-27 01:45:57
Application	Global	Inserted	16
Update source		Updated	745
Parent		Deleted	964
State	Committed	Collisions	0
Loaded	2018-06-26 23:24:01	Total	1,725
Description			
Application name	Global		

6. Click individual entries and make sure that there are no data sets.

Step 3. Create a new user at ServiceNow

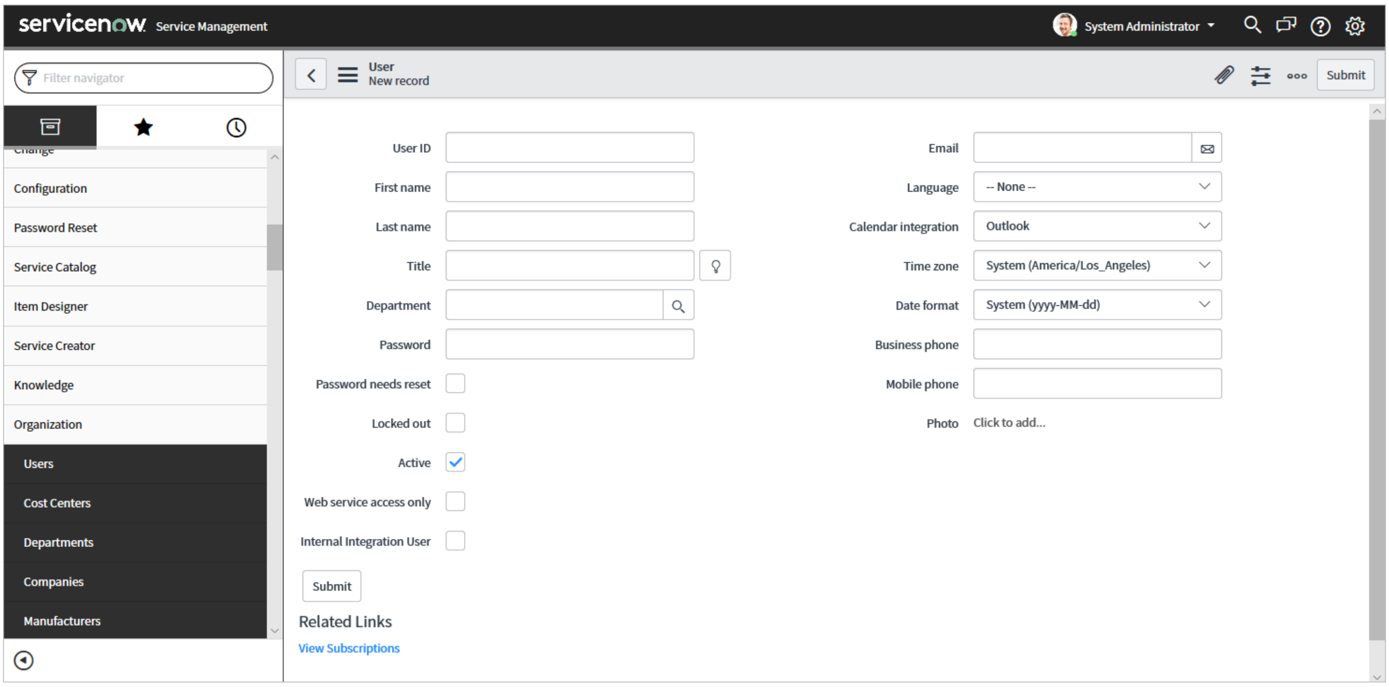
Create a user in the Ordr SCE platform to communicate with the ServiceNow platform. The user is used to call the ServiceNow REST APIs to push data from the Ordr SCE platform.

1. On the ServiceNow home page, go to **Organization** > **Users** and then click **New**.



User ID	Name ▲	Email	Active	Created	Updated
abel.tuter	Abel Tuter	abel.tuter@example.com	true	2012-02-17 19:04:52	2020-01-21 10:07:53
abraham.lincoln	Abraham Lincoln	abraham.lincoln@example.com	true	2013-07-23 17:15:54	2020-01-21 10:07:58
adela.cervantsz	Adela Cervantsz	adela.cervantsz@example.com	true	2012-02-17 19:04:50	2020-01-21 10:07:47
aileen.mottern	Aileen Mottern	aileen.mottern@example.com	true	2012-02-17 19:04:49	2020-01-21 10:07:54
alejandra.prenatt	Alejandra Prenatt	alejandra.prenatt@example.com	true	2012-02-17 19:04:52	2020-01-21 10:07:48
alejandro.mascall	Alejandro Mascall	alejandro.mascall@example.com	true	2012-02-17 19:04:52	2020-01-21 10:07:57
alene.rabeck	Alene Rabeck	alene.rabeck@example.com	true	2012-02-17 19:04:53	2020-01-21 10:07:59
alfonso.griglen	Alfonso Griglen	alfonso.griglen@example.com	true	2012-02-17 19:04:51	2020-01-21 10:07:47
alissa.mountjoy	Alissa Mountjoy	alissa.mountjoy@example.com	true	2012-02-17 19:04:52	2020-01-21 10:07:54
allan.schwantd	Allan Schwantd	allan.schwantd@example.com	true	2012-02-17 19:04:53	2020-01-21 10:07:58
allie.pumphrey	Allie Pumphrey	allie.pumphrey@example.com	true	2012-02-17 19:04:52	2020-01-21 10:07:58

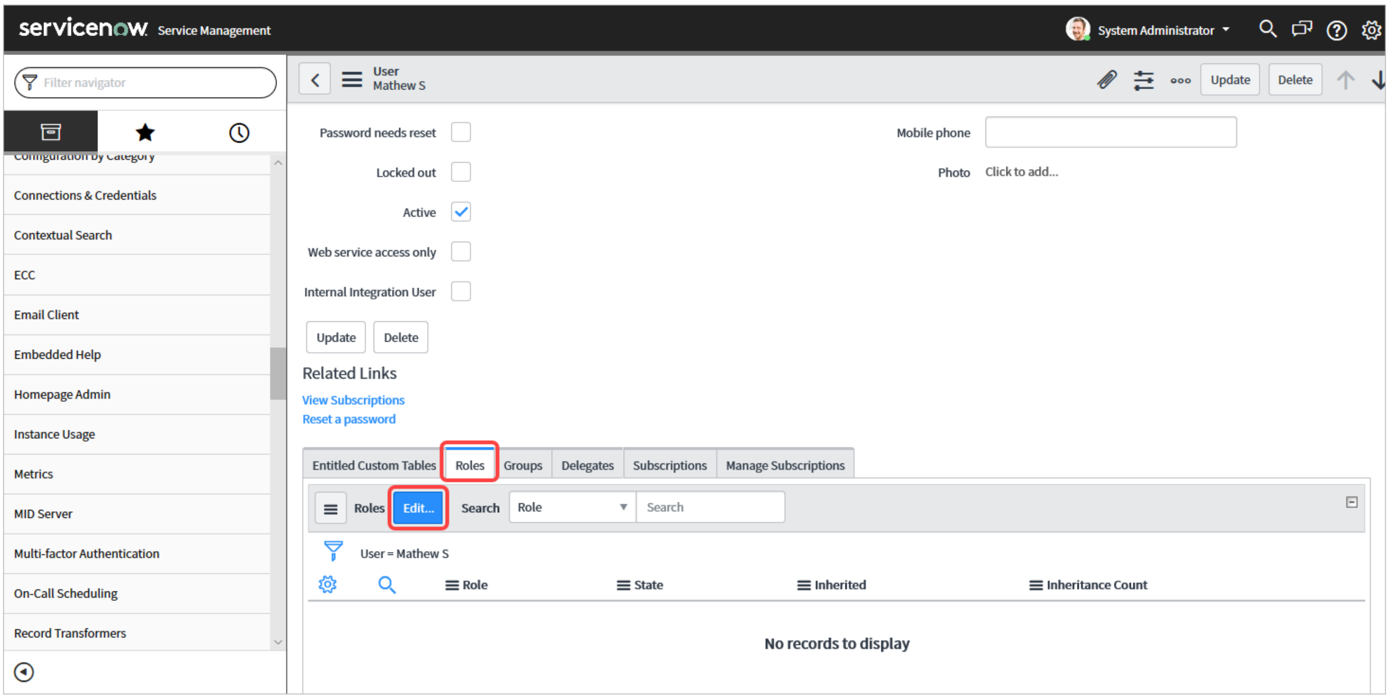
2. Type a unique user id and other relevant information and click **Submit**. Make sure to record the Username/Password combination.



User ID	
First name	
Last name	
Title	
Department	
Password	
Password needs reset	□
Locked out	□
Active	☑
Web service access only	□
Internal Integration User	□
Email	
Language	-- None --
Calendar integration	Outlook
Time zone	System (America/Los_Angeles)
Date format	System (yyyy-MM-dd)
Business phone	
Mobile phone	
Photo	Click to add...

3. Search for the newly created account and then click the newly created user account to begin editing.

4. Click **Roles** > **Edit**.



Password needs reset □

Locked out □

Active ☑

Web service access only □

Internal Integration User □

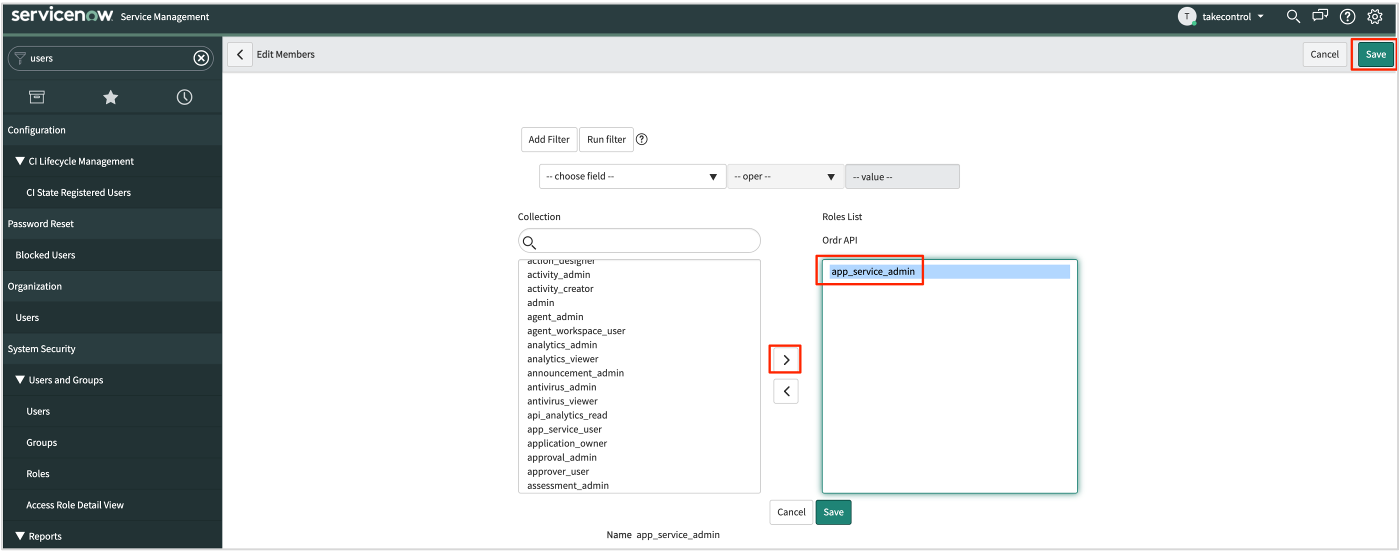
Mobile phone

Photo Click to add...

User = Mathew S

No records to display

5. Assign '*app_service_admin*' privileges to the user account, and then click **Save**.



action_designer
activity_admin
activity_creator
admin
agent_admin
agent_workspace_user
analytics_admin
analytics_viewer
announcement_admin
antivirus_admin
antivirus_viewer
api_analytics_read
app_service_user
application_owner
approval_admin
approver_user
assessment_admin

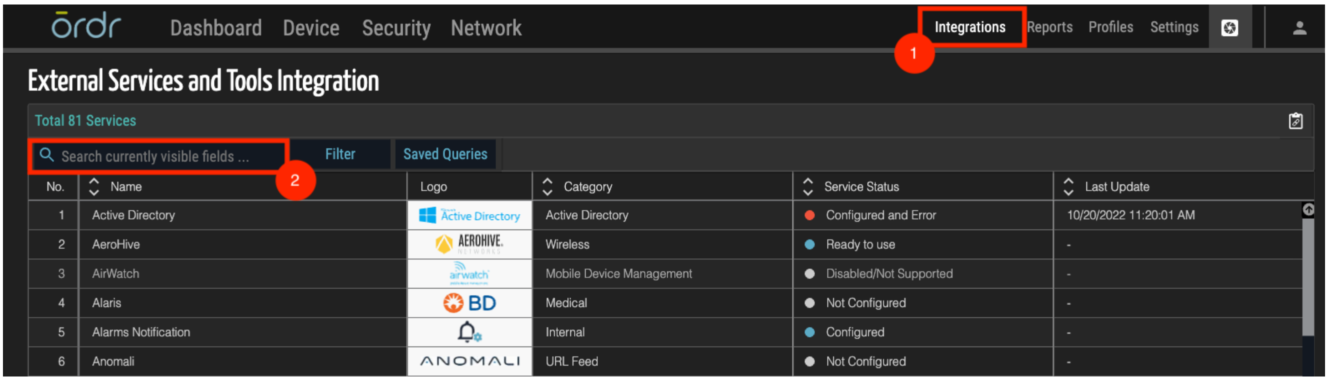
app_service_admin

Name app_service_admin

Step 4. Ordr ServiceNow Configuration

NOTE: Before creating a new configuration setting, delete any existing settings.

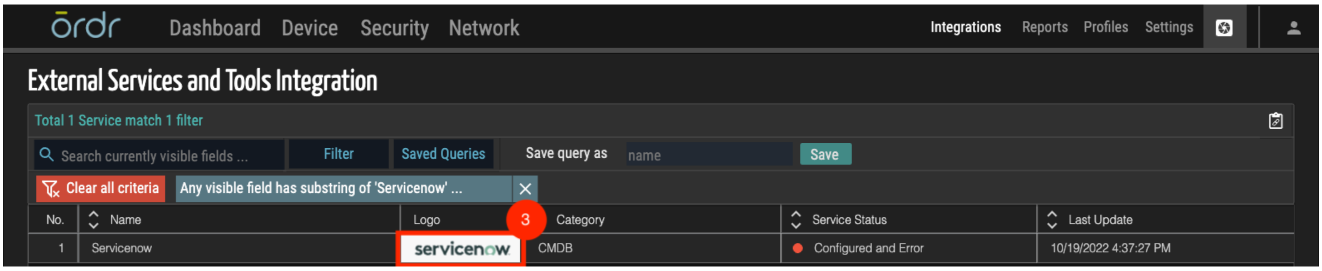
1. On the main menu bar of the Ordr SCE application, click **Integrations**.
2. Under **External Services and Tools Integration** search for **Servicenow.**
3. Click on **Servicenow**.



External Services and Tools Integration

Total 81 Services

No.	Name	Logo	Category	Service Status	Last Update
1	Active Directory	Active Directory	Active Directory	● Configured and Error	10/20/2022 11:20:01 AM
2	AeroHive	AEROHIVE	Wireless	● Ready to use	-
3	AirWatch	airwatch	Mobile Device Management	● Disabled/Not Supported	-
4	Alaris	BD	Medical	● Not Configured	-
5	Alarms Notification		Internal	● Configured	-
6	Anomali	ANOMALI	URL Feed	● Not Configured	-



External Services and Tools Integration

Total 1 Service match 1 filter

Any visible field has substring of 'Servicenow' ...

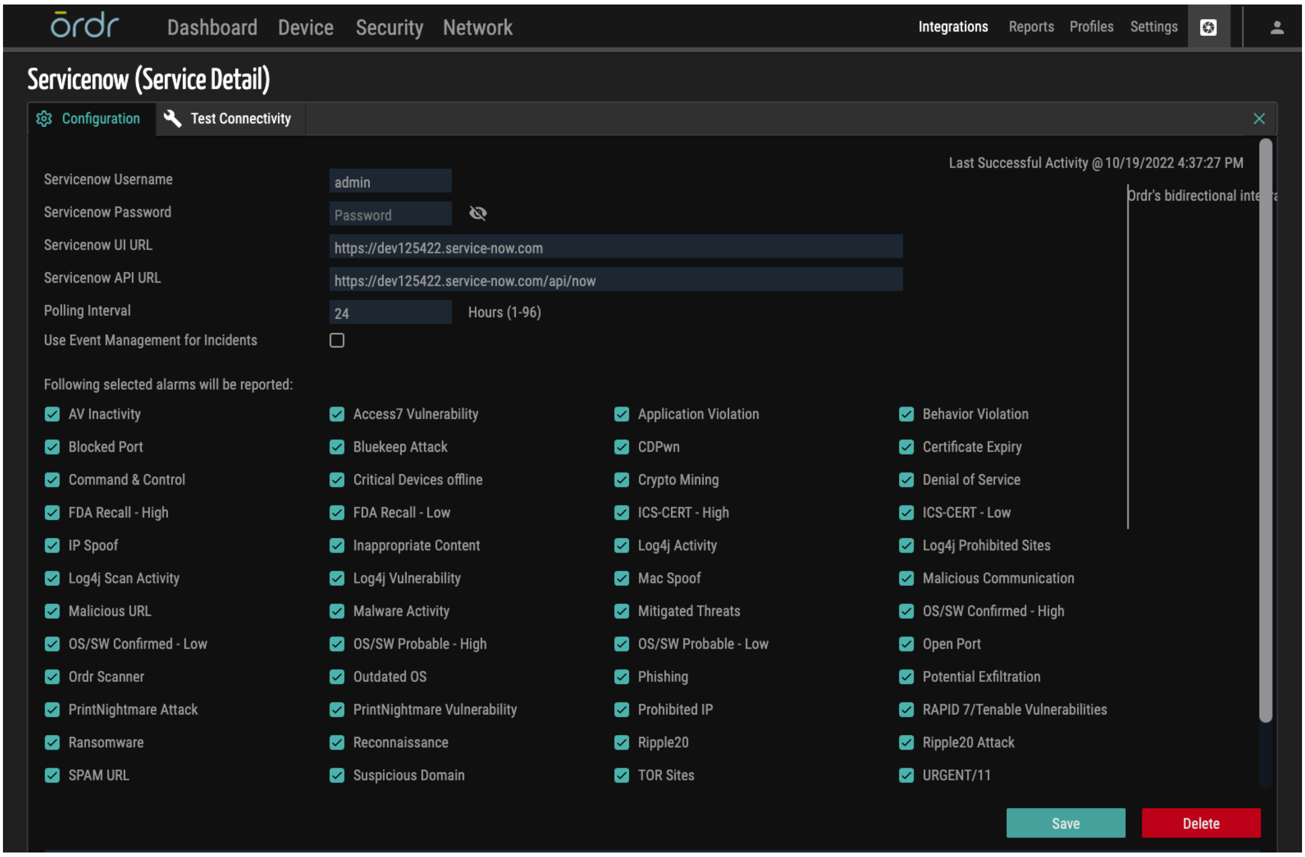
No.	Name	Logo	Category	Service Status	Last Update
1	Servicenow	servicenow	CMDB	● Configured and Error	10/19/2022 4:37:27 PM

4. Enter the ServiceNow username and password in the corresponding fields previously created in ServiceNow.
5. Enter the **ServiceNow UI URL** and **API URL** in the corresponding fields, examples of the UI & API URL's are below

   a. **UI URL example** for your ServiceNow system would be https://dev123456.service-now.com

   b. **API URL example** for your ServiceNow system would be https://dev123456.ser- vice-now.com/api/now

6. Enter the polling interval in minutes (30– 360) in the **Polling Interval** field. By default, it is configured for 30 minutes, please see the note below for changes made in the SCE platform related to polling interval frequency.
7. (Optional) To create alerts as events, select the Use Event Management for Incidents check box.
8. Choose any of the alarms to be reported to ServiceNow. All alarms are selected by default.
9. To save the configuration settings, click **Save**.



Servicenow (Service Detail)

Last Successful Activity @ 10/19/2022 4:37:27 PM

Ordr's bidirectional inte

Servicenow Username: admin

Servicenow Password: Password

Servicenow UI URL: https://dev125422.service-now.com

Servicenow API URL: https://dev125422.service-now.com/api/now

Polling Interval: 24 Hours (1-96)

Use Event Management for Incidents ☐

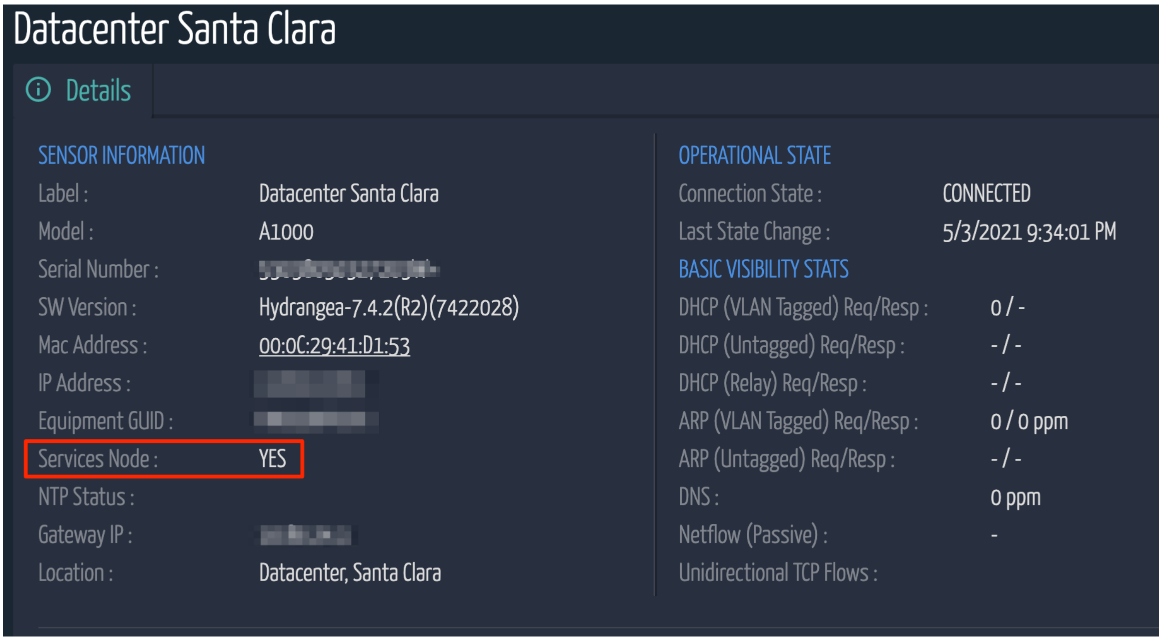
Following selected alarms will be reported:

- ☑ AV Inactivity
- ☑ Access7 Vulnerability
- ☑ Application Violation
- ☑ Behavior Violation
- ☑ Blocked Port
- ☑ Bluekeep Attack
- ☑ CDPwn
- ☑ Certificate Expiry
- ☑ Command & Control
- ☑ Critical Devices offline
- ☑ Crypto Mining
- ☑ Denial of Service
- ☑ FDA Recall - High
- ☑ FDA Recall - Low
- ☑ ICS-CERT - High
- ☑ ICS-CERT - Low
- ☑ IP Spoof
- ☑ Inappropriate Content
- ☑ Log4j Activity
- ☑ Log4j Prohibited Sites
- ☑ Log4j Scan Activity
- ☑ Log4j Vulnerability
- ☑ Mac Spoof
- ☑ Malicious Communication
- ☑ Malicious URL
- ☑ Malware Activity
- ☑ Mitigated Threats
- ☑ OS/SW Confirmed - High
- ☑ OS/SW Confirmed - Low
- ☑ OS/SW Probable - High
- ☑ OS/SW Probable - Low
- ☑ Open Port
- ☑ Ordr Scanner
- ☑ Outdated OS
- ☑ Phishing
- ☑ Potential Exfiltration
- ☑ PrintNightmare Attack
- ☑ PrintNightmare Vulnerability
- ☑ Prohibited IP
- ☑ RAPID 7/Tenable Vulnerabilities
- ☑ Ransomware
- ☑ Reconnaissance
- ☑ Ripple20
- ☑ Ripple20 Attack
- ☑ SPAM URL
- ☑ Suspicious Domain
- ☑ TOR Sites
- ☑ URGENT/11

Once connectivity is established, the ‘Service Status’ shows ‘Successful’ and the tile banner turns green.

NOTE: Connectivity to ServiceNow is via the sensor that is running as a service-node. If you have more than one sensor deployed, you can find the sensor defined with service-node capability enabled. Note that there is only one per deployment.

To locate the sensor running in this mode, go to **Network** > **SCE Sensors,** and within the sensor configuration located ‘*service node*’, the sensor set as **YES** is the relevant sensor. For clarity, this sensor is sometimes referred to as the proxy-sensor, or thick-sensor.



Datacenter Santa Clara

SENSOR INFORMATION

Label : Datacenter Santa Clara
Model : A1000
Serial Number : [redacted]
SW Version : Hydrangea-7.4.2(R2)(7422028)
Mac Address : 00:0C:29:41:D1:53
IP Address : [redacted]
Equipment GUID : [redacted]
Services Node : YES
NTP Status :
Gateway IP : [redacted]
Location : Datacenter, Santa Clara

OPERATIONAL STATE

Connection State : CONNECTED
Last State Change : 5/3/2021 9:34:01 PM

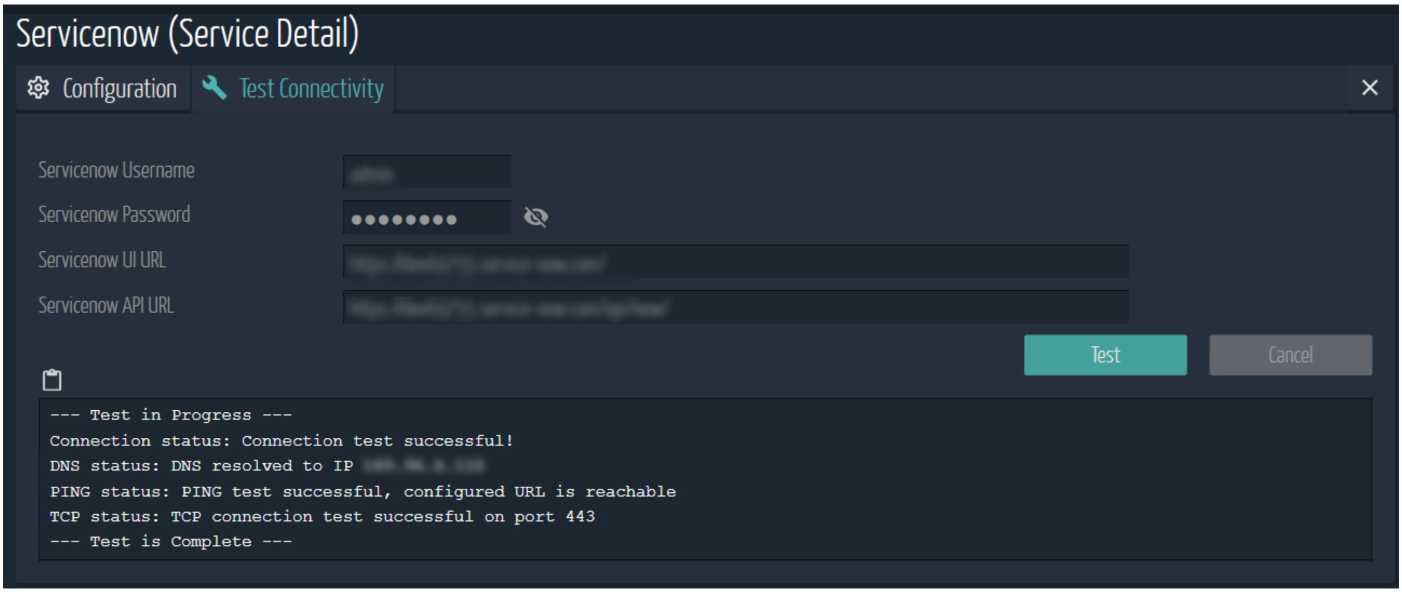
BASIC VISIBILITY STATS

DHCP (VLAN Tagged) Req/Resp : 0 / -
DHCP (Untagged) Req/Resp : - / -
DHCP (Relay) Req/Resp : - / -
ARP (VLAN Tagged) Req/Resp : 0 / 0 ppm
ARP (Untagged) Req/Resp : - / -
DNS : 0 ppm
Netflow (Passive) : -
Unidirectional TCP Flows :

Test Connectivity

This option allows you to validate the credentials and access rights before establishing the integration.

1. The username, UI URL, and API URL fields are carried over from the configuration tab prepopulated by default.
2. Enter the Servicenow password in the corresponding field.
3. Click **Test**. The test results appear on the screen.
4. (Optional) To copy the connectivity test results to the clipboard, click 📋.



Servicenow (Service Detail)

Servicenow Username [redacted]
Servicenow Password ●●●●●●●●●
Servicenow UI URL [redacted]
Servicenow API URL [redacted]

```
--- Test in Progress ---
Connection status: Connection test successful!
DNS status: DNS resolved to IP [redacted]
PING status: PING test successful, configured URL is reachable
TCP status: TCP connection test successful on port 443
--- Test is Complete ---
```

Device Inventory Push

Ordr pushes discovered inventory into various target tables at ServiceNow based on device category. For some device categories, Ordr pushes inventory to existing tables in ServiceNow (Network Gear, Printer, Personal Computer, Server) and custom Ordr related tables for other categories. The below table captures these table mappings.

Ordr Category	ServiceNow Table
Facility Devices	CPN Facility Devices
Media Devices	CPN Media Devices
Medical Devices	CPN Medical Devices
Misc Devices	CPN Discovered Equipments
Mobile Phones and Tablets	CPN Mobiles
Network Devices	Network Gear
Physical Security Devices	CPN Physical Security Devices
Printers and Copiers	Printers
Retail Devices	CPN Retail Devices
Servers	Servers
Storage Devices	Storage Server
Workstations	Personal Computer
Others	CPN Discovered Equipments

Attributes that Ordr uses to push also depend on ServiceNow Table and the below table captures these attributes.

Ordr Attribute	Ordr Tables	Server	Storage Server	Network Gear	Personal Computer
Mac Address	MAC Address	MAC Address	MAC Address	MAC Address	MAC Address
IP Address	IP Address	IP Address	IP Address	IP Address	IP Address
Manufacturer	Manufacturer	Manufacturer	Manufacturer	Manufacturer	Manufacturer
DHCP Hostname	Hostname	Hostname	Hostname	Name	Name
Model Name/No	Model number	Model number	Model number	Model number	Model number
Serial No	Serial number	Serial number	Serial number	Serial number	Serial number
Device Description	Description	Description	Description	Description	Description
OS Type	Operating System	OS Domain	OS Domain		OS Domain
OS Version	Software Version	OS Version	OS Version		OS Version
SW Version	Software Version				
Can switch IP				Can switch IP	
Port Count				Port	

Device Inventory Pull

Ordr also pulls and consolidates inventory from ServiceNow Tables. By default inventory details are pulled from the following tables:

- Server
- Facility Hardware
- Virtual Machine Instance
- Network Gear
- Imaging Hardware
- IP Phone
- Monitoring Equipment
- Personal Computer
- Printer

Ordr has the flexibility to customize pull functionality to specify ServiceNow Tables and their attributes. A YAML file has to be prepared and loaded into the Ordr system to achieve this, use and loading of this YAML file requires support from the ORDR customer support team. Please refer to the appendix for the sample YAML file used for customized inventory pull.

NOTE: If you want to leverage the YAML file for advanced inventory pull configuration, see '*Appendix A – Schema for SCE's Event Field Names*'.

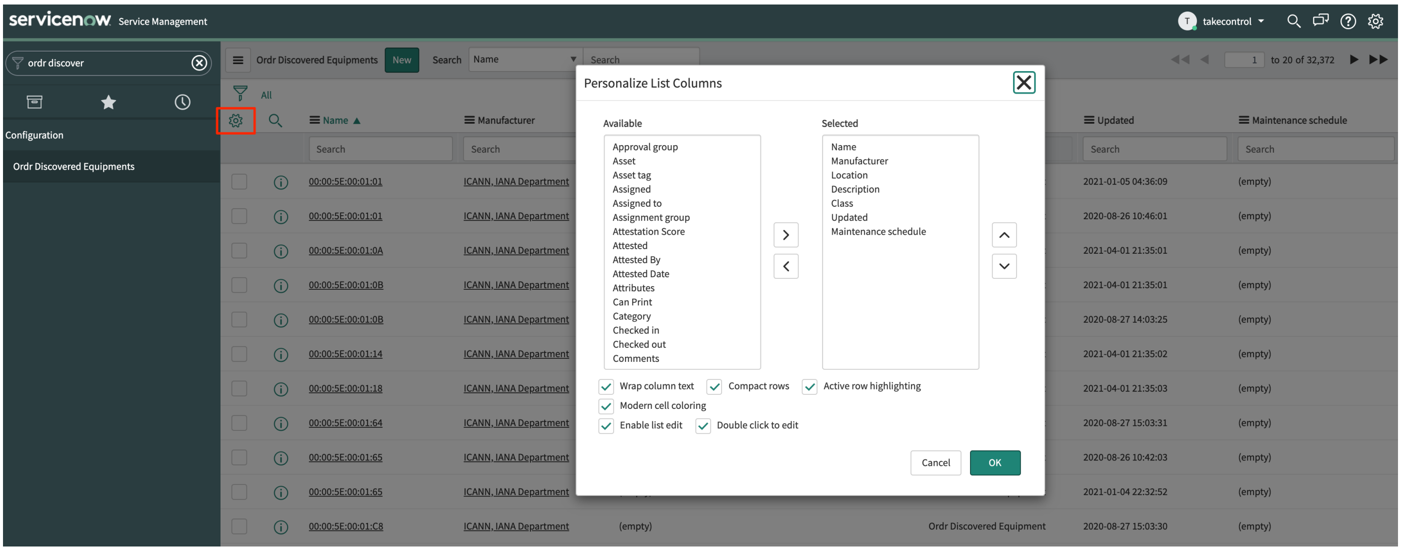
Step 5. Ordr Discovered Equipments Verification

You can view the Ordr discovered devices that have been pushed into the ServiceNow CMDB system from the entries created in the custom tables (Ordr Discovered Equipments) as well as from the default tables (Personal Computers, Printers, Network Gear & Servers) based on the classification.

1. On the ServiceNow homepage, search '*Ordr*'.

2. To view, the Ordr discovered devices, click **Ordr Discovered Equipments**.

3. (Optional) To filter Ordr discovered devices from generic assets such as personal (laptops and desktops), printers, and so on, use the **Created By** field in ServiceNow, and click the gear ⚙ as highlighted below.


servicenow Service Management
takecontrol
ordr discover
Configuration
Ordr Discovered Equipments
Ordr Discovered Equipments
New
Search
Name
Search
All
1
to 20 of 32,372

Personalize List Columns

Available:
Approval group
Asset
Asset tag
Assigned
Assigned to
Assignment group
Attestation Score
Attested
Attested By
Attested Date
Attributes
Can Print
Category
Checked in
Checked out
Comments

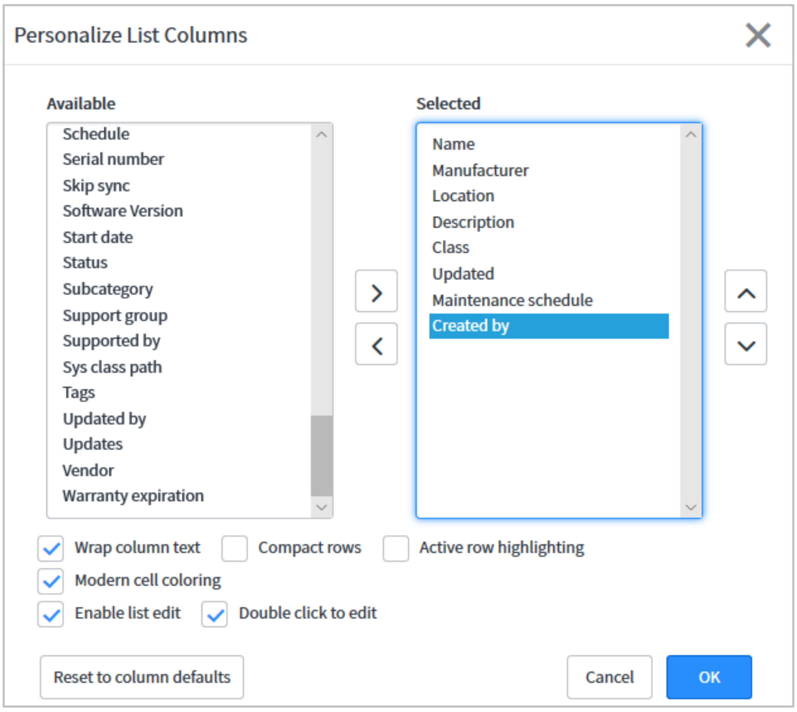
Selected:
Name
Manufacturer
Location
Description
Class
Updated
Maintenance schedule

☑ Wrap column text ☑ Compact rows ☑ Active row highlighting
☑ Modern cell coloring
☑ Enable list edit ☑ Double click to edit

Cancel OK

Name	Manufacturer			Updated	Maintenance schedule
00:00:5E:00:01:01	ICANN, IANA Department			2021-01-05 04:36:09	(empty)
00:00:5E:00:01:01	ICANN, IANA Department			2020-08-26 10:46:01	(empty)
00:00:5E:00:01:0A	ICANN, IANA Department			2021-04-01 21:35:01	(empty)
00:00:5E:00:01:0B	ICANN, IANA Department			2021-04-01 21:35:01	(empty)
00:00:5E:00:01:0B	ICANN, IANA Department			2020-08-27 14:03:25	(empty)
00:00:5E:00:01:14	ICANN, IANA Department			2021-04-01 21:35:02	(empty)
00:00:5E:00:01:18	ICANN, IANA Department			2021-04-01 21:35:03	(empty)
00:00:5E:00:01:64	ICANN, IANA Department			2020-08-27 15:03:31	(empty)
00:00:5E:00:01:65	ICANN, IANA Department			2020-08-26 10:42:03	(empty)
00:00:5E:00:01:65	ICANN, IANA Department			2021-01-04 22:32:52	(empty)
00:00:5E:00:01:C8	ICANN, IANA Department	(empty)	Ordr Discovered Equipment	2020-08-27 15:03:30	(empty)

4. Select the '*Created by*' column name from the **Available** list and then click '**>**'. The '*Created by*' column name is moved to the **Selected** list. Click **OK**.


Personalize List Columns

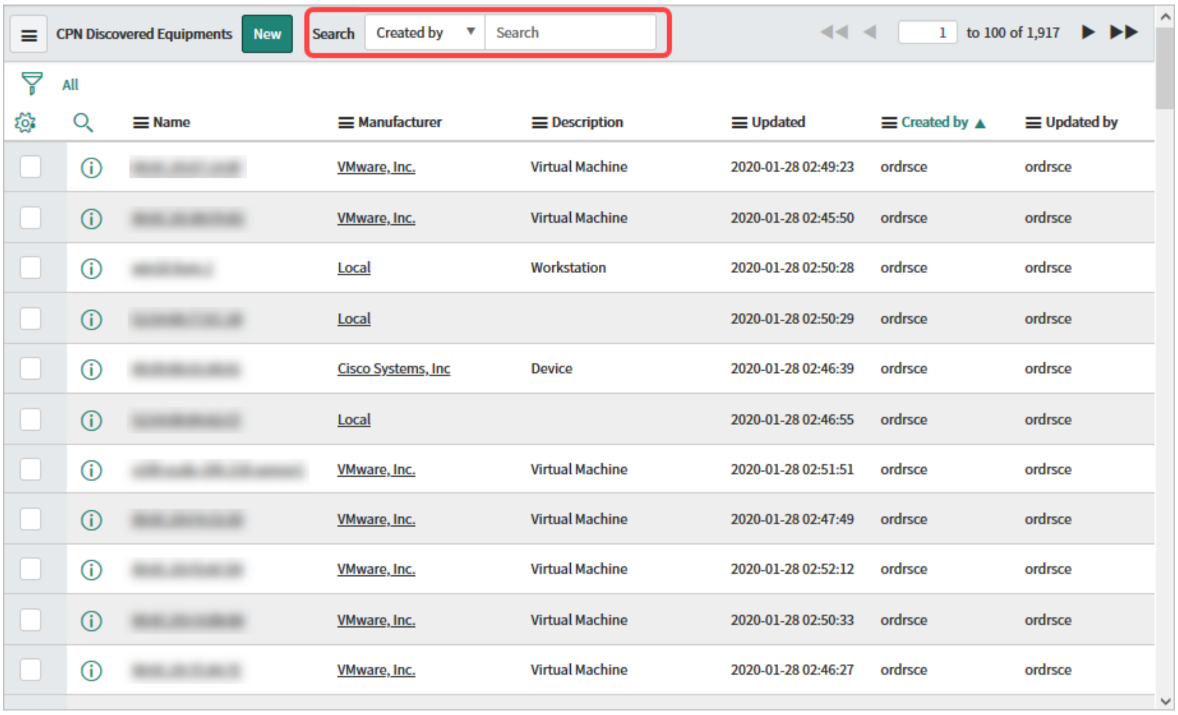
Available:
Schedule
Serial number
Skip sync
Software Version
Start date
Status
Subcategory
Support group
Supported by
Sys class path
Tags
Updated by
Updates
Vendor
Warranty expiration

Selected:
Name
Manufacturer
Location
Description
Class
Updated
Maintenance schedule
Created by

☑ Wrap column text □ Compact rows □ Active row highlighting
☑ Modern cell coloring
☑ Enable list edit ☑ Double click to edit

Reset to column defaults Cancel OK

5. (Optional) From the **Search** drop-down list, select **Created by** and type a unique user id in the **Search** field. In this example, ‘*ordrsce*’ is the user id.
   The list of devices discovered by Ordr SCE is displayed.

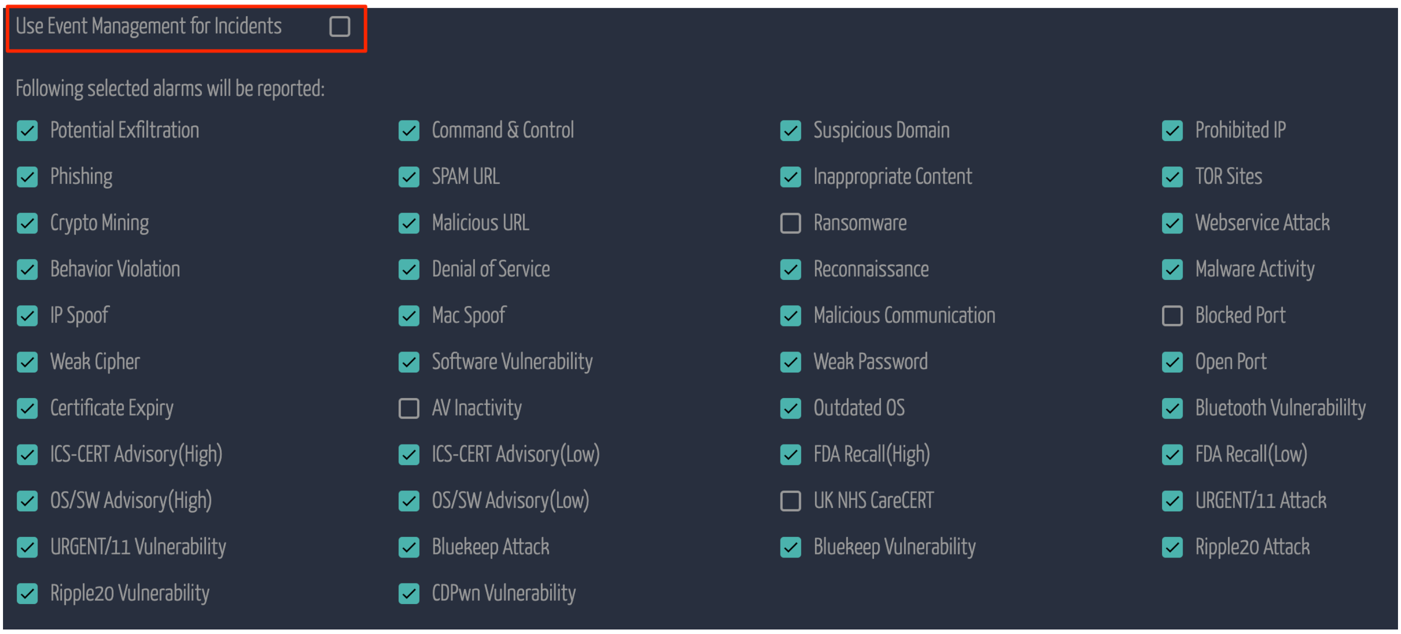


Name	Manufacturer	Description	Updated	Created by ▲	Updated by
[redacted]	VMware, Inc.	Virtual Machine	2020-01-28 02:49:23	ordrsce	ordrsce
[redacted]	VMware, Inc.	Virtual Machine	2020-01-28 02:45:50	ordrsce	ordrsce
[redacted]	Local	Workstation	2020-01-28 02:50:28	ordrsce	ordrsce
[redacted]	Local		2020-01-28 02:50:29	ordrsce	ordrsce
[redacted]	Cisco Systems, Inc	Device	2020-01-28 02:46:39	ordrsce	ordrsce
[redacted]	Local		2020-01-28 02:46:55	ordrsce	ordrsce
[redacted]	VMware, Inc.	Virtual Machine	2020-01-28 02:51:51	ordrsce	ordrsce
[redacted]	VMware, Inc.	Virtual Machine	2020-01-28 02:47:49	ordrsce	ordrsce
[redacted]	VMware, Inc.	Virtual Machine	2020-01-28 02:52:12	ordrsce	ordrsce
[redacted]	VMware, Inc.	Virtual Machine	2020-01-28 02:50:33	ordrsce	ordrsce
[redacted]	VMware, Inc.	Virtual Machine	2020-01-28 02:46:27	ordrsce	ordrsce

Incidents

ORDR SCE can turn SCE events, alerts into ServiceNow Incident tickets. An extensive list of incidents can be created. As a review process, when configuring the ServiceNow tile, the optional ability to enable '**Use Event Management for Incidents**' exists. This provides the ability to enable/disable an extensive list of different incident-based alerts.

This is the list of events supports under 7.4.2R2

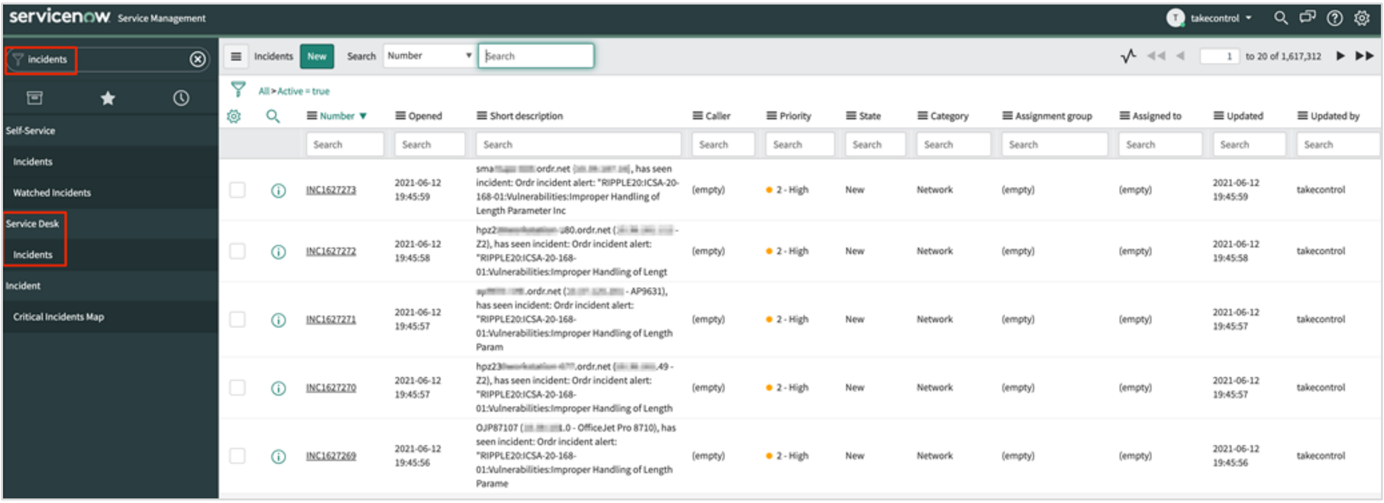


Use Event Management for Incidents ☐

Following selected alarms will be reported:

- ☑ Potential Exfiltration
- ☑ Phishing
- ☑ Crypto Mining
- ☑ Behavior Violation
- ☑ IP Spoof
- ☑ Weak Cipher
- ☑ Certificate Expiry
- ☑ ICS-CERT Advisory(High)
- ☑ OS/SW Advisory(High)
- ☑ URGENT/11 Vulnerability
- ☑ Ripple20 Vulnerability
- ☑ Command & Control
- ☑ SPAM URL
- ☑ Malicious URL
- ☑ Denial of Service
- ☑ Mac Spoof
- ☑ Software Vulnerability
- ☐ AV Inactivity
- ☑ ICS-CERT Advisory(Low)
- ☑ OS/SW Advisory(Low)
- ☑ Bluekeep Attack
- ☑ CDPwn Vulnerability
- ☑ Suspicious Domain
- ☑ Inappropriate Content
- ☐ Ransomware
- ☑ Reconnaissance
- ☑ Malicious Communication
- ☑ Weak Password
- ☑ Outdated OS
- ☑ FDA Recall(High)
- ☐ UK NHS CareCERT
- ☑ Bluekeep Vulnerability
- ☑ Prohibited IP
- ☑ TOR Sites
- ☑ Webservice Attack
- ☑ Malware Activity
- ☐ Blocked Port
- ☑ Open Port
- ☑ Bluetooth Vulnerabililty
- ☑ FDA Recall(Low)
- ☑ URGENT/11 Attack
- ☑ Ripple20 Attack

Enabling this option will allow SCE to automatically create an incident for the above-selected events. The events can be located in ServiceNow by searching the navigation bar for '*Incidents*'. Notice they appear under **Service Desk** and not **Self Service**.



Number	Opened	Short description	Caller	Priority	State	Category	Assignment group	Assigned to	Updated	Updated by
INC1627273	2021-06-12 19:45:59	sma[redacted]ordr.net ([redacted]), has seen incident: Ordr incident alert: "RIPPLE20:ICSA-20-168-01:Vulnerabilities:Improper Handling of Length Parameter Inc	(empty)	● 2 - High	New	Network	(empty)	(empty)	2021-06-12 19:45:59	takecontrol
INC1627272	2021-06-12 19:45:58	hpz2[redacted]80.ordr.net ([redacted] - Z2), has seen incident: Ordr incident alert: "RIPPLE20:ICSA-20-168-01:Vulnerabilities:Improper Handling of Lengt	(empty)	● 2 - High	New	Network	(empty)	(empty)	2021-06-12 19:45:58	takecontrol
INC1627271	2021-06-12 19:45:57	[redacted].ordr.net ([redacted] - AP9631), has seen incident: Ordr incident alert: "RIPPLE20:ICSA-20-168-01:Vulnerabilities:Improper Handling of Length Param	(empty)	● 2 - High	New	Network	(empty)	(empty)	2021-06-12 19:45:57	takecontrol
INC1627270	2021-06-12 19:45:57	hpz23[redacted].ordr.net ([redacted].49 - Z2), has seen incident: Ordr incident alert: "RIPPLE20:ICSA-20-168-01:Vulnerabilities:Improper Handling of Length	(empty)	● 2 - High	New	Network	(empty)	(empty)	2021-06-12 19:45:57	takecontrol
INC1627269	2021-06-12 19:45:56	OJP87107 ([redacted]1.0 - OfficeJet Pro 8710), has seen incident: Ordr incident alert: "RIPPLE20:ICSA-20-168-01:Vulnerabilities:Improper Handling of Length Parame	(empty)	● 2 - High	New	Network	(empty)	(empty)	2021-06-12 19:45:56	takecontrol

Appendix A – Schema for SCE's Event Field Names

The table describes the field names available under **Event Management** > **All Events**.

An event is a notification from one or more monitoring tools that indicate such as a log message, warning, or error has occurred.

Field	Description
Time of Event	The time that the event occurred in the network node time zone.
Source	Event monitoring software that generated the event.
Description	Reason for event generation.
Node	Node name, fully qualified domain name (FQDN), IP address, or MAC address that is associated with the event.
Type	A pre-defined event type, such as high CPU, is used to identify an event record.
Resource	Node resource that is relevant to the event.
Message key	Unique event identifier to identify multiple events that relate to the same alert.
State	The status of the event. • **Ready**: Event received and waiting to be processed. • **Queued**: Event queued by the event processor job. • **Processed**: Event successfully processed. • **Error**: Failure occurred while processing the event. • **Ignored**: Value not in use.
Severity	The severity level of the event. • **Critical**: Immediate action is required. The resource is either not functional or critical problems are imminent. • **Major**: Major functionality is severely impaired, or performance has degraded. • **Minor**: Partial, non-critical loss of functionality or performance degradation occurred. • **Warning**: Attention is required, even though the resource is still functional. • **Info**: An alert is created. The resource is still functional. • **Clear**: No action is required. An alert is not created from this event. Existing alerts are closed.
Alert	If an alert was created because of the event, this field contains the unique ID that Event Management generates to identify the alert.

Appendix B - Sample YAML for Customized Inventory Pull

Sample YAML file for customized inventory pull is as below:

```
---
# List of Tables
Tables:
Video Equipment: u_cmdb_ci_video_equipment
# List of columns for each table
Video Equipment:
MAC Address: mac_address
Serial number: serial_number
Location Notes: u_location_notes_str
Model Id: model_id
Description: short_description
Operating System Version: u_op_sys_version
Firmware Version: u_firmware_version
Name: name
Class: sys_class_name
Vendor: vendor
Device Type: u_device_type
Default Support Group: u_default_support_group
Secondary Support Group: u_secondary_support_group
Level 3 Support Group: u_level_3_support_group
Execution Environment: u_execution_env
NAC Whitelisted: u_nac_white_listed
...
```

Summary

Without Ordr Systems Control Engine, customers can struggle for months or years to achieve comprehensive inventory and device visibility. Coupled with the existing asset detail that ServiceNow offers, the coverage and upkeep of asset detail inside of ServiceNow will be up-to-date and require little maintenance and burden to ensure the latest information is populating the CMDB.

With the ability to automate the creation of ServiceNow incidents for specific chosen events the end-to-end process of inventory, incidents are significantly simplified under an ORDR SCE deployment.

ōrdr

info@ordr.net
www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054