



BeyondTrust

Privileged Remote Access Smart Card Support

Table of Contents

Smart Cards for Remote Authentication in the Access Console	3
Prerequisites	3
Install the Smart Card Feature	4
Install a Jump Client or Jumpoint for Elevated Privileged Remote Access Session Start	6
Jumpoint Installation	6
Jump Client Installation	6
Use a Virtualized Smart Card	7
Use Case 1: Log Into the Remote Endpoint Using Smart Card Credentials	9
Use Case 2: Run As the Smart Card User	10

Smart Cards for Remote Authentication in the Access Console

During an access session using the Desktop Access Console, 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, Privileged Remote Access enables the user to share a local smart card within a session so that it can be used as an authentication source on the endpoint system.

To achieve this, the access console user's system must have a Virtual Smart Card User driver installed and the endpoint system must have a Virtual Smart Card Endpoint driver installed. The Virtual Smart Card Endpoint driver can either be pre-installed on the endpoint system or pushed to the system during the Jump process. For the latter, the Virtual Smart Card Endpoint is uninstalled when the session ends. If the session is pinned, the Virtual Smart Card Endpoint remains installed until the pinned client is uninstalled.



Note: This feature is not supported for ARM-based Windows systems.



Note: Only the Desktop Access Console supports sharing a smart card into a support session. The Privileged Web Access Console does not support smart cards.



For more information about specific smart cards supported and supported smart card standards, please [Contact Support](https://www.beyondtrust.com/docs/index.htm) at <https://www.beyondtrust.com/docs/index.htm>.

Prerequisites

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

- The target being supported is a member of a PKI enabled Active Directory Domain.
- The smart card being shared into the support session contains credentials that are valid within the target Active Directory Domain.
- The user's computer has the appropriate Privileged Remote Access Virtual Smart Card User installed.
- Each endpoint computer has the appropriate Privileged Remote Access Virtual Smart Card Endpoint installed.
- Each endpoint computer must be running Windows 7 or newer.
- Each endpoint computer must be accessible by a Privileged Remote Access Jump Client running in elevated mode.



Note: When Jump To is used to access the remote system, the Virtual Smart Card Endpoint driver does NOT have to be pre-installed.

Install the Smart Card Feature

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

Virtual Smart Card

Choose Windows® Architecture:

— Select —

[Download Virtual Smart Card Installer](#)

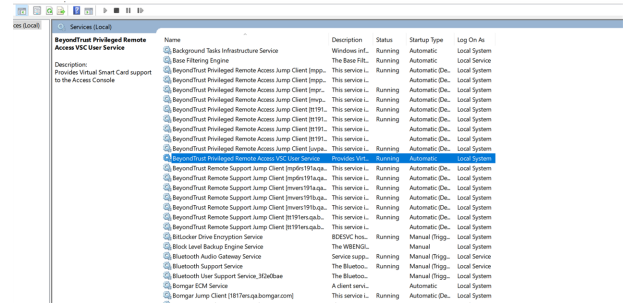
Requires Microsoft® Windows® 7 or newer.

If a Privileged Remote Access User needs to use their local smart card on an endpoint being supported, then BeyondTrust Privileged Remote Access Virtual Smart Card driver must be installed on both the user's system and endpoint systems. Download and distribute the appropriate BeyondTrust Privileged Remote Access Virtual Smart Card User (VSC User Installer) driver to all users within your organization 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: Privileged Remote Access VSC User Service.

Next download and distribute the appropriate BeyondTrust Privileged Remote Access Virtual Smart Card Endpoint (VSC Endpoint Installer) driver. (If Local Jump or Remote Jump is used to access the remote system, the BeyondTrust Privileged Remote Access Virtual Smart Card Endpoint driver does NOT have to be pre-installed.) Distribute the BeyondTrust Privileged Remote Access Virtual Smart Card Endpoint driver to all endpoints 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: Privileged Remote Access VSC Endpoint Service.


3. Install the user virtual smart card.

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



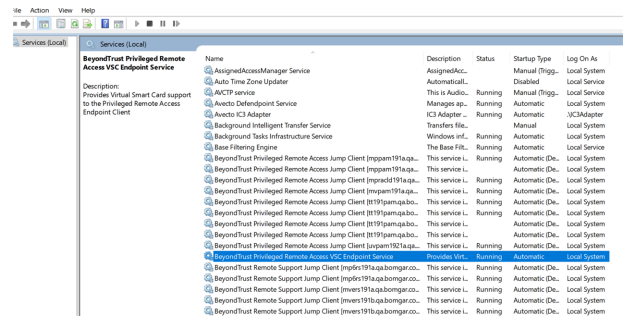
Name	Description	Status	Startup Type	Log On As
Background Tasks Infrastructure Service	Windows inf...	Running	Automatic	Local System
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access VSC User Service	Provides Vir...	Running	Automatic	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BitLocker Drive Encryption Service	BEESVC Inco...	Running	Manual (Trigg...	Local System
Block Level Backup Engine Service	The WBSNG...	Manual	Manual (Trigg...	Local System
Bluetooth Audio Gateway Service	Service supp...	Running	Manual (Trigg...	Local Service
Bluetooth Support Service	The Bluetoo...	Running	Manual (Trigg...	Local Service
Bluetooth User Support Service_BTMdsae	The Bluetoo...	Manual (Trigg...	Manual (Trigg...	Local System
Bomgar ECM Service	A client serv...	Automatic	Automatic	Local System
Bomgar Jump Client [H171en1qabomgar.com]	This service i...	Running	Automatic (De...	Local System

4. Install the endpoint virtual smart card.



Note: If a Jump Item is used to access the remote system, the endpoint virtual smart card does NOT have to be pre-installed.

- Distribute the VSC Endpoint Installer to all remote computers to which you will need to pass smart card credentials.
- The endpoint smart card can be installed manually or via a software deployment tool.
- Once the endpoint smart card is installed, it creates a service called **BeyondTrust Privileged Remote Access VSC Endpoint Service**.



Name	Description	Status	Startup Type	Log On As
AssignedAccessManager Service	AssignedAcc...	Manual (Trigg...	Manual (Trigg...	Local System
Auto Time Zone Updater	AutomaticAl...	Disabled	Automatic	Local Service
AVCIP Service	This is Avco...	Running	Manual (Trigg...	Local Service
Axacta Endpoint Service	Manages ep...	Running	Automatic	Local System
Axacta IC3 Adapter	IC3 Adapter	Running	Automatic	IC3Adapter
Background Intelligent Transfer Service	Transfers fil...	Manual	Manual	Local System
Background Tasks Infrastructure Service	Windows inf...	Running	Automatic	Local System
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Privileged Remote Access VSC Endpoint Service	Provides Vir...	Running	Automatic	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System
BeyondTrust Remote Support Jump Client [Imp...]	This service i...	Running	Automatic (De...	Local System

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.

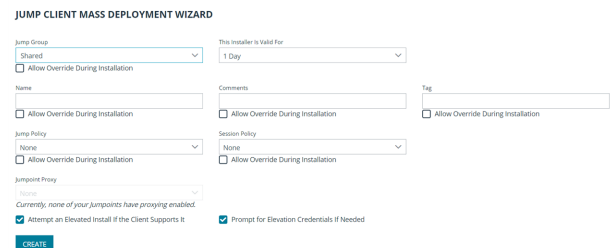
Jumpoint Installation

To install a Jumpoint, see [Jumpoint: Set Up Unattended Access to a Network](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jumpoint.htm) 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 B Series 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](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-clients.htm) at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-clients.htm.
 - 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.



Jump Client Mass Deployment Wizard

Download or Install the Client Now:

Platform

Windows® (x64)

Download

Deploy to Email Recipients:

Email

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 smart card software must be installed on 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 VSC Endpoint Service to be pre-installed on the remote system. In this scenario, BeyondTrust installs the VSC Endpoint Service as part of the Jump to the endpoint being accessed.



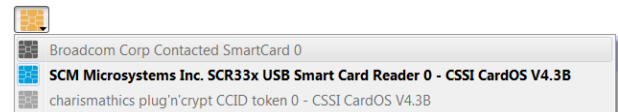
Note: The VSC Endpoint Service is installed during a Jump Item push only when the user performing the Jump has the VSC User Service installed on their local system.

Begin a screen sharing session, and then click the **Smart Card** button to access a dropdown of available smart card readers on your system.



Tip: If the **Smart Card** button does not appear in the screen sharing tool bar, make sure the VSC User Service is running on your local computer. If the **Smart Card** button is present but disabled, make sure the VSC Endpoint Service is running on the remote computer.

The smart card dropdown menu displays the name(s) of the available smart card readers and smart cards. A reader in bold text is being shared in the current active session. An icon indicates the availability of each card reader or presence of each card:



- **Black icon:** Card not present
- **Blue icon:** Card present
- **Gray icon:** Reader/card is shared in another session.

Click 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 selected reader is now available to use on the remote computer, and a smart card inserted locally is virtualized and operates as if it were physically present on the remote system being supported.

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 unshared and must be shared again 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.

If the virtual smart card feature is available in a session that 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, provided the certificates are associated with accounts that have the appropriate permissions.



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

Elevation causes the customer client to restart to become elevated. The restart makes the shared reader unshared, and it must be shared again with the elevated session if it is required for use.



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

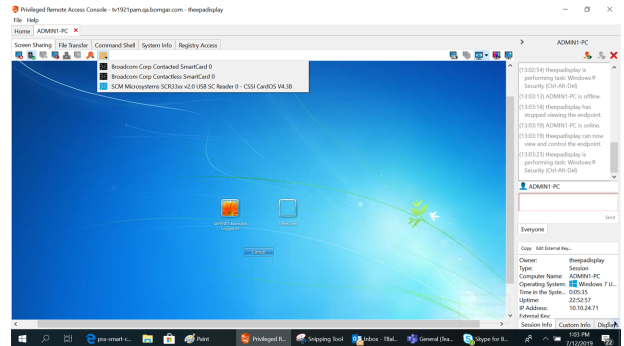


Note: This feature is not supported for ARM-based Windows systems.

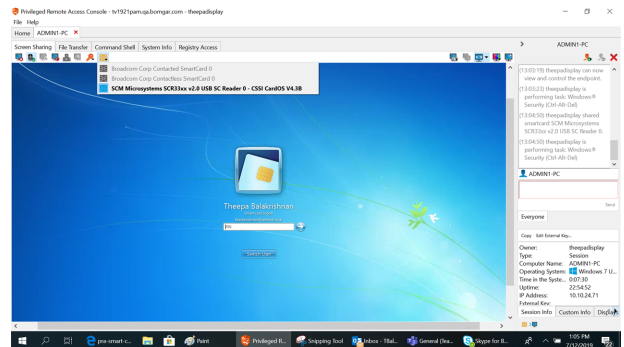
Use Case 1: Log Into the Remote Endpoint Using Smart Card Credentials

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.

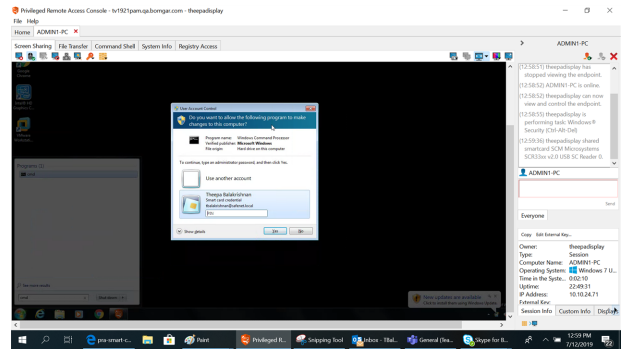


Click the smart card user, enter the PIN, and log in.



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.