

ServiceNow NCM Self-Service Plug-In Administrator Guide

Third-Party Integrations 1.6.1

November 27, 2023

Contents

NCM Self-Service Plug-in for ServiceNow.....	3
Roles and Responsibilities.....	3
Prerequisites for NCM Self-Service Plug-in for ServiceNow.....	5
Required Table Permissions.....	6
Assigning Access to Tables.....	7
Assigning System Property.....	8
Modifying the Security Check Policies for Connection.....	8
Enabling the Email Server.....	9
Configuring LDAP in ServiceNow.....	9
Configuring CyberArk in ServiceNow.....	11
Viewing the MID Server Status.....	12
Configuring Service Portal.....	12
Clustered MID Server for Load Balancing or Failover Support.....	14
NCM Self-Service Plug-in Version Upgrade.....	16
Installing NCM Self-Service Plug-in from the ServiceNow Store.....	17
Configuring the Application Properties.....	17
Sync Operation.....	22
Importing NCM Self-Service Resources Using the Sync Operation.....	23
Inventory Sync.....	24
Catalog Item Creation.....	31
Assigning a Blueprint, Runbook, or MPI to a User.....	31
Available Actions on a Catalog Item.....	33
Viewing Application Action Request Details.....	34
Viewing Support Details.....	34
Viewing Logs.....	35
 Copyright.....	 36

NCM SELF-SERVICE PLUG-IN FOR SERVICENOW

NCM Self-Service plug-in for ServiceNow enables you to launch NCM Self-Service blueprints, runbooks, or MPIs in ServiceNow platform as service catalog items. The NCM Self-Service plug-in helps to automate the application provisioning and life-cycle management of NCM Self-Service product. The plug-in allows you to control the resources by using IT services management (ITSM) and IT operations management (ITOM) processes that are defined by the customers in ServiceNow to reduce the time in Nutanix Marketplace.

Note: To configure and use NCM Self-Service plug-in, you must be familiar with the basic concepts of NCM Self-Service and ServiceNow platform.

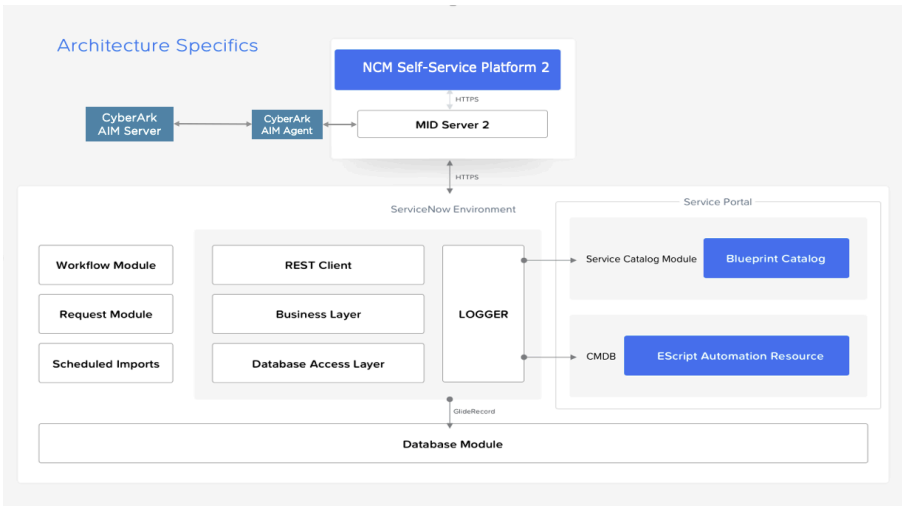


Figure 1: Architecture

Supported Versions

The following table shows the supported versions in this release.

Entity	Supported versions
ServiceNow	Tokyo, Utah, and Vancouver
NCM Self-Service	3.5.0 (SaaS), 3.7, and 3.7.1
Web-browser	Latest versions of Chrome and Firefox

Note: If you are upgrading the NCM Self-Service plug-in to version 1.2 or later, click the **Save Properties** button in **Application Properties** page. The page automatically displays the NCM Self-Service version.

Roles and Responsibilities

You must have access privileges to perform certain actions. The following table describes the various roles and their respective responsibilities.

Table 1: Roles and Responsibilities

Role	Responsibility
System administrator	<ul style="list-style-type: none"> Assigns NCM Self-Service administrator role to one of the LDAP imported users.
x_nuta2_nutanix_ca.calm_admin	<ul style="list-style-type: none"> Plug-in configuration Runtime configuration Importing NCM Self-Service resources in ServiceNow platform Creating catalog items Entitling users or groups
catalog	<ul style="list-style-type: none"> Accesses and launches catalog items on ServiceNow Native UI.
x_nuta2_nutanix_ca.user	<ul style="list-style-type: none"> Launch catalog items Perform actions on applications Check logs <div> <p>Note: When the NCM Self-Service administrator creates a catalog item in the ServiceNow application, the x_nuta2_nutanix_ca.user role is automatically allocated to either LDAP imported users or groups and local group if the Use Local Groups option is enabled on the Application property page.</p> </div>
mid_server	<ul style="list-style-type: none"> Connects NCM Self-Service environment by using CyberArk integrations with ServiceNow action designer. <div> <p>Note: When the NCM Self-Service administrator creates a catalog item by using CyberArk setup in the ServiceNow application, the mid_server role is automatically allocated to either LDAP imported users or groups and local group if the Use Local Groups option is enabled on the Application property page.</p> </div>
approval_user	<ul style="list-style-type: none"> Approves or rejects approval requests.
ITIL	<ul style="list-style-type: none"> The IT Infrastructure Library (ITIL) role is assigned to a NCM Self-Service Plug-in Admin or NCM Self-Service Plug-in End User to access the inventory data on the dashboard.

Prerequisites for NCM Self-Service Plug-in for ServiceNow

Before you start using the NCM Self-Service plug-in, ensure that the following prerequisites are completed:

Warning: When you migrate from a previous version of NCM Self-Service Plug-in for ServiceNow to version 1.4, the following custom tables are deleted:

Nutanix, AWS, GCP, VMware, Azure, Storage, Disk, Blank Disks, Disk List, Data Disks, Networking, Network Profiles, Secrets, Tag List, Staging VMware, Staging Nutanix, Staging Azure, Staging GCP, and Staging AWS.

You must take a backup of the required data before the migration.

- You need system administrator privileges to install the NCM Self-Service plug-in.
- If the plug-in administrator wants to add or edit any new user or group to an existing or a newly created catalog item, the administrator has to ensure that the user or group is assigned with the following roles.
 - mid_server
 - catalog
 - user
- If you use the connect to NCM Self-Service option by using the ServiceNow credential store object with CyberArk as the external storage, the following components must be enabled.
 - External credential store plug-in
 - Discovery plug-ins
 - ServiceNow IntegrationHub Standard pack Installer if you are using New York version
- You must configure NCM Self-Service and ServiceNow with the same AD or LDAP instance. This configuration is required because the user entitlement on either side is based on the user mapped to catalog item on the ServiceNow side and Project users on the NCM Self-Service side.
- You need an ITSM license that includes incident management module. This license is used to create incidents to report blueprint and other events launch failures.

Note: Without the ITSM license, installation of application from the store does not work as this dependency is bundled with the application.

- You must enable the user criteria scoped API plug-in (ID:com.glideapp.user_criteria.scoped.api). This plug-in is used to create, modify, or delete user criteria records by using scripts.
- You must install and configure the ServiceNow MID server. For information on how to install and configure MID server, refer to the MID Server section in the [ServiceNow Documentation](#). To refer to a video about setting up a MID server, [click here](#).
- You must ensure that the MID server is running in your environment. NCM Self-Service is reachable from the machine or environment where MID server is installed.
- MID server users (users managing the MID server) must have the "mid_server" role privileges.
- The MID server must be up and validated.
- You need to contact your ServiceNow Administrator (one who manages the entire instance) for making the plug-in available on to the ServiceNow instance from the ServiceNow application store.

- When the application is installed, the ServiceNow administrator must manually assign the NCM Self-Service administrator role to one of the LDAP imported users. The NCM Self-Service administrator must have the following roles:
 - mid_server (to access MID server)
 - catalog
 - x_nuta2_nutanix_ca.calm_admin
 - x_nuta2_nutanix_ca.user

Users with the NCM Self-Service Administrator role can configure and manage the NCM Self-Service application plug-in installed on the ServiceNow instance.

- Your endpoint must have a CA signed certificate for connection. With the ServiceNow Quebec release, ServiceNow has enhanced their security with the TLS MID Server certificate check policies. If the on-premise version of NCM Self-Service has an untrusted certificate for connection, the connection will be refused. For more information, [click here](#). Your system administrator can modify the certificate check policies for connection. For more information, see [Modifying the Security Check Policies for Connection](#) on page 8.
- All applications and operations must have access and permissions of the tables. ServiceNow plug-in provides default permissions to a few tables. For more information about the table permissions, see [Required Table Permissions](#) on page 6. If a table does not have the access permission, assign the access to the table. For more information about assigning access to a table, see [Assigning Access to Tables](#) on page 7.
- You must set the glide.sc.guide.tab.validate system property to true. For more information about assigning the system property, see [Assigning System Property](#) on page 8.

Note: When you log on with administrator credentials, you need to be in the Global application scope. For information on how to select the Global application scope, see [ServiceNow Documentation](#). When you do not use administrator credentials to log on, the platform automatically takes care of the selection of scope.

- You must set the glide.sc.reset_cascade system property to true. For more information about assigning the system property, see [Assigning System Property](#) on page 8.

Note: When you log on with administrator credentials, you need to be in the Global application scope. For information on selecting the Global application scope, see [ServiceNow Documentation](#). When you do not use administrator credentials to log on, the platform automatically takes care of the selection of scope. This is an out-of-the-box ServiceNow property that is used to manage the cascading of the variables and their values.

- You must enable the email server to send and receive email notifications.

Required Table Permissions

The following table displays the table permissions for the applications and operations.

Note: By default, ServiceNow plug-in provides read, create, update, and delete permissions to few tables. If any of the following tables do not have the access permission, assign the access to the table. For more information about assigning access to table, see [Assigning Access to Tables](#) on page 7.

Table 2: Required Table Permission for NCM Self-Service ServiceNow Plug-in

Table name	Label	Permission			
		Read	Create	Update	Delete
catalog_script_client	Catalog Client Scripts	Yes	No	Yes	No
sys_user_has_role	User Role	Yes	Yes	Yes	No
sys_user_grmember	Group Member	Yes	Yes	Yes	No
sys_group_has_role	Group Role	Yes	Yes	Yes	No
item_option_new	Variable	Yes	Yes	Yes	No
sys_user_group	Group	Yes	Yes	Yes	No
sc_category	Category	Yes	Yes	Yes	No
sc_catalog	Catalog	Yes	Yes	Yes	No
catalog_ui_policy	Catalog UI Policy	Yes	Yes	Yes	No
question	Question	Yes	Yes	Yes	No
question_choice	Question Choice	Yes	Yes	Yes	No
sysapproval_approver	Approvals	Yes	Yes	Yes	No

Note:

- If the table permission is mentioned as *Yes*, you have to assign the permission for the table. For more information, see [Assigning Access to Tables](#) on page 7.
- If the table permission is mentioned as *No*, you do not require any permission to perform the operation.

Assigning Access to Tables

The system administrator needs to assign access of different tables to the applications.

About this task

Note: If you have log on by using the administrator credentials, then you need to be in the Global application scope. For information on how to select Global application scope, see [ServiceNow Documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.

Procedure

1. Log on to the ServiceNow.
2. Select **Global** as the application scope.
3. Click **System Definition > Tables**.
4. Enter the table name in the **Search** field.

5. Click **To edit this record** [click here](#).
6. Under the **Application Access** tab, assign permissions for the required tables. If any of the table do not have the access permission, assign the access to the table. For more information about assigning access to table, see [Assigning Access to Tables](#) on page 7.
7. Click **Update** to save your changes.

Assigning System Property

The system administrator needs to assign the system property to work with the NCM Self-Service plug-in for ServiceNow.

About this task

Perform the following procedure to assign the system property:

Procedure

1. Do the following to set the **glide.sc.guide.tab.validate** system property to true:
 - a. In the left navigation pane, type `sys_properties.LIST` and press **Enter**.
 - b. Under the **Name** column, in the **Search** field, type `glide.sc.guide.tab.validate` and press **Enter**.
 - c. Set the value to true.
2. Do the following to set the **glide.sc.reset_cascade** system property to true:
 - a. In the left navigation pane, type `sys_properties.LIST` and press **Enter**.
 - b. Under the **Name** column, in the **Search** field, type `glide.sc.reset_cascade` and press **Enter**.
 - c. Set the value to true.

Modifying the Security Check Policies for Connection

Perform the following steps to modify the TLS MID server certificate check policies and disable the check for untrusted certificates to connect them insecurely. You do not need to perform steps provided in this section if the endpoint has CA signed certificate.

About this task

You must be a system administrator in ServiceNow to modify the TLS MID server certificate check policies.

Procedure

1. Log on to ServiceNow as a system administrator.
2. Search for MID security policy in the left pane.
3. In the Intranet record, set the following values to false:
 - **Certificate Chain Check:** false
 - **Hostname Check:** false
 - **Revocation Check:** false
4. Restart the MID server.

Enabling the Email Server

To send and receive email notifications, you must enable the email server.

Procedure

1. Log on to the ServiceNow as administrator.
2. Click **System Properties > Email Properties** to configure the email notifications.

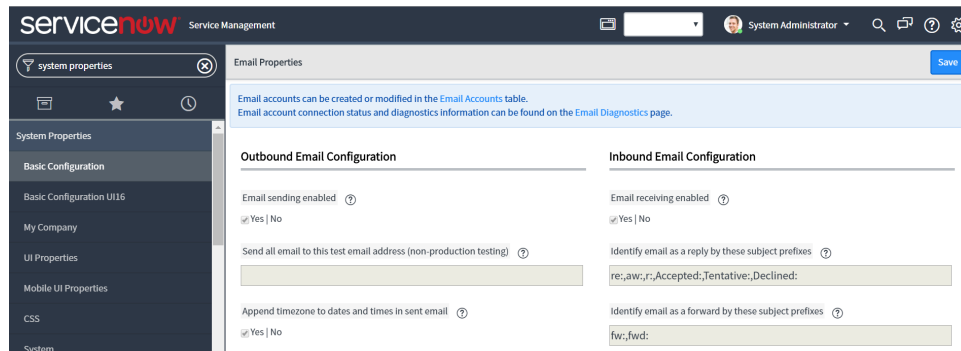


Figure 2: Email Properties Window

3. In the **Outbound Email Configuration** panel, select **Yes** checkbox against the **Email sending enabled** to enable sending email.
4. In the **Inbound Email Configuration** panel, select **Yes** checkbox against the **Email receiving enabled** to enable receiving email.
5. Click **Save** to save the email notification settings.
The email server is configured to send and receive email notifications.
6. ServiceNow application sends an email to the user when the following actions are performed in the application.
 - a. Blueprint launch request is approved by the approval mechanism set on the configuration page, an email is sent to the user who launched the blueprint.
 - b. Blueprint launch request is completed, an email is sent to the user who launched the blueprint.
7. If you do not want to send out the notification email, then click **System Notifications > Notifications**.
8. Set **Request Approved** and **Request Completed** to active false.
For more details on email setup, you can refer to the [ServiceNow Documentation](#).

Configuring LDAP in ServiceNow

A system administrator can enable LDAP integration to allow single sign-on of users from their company LDAP directory. Imported users from AD to ServiceNow can be assigned with either NCM Self-Service administrator or user role.

About this task

Note:

- The default AD or LDAP configuration in ServiceNow uses a Principal name that is mapped to a user email field in the user table. The same Principal name is used for Prism Central

authentication used by the Plug-in. If the user tables or fields are customized, contact your ServiceNow administrator to map the fields appropriately.

- If you have log on by using the administrator credentials, then you need to be in the Global application scope. For information on how to select Global application scope, see [ServiceNow Documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.
- If you already have an existing LDAP configured on your ServiceNow instance, then ensure that your configuration is inline with the OU definition mentioned in the step 5 of the following procedure. Also, perform Scheduled Load so that all groups are immediately synced and there is no difference between users of ServiceNow and your AD.
- If you do not have an existing LDAP configuration on your ServiceNow instance, then perform the following procedure.
- To create an AD, see [Adding users to AD](#).

Procedure

1. Log on to the ServiceNow.
2. Click **System LDAP > Create New Server**.
In the New LDAP server window, Active Directory option is selected by default.
3. Scroll down the window and click **Submit**.
4. In the LDAP server window, enter the name of the server in the **Name** field.
5. Select **Active** checkbox, if the server is active.
The checkbox is enabled by default.
6. Enter the distinguished name (DN) of the user authenticating the LDAP connection in the **Login distinguished name** field.
7. Enter the server password in the **Login password** field.
8. Enter the relative distinguished name (RDN) of the default search directory in the **Starting search directory** field.
9. Under LDAP server URLs, click **+** to add an LDAP server URL.
Enter the URLs of the primary and back up LDAP servers. Servers are first ordered by operational status, with servers that are Up listed first, then ordered by the order value that you specify. The first server listed is the primary LDAP server. The others are redundant servers.
10. Under **Advance Options** panel, enter connection timeout value in the **Connection timeout** field.
Specify the maximum number of seconds that the instance has to establish an LDAP connection. If no connection is made by this time, the connection is terminated.
11. Specify the number of seconds the integration has to read LDAP data in the **Read timeout** field.
The integration stops reading LDAP data after the connection exceeds the read timeout.
12. Select **Listener** checkbox to enable the integration to periodically poll Microsoft Active Directory servers or LDAP servers that support persistent search request control.

13. Enter the listener timeout value in minutes in the **Listen interval** field.
Specify the listener timeout value in the number of minutes that the integration listens for LDAP data with every connection. The integration stops listening for LDAP data after the connection exceeds the listen interval.
14. Select **Paging** checkbox to have the LDAP server split up LDAP attribute data into multiple result sets rather than submit multiple queries.
15. Under **Related Links**, click **Test Connection** to test the connection configuration.
16. Under **LDAP OU Definitions**, click **New** to define an organization unit (OU) definition for importing.
17. In the LDAP OU Definition New record, enter the name the integration uses when referencing this OU in the **Name** field.
The name you enter here becomes an LDAP target in the data source record.
18. Enter the relative distinguished name of the subdirectory you want to search in the **RDN** field.
This RDN is combined with the start-searching directory from the LDAP server definition to identify the subdirectory containing information for this organizational unit.
19. Enter the name of the attribute within the LDAP server to query for records in the **Query field**.
The query field must be unique in both single and multiple domain instances.
20. Select **Active** checkbox to activate the OU definition and to allow administrators to test importing data. However, the integration can only bring data into the system from active OU definitions.
21. Select server by clicking the search icon and select from the available list of servers.
22. Specify the table that receives the mapped data from your LDAP server.
23. Enter an LDAP filter string in the **Filter** field to select specific records to import from the OU.
24. Click **Submit**.
25. Under **Related Links**, click **Test Connection** to test the connection.
26. Click **System LDAP > Schedule Loads** to execute the users import schedule job.
27. From the listed LDAPs, click the LDAP you have imported.
28. In the Scheduled data Import window, click **Execute Now** .
For more information about how to configure LDAP, you can refer to the [ServiceNow documentation](#).

Configuring CyberArk in ServiceNow

If you want to use CyberArk application for authentication, you must configure cyberArk in ServiceNow.

Before you begin

If you use connect to NCM Self-Service option by using the ServiceNow credential store object with CyberArk as the external storage, the following components should be enabled.

- External credential store plug-in
- Discovery plug-ins
- ServiceNow IntegrationHub Standard pack Installer if you are using New York version

Procedure

CyberArk configuration procedures include both CyberArk and ServiceNow configuration tasks. For more information, see [ServiceNow documentation](#).

Viewing the MID Server Status

The ServiceNow MID server works as a communication bridge between the ServiceNow platform and NCM Self-Service plug-in.

About this task

Note: If you have log on by using the administrator credentials, then you need to be in the NCM Self-Service application scope. For information on how to select NCM Self-Service application scope, see [ServiceNow documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.

Procedure

1. Log on to the ServiceNow.
2. Click **MID Server > Dashboard**.

The MID server dashboard displays the basic information about the configured MID server.

MID Server Dashboard										
MID Server Status										
Name	Host name	Status	Validated	Version	Logged in user	Max memory used %	Mean CPU used %	Pending jobs	Processing jobs	
calm_subho	subhabrata-banerjee.dev.nutanix.com	Up	Yes	kingston-10-17-2017_patch12-11-28-2018...	midserver	7	0	137	0	

MID Server Issues						
MID Server	Short description	Issue source	State	Created	Last detected	Count
No records to display						

Figure 3: MID Server Dashboard

3. Check the **Status** column to view the status of the MID server.

Note: To perform any operations on the NCM Self-Service plug-in, the MID server status must be **Up** and the validation must be **Yes**.

What to do next

For detailed information about the MID server, see [MID Server Documentation](#).

Configuring Service Portal

Perform the following steps in Global Scope to configure Service Portal. This configuration is optional.

Procedure

1. Navigate to **Service Portal > Portals**

2. Click Service Portal.

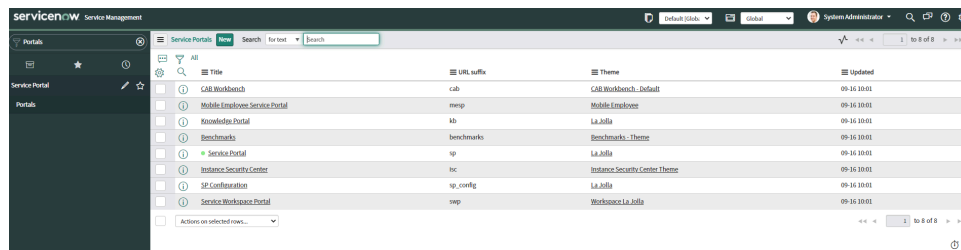


Figure 4: Service Portal

3. Navigate to the **Catalogs** tab and click **Edit**.

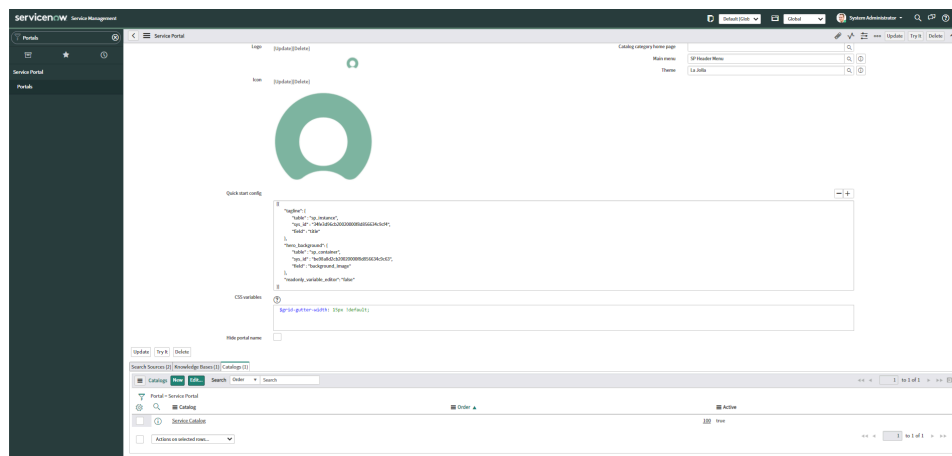


Figure 5: Catalogs

4. Search for **NCM Self Service** in the collection and drag it to catalog list.

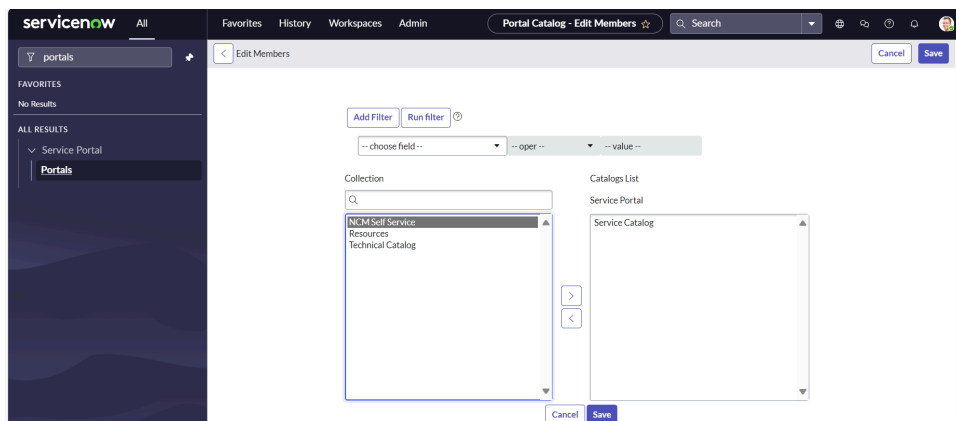


Figure 6: Collection

5. Click Save.

6. Click **Update** to update the changes.

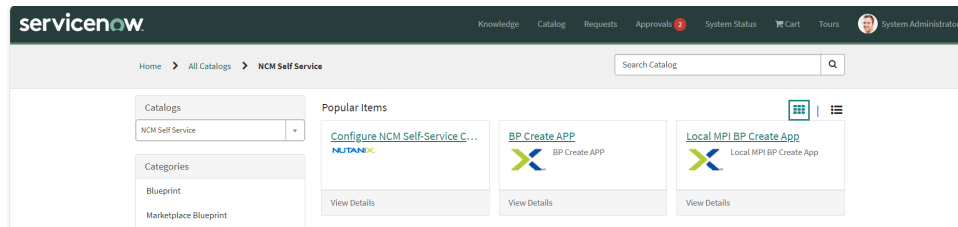


Figure 7: Blueprint

Note: To hide the Order Guide Catalog items on Service Portal, run the following script in the background.

```
var cat_sys_id
=[ '12f00e3337d12300fdcf097973990e35', 'b3800e3337d12300fdcf097973990e3c',
'd4d3da7f37d12300fdcf097973990e11', 'dae4cbd637512300fdcf097973990e0d' ];
for(var cat in cat_sys_id) {
var catalog_gr = new GlideRecord('sc_cat_item');
if(catalog_gr.get(cat_sys_id[cat])) {
catalog_gr.hide_sp = 'true';
catalog_gr.update();
}
}
```

Clustered MID Server for Load Balancing or Failover Support

MID Server clusters configuration enables the grouping of multiple MID Servers with the appropriate capabilities for load balancing and fail-over protection.

MID Server Capabilities

MID Server capabilities define the specific functions of a MID Server within an IP address range.

Several applications, such as Discovery, Service Mapping, Cloud Management, and Orchestration, can use capabilities, IP ranges, and MID Server selection to narrow the pool of MID Servers that the applications need.

Clusters Workflow

MID Servers in clusters must be able to connect to all the instances and devices with which it needs to communicate. Make sure all the MID Servers get added to any **Access Control List (ACL)** in use. MID Server clusters are managed by the **MID Server Cluster Management** business rule, which checks if the MID Server assigned to a job in the ECC Queue belongs to a cluster.

Load Balancing

- If the cluster business rule determines that a MID Server is part of a load balancing cluster, the application using the MID Server automatically balances the work between the MID Servers in that cluster.
- It is recommended to put MID Servers with the same capabilities in a load balancing cluster.

Fail-over Protection

- Each MID Server in a fail-over cluster has a configured order that the platform uses to determine the MID Server to be used next in the case of failure.

- MID Servers in a fail-over cluster work independently and do not load balance with other MID Servers in that cluster (although they might also be members of the load balancing clusters).
- When a MID Server fails, the MID-Server Cluster-Management business rule selects the highest available MID Server to take over the work. The selected MID Server checks the ECC Queue and starts with jobs that are either processing or ready.
- For performance and reliability reasons, do not use the following data sources with MID Server clusters:
 - LDAP
 - Export sets
 - JDBC data sources

Note: It is always preferred to have a different set of Mid Servers for Load Balancing and Fail-over protection.

MID Server Cluster Event

The following event is triggered when the platform cannot find a MID Server with the appropriate capabilities to replace a MID Server in a fail-over cluster. Use this event to notify the appropriate users about cluster failure through an email.

Event	Table	Description	Business Rule
mid_server.cluster.down	MID Server Cluster [ecc_agent_cluster]	A MID Server cluster has failed.	MID Server Cluster Management

Combining Clusters

You can add a MID Server to two types of clusters simultaneously. The following diagram shows a scenario where a MID Server from a load balancing cluster (MID Server D) is also present in a fail-over cluster. If MID Server D fails, MID Server E in the fail-over cluster becomes available to the load balancing cluster to perform the tasks previously assigned to MID Server D.

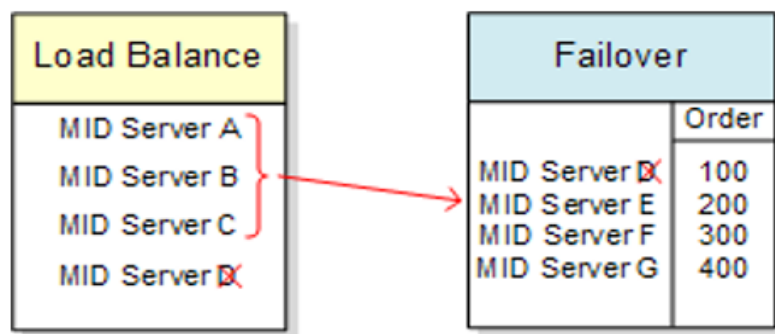


Figure 8: Combining Clusters

Configure a MID Server Cluster

- Group multiple MID Servers to form clusters, then configure clusters for fail-over protection or load balancing.

- Load-balancing clusters automatically balance work between each MID Server to improve stability and performance.
- Fail-over clusters have a configured order used to determine the MID Server to be used next if a failure occurs.
- Ensure that each MID Server in the cluster has the appropriate capabilities for the job. A MID Server in a fail-over cluster must have the same capabilities (or expanded capabilities) as the MID Server it is expected to replace.
- An administrator role is required to configure a MID server cluster.

For detailed information on setup, see [Configure a MID Server cluster](#) section in the [ServiceNow Documentation](#).

NCM Self-Service Plug-in Version Upgrade

The following table describes the version you must install to perform an upgrade from your current version to the latest version of NCM Self-Service plug-in.

Important:

- NCM Self-Service Plug-in supports only incremental upgrade. Any direct upgrade from an older version to the latest version is not supported.
- You must click the **Sync Now** button on the application properties page to trigger the migration after every upgrade. See [Sync Operation](#) on page 22.

Table 3: NCM Self-Service Plug-in Version Upgrade Summary

Upgrade from	Upgrade to V 1.3.2	Upgrade to V 1.4.2	Upgrade to V 1.4.3	Upgrade to V 1.4.4	Upgrade to V 1.4.5	Upgrade to V 1.5.1	Upgrade to V 1.5.2	Upgrade to V1.6	Upgrade to V1.6.1
V 1.3.2	Not Applicable	Yes	No	No	No	No	No	No	No
V 1.4.2	Not Applicable	Not Applicable	Yes	No	No	No	No	No	No
V 1.4.3	Not Applicable	Not Applicable	Not Applicable	Yes	No	No	No	No	No
V 1.4.4	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Yes	No	No	No	No
V 1.4.5	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Yes	No	No	No
V 1.5.1	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Yes	No	No
V 1.5.2	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Yes	No
V 1.6	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Yes

Installing NCM Self-Service Plug-in from the ServiceNow Store

You can install the plug-in directly from the ServiceNow store.

About this task

You can download the NCM Self-Service plug-in from the ServiceNow store. To refer to a video about downloading the plug-in, [click here](#).

Before you begin

Ensure that you meet the prerequisites before you install NCM Self-Service Plug-in. For more information, see [Prerequisites for NCM Self-Service Plug-in for ServiceNow](#) on page 5.

Procedure

1. Download the application from the ServiceNow store.
The platform auto-manages the installation and there is no need for fixing any errors or committing.
2. You can track the installation from **System Applications > Applications page**.

What to do next

After installation, the platform displays the detail of the application such as version number and state.

Configuring the Application Properties

Using the application properties, you can view and update the NCM Self-Service plug-in properties and the following attributes.

About this task

Note: If you have logged on by using the administrator credentials, then you need to be in the NCM Self-Service application scope. For more information about selecting a scope, see [ServiceNow Documentation](#). If you have not used the administrator credentials to log on, then the selection of the scope is automatically taken care by the platform.

- NCM Self-Service Instance URL: NCM Self-Service plug-in uses the mentioned URL to import all the NCM Self-Service resources.
- Approval Workflow: The system uses the approval workflow for approvals, when you create any request blueprint launch operation.
- Support URL: User can use the support URL to contact NCM Self-Service support.
- Logs: Administrator can set the logs that are displayed to the user.

Procedure

1. Log on to the ServiceNow.

2. Click **NCM Self-Service > Configuration > Application Properties** to view the NCM Self-Service application properties.

The screenshot shows the 'Plugin Properties' window for the Nutanix NCM Self-Service plugin. The window has a title bar with 'Plugin Properties' and buttons for 'Save Properties', 'Sync Now', and 'Delete Inventory'. The main content area is divided into two tabs: 'Configuration' (selected) and 'Action Workflow Configuration'. The 'Configuration' tab contains several fields and checkboxes:

- Plugin version:** v1.6.1
- Service Catalog:** NCM Self-Service
- Connect to NCM Self-Service on Public Cloud:** ☐
- MID Server:** dev124547_Mid_Server (with search and lock icons)
- NCM Self-Service Instance:** (with a lock icon)
- NCM Self-Service Version:** 3.7
- Use external credential system?** ☐
- Enable Service Portal:** ☒ (with a tooltip: 'Enabling this option allows you to launch the catalog item on service portal')
- NCM Self-Service Admin Username:** admin
- NCM Self-Service Admin Password:** (masked with asterisks)
- Show Help Text:** ☐

The 'Action Workflow Configuration' tab contains:

- Approval Workflow:** Nutanix - Auto Approve (with search and lock icons)
- Assignment Group:** Analytics Settings Managers (with search and lock icons)
- Support URL:** https:// (with a lock icon)
- Use Local Groups:** ☐
- Create Incidents?** ☒
- Log Verbosity:** Warning (dropdown menu)

At the bottom of the window are buttons for 'Save Properties', 'Sync Now', and 'Delete Inventory'.

Figure 9: Application Properties

3. The **Service Catalog** field displays the name of the service catalog item. The default value for the **Service Catalog** field is NCM Self-Service. The catalog name groups all the catalog items that are created in the ServiceNow application.
4. Do the following in the **MID Server** field.
 - a. Click the tooltip icon to view the MID server details.
 - b. Click the search icon to view the status of the MID server.

In the MID servers window, check the status column to determine whether the server is up or down.
5. Do the following in the **NCM Self-Service Instance** field.
 - a. Click the lock icon to edit the field.
 - b. Enter the URL of the NCM Self-Service instances that needs to be registered. For example, https://10.0.1.20:9440.
 - c. Click the unlock icon to lock the field.
6. Enter the administrator username in the **NCM Self-Service Admin Username** field.
7. Enter the administrator password in the **NCM Self-Service Admin Password** field.

8. Optionally, if you want to connect to NCM Self-Service by using the ServiceNow credential store object with CyberArk as the external storage, select the **Use external credential system?** checkbox. Selecting the **Use external credential system?** checkbox enables the **Credential** and **MID Application** fields.

Figure 10: Plug-in Properties

Do the following in the **Credential** field.

- Click the search icon to view the available credentials in the store.
- From the list of the available credentials, select the credential you want to use.

Do the following in the **MID Application** field.

- Click the search icon to view the available MID applications in the ServiceNow instance.
- From the list of the available MID applications, select the MID application you want to use.

By default, the **Show Help Text** checkbox is set to true to show annotations for all the fields and assist users to fill correct details.

9. Select the **Enable Service Portal** checkbox if you want to launch the Catalog item on the service portal.

10. Optionally, to connect to the cloud-based NCM Self-Service instance, select the **Connect to NCM Self-Service on Public Cloud** checkbox.

When you select the **Connect to NCM Self-Service on Public Cloud** checkbox, you can connect to NCM Self-Service instance directly without using the MID Server.

The screenshot shows the 'Plugin Properties' window for the NCM Self-Service plugin. The 'Service Catalog' is set to 'NCM Self-Service'. The 'Connect to NCM Self-Service on Public Cloud' checkbox is selected. The 'MID Server' field is set to 'dev124547_Mid_Server'. The 'NCM Self-Service Instance' field is empty, with a lock icon to its right. A blue banner below this field states: 'You cannot edit the NCM Self-Service Instance URL once it is successfully authenticated. Delete inventory (that cleans up the entire CMDB) re-enables edit option on NCM Self-Service Instance'. Below this, the 'NCM Self-Service Version' is '3.7', 'Use external credential system?' is unchecked, and 'Enable Service Portal' is checked. A blue banner below this states: 'Enabling this option allows you to launch the catalog item on service portal'. The 'NCM Self-Service Admin Username' is 'admin' and the 'NCM Self-Service Admin Password' is masked with dots. The 'Show Help Text' checkbox is unchecked. The 'Configuration' tab is active, showing 'Approval Workflow' as 'Nutanix - Auto Approve', 'Assignment Group' as 'Analytics Settings Managers', 'Support URL' as 'https://', 'Create Incidents?' as checked, 'Log Verbosity' as 'Warning', and 'Use Local Groups' as unchecked.

Figure 11: Plug-in Properties: Public Cloud

Do the following:

- a. Click the lock icon in the **NCM Self-Service Instance** field, and enter the URL of the NCM Self-Service instances that needs to be registered. For example, <https://10.0.1.20:9440>. Click the unlock icon to lock the field.
- b. Enter the administrator username in the **NCM Self-Service Admin Username** field.
- c. Enter the administrator password in the **NCM Self-Service Admin Password** field.

Note:

- For cloud-based NCM Self-Service instance, you need an API key to configure NCM Self-Service plug-in. You cannot configure the plug-in with a local user.
- The IDP configuration is not qualified for cloud-based NCM Self-Service instance.

11. Under the **Configuration** tab, do the following in the **Approval Workflow** field to select an approval workflow.

- a. Click the search icon and select the required workflow.

Workflows are defined for the following tasks.

- Auto approval workflow for Catalog Creation: Created on the table **sc_req_item**.
- Auto approval workflow for Catalog Launch: Created on the table **sc_req_item**.
- Auto approval workflow for Application action creation: Created on the table **x_nuta2_nutanix_ca_app_action_workflow_trigger**.

There are two approval workflows configured for:

- System: The type is set to *system*.
- User: The type is set to *user*.

Note:

- An Approver must have an **approval_user** role to approve the assigned request.
- You can customize workflows according to your requirements and use them within the plug-in. You can also create and use additional workflows on the mentioned tables.

- b. Click the tool tip icon to view details of the selected workflow.

12. From the **Assignment Group** dropdown menu, select an assignment group to whom the incident needs to be triggered for resolution.

When a request associated with a Catalog item creation or launch fails, an incident is created and assigned to the assignment group.

Note: To work on the assigned incident, the assignment group must have the *itil* or *sn_incident_read* role.

13. Do the following in the **Support URL** field.

- a. Click the lock icon to unlock the field.
- b. Enter the support URL to direct the users in failure instances.
The mentioned support URL is displayed in the support page.
- c. Click the unlock icon to lock the field.

14. Select **Create Incidents** checkbox to automatically create incidents in failure instances.

If the checkbox is not selected, then application only logs a message under logs and does not create an incident.

15. Select the applicable log to show the users from the **Log Verbosity** dropdown menu.

16. To assign the catalog item to the local ServiceNow group, click the **Use Local Groups** field.

- By default, the NCM Self-Service plug-in uses the LDAP groups that are imported using the AD or LDAP configured within ServiceNow for entitlement.
- Select the **Use Local Groups** checkbox to use the local groups that are created within ServiceNow for entitlement during the catalog creation process.

Note: If the NCM Self-Service administrator uses the local group support, users belonging to the local groups can be entitled to any catalog item along with applications and actions associated with it. All the requests carried out by local users on the ServiceNow side get processed as an admin user on the NCM Self-Service side.

17. Optionally, to manage the workflow of application actions in ServiceNow, click the **Enable/Disable workflow for action** checkbox and do the following.

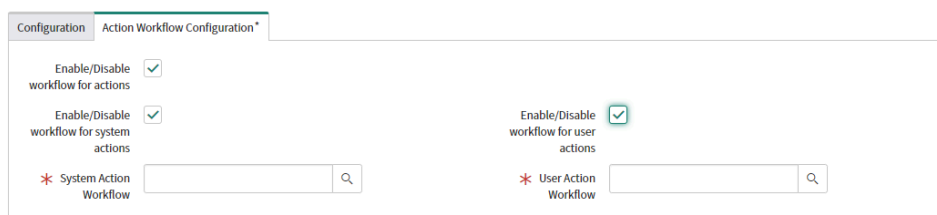


Figure 12: Action Workflow Configuration

The **Enable/Disable workflow for system actions** and the **Enable/Disable workflow for user actions** fields are available for selection.

- a. Click the **Enable/Disable workflow for system actions** field to trigger this workflow on any system action triggered by the user.
- b. Click the **Enable/Disable workflow for user actions** field to trigger this workflow on any user action triggered by the user.

Note: NCM Self-Service plug-in provides two default workflows as **Nutanix - User Actions Auto Approval** and **Nutanix - System Actions Auto Approval**. If you want to create a custom workflow for user or system action, you can create it on **Application Action Request** table after setting the value of `approval_status` as either approved or rejected. You must create the custom workflow as per the appropriate guidelines that Nutanix has defined for these workflows. For details about these guidelines, contact Nutanix Support.

18. Click **Save Properties** to save the application properties.
After the authentication is successful, **Sync Now** and **Delete Inventory** buttons are displayed and the **NCM Self-Service Version** field is automatically filled.
19. After you get the Authentication Successful message, click the **Sync Now** option to sync the data. See [Sync Operation](#) on page 22.

Sync Operation

The Sync operation imports NCM Self-Service resources such as projects, blueprints, marketplace items, applications, endpoints, runbooks, profiles, and actions.

You can run the sync operation after the application properties are configured and the authentication is successful. A NCM Self-Service administrator creates catalog items based on the data that the sync operation imports.

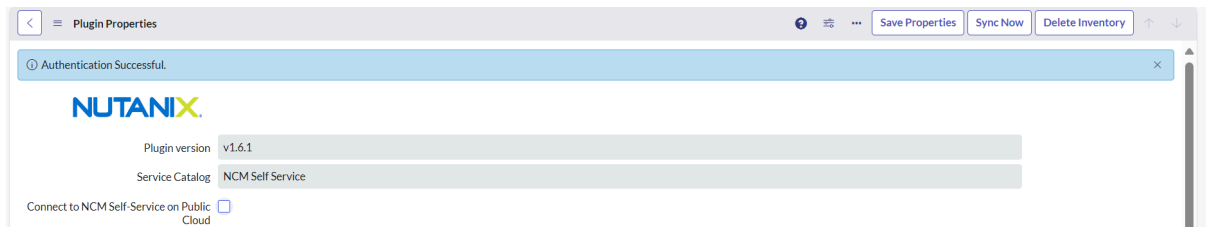


Figure 13: Sync Operation

Note: Whenever you perform a NCM Self-Service Plug-in version upgrade, you must run the sync operation to sync the data with NCM Self-Service.

The Sync Now option is not displayed in the following cases:

- When NCM Self-Service is not authenticated.
- When the sync or delete operation for the inventories is in progress.

Importing NCM Self-Service Resources Using the Sync Operation

The Sync operation imports NCM Self-Service resources such as projects, blueprints, marketplace items, applications, endpoints, runbooks, profiles, and actions so that the imported data can be used to create catalog items.

About this task

To optimize the inventory sync duration, the sync operation also provides the option to select individual NCM Self-Service entities and sync each of them separately. You can run the sync operation for Projects, Blueprints, Runbooks, Marketplace Items, or Applications at different times. You can also sync all the entities together.

Procedure

1. Log on to the ServiceNow.
2. Click **NCM Self-Service > Configuration > Application Properties** to view the NCM Self-Service application properties.
3. Click **Sync Now**.

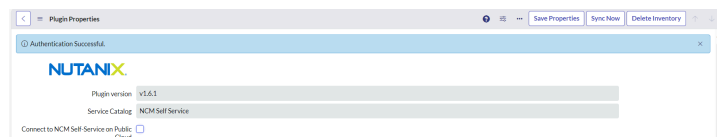


Figure 14: Sync Now

4. In the Sync Now window, select the NCM Self-Service entity that you want to sync with ServiceNow. Your options are:

- » All
- » Projects
- » Blueprints
- » Runbooks
- » Marketplace Items
- » Applications

5. Click **Sync**.

What to do next

You can view the status of the sync operation on the application properties page.

Inventory Sync

Inventory sync menu option is used to sync the ServiceNow application with the NCM Self-Service database. By using Inventory sync, you can do the following:

- View the draft and published blueprints. Only the active blueprints and published MPIs are synced.
- Run and view the jobs that are scheduled to run at a predefined time interval.

Inventory sync updates the following objects in Configuration Management Database (CMDB):

Table 4: Inventory Sync

Entity	Objects
Projects	<ul style="list-style-type: none">• Environments• Providers• Credentials
Blueprints	<ul style="list-style-type: none">• Blueprints• Marketplace blueprints
Applications	<ul style="list-style-type: none">• Actions• Run logs• Recovery points
Runbooks	<ul style="list-style-type: none">• Runbooks• Marketplace runbooks
Endpoints	

The following table lists the CMDB tables and the columns that are updated by NCM Self-Service Plug-in.

Table 5: CMDB Table

CMDB Table Label	CMDB Table Name	Field Label	Field Name
Service	x_nuta2_nutanix_ca_service	Name	name
		Cores per CPU	cores_per_cpu
		CPUs	cpus
		Memory (MB)	memory
		Provider	provider
		State	state
		IP Address	ip_address
Application	x_nuta2_nutanix_ca_nutanix_calm_application	Name	name
		UUID	uuid
		Application State	state
		Owner Reference	owner_reference
		Description	description
		Creation Time	creation_time
		Last Update Time	last_update_time
		Cloned From	cloned_from
		Application Cost	application_cost
IP Address	cmdb_ci_ip_address	IP Address	ip_address
		IP Version	ip_version

For detailed information about CMDB, see [Configuration Management Database Documentation](#).

Data Migration after Upgrading to Version 1.5 and later

NCM Self-Service Plug-in version 1.5 and later migration scenarios are controlled automatically.

- Blueprints that have common profile variables (variables with the same name) between multiple profiles are deleted, and the catalog items associated with the blueprints are marked inactive.
- Specific log messages are added in the log and on the Application Properties page.
- After the sync operation, the deleted blueprints are synchronized again and are made available for the catalog creation.

Inventory Negative Sync

NCM Self-Service plug-in for ServiceNow runs a scheduled or on-demand job to synchronize the NCM Self-Service entities, for example, blueprints, marketplace blueprints, projects, and applications with ServiceNow Configuration Management Database (CMDB).

Negative sync refers to the updating of ServiceNow CMDB after the corresponding entities in NCM Self-Service are removed or the state of the entity is changed. An onLoad script runs on the **Catalog Launch** page to check any changes in the entities.

The following table shows how a catalog item is impacted in ServiceNow after the sync when you make changes to the associated blueprint or Marketplace item in NCM Self-Service.

Table 6: Catalog Item Impact - Negative Sync

Impact	Changes in NCM Self-Service
Catalog Item Becomes Inactive	When the project associated with the catalog item is deleted.
	When the blueprint associated with the catalog item has only one project, and the project was deleted.
	When the blueprint associated with the catalog item has only one profile, and the project was deleted.
	When the blueprint associated with the catalog item is deleted.
	When the Marketplace item associated with the catalog item is deleted.
	When a new variable is added or an existing variable is deleted from the blueprint or runbook associated with the catalog item.
Catalog Item is Updated	When the private state of profile variable in the associated blueprint is changed.
	When the runtime-config of the profile variable in the associated blueprint is changed.
	When the type of the profile variable in the associated blueprint is changed.
	When the name of the profile variable in the associated blueprint is changed.
	When the catalog item has multiple projects within the blueprint and a project is deleted.
	The deleted profile becomes unavailable for selection during the ordering (launch) operation.
	When the catalog item has multiple profiles within the blueprint and a profile is deleted.
	The deleted profile becomes unavailable for selection during the ordering (launch) operation.

Impact	Changes in NCM Self-Service
Catalog Item Remains Unchanged	When the VM specifications (vCPU, Cores Per vCPU, or Memory) in the associated blueprint are updated.
	When the disk specifications are updated.
	When the network specifications in the associated blueprint are updated.
	When the categories defined in the associated blueprint are updated.
	When there is any addition or deletion of services in the blueprint associated with the catalog item.
	When there are any updates in the tasks or actions in the blueprint associated with the catalog item.

Note:

- If you change a variable in a blueprint that is already synced in ServiceNow, user with admin or x_nuta2_nutanix_ca.calm_admin role can delete blueprint from serviceNow by clicking the **Delete** button till the next sync operation is performed. It deletes the blueprint record from CMDB, and removes all its references on the plug-in side and the catalog item related to that blueprint is marked as inactive.
- The catalog items created from a marketplace item that is marked as draft are not affected by the negative sync.

Deleting Inventory

About this task

When you have successfully authenticated and synced the inventory, the **Delete Inventory** button appears.

Note: The NCM Self-Service admin must have the permission to use the **Delete Inventory** option.

You can only use the **Delete Inventory** option in the following cases:

- If you want to register a new NCM Self-Service instance for the plug-in.
- If it is essential to delete the entire plug-in synced data within ServiceNow.

Note: Data once deleted using the **Delete inventory** option will no longer be available in ServiceNow.

Schedule Jobs

Schedule Jobs are automated pieces of work that can be performed at either a particular time, or on a recurring schedule. Schedule jobs enable you to sync the NCM Self-Service plug-in with NCM Self-Service and update the ServiceNow database as per the job script.

Schedule jobs are accessible to a System Administrator with a “Write” role where the administrator can edit the job run duration and other conditions. Schedule jobs are also accessible to users with the NCM Self-Service Plug-in Admin role with a “Read” role where the user can only execute a schedule job. An NCM Self-Service Plug-in user cannot view or edit scheduled jobs.

The default setting is set to run the schedule job (Nutanix Import Inventories Job) daily at time 01:00 hours.

Note: You can also use the **Sync Now** button on the Application Properties page to sync the ServiceNow NCM Self-Service plug-in with NCM Self-Service.

Executing a Schedule Job

Scheduled jobs enable you to sync the NCM Self-Service plug-in with NCM Self-Service and update the ServiceNow database as per the job script.

About this task

Note: If you have log on by using the administrator credentials, then you need to be in the NCM Self-Service application scope. For information on how to select NCM Self-Service application scope, see [ServiceNow documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.

Procedure

1. Log on to the ServiceNow.
2. Click **NCM Self-Service > Inventory Sync > Schedule Jobs** to view the scheduled jobs.
3. Click the scheduled job to view the job details.
4. Click **Execute Now** to run the job.
After the data is imported in the NCM Self-Service plug-in, you can browse to blueprint and marketplace to view the imported data and assign these catalog items to the users as a runtime variable.

Viewing Nutanix Projects

The Nutanix Projects window displays the list of available projects in the NCM Self-Service plug-in. You can also view the blueprints associated with a project.

About this task

Note:

- If you have log on by using the administrator credentials, then you need to be in the NCM Self-Service application scope. For information on how to select NCM Self-Service application scope, see [ServiceNow documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.
- The NCM Self-Service v1.3 plug-in provides support for multi-PC architecture in NCM Self-Service.

Procedure

1. Log on to the ServiceNow.
2. Click **NCM Self-Service > Inventory Sync > Nutanix Projects** to view the projects.

- Click the project name to view the project details.

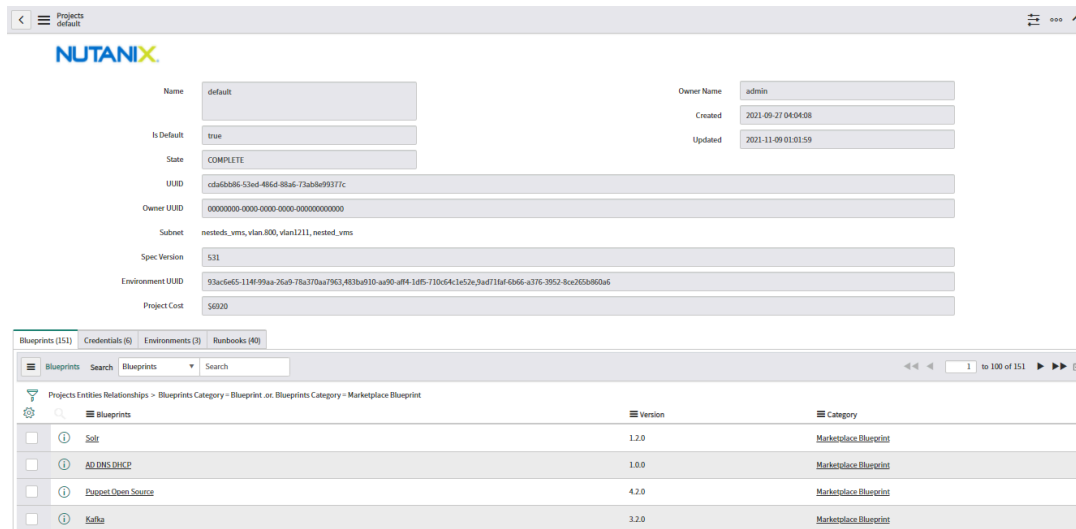


Figure 15: NCM Self-Service Projects

The list of associated blueprints, marketplace blueprints, environments, runbooks, and marketplace runbooks is displayed at the bottom.

Viewing Nutanix Blueprints

The Nutanix Blueprints window displays the list of blueprints available in the NCM Self-Service plug-in. From this window, you can also view the list of available variable and application profiles associated with a blueprint.

About this task

Note: If you have log on by using the administrator credentials, then you need to be in the NCM Self-Service application scope. For information on how to select NCM Self-Service application scope, see [ServiceNow Documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.

Procedure

- Log on to the ServiceNow.
- Click **NCM Self-Service > Inventory Sync > Blueprints** to view the blueprints.
The list of active blueprints is displayed.

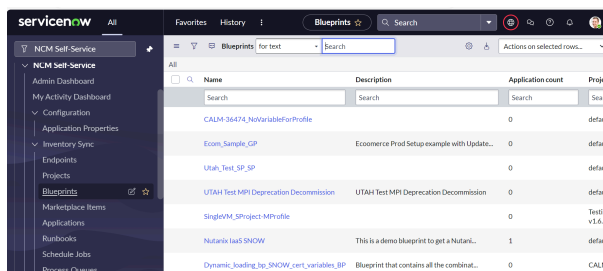


Figure 16: Nutanix Blueprints

3. Click the blueprint name to view the blueprint details.

The list of available variables and application profiles is displayed at the bottom.

Nutanix Marketplace Items

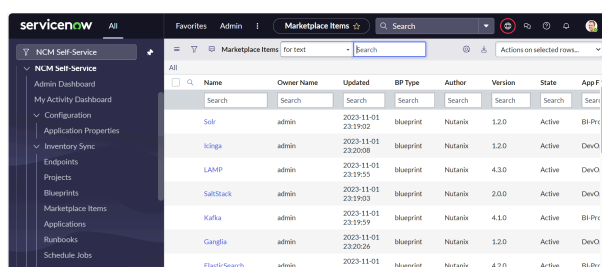
The Nutanix Marketplace Items window displays the list of published MPIs available in the NCM Self-Service plug-in. From this window, you can also view the list of available variable and associated application profiles available in a blueprint.

About this task

Note: If you have log on by using the administrator credentials, then you need to be in the NCM Self-Service application scope. For information on how to select NCM Self-Service application scope, see [ServiceNow Documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.

Procedure

1. Log on to the ServiceNow.
2. Click **NCM Self-Service > Inventory Sync > Marketplace Items** to view the blueprints.



Name	Owner Name	Updated	BP Type	Author	Version	State	App F
Sole	admin	2023-11-01 23:19:02	Blueprint	Nutanix	1.2.0	Active	BI-Pr
Kafka	admin	2023-11-01 23:20:08	Blueprint	Nutanix	1.2.0	Active	DevO
LAMP	admin	2023-11-01 23:19:05	Blueprint	Nutanix	4.3.0	Active	DevO
SelfStack	admin	2023-11-01 23:19:03	Blueprint	Nutanix	2.0.0	Active	DevO
Kafka	admin	2023-11-01 23:19:09	Blueprint	Nutanix	4.1.0	Active	BI-Pr
Ganglia	admin	2023-11-01 23:20:26	Blueprint	Nutanix	1.2.0	Active	DevO
ElasticSearch	admin	2023-11-01 23:20:32	Blueprint	Nutanix	4.2.0	Active	BI-Pr

Figure 17: Nutanix Marketplace Items

3. Click the MPI name to view the MPI details.

The list of available variables and application profiles is displayed at the bottom.

Viewing Nutanix Applications

The applications window displays the list of applications available in the NCM Self-Service plug-in.

About this task

Note: If you have log on by using the administrator credentials, then you need to be in the NCM Self-Service application scope. For information on how to select NCM Self-Service application scope, see [ServiceNow Documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.

Procedure

1. Log on to the ServiceNow.
2. Click **NCM Self-Service > Inventory Sync > Applications** to view the deployed applications.

3. Click the application name to view the application details.

You can view the list of available actions, recovery points, and audit logs.

Note:

- Recovery Points tab is only available for single VM applications running on Nutanix and VMware cluster.
- AMIs tab is only available for single VM applications running on AWS cluster.

Catalog Item Creation

NCM Self-Service administrator can use the catalog item creation feature to mark the attributes while creating the catalog item so that those attributes can be modified at the time of launching the application blueprint. NCM Self-Service administrator has access to runtime configuration flow to create a catalog item and performs user entitlement. From this window, administrator can also assign a catalog item to the users.

Assigning a Blueprint, Runbook, or MPI to a User

Perform the following procedure to assign a blueprint, runbook, or MPI to a user.

About this task

Note: If you have log on by using the administrator credentials, then you need to be in the NCM Self-Service application scope. For information on how to select NCM Self-Service application scope, see [ServiceNow Documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.

You can also upload a custom logo for Marketplace items, unpublished blueprints, and runbooks while assigning a catalog item.

Procedure

1. Log on to the ServiceNow.
2. Click **NCM Self-Service > Catalog Management > Catalog Items**.
3. Click **New**.

Note: The **New** button is not displayed when an inventory sync or deletion is in progress.

4. In the **Select Type of Blueprint/Runbook to Configure** field, select one of the following.
 - **Blueprints:** To assign an active blueprint to a user, an administrator can view the list of active blueprints in the **Blueprints** option under the **Inventory Sync** menu.
 - **Marketplace blueprints:** To assign a marketplace blueprint to a user, an administrator can view the list of published blueprints in the **Marketplace Items** option under the **Inventory Sync** menu.
 - **Runbooks:** To assign an active runbook to a user, an administrator can view the list of active runbooks in the **Runbooks** option under the **Inventory Sync** menu.
 - **Marketplace runbooks:** To assign a marketplace runbook to a user, an administrator can view the list of published runbooks in the **Marketplace Items** option under the **Inventory Sync** menu.

5. If the type is **Blueprints** or **Marketplace blueprints**, then do the following:

- a. Click the **Click to add...** link under the Upload Custom Logo section to select and add the custom logo.
The supported file formats for the logo are .png, .jpg, .jpeg, and .svg. The minimum acceptable unit of image resolution is 100 px by 100 px and the maximum acceptable file size is 200 KB.
The uploaded logo also appears as an icon in Catalogs and Service Portal.
- b. From the **Blueprint** dropdown list, select a blueprint or marketplace blueprint.
- c. From the **Project** dropdown list, select a project.
 - In the case of a single project associated with blueprint, the project gets updated automatically on the list.
 - In the case of multiple projects associated with the blueprint, you get an option to select a project from the available list.
- d. From the **Environment** dropdown list, select an environment from the available list.
- e. From the **Application Profile** dropdown list, select an application profile for a blueprint or MPI.
 - In the case of a single profile associated with the blueprint, the profile gets updated automatically on the list.
 - In the case of multiple profiles associated with the blueprint, you get an option to select a profile from the available list.
- f. Click **Choose Options**.
In the **Choose Options** window, the available fields in the **Variables**, **Service configuration**, **Credentials**, and **General Settings** tabs are dynamic. The available fields for the tabs may differ for each blueprint.

Note: Advance variable support is available for NCM Self-Service v2.7 or above.
- g. Under the **General Configuration** tab, do the following.
 - In the **Item Name** field, enter the item name.
 - (Optional) In the **Description** field, update the description for the catalog in the markdown format.
 - In the **Assign User** field, click the lock icon to unlock the **Assign User** field.
 - In the **Assign Group** field, click the lock icon to unlock the **Assign Group** field.
 - Click the lock icon to unlock the **Support URL** field.
- h. In the **Choose Options** window, enter the values for all the mandatory fields.
- i. Click **Checkout**.
The catalog item is assigned to a user or group.

6. If the type is **Runbooks** or **Marketplace runbooks**, then do the following:

- a. Click the **Click to add...** link under the Upload Custom Logo section to select and add the custom logo.
The supported file formats for the logo are .png, .jpg, .jpeg, and .svg. The minimum acceptable unit of image resolution is 100 px by 100 px and the maximum acceptable file size is 200 KB.
The uploaded logo also appears as an icon in Catalogs and Service Portal.
- b. From the **Runbook** dropdown list, select a runbook or marketplace runbook.
- c. From the **Project** dropdown list, select a project.
 - In the case of a single project associated with the runbook, the project gets updated automatically on the list.
 - In the case of multiple projects associated with the runbook, you get an option to select a project from the available list.
- d. From the **Endpoint** dropdown list, select an endpoint from the available list.
- e. Click **Choose Options**.
In the **Choose Options** window, the available fields in the **Variables** and **General Settings** tabs are dynamic. The available fields for the tabs may differ for each runbook.
- f. Under the **General Configuration** tab, do the following.
 - In the **Item Name** field, enter the item name.
 - (Optional) In the **Description** field, update the description for the catalog in the markdown format.
 - In the **Assign User** field, click the lock icon to unlock the **Assign User** field.
 - In the **Assign Group** field, click the lock icon to unlock the **Assign Group** field.
 - Click the lock icon to unlock the **Support URL** field.
- g. In the **Choose Options** window, enter the values for all the mandatory fields.
- h. Click **Checkout**.
The catalog item is assigned to a user or group.

Available Actions on a Catalog Item

The following actions are available on a catalog item.

- **Launch:** Launches the catalog item.
- **Edit:** Edits the catalog item.
- **Delete:** Deletes the catalog item.

Note: Delete action is an irreversible action, that means the deleted catalog items cannot be retrieved. However, you can view the deleted catalog items by clicking the **Show Deleted Catalogs** button.

- **Move to Draft:** Moves the catalog item to draft stage and the item is not available to the entitled users. After moving the catalog item to draft, the item appears as **Active catalog item**.
- **Active Catalog Item:** Reactivates the draft catalog item. This action appears when the catalog item is in draft stage.

Viewing Application Action Request Details

Perform this procedure to track the approval state of an action performed on an application. If any action is performed by user, it go for the approval flow. We can check our action approval state here.

Procedure

1. Log on to the ServiceNow.
2. Click **NCM Self-Service > Tracking > Application Action Requests > .**

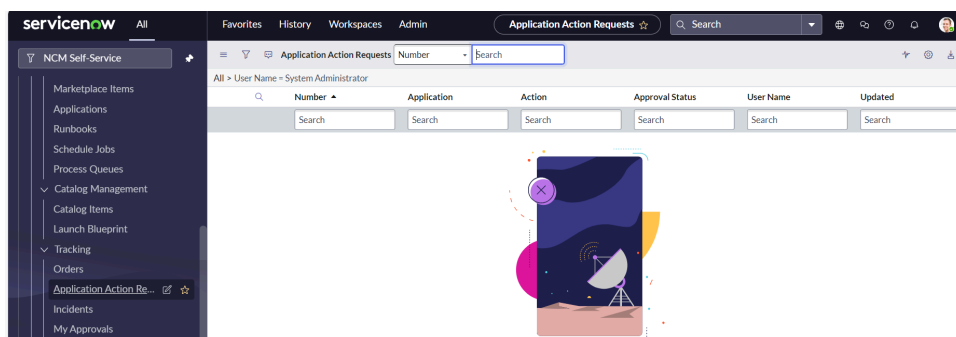


Figure 18: Application Action Request

The **Application Action Requests** page displays the list of actions performed by users.

Viewing Support Details

NCM Self-Service administrator and end-user can access the NCM Self-Service support contact details.

About this task

If you have log on by using the administrator credentials, then you need to be in the NCM Self-Service application scope. For information on how to select NCM Self-Service application scope, see [ServiceNow Documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.

Note:

The NCM Self-Service Plug-in is certified on the vanilla ServiceNow instances. If your ServiceNow instance is customized in anyway and that customization affects the NCM Self-Service Plug-in, Nutanix cannot provide support in such cases.

In addition, if you modify files in the NCM Self-Service Plug-in or modify the files that are generated by the NCM Self-Service Plug-in, it might result in failures in the functionality or the upgrade. Nutanix will not be responsible for any breakage in the product functionality caused by such modifications and cannot provide support for such scenarios.

As a best practice, you must install and use the NCM Self-Service Plug-in on a plain, vanilla ServiceNow instance first to ensure that the basic use cases of catalog creation and catalog consumption are working as expected.

Procedure

1. Log on to the ServiceNow.

2. Click **NCM Self-Service > Support > Contact Support**.

The contact support detail is displayed.

Contact Support

Nutanix

Important:- Perform action mentioned against your role.

Your Role	Action
Non-Admin Users	Report to Admin Users.
Admin Users	Check The Error Logs and Consult The Documentation. If issue is not Resolved or not mentioned in the Document Contact us by visiting The Portal at Nutanix ServiceNow Plugin support website

Note:- Use This Option Only When Required.

Figure 19: Support Details

Viewing Logs

Logs module is visible to both NCM Self-Service administrator and end user. From the Logs menu, user can access the following options:

About this task

- Emails: To view the various notifications sent or received.
- User Logs: To view the error details.

Note: If you have log on by using the administrator credentials, then you need to be in the NCM Self-Service application scope. For information on how to select NCM Self-Service application scope, see [ServiceNow Documentation](#). If you have not used the administrator credentials to log on, then the selection of scope is automatically taken care by the platform.

Procedure

1. Log on to the ServiceNow.
2. Click **NCM Self-Service > Logs > Emails or User Logs**.

The logs detail is displayed.

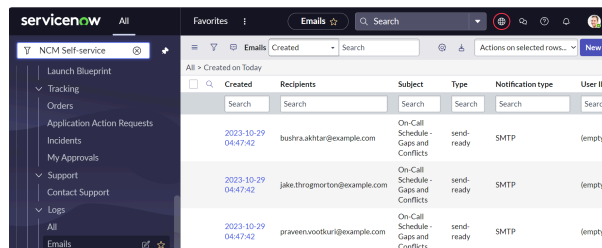


Figure 20: Email Logs

COPYRIGHT

Copyright 2023 Nutanix, Inc.

Nutanix, Inc.

1740 Technology Drive, Suite 150

San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.