



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Atos Syntel

Website: www.atos-syntel.net

Name of Product: SyntBots

Version: v2.3

Date: 19 November 2019 (4 November 2020)

SYNTBOTS OVERVIEW

SyntBots is an automation platform which is used to automate IT operations across different services like Infra/Application support, DevOps, and Process automation.

The latest version is SyntBots v2.3

The major components of the platform are:

- SyntBots Process Orchestrator Server
- SyntBots Services & Portal Server
- SyntBots Agent

KEY BENEFITS

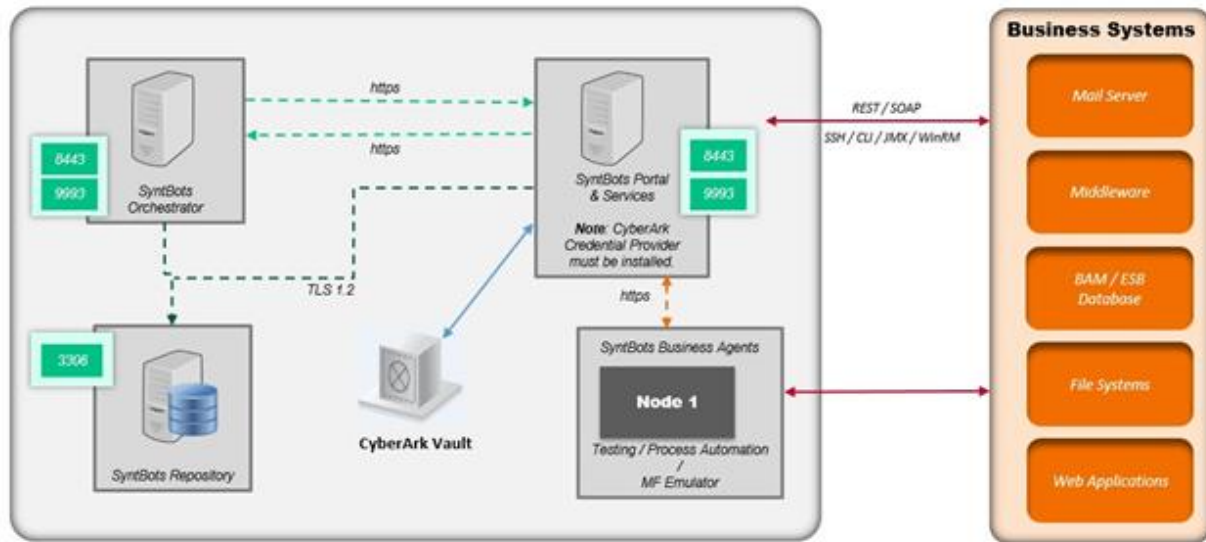
SyntBots is a **Robotic Process Automation (RPA)** platform which helps in automating the bots with the help of SSM and Agent components. A **Bot** is an automation script/application that is developed and placed in the SyntBots Agent.

- This RPA platform allows tasks to be completed faster.
- SyntBots is flexible and simple to use.
- Lower human involvement lessens the risk of errors and mistakes.

SyntBots platform uses Database to store credentials. With the CyberArk integration, the credentials related to the working of the bot are stored and fetched from the CyberArk Vault.

- It is considered to be very secure because the CyberArk Agent installed in the host machine makes a secure connection with the Vault to fetch the credentials.
- Level of decrypting the password is difficult.
- It is highly confidential because we cannot create a connection with the vault unless the bot is triggered.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

Secrets Manager is integrated with SyntBots Service Manager (SSM/Portal).

Location of integration: Mid-Tier or Central Server

SSM acts as the mid-tier to connect with the Vault.

CREDENTIAL RETRIEVAL

When an RPA bot that needs to fetch the credentials from CyberArk is triggered, it checks for the parameters in SSM/Portal and sends it to the Vault which in turn fetches the details and provides it to the agent component for the execution.

The CyberArk Agent installed in the host machine (where SSM is set up) helps in making a connection between SyntBots platform and the CyberArk Vault.

The credential is retrieved only when the bot is triggered for execution.

Currently the SyntBots platform is developed to support on Windows and is working on compatibility for additional platforms.

SECRETS MANAGER INSTALLATION

Refer to the [“Credential Provider and ASCP Implementation Guide” for CyberArk Agent based installation and configuration.](#)

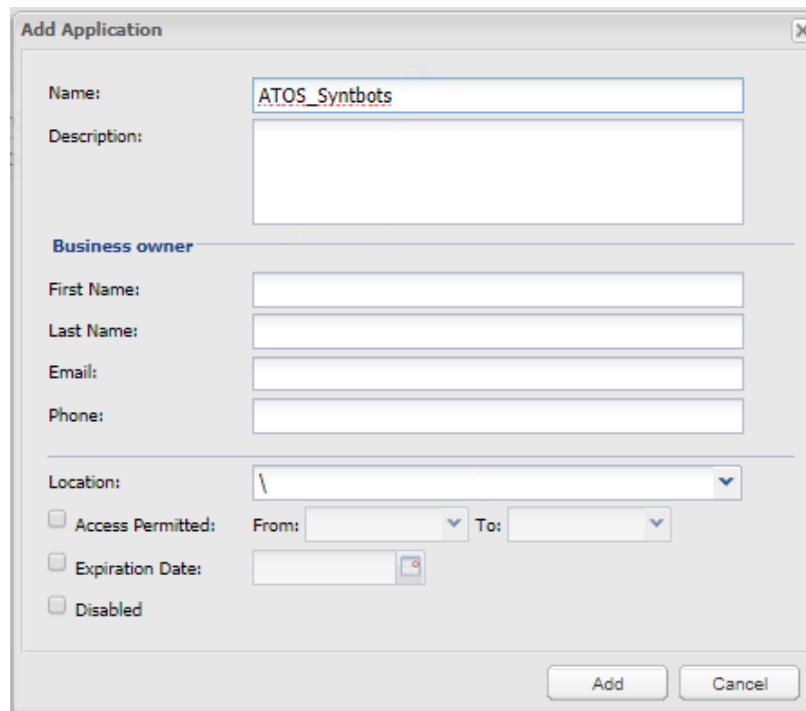
SECRETS MANAGER CONFIGURATION

The following sections provide details on SyntBots configuration with CyberArk Secrets Manager.

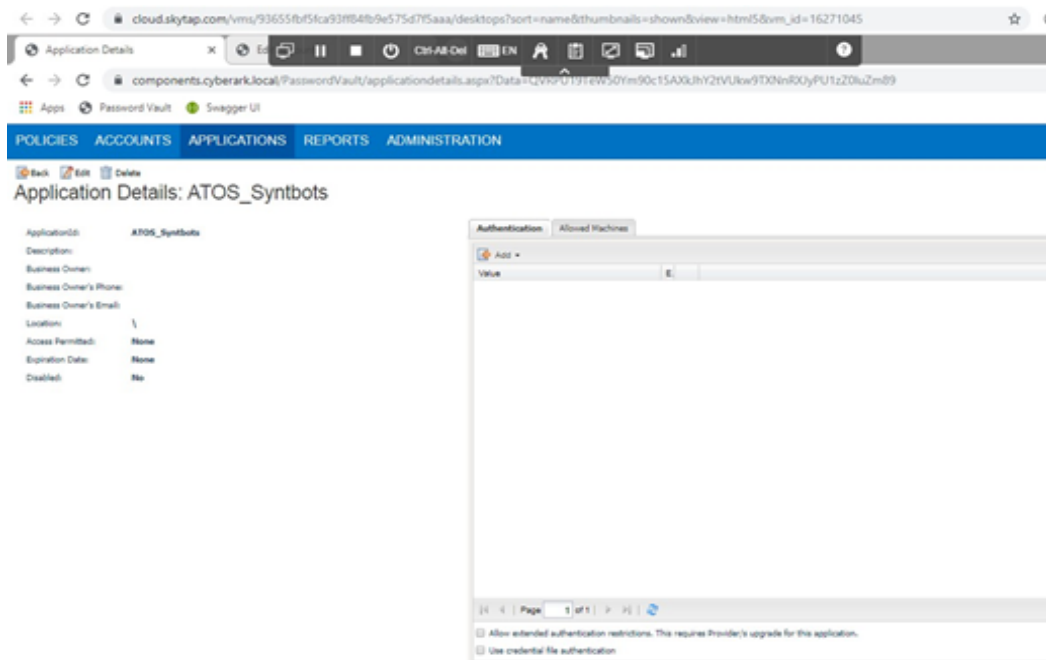
DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

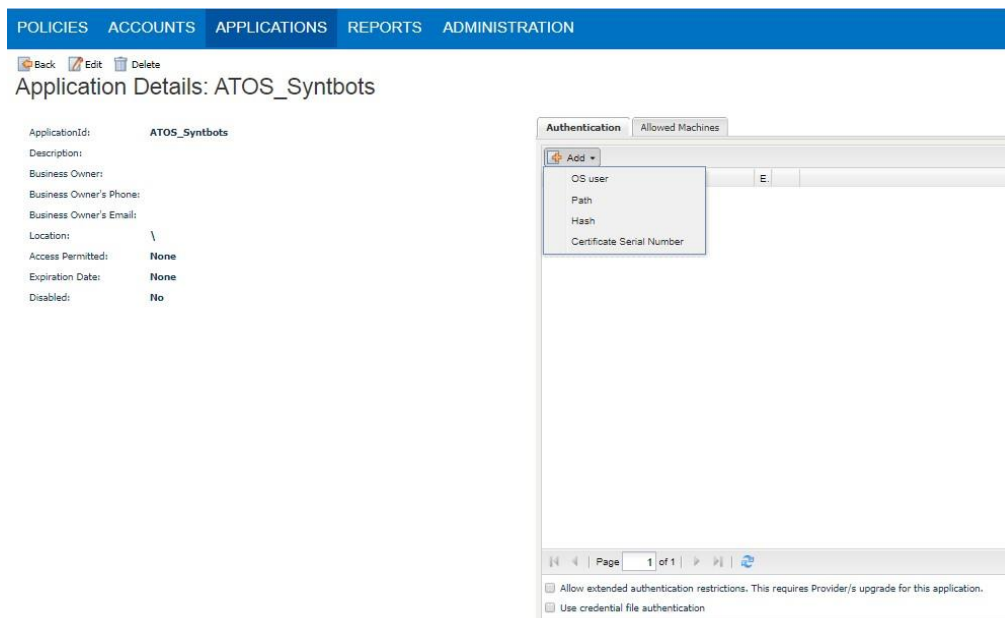
- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



- ☐ Specify the following information:
 - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: ATOS_Syntbots
 - In the **Description** box, specify a short description of the application that will help you identify it.
 - In the **Business owner** section, specify contact information about the application's business owner.
 - In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.

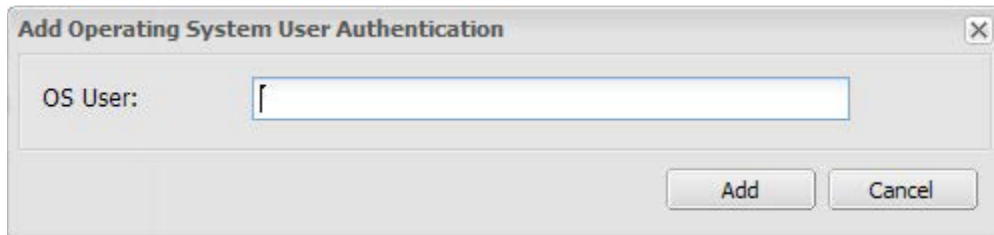


- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. Partner should suggest the authentication details to secure the access by the partner's application.



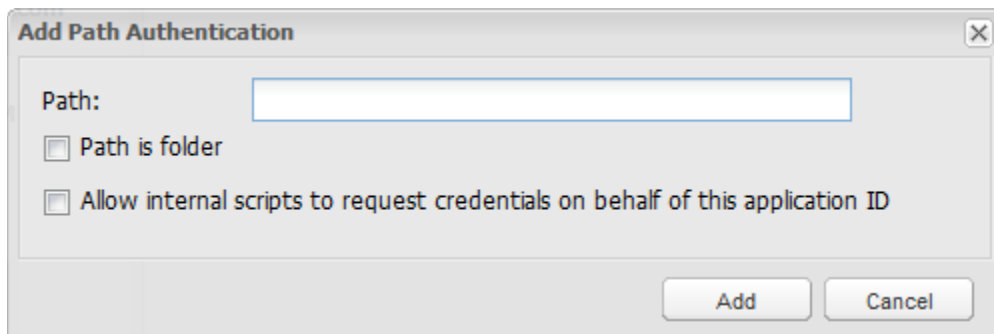
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.

- ☐ Select the authentication characteristic to specify.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.



The dialog box is titled "Add Operating System User Authentication". It contains a label "OS User:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Select **Path**. The Add Path Authentication window appears.



The dialog box is titled "Add Path Authentication". It contains a label "Path:" followed by a text input field. Below the input field, there are two checkboxes: "Path is folder" and "Allow internal scripts to request credentials on behalf of this application ID". At the bottom right, there are two buttons: "Add" and "Cancel".

- ☐ In the **Path** box, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.
- ☐ Click **Add**. The Path is added as an authentication characteristic with the information that you specified.

- ☐ Specify a hash:
 - Run the AIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is returned by the utility.
 - In the PVWA, select **Hash**. The Add Hash window appears.



The dialog box is titled "Add Hash Authentication". It contains a label "Hash:" followed by a text input field. The input field contains the hash value "F7A5215FB5F88F7165C418F1C0FF116697F81165". At the bottom right, there are two buttons: "Add" and "Cancel".

- In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.

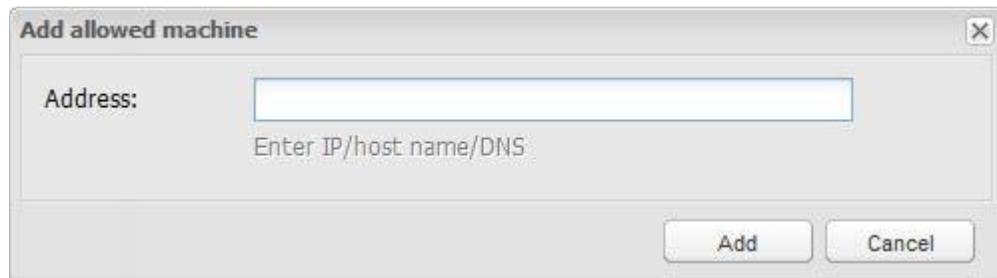
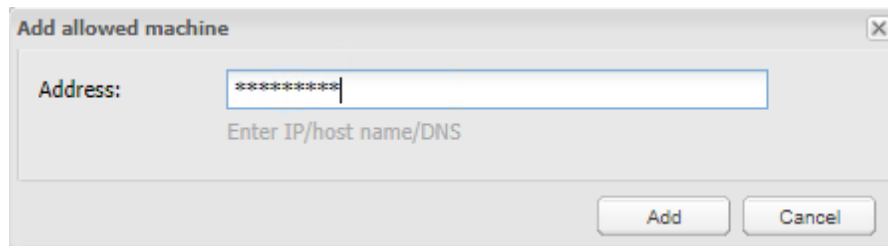
For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2

Note: The comment must not include a colon or a semicolon.

- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.

☐ Specify the application's Allowed Machines. This information enables the Credential Provider to make sure that only applications that run from specified machines can access their passwords.

- In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.

A screenshot of a Windows-style dialog box titled "Add allowed machine" with a close button (X) in the top right corner. Inside the dialog, there is a label "Address:" followed by a text input field. Below the input field, there is a hint text "Enter IP/host name/DNS". At the bottom right of the dialog, there are two buttons: "Add" and "Cancel".A screenshot of the same "Add allowed machine" dialog box. The text input field now contains a series of asterisks (*****), indicating that the input is masked. The rest of the dialog, including the "Address:" label, the hint text "Enter IP/host name/DNS", and the "Add" and "Cancel" buttons, remains the same.

- In the **Address** box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab.

Make sure the servers allowed include all mid-tier servers or all endpoints where the Secrets Manager Credential Providers were installed.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

- **Manually** – Add accounts manually one at a time, and specify all the account details.
- **Automatically** – Add multiple accounts automatically using the Password Upload feature.

For this step, you require the **Add accounts** authorization in the Password Safe.

POLICIES ACCOUNTS APPLICATIONS REPORTS ADMINISTRATION

Add Account

Store in Safe: Test
Device Type: Operating System
Platform Name: Windows Desktop Local Accounts

Required Properties:
Address: 10.0.1.20
Username: AS5044762

Optional Properties:
☐ Logon To:
☐ Location:
☐ Owner Name:

Password Content
Password: *****
Confirm Password: *****
Name: ☒ Auto-generated (Name pattern: DeviceType-PolicyID-Address-Username-vty-DSIN-ServiceName-TaskName-SystemNumber-Client)
☐ Custom

☐ Disable automatic management for this account
Reason:

Save Cancel

For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide**.

Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

☐ Add the Provider user as a Safe Member with the following authorizations:

- List accounts
- Retrieve accounts
- View Safe Members

Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

Add Safe Member

Search: Search In: **Vault**

Selected Search: Display 41 result(s)

	Name	Business Email	Full Name
	Vault Admins		
	Pro/_COMPONENTS		
	[REDACTED]		
	[REDACTED]		
	[REDACTED]		
	[REDACTED]		
	[REDACTED]		

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☒ View Safe Members

☐ Workflow

☐ Add the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve accounts

Add Safe Member

Search: Search In: **Vault**

Selected Search: Display 41 result(s)

	Name	Business Email	Full Name
	SCIM-user		
	Client-user		
	PasswordManager		
	ATOS_Syntbots		
	Atos_Syntel_testing		
	Backup		
	Operator		
	--		

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

☐ Workflow

- ☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

SYNTBOTS INSTALLATION & INTEGRATION CONFIGURATION

Refer to SyntBots for SyntBots installation.

APPLICATION REGISTRATION:

For any bot to be executed, it needs to be registered with its respective details in SSM. When the bot is triggered, the agent component fetches these details for its execution. To register an application, complete the following steps:

- Navigate to Process Automation > Application Registration in SSM.
- Feed all the necessary data for the application.
- To register the application that will fetch the credential from CyberArk, select CyberArk_Credential in Id for Update Operation and Id for Read Operation.
- Provide a CyberArk Username for the application that is to be registered.

The screenshot shows the SyntBots web interface with the 'Application Details' modal form open. The form contains the following fields and options:

- Application Code***: AS005
- Application Name***: FinanceDemo
- Id for update Operation***: Cyberark Credential (dropdown)
- Id for Read Operation***: Cyberark Credential (dropdown)
- Window Focus Required***: ☐ Yes ☒ No
- Bot Type***: Web (dropdown)
- Cyberark Username***: SM5050573
- Active Sessions Per UserId***: -1 (dropdown)
- Multiple Instance Restriction per Node***: ☐ Yes ☒ No
- Session Time Out*(mins)**: -1 (dropdown)
- Keep Session Alive***: ☐ Yes ☒ No

At the bottom of the modal are 'Save' and 'Cancel' buttons. The background shows the 'Application Registration' table with columns for Application Code, Application Name, and Window Focus Required.

- Click Save. It gets added to the database.

PARAMETERS TO BE ADDED IN SSM:

In order the fetch the credentials, the CyberArk Vault needs certain values which is fed to SSM. When the bot is triggered which is related to CyberArk Credential, SSM fetches the details for the parameters mentioned below to make a connection with the vault.

- CyberArkAppID
- CyberArkSafe
- CyberArkFolder

- CyberArkObjectVal
- CyberArkReason

Ensure that the respective values are passed to the above parameters in Syntbots Service Manager.

- Traverse through Administration > System Configuration > Group Entries Setup.
- Search for rpa_agent_props_group in General Group Header List.

The screenshot shows the SyntBots web application interface. The top navigation bar includes the SyntBots logo, user information (Welcome SuperAdmin, Last login: 26 Sep 2019 11:19:17), and links for Change Password and Sign Out. The main navigation menu includes HOME, ADMINISTRATION, PROCESS MANAGEMENT, PROCESS CONFIGURATION, PROCESS AUTOMATION, REPORTS, and HELP. The breadcrumb trail indicates the current location: Administration > System Configuration > Group Entries Setup.

The 'General Group Header List' section is displayed, featuring a search bar with the value 'rpa'. The table below shows one entry:

Group Id	Group Name	Group Description	Deleted	Actions
2	rpa_agent_props_group	RPA Agent Properties Group	No	

Below the table, it states 'Showing 1 to 1 of 1 entries (filtered from 28 total entries)'.

The 'Group Details List' section is also visible, with a search bar containing 'cyberark'. The table below shows five entries:

Group Detail Id	Group Detail Name	Group Detail Description	Deleted	Actions
376	cyberarkReason		No	
375	cyberarkObjectVal		No	
374	cyberarkFolder		No	
373	cyberarkSafe		No	
372	cyberarkAppID		No	

Below the table, it states 'Showing 1 to 5 of 5 entries (filtered from 170 total entries)'.

- Add the values by clicking on the icon in Group Details List.

PARTNER CONTACT INFO

Business Contact	Name	Meenakshisundaram Chinnappan
	Email	meenakshisundaram.chinnappan@atos.net

	Tel	
Technical Contact	Name	SaswatKumar Sahoo
	Email	saswat-kumar.sahoo@atos.net
	Tel	
Support Contact	Name	Ambikeswari Sundarvel
	Email	ambikeswari.sundarvel@atos.net
	Tel	