

Configure CA Service Desk with Password Safe Ticket System

Integrating CA Service Desk Manager with Password Safe ticket system does not require a BeyondInsight connector. There are two ways to configure CA Service Desk with Password Safe:

- Use a functional account that has permissions to access CA Service Desk Manager
- Use a PKI Certificate

Use a Functional Account for Access

Create the Functional Account

1. In the console, click **Configuration**.
2. Under **Privileged Access Management**, click **Password Safe**.
3. In the **System Configuration** pane, click **Functional & Login Accounts**.
4. In the **Account Alias** pane, click **+ (Add New Account)**.
5. Select **CA Service Desk** from the **Platform** list.
6. Enter the full URL to the CA Service Desk Manager API in the **Domain** box.
7. Enter the CA Service Desk Manager credentials. The user requires the `Passwordsafe_ticket_system` role. The unique name to find this role is `x_bets_bi_integrat.passwordsafe_ticket_system`.
8. Configure the remaining settings.
9. Click **Save**.

Functional Account Detail

Platform	CA Service Desk
Domain	cts-rbgdweb04b:8080/axis/services/USD_R11_WebService
User Name	TestUser <input type="button" value="Set New Password"/>
Password	*****
Confirm Password	*****
Alias	CATestUser
Description	
Associated Managed Systems	0 associated system(s)
Workgroup	All
Enable Automatic Password Management	<input type="checkbox"/>
Password Rule	Default Password Rule
Change Frequency	<input checked="" type="radio"/> First day of the month <input type="radio"/> Last day of the month <input type="radio"/> Every <input type="text" value="1"/> days
Change Time	12:00 AM
Next Change Date	09/16/2016
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Create the Access Policies

Create two access policies for the following scenarios:

- Users that need ticket validation (approval required)
- Emergency access (auto approve)

1. In the console, click **Configuration**.
2. Under **Privileged Access Management**, click **Password Safe**.

3. In the **System Configuration** pane, click **Access Policies**.
4. In the **Access Policy** pane, click **+ (Create new access policy)**.
5. Name the policy and save it.
6. Click **+** again to create the second policy and save it.
7. In the **Access Policy** pane, select the policy that requires approval and then click **Create New Schedule**.
8. Configure the access schedule settings: **Time, Recurrence, Range, and Location**.
9. For each **Type**, under **Approvers**, select at least **1** from each list and then click **Save**.

Type	Record	Keystroke Logging	ESA	Approvers	Concurrent	Logoff on Disconnect	Force Termination	Connection Profile (SSH)
<input checked="" type="checkbox"/> View Password	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> RDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/> Unlimited	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> SSH	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/> Unlimited	<input type="checkbox"/>	<input type="checkbox"/>	None
<input checked="" type="checkbox"/> Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/> Unlimited	<input type="checkbox"/>	<input type="checkbox"/>	None

10. In the **Access Policy** pane, select the policy that you created for emergency access and then click **Create New Schedule**.
11. Configure the access schedule settings: **Time, Recurrence, Range, and Location**.
12. For each **Type**, under **Approvers**, click the down arrow in each box until **Auto Approve** appears checked, and then click **Save**.

Type	Record	Keystroke Logging	ESA	Approvers	Concurrent	Logoff on Disconnect	Force Termination	Connection Profile (SSH)
<input checked="" type="checkbox"/> View Password	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Auto Approve	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> RDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Auto Approve	<input checked="" type="checkbox"/> Unlimited	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> SSH	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Auto Approve	<input checked="" type="checkbox"/> Unlimited	<input type="checkbox"/>	<input type="checkbox"/>	None
<input checked="" type="checkbox"/> Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Auto Approve	<input checked="" type="checkbox"/> Unlimited	<input type="checkbox"/>	<input type="checkbox"/>	None

Create the Ticket System

1. In the console, click **Configuration**.
2. Under **Privileged Access Management**, click **Password Safe**.
3. In the **System Configuration** pane, click **Ticket Systems**.
4. In the **Ticket Systems** pane, click **+ (Create New Ticket System)**.
5. Select **CA Service Desk Ticket System** from the **Platform** list.
6. Select the functional account, and then enter a name for the system. **Access Policy Certificate Common Name** and **Access Policy Code** are not required.
7. Select all three check boxes and then click **Update**.

Ticket System Detail

Platform	CA Service Desk Ticket System
Functional Account	CATestUser (cts-rbqsdweb04b:8080/ax)
Name	CA ticket system
Description	<input type="text"/>
Access Policy Certificate Common Name	<input type="text"/>
Access Policy Code	<input type="text"/>
	<input checked="" type="checkbox"/> Auto Approve on Ticket Number Validation
	<input checked="" type="checkbox"/> Enable Emergency Approval Without Ticket Number
	<input checked="" type="checkbox"/> Make this ticket system the default
	<input type="button" value="Update"/> <input type="button" value="Cancel"/>



Note: For any tickets being verified using this ticket system, you must ensure within the CA Service Desk Manager, the **Requestor** is populated in the **Assignee** field. The User ID here must match the Password Safe User ID.

Configure Global Settings

1. In the console, click **Configuration**.
2. Under **Privileged Access Management**, click **Password Safe**.
3. In the **System Configuration** pane, click **Global Settings**.
4. Ensure the following check boxes are selected:
 - Ticket Settings
 - Reason is required for new requests
5. Select other settings as needed.
6. Click **Update**.

Use a PKI Certificate Access Policy

An alternative way to set up access to CA Service Desk Manager is to use a PKI certificate.

Import the PKI Certificate

1. Enable PKI login in CA Service Desk Manager. Instructions are in `\Java\PKI_loginServiceManaged_JAVA_steps.doc` located on the CA SDM server.
2. Copy and install the certificate generated above to the Password Safe server.
 - a. Open the mmc console.
 - b. Add the **Certificates** snap-in.
 - c. Select computer account and local computer.
 - d. Expand the **Personal** folder, and then right-click **Certificates** folder.
 - e. Select **All Tasks > Import**.
 - f. Click **Next** and browse to certificate location.
 - g. Set file types to **All Files (*.*)**.
 - h. Select the certificate and open it.
 - i. On the **Private key protection** page, enter the certificate password and then select the **Mark this key as exportable** check box. This will allow you to back up or transport your keys at a later time.
 - j. On the **Certificate Store** page, select **Personal**.
 - k. Click **Finish**.
3. Assign **IIS_IUSRS** permissions to use keys.
 - a. Right-click the certificate, and then select **All Tasks > Manage Private Keys**.
 - b. Add local computer **IIS_IUSRS**.
 - c. Assign **Full Control**.

Create the Functional Account

1. In the console, click **Configuration**.
2. Under **Privileged Access Management**, click **Password Safe**.

3. In the **System Configuration** pane, click **Functional & Login Accounts**.
4. In the **Account Alias** pane, click **+ (Add New Account)**.
5. From the **Platform** list, select **CA Service Desk**.
6. In the **Domain** box, enter the URL to the CA Service Desk web service.
7. Enter a username and password. The information is not used in this implementation so can be anything.
8. Set the remaining fields as needed.
9. Click **Save**.

Create the Access Policies

i Two access policies are required, as documented above for functional account access. Please see "[Create the Access Policies](#)" on page 1 .

Create the Ticket System

1. In the console, click **Configuration**.
2. Under **Privileged Access Management**, click **Password Safe**.
3. In the **System Configuration** pane, click **Ticket Systems**.
4. In the **Ticket Systems** pane, click **+ (Create New Ticket System)**.
5. Select **CA Service Desk Ticket System** from the **Platform** list.
6. Select the functional account, and then enter a name for the system.
7. Enter **ServiceDesk DEFAULT** in the **Access Policy Certificate Common Name** box.
8. Enter **DEFAULT** in the **Access Policy code** box.
9. Select all three check boxes and then click **Update**.

Ticket System Detail

Platform	CA Service Desk Ticket System
Functional Account	CATestUser (cts-rbqsdweb04b:8080/ax)
Name	CA ticket system
Description	<input type="text"/>
Access Policy Certificate Common Name	ServiceDesk DEFAULT
Access Policy Code	DEFAULT
	<input checked="" type="checkbox"/> Auto Approve on Ticket Number Validation <input checked="" type="checkbox"/> Enable Emergency Approval Without Ticket Number <input checked="" type="checkbox"/> Make this ticket system the default
	<input type="button" value="Update"/> <input type="button" value="Cancel"/>