

# BeyondTrust Password Safe Enterprise Integration with ServiceNow

The BeyondTrust Password Safe Enterprise integration with ServiceNow provides organizations the ability to seamlessly request and approve access to managed systems and accounts, all without having to change user interfaces whilst adhering to a company's incident and change management processes.

A ServiceNow user can request to check out credentials or sessions for privileged accounts managed by Password Safe, using any of the ITSM access approval flows: Incident, Change Request, and Problem. The user only gains access to the asset and the privileged account that was requested and approved. Once approved, the user can initiate an RDP or SSH session right from ServiceNow using their native connectivity tools, such as Remote Desktop Connection or Putty.

## Key Features

- Validate ticket before access.
- Auditing around who approved the request and to which privileged account and asset.
- Request to check out credentials or sessions for privileged accounts managed by Password Safe.
- Opening a session checks approval status before allowing privileged user access.
- All actions now take place within ticket/incident, such as request, approve and open session, consistent with the RS and PRA integration.
- Allows you to configure the ticket types, such as Incident, Change, Request, Problem, and Request.
- Workspace views support (e.g. Service Operations Workspace).
- Simplified installation and configuration.
- Users cannot impersonate another account or launch a session logged in as a different requestor, which prevents unauthorized access.

## Requirements for the ServiceNow Integration with BeyondTrust Password Safe

Outlined below are requirements for the BeyondTrust Password Safe and ServiceNow integration. If any of the integration requirements are not yet met, they must be in place prior to starting the integration setup process unless the associated features of the integration are not required.

- ServiceNow instance with:
  - Version currently supported by ServiceNow.
  - A working Service Desk and/or change management application.
  - Administrative access to the ServiceNow portal.
- BeyondTrust Password Safe Cloud instance or BeyondInsight appliance with:
  - Version 22.2 or higher.
  - If using a BeyondInsight appliance, a ServiceNow MID Server might be required.
  - Administrative access in the Password Safe console.

- Network firewall rules to allow:
  - If using BeyondInsight appliance and ServiceNow MID Server, TCP port 443 traffic for the appliance to the MID Server must be allowed in both directions for the SOAP web service.

**i** For more information on MID Servers, please see [MID Server](https://docs.servicenow.com/en-US/bundle/utah-servicenow-platform/page/product/mid-server/concept/mid-server-landing.html) at <https://docs.servicenow.com/en-US/bundle/utah-servicenow-platform/page/product/mid-server/concept/mid-server-landing.html>.

## Configure Password Safe

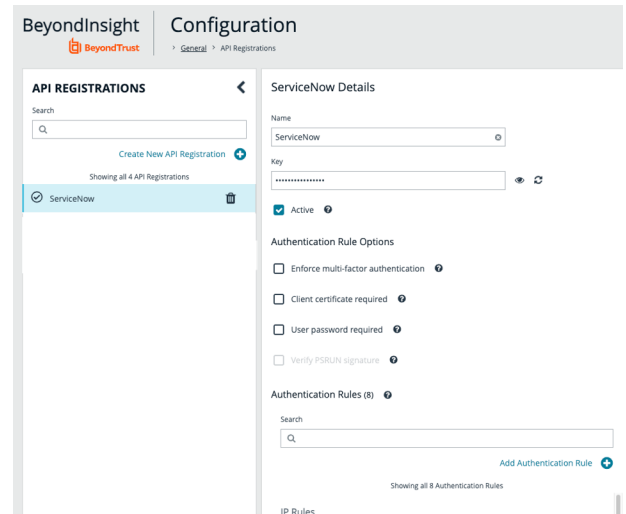
The following items must be configured in Password Safe to use the integration:

- API Registration.
- Managed Accounts must be API enabled.
- A Password Safe group to assign the API registration to. This group must contain the requestor accounts.
- Managed Systems exist in Password Safe with the exact name as in ServiceNow Configuration Management database. The naming convention for the system in ServiceNow must match how it appears in the Password Safe requestors WebUI page, i.e., short name or FQDN.
- Access Policy that allows the API group/user to request the managed account.

## API Registration

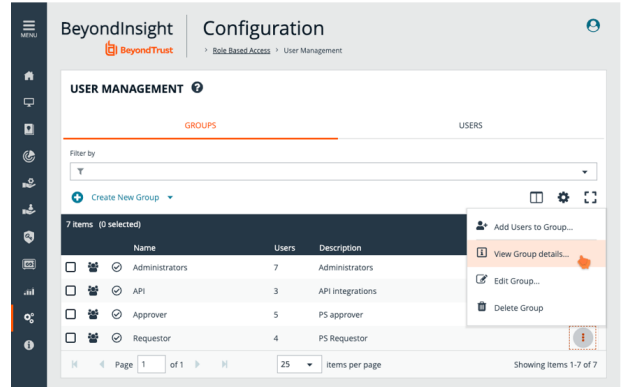
In Password Safe, an API registration is required that will be used by ServiceNow directly (or via MID Server) to access the Password Safe API, when requests are queued by the applications for calls.

1. Register a new API.
  - In the web console, navigate to **Configuration > API Registration** and click **Create New API Registration**.
  - Add a name.
  - Add the IP address of your ServiceNow instance as an IP authentication rule. Make note of the API key; it is required for the integration configuration in ServiceNow.

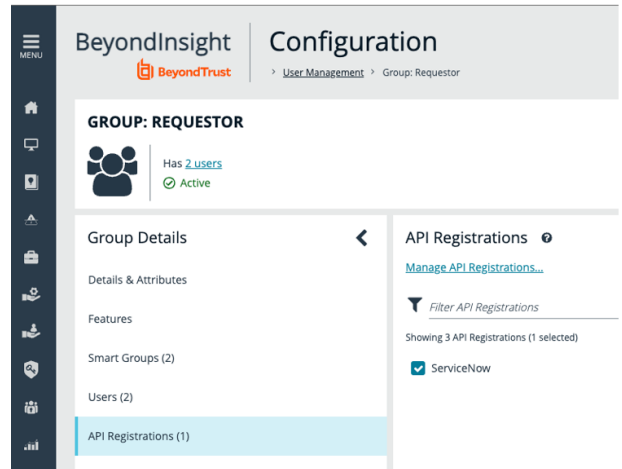


- The API registration must be assigned to a group that contains any Password Safe user that requests access. Creating a new API Group is optional, because we are actually using the user credentials instead of a generic service account, so the API can be registered to the Requestors Group, for example.

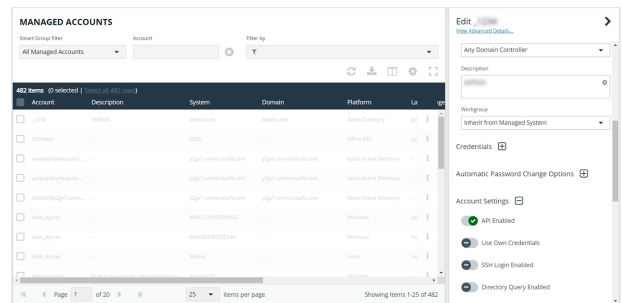
To assign the API to the **Requestors** group, navigate to **Configuration > Role Based Access > User Management**. In the list of groups, select the one you previously set up as Requestors and select **View Group Details**.



- Assign the registered API to the group.



- Managed accounts that display in ServiceNow require API access. Toggle **API Enabled** to **yes**. Repeat this step for any managed account that you want to use with the integration.



**Note:** If you don't have a requestor type group set up yet, see the following to set one up: [Create a Group and Assign Roles at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cloud/admin/role-based-access/create-group-assign-roles.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cloud/admin/role-based-access/create-group-assign-roles.htm)

## Prepare and Set Up Application in ServiceNow

### Install Password Safe integration from the ServiceNow App Store

For a production ServiceNow instance, you can download the application from the ServiceNow Application Store.

**i** For details on how to install an application from the ServiceNow store, please see [Install a ServiceNow Store application at https://docs.servicenow.com/bundle/tokyo-application-development/page/build/applications/task/t\\_\\_InstallApplications.html](https://docs.servicenow.com/bundle/tokyo-application-development/page/build/applications/task/t__InstallApplications.html).

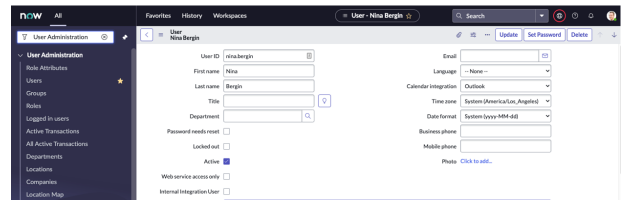
### Users and Role Assignment in ServiceNow

ServiceNow user account names must match the corresponding user account name in Password Safe. In a production environment, it is likely that users already exist in both ServiceNow and Password Safe, leveraging account information from the same centralized directory service.

For example, user nina.bergin must exist in both ServiceNow and Password Safe.

For each account, add the following roles:

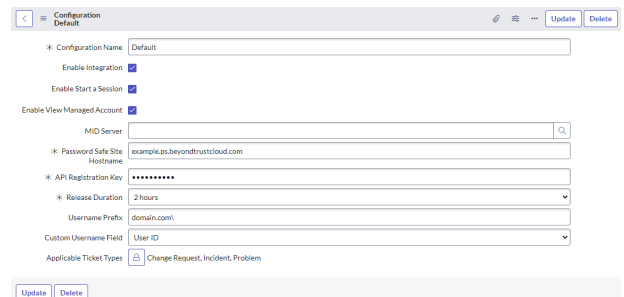
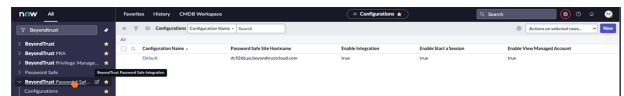
- **x\_bets\_pwdsafe.app\_admin:** Users can view and edit configuration for the application.
- **x\_bets\_pwdsafe.session\_user:** Users can see and use the Start Session UI Action to initiate a session using the selected managed account.
- **x\_bets\_pwdsafe.credential\_user:** Users can see and use the **View Managed Account** UI action to retrieve the password for the selected managed account.



### Configure the Application in ServiceNow

1. In the ServiceNow portal, search for *BeyondTrust Password Safe Integration* in main menu.
2. Click **Default**. If it doesn't exist, then click **New** at the top right.
3. Fill out the following:

- **Configuration Name:** Use **Default**.
- **Enable Integration:** Check the box.
- **Enable Start a Session:** Check the box to allow users to request a session.
- **Enable View Managed Account:** Check the box to allow users to view the password of a managed account.
- **MID Server:** Select the appropriate MID Server with access to your BeyondInsight Appliance.
- **Password Safe Site Hostname:** The hostname only. Do not include https:// or any other URL components.





**Note:** If using a BeyondInsight appliance, then enter a DNS name that can resolve to the main appliance.

- **API Registration Key:** See earlier in the guide.
- **Release Duration:** The length of time the request is valid and active. The default value is 2 hours.
- **Username Prefix:** The value to prepend to the ServiceNow account usernames that would be expected by Password Safe to successfully identify a user. This is typically a domain prefix such as **example.com\**.
- **Custom Username Field:** To be used when a user's ServiceNow User ID does not match their username in Password Safe. Simply select the appropriate field from the dropdown list. The list contains all string type fields in the User table (sys\_user) with the default being User ID.
- **Applicable Ticket Types:** Select the types of tickets the enabled features apply to. For example, Change Request or Incident. Any task type ticket are available to choose.

4. Click **Submit**.

## Configure the Configuration Management Database

The CMDB in ServiceNow must be populated with records for assets that have the same name as the managed systems in Password Safe.

Password Safe Cloud and BeyondInsight allow you to export asset data to your ServiceNow instance using connectors.

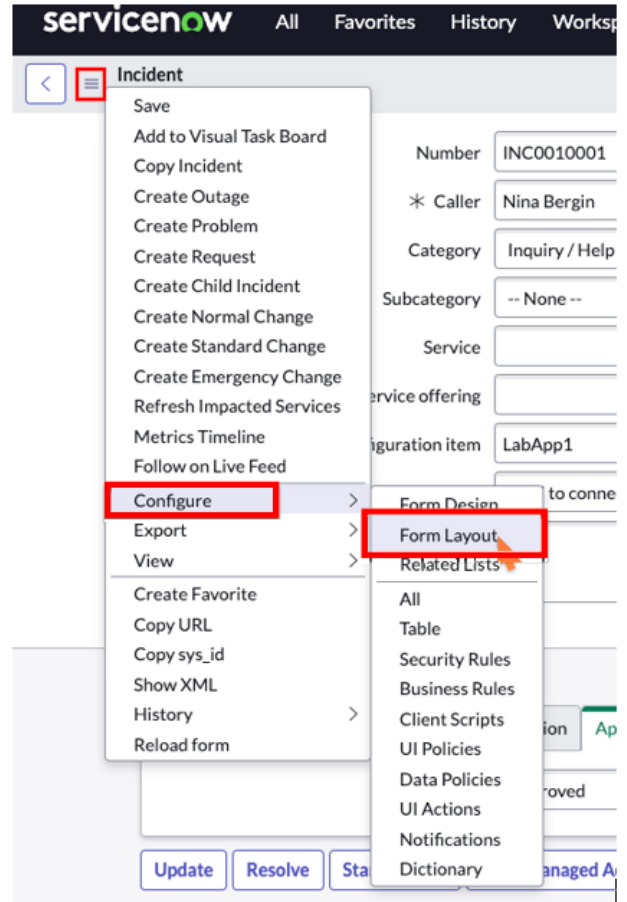


For more information on how to set up the connector, please see [Configure ServiceNow Export Connector](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/integrations/servicenow/export-connector.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/integrations/servicenow/export-connector.htm>

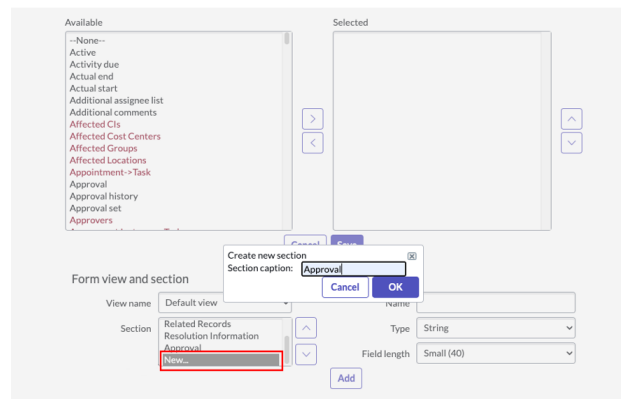
## Configure the Approval Option for Incidents

If using incident management as a workflow, you might need to add the **Approval** menu setting to the incident form. The ticket must be approved before you can start a session or view a managed account.

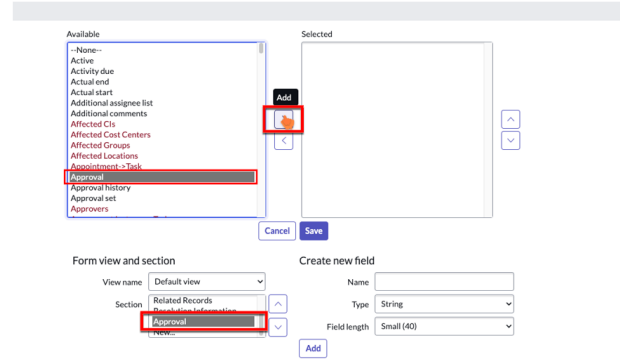
1. Go to any Incident, right-click the hamburger button at the top left, and navigate to **Configure > Form Layout**.



2. In the **Form View and Section** area, click **New** and name the section *Approval*.

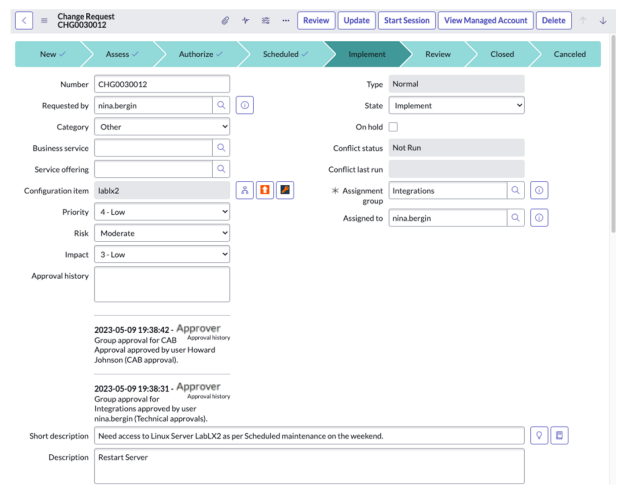
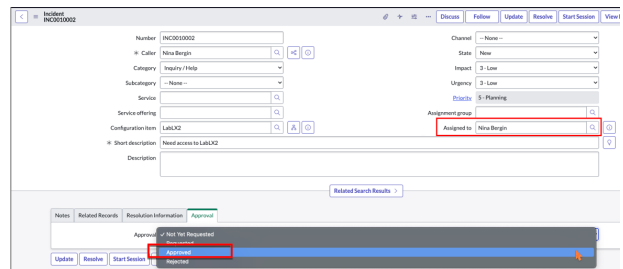


3. Make sure **Approval** is selected in the **Section** list.
4. In the **Available** column, select **Approval** and click **Add** to move it to the **Selected** column.
5. Click **Save**.



## Test the Integration

1. In ServiceNow, log in as the user that will request a session or view managed account password (for example nina.bergin) and create an incident or change request.
2. On a different browser, log in as a ServiceNow user that has the role to approve an incident or change request. Assign the incident or task (if change request) to the requestor user from the previous step and approve it.
3. If testing a change request, then it will have to do the change approval steps, and the status must be in the **Implement** state and approved.

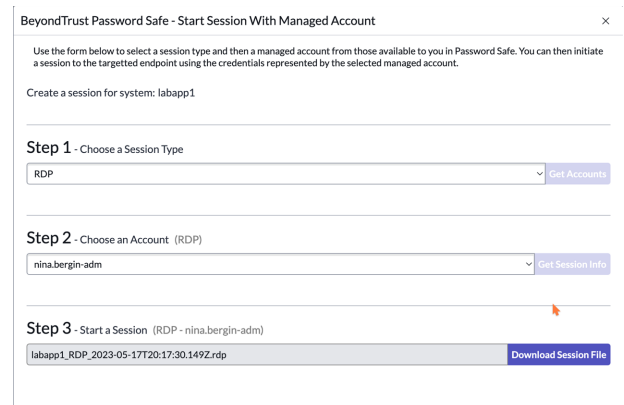


4. In the browser that is logged in as the requestor, refresh the incident/change request page.

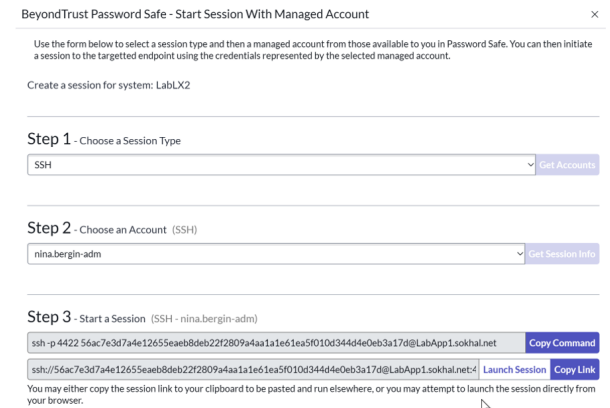
5. Test a session:

- a. Click **Start Session**.
- b. Select the type of session and privileged account.

A downloadable RDP file initiates a session using your default remote connection tool.



For an SSH session, you are presented with a command or link to use with your SSH tool, or you can click **Launch Session**.



- c. The requestor has now initiated a session via Password Safe to that managed asset.



**Note:** To get the **Launch Session** button to work from a Windows Desktop requires an update to tell the browser which native SSH tool to use. Generally, this is something BeyondTrust Professional Services team can help configure. Initially, the copy command might be the easiest to test for now from a shell tool that allows SSH.

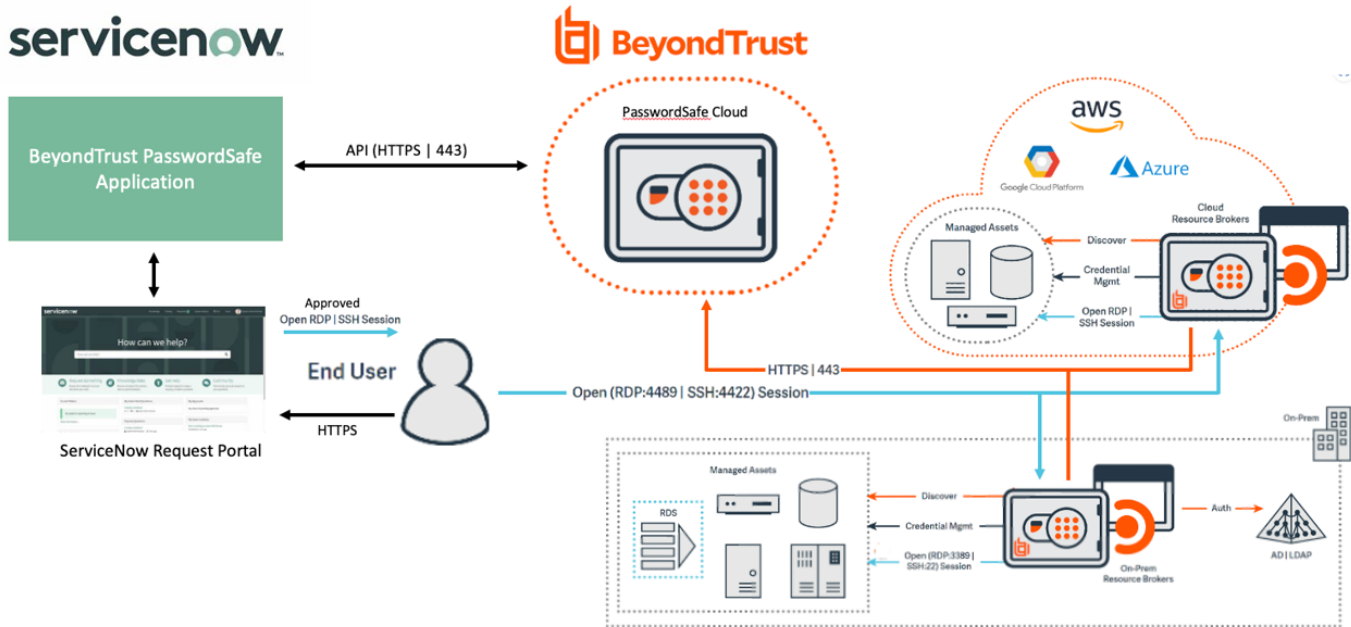
6. Check out a password for a managed account:

- Click **View Managed Account**.
- From the menu, select the managed account, and then click **Get Password**.
- Click **Copy to Clipboard**.
- If checking out a Windows account, test an RDP session to a managed asset that uses that managed account. Similarly, if checking out an account that is for SSH, test a session to that asset using the SSH tool of preference.
- The requestor has now initiated a session via Password Safe to that managed asset.

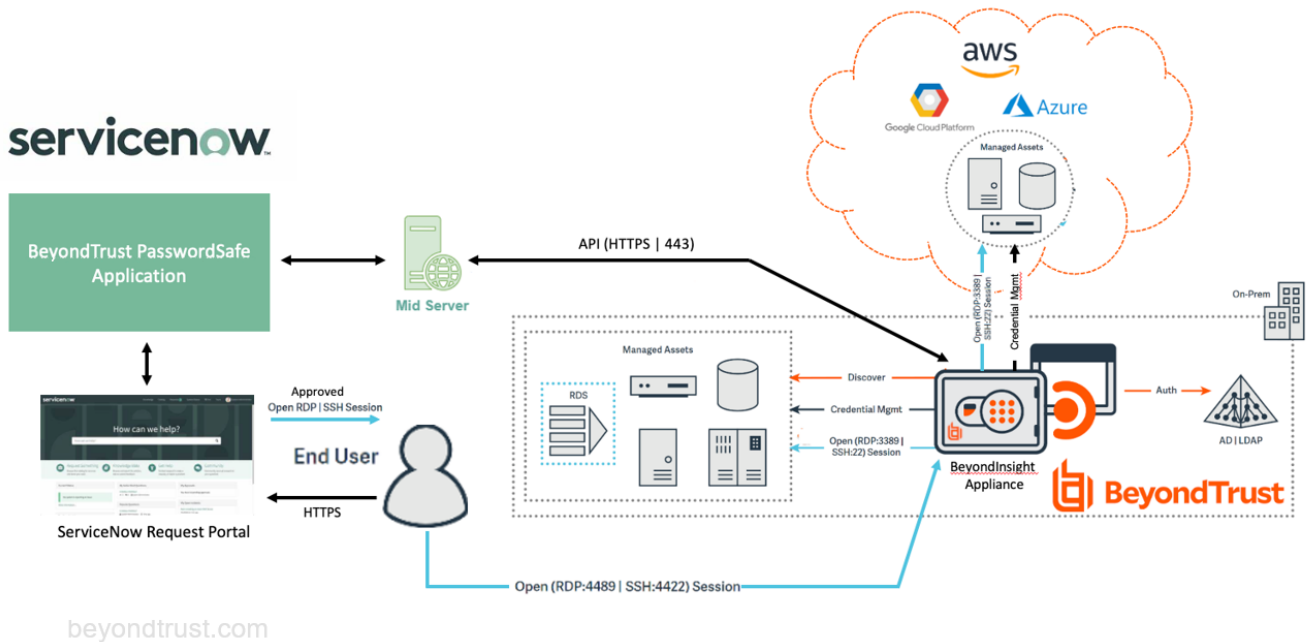


# ServiceNow Password Safe Integration Architecture Diagrams

## Password Safe Cloud & ServiceNow



## BeyondInsight and ServiceNow



beyondtrust.com