BeyondTrust

Privileged Remote Access
Smart Card Support

TC:2/8/2019

Table of Contents

Smart Cards for Remote Authentication in the Access Console

During an access session, a user may need to operate with administrative rights in order to access the remote computer. In environments where security implementations require smart card use for authentication, BeyondTrust enables the user to pass administrative credentials to the remote computer from a smart card resident on the user's local system.

Prerequisites

To use BeyondTrust smart card support through a Jump Client, the following prerequisites must be met:

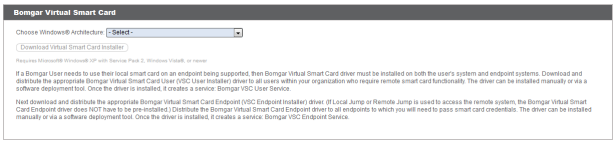
- Your BeyondTrust Appliance must be running software version 15.1 or higher.
- The user's computer must have a BeyondTrust virtual smart card driver installed.
- Each endpoint computer must have a BeyondTrust virtual smart card driver installed.
- Each endpoint computer must be running Windows Vista or above.
- Each endpoint computer must be accessible by a BeyondTrust Jump Client running in elevated mode.

BeyondTrust smart card support can be used with Jump Items when the following prerequisites are met:

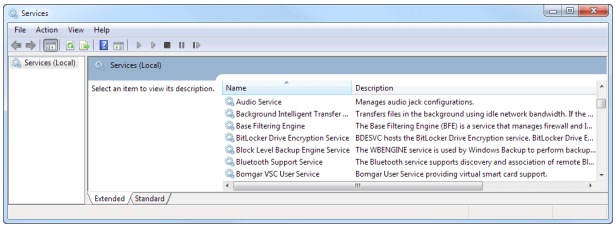
- Your BeyondTrust Appliance must be running software version 15.1 or higher.
- The user's computer must have a BeyondTrust virtual smart card driver installed.
- Each endpoint computer must be running Windows Vista or above.

Install the Smart Card Drivers

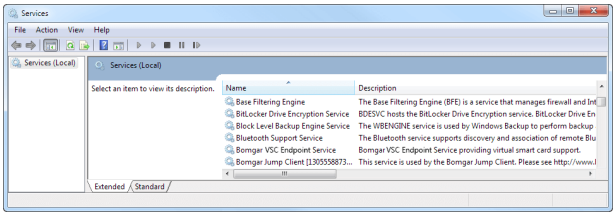
1. Go to **/login > My Account :: BeyondTrust Virtual Smart Card**.
2. Download the user installation package and the endpoint installation package for the appropriate versions of Windows.



3. Install the user virtual smart card driver.
    - Distribute the user driver installer to all users within your company who require remote smart card functionality.
    - The driver can be installed manually or via a software deployment tool.
    - Once the driver is installed, it creates a service: **BeyondTrust VSC User Service**.



4. Install the endpoint virtual smart card driver. (If a Jump Item is used to access the remote system, the endpoint virtual smart card driver does NOT have to be pre-installed.)
    - Distribute the endpoint driver installer to all remote computers to which you will need to pass smart card credentials.
    - The driver can be installed manually or via a software deployment tool.
    - Once the driver is installed, it creates a service: **BeyondTrust VSC Endpoint Service**.



Install a Jump Client or Jumpoint for Elevated Privileged Remote Access Session Start

When attempting to operate with the credentials on a smart card, the user is prompted to enter a PIN. This UAC prompt is inaccessible to the user if the endpoint client is not already running in elevated mode. It is therefore necessary to access the remote endpoint in one of two ways:

- A Jump Client running as a system service
- A Jumpoint or local network Jump, using administrative credentials

Accessing the remote endpoint in elevated mode allows the user to interact with UAC prompts in order to enter the smart card PIN.

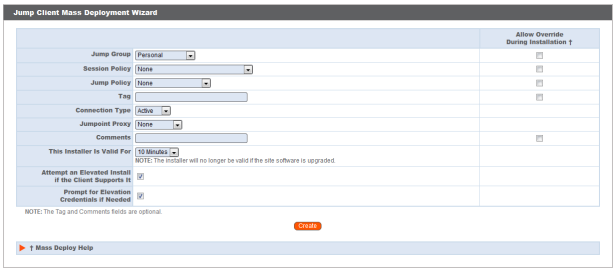
Jumpoint Installation

To install a Jumpoint, see Jumpoint: Set Up Unattended Access to a Network at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jumpoint.htm. No special setup is required.

Jump Client Installation

To install a Jump Client in preparation for using smart card support, you must set certain options as described below.

1. From the /login interface of your BeyondTrust Appliance, go to **Jump > Jump Clients**.
2. Configure the Jump Client settings as needed. For details, see Jump Clients: Manage Settings and Install Jump Clients for Unattended Access at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-clients.htm.
    - The connection type can be either active or passive.
    - Be sure to check **Attempt an Elevated Install if the Client Supports It** as well as **Prompt for Elevation Credentials if Needed**.
3. Click **Create**.
4. From this page, you may email the Jump Client installer to one or more remote users.
5. Alternatively, select a platform and download the Jump Client installer to your local system. You may then distribute this installer to multiple systems for manual installation, or you may distribute it via a software deployment tool.



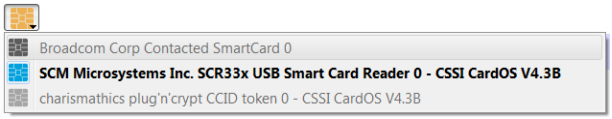
Use a Virtualized Smart Card

To use smart card credentials on a remote system, you must Jump to that system using a Jump Client, and the Jump Client must be running in service mode. The appropriate virtual smart card drivers must be installed on both your local system and the remote system, with their services running.

Alternatively, a system can be accessed using a Jump Item. Using a Jump Item does not require the virtual smart card driver to be pre-installed on the remote system. In this scenario, BeyondTrust installs the driver as part of the Jump to the endpoint being accessed.

> ***Note:*** *The endpoint smart card driver is installed during a Jump Item push ONLY when the user performing the Jump has the user smart card driver installed on their local system.*

Begin a screen sharing session, and then click the **Smart Card** button to access a dropdown of available smart card readers on your system.[1] Select the reader you would like to share with the remote computer. Once the reader has been virtualized on the remote system, a message indicating that you have shared this reader is logged in the chat window. The smart card in the selected reader is now available to use on the remote computer, just as if it were physically present on the system being supported.



The smart card dropdown menu displays the name(s) of the available smart card readers and smart cards, along with an icon indicating the availability of each card reader or presence of each card:

- **Black icon** - Card not present
- **Blue icon** - Card present
- **Gray icon** - Reader and card not available

Once you have shared a reader, it remains selected and available for use throughout the session, as long as you do not log out the current user. If you do log out the current user on the remote computer, the shared reader is deselected and must be re-selected if you need it later in the session.

When screen sharing, use a virtual smart card to perform administrative actions. You can run programs in another user context, or even log in as a different user.

Also, if the virtual smart card feature is available in a session which is not elevated and a smart card reader has been shared into the session, then certificates stored on the inserted smart card can be selected and used for elevation.

> ***Note:*** *Elevation performed using this feature takes slightly longer due to the extra transactions required to the virtual smart card reader.*

> ***Note:*** *A smart card reader can be attached to only one active session at a time. From the* ***Smart Card*** *dropdown, you can deselect a virtualized reader to free it for use in another session.*

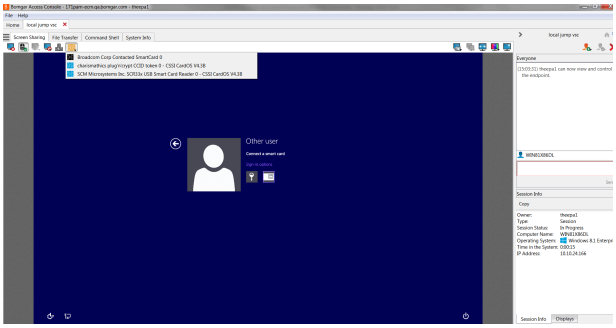
---

[1] If the smart card button does not appear in the screen sharing tool bar, make sure the user smart card service is running on your local computer. If the smart card button is present but disabled, make sure the endpoint smart card service is running on the remote computer.

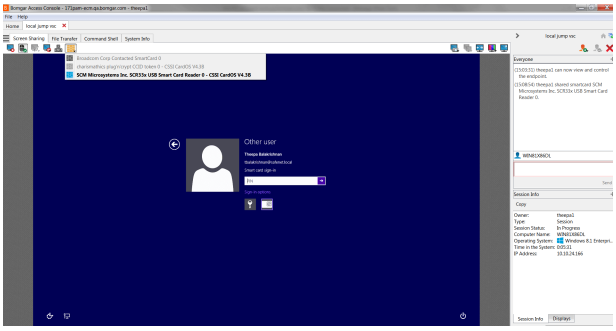
Use Case 1:
Log Into the Remote Endpoint Using Smart Card Credentials

After Jumping to a remote endpoint, you may find that the computer is locked. Alternatively, you may need to perform administrative functions not permitted in the current user context.

Go to the remote login screen, logging out the current user if necessary. Click the **Smart Card** button and select a smart card reader to virtualize on the remote system. The smart card now appears as a user login option.

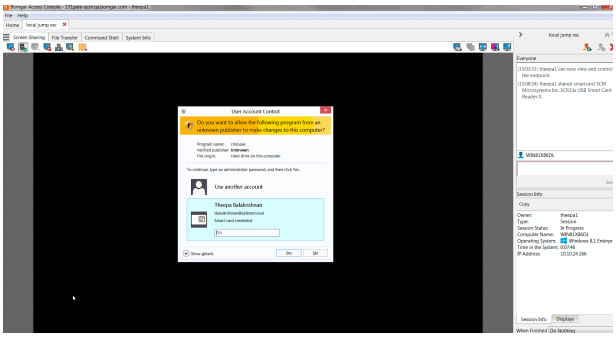


Click the smart card user, enter the PIN, and log in.



Use Case 2:
Run As the Smart Card User

While accessing or troubleshooting a remote system, you may need to run a specific application with privileges not available in the current user context. Within a screen sharing session, click the **Smart Card** button and select a smart card reader to virtualize on the remote system. Right-click the desired application and choose **Run As**. From the UAC prompt that appears, select the smart card and enter the PIN to run the application in the smart card user context.



> ***Note:*** *Smart card credentials cannot be used to run elevated tasks from the* ***Special Actions*** *menu.*