THALES

# SafeNet Agent for Remote Desktop Gateway 2.0.4

## INSTALLATION AND CONFIGURATION GUIDE

**Document Information**

| | |
|---|---|
| **Product Version** | 2.0.4 |
| **Document Part Number** | 007-000364-002, Rev. D |
| **Release Date** | January 2022 |

### Trademarks, Copyrights, and Third-Party Software



### Disclaimer

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make **any change or** improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

# CONTENTS

# PREFACE

This document describes how to install and configure the **SafeNet Agent for Remote Desktop Gateway**.

## Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet users and security officers, key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

## Document Conventions

This section describes the conventions used in this document.

### Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

| Convention | Description |
|---|---|
| **bold** | The bold attribute is used to indicate the following:<br>> Command-line commands and options (Type **dir /p**.)<br>> Button names (Click **Save As**.)<br>> Check box and radio button names (Select the **Print Duplex** check box.)<br>> Window titles (On the **Protect Document** window, click **Yes**.)<br>> Field names (**User Name:** Enter the name of the user.)<br>> Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.)<br>> User input (In the **Date** box, type **April 1**.) |
| *italic* | The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.) |
| Double quote marks | Double quote marks enclose references to other sections within the document. |

| | |
|---|---|
| | For example: Refer to "**Error! Reference source not found.**" on page **Error! Bookmark not defined.**. |
| <variable> | In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets. |
| [ optional ]<br>[ <optional> ] | Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task. |
| [ a \| b \| c ]<br>[<a> \| <b> \| <c>] | Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars. |
| { a \| b \| c }<br>{ <a> \| <b> \| <c> } | Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars. |

## Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

### Tips

Tips are used to highlight information that helps to complete a task more efficiently.

> **TIP:** This is some information that will allow you to complete your task more efficiently.

### Notes

Notes are used to highlight important or helpful information.

> **NOTE:** Take note. Contains important or helpful information.

### Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

> **CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

### Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

> ****WARNING** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.**

# Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

## Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click the **REGISTER** link.

## Telephone Support

The support portal also lists telephone numbers for voice contact (Contact Us).

## Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.

# CHAPTER 1: Introduction

## Microsoft Remote Desktop Gateway

A gateway is any computer that connects two networks that use different network protocols. A gateway reformats information from one network so that it is compatible with the other network.

The Microsoft Remote Desktop Gateway (RD Gateway) server is a type of gateway that enables authorized users to connect to remote computers on a corporate network from any computer with an Internet connection. RD Gateway uses the Remote Desktop Protocol (RDP) along with the HTTPS protocol to help create a more secure, encrypted connection.

The RD Gateway server enables remote desktop connections to a corporate network without having to set up virtual private network (VPN) connections.

## SafeNet Agent for Remote Desktop Gateway

The SafeNet Agent for RD Gateway is a solution to enable strong, Two-Factor Authentication (2FA) on users who wish to access any protected RD resource behind a Remote Desktop Gateway.

### Features

Following are the features of the SafeNet Agent for RD Gateway:

- **Native Push OTP Support**: The SafeNet Agent for RD Gateway 2.0.3 (and above) supports the Push OTP function with MobilePASS+ when working with SAS Cloud and SAS PCE/SPE 3.9.1 (and above) versions.
- **Management Console**: The agent now features its own management console, to allow easy modification of configuration settings. The following tabs are available: **Communications** and **Logging**.
- **FIPS Support**: The SafeNet Agent for RD Gateway 2.0.1 (and above) provides FIPS support for the operating system with AES-GCM and RSA key standards. The agent also utilizes FIPS supported methods to decrypt its BSID key.

## Platform Environment

This guide is applicable to the following:

| | |
|---|---|
| **Supported Operating Systems** | • Windows 2012 R2 (64-bit)<br>• Windows Server 2016 (64-bit)<br>• Windows Server 2019 (64-bit) |

| | |
|---|---|
| **Supported Architecture** | 64-bit |

# Applicability

The information in this document applies to the following:

- **SafeNet Trusted Access (earlier, SAS Cloud)** — The SafeNet's cloud-based authentication service.
- **SafeNet Authentication Service - Service Provider Edition (SAS SPE)** — The on-premises, server version targeted at service providers interested in hosting SAS in their data center(s).
- **SafeNet Authentication Service - Private Cloud Edition (SAS PCE)** — The on-premises, server version targeted at organizations interested in hosting SAS in their private cloud environment.

# Prerequisites

- Administrative rights are required for installation and configuration of the SafeNet Agent for RD Gateway.
- RD Gateway server should be up and running on the machine, proposed for the agent installation.
- Remote machine (session host) that needs to be accessed should have the remote desktop services running. Also, it should be accessible from the remote desktop gateway, and should be on the same domain as the remote desktop gateway.
- Ensure that the RD Gateway service (tsgateway) is running, and the mode is set to **Automatic**.
- .NET framework 4.0 (or above) must exist on the RD Gateway machines.
- Communication is established between the agent and the SafeNet server. To configure, add an Auth Node in SAS as follows:
  - In the SAS Management Console, select **VIRTUAL SERVERS** > **COMMS** > **Auth Nodes**.
  - Enter the name or IP address of the computer where the agent is installed.

  For details, refer to the *SafeNet Authentication Service (SAS) Service Provider Administrator Guide*.

> **NOTE:** Installation of RD Gateway agent would disable the existing Remote Desktop Connection Authorization Policies (RD CAP) and Resource Authorization Policies (RD RAP). Policy settings that are configured prior to the Remote Desktop Gateway integration would cease to work.

# CHAPTER 2: Installation

## Installing the Agent

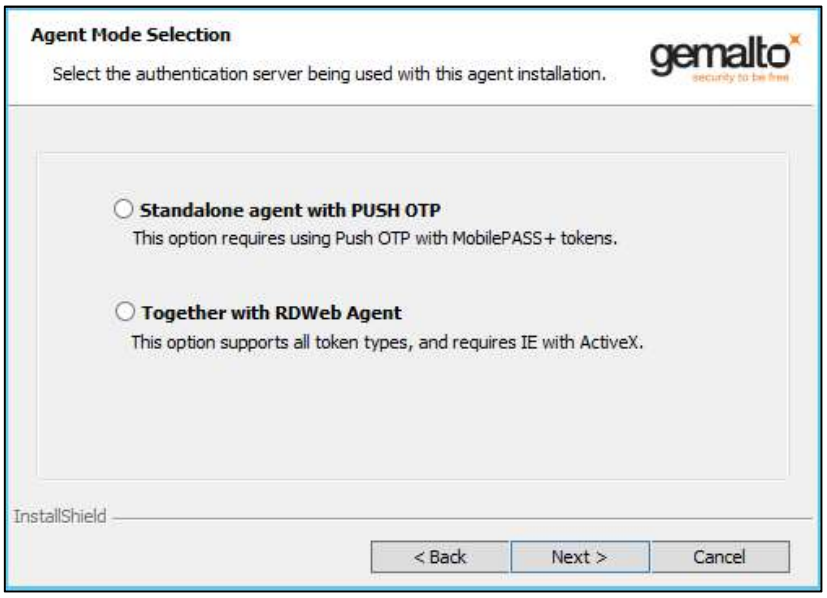
1. Execute the **SafeNet Agent for Microsoft RDGateway** installer.

   **NOTE:** If you have logged into the system as an administrator or if you are a member of the Domain Admin group, the installation process will execute successfully. Otherwise, a window will appear requiring you to provide administrator credentials.

2. On the ***Welcome…*** window, click **Next**.


3. On the **License Agreement** window, select **I accept the terms in the license agreement**, and click **Next**.


4. On the **Agent Mode Selection** screen, select the **Standalone agent with PUSH OTP** radio option, and click **Next**.

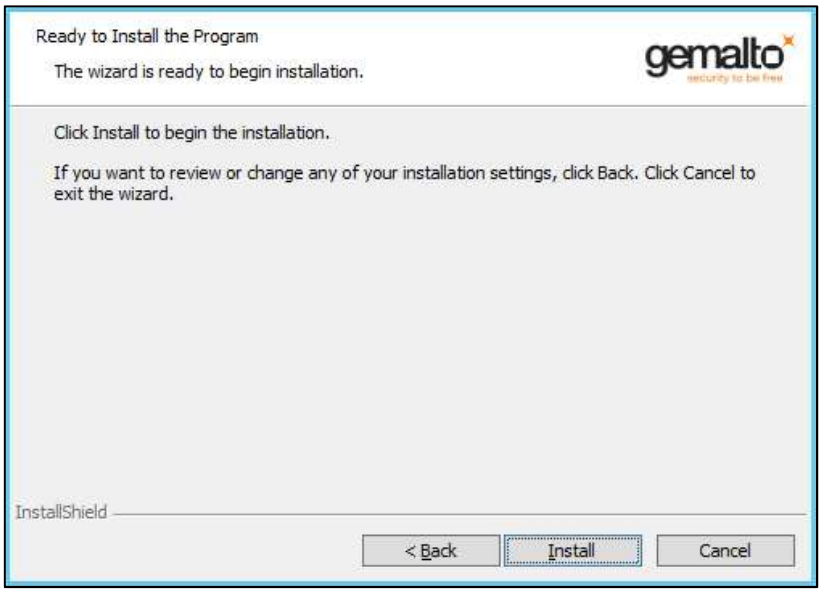



> **NOTE:** The **Together with RDWeb Agent** option is available during the installation process, and allows the agent to function, as earlier, using the RD Web interface. Existing documentation set is available for this agent mode, and must be referred for details.

5. To change the installation folder, click **Change** and navigate to the required folder, and then click **Next**.

   To accept the default installation folder as displayed, click **Next**.


6. On the ***Ready to Install the Program*** window, click **Install** to begin the installation.




7. When the installation is completed, the ***InstallShield Wizard Completed*** window is displayed. Click **Finish** to exit the installation wizard.


# Uninstalling the Agent

To uninstall the SafeNet Agent for RD Gateway, perform the steps:

1. Navigate to **Start** > **Control Panel** > **Programs and Features**.
2. Select the **SafeNet Agent for RD Gateway** program.
3. Click **Uninstall**.

# Upgrading the Agent

The SafeNet Agent for RD Gateway 2.0.4 of the type, **Standalone agent with PUSH OTP** supports upgrade from version 2.0.0 (and above).

Upgrade from earlier versions (v1.0, v1.1.0 and v1.1.1) is not supported.

> **NOTE:** While upgrading the agent, if the user replaces the default BSIDKEY, then the agent BSIDKEY needs to be replaced again after the upgrade.

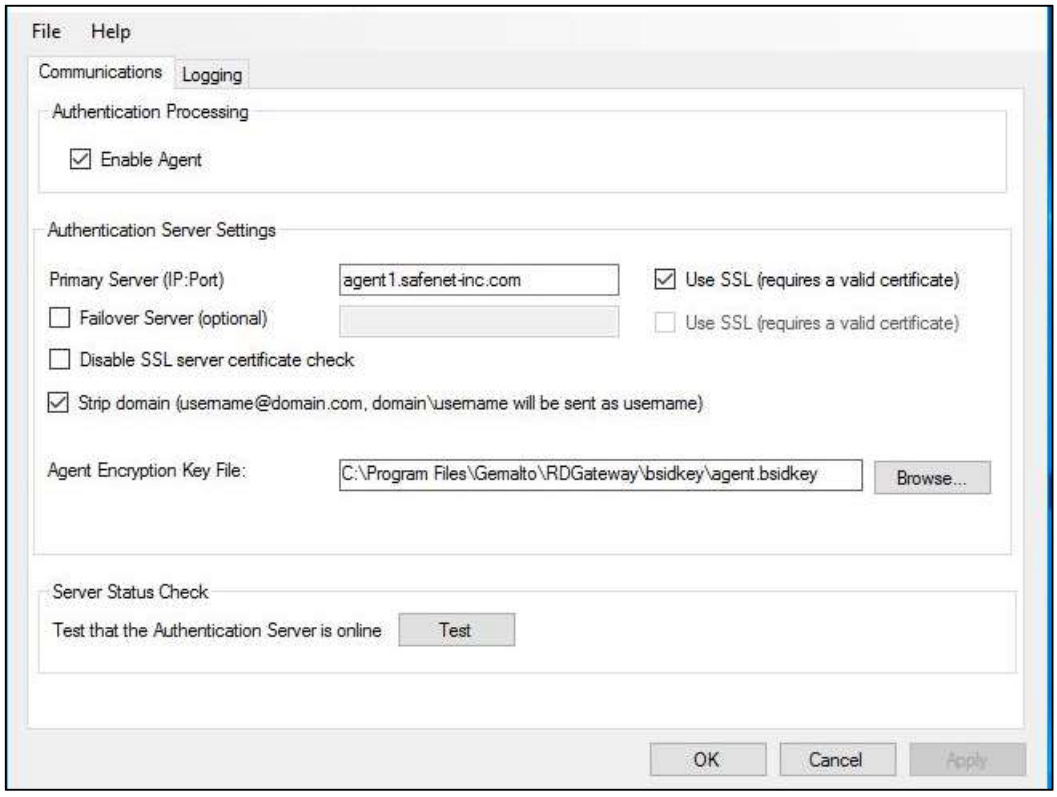
# CHAPTER 3: Configuration

## Configuring SafeNet Microsoft RDGateway Manager

Configure the agent using the **SafeNet Microsoft RDGateway Manager**.

### Communications

On the **SafeNet Microsoft RDGateway Manager**, click **Communications** tab.




Complete the following fields, and click **Apply**.

**Authentication Processing**

> **Enable Agent**: Select the check box to enable the agent.

**Authentication Server Settings**

> **Primary Server (IP:Port)**: This setting is used to configure the IP address/ hostname of the primary SAS server. Default Port: **80**
> Alternatively, **Use SSL** check box option can also be selected.
> Default TCP Port for SSL Requests: **443**

- **Failover Server (optional)**: This setting is used to configure the IP address/ hostname of the failover SAS server. Default Port: **80**
  Alternatively, **Use SSL** check box option can also be selected.
  Default TCP Port for SSL Requests: **443**

  **NOTE:** We strongly recommend using SSL.

- **Disable SSL server certificate check**: Select the check box option to disable the SSL server certificate error check.

  If the option is cleared, the agent checks if the certificate from the SAS server is correct. If selected, the certificate is not verified.

- **Strip domain (username@domain.com, domain\username will be sent as username)**: Select if the SAS username is required without the prefix **domain\ or** the suffix **@domain.**

- **Agent Encryption Key File**: This setting is used to specify the location of the agent's key file. The agent uses an encrypted key file to communicate with the authentication web service. This ensures all communication attempts made against the web service are from valid recognized agents.

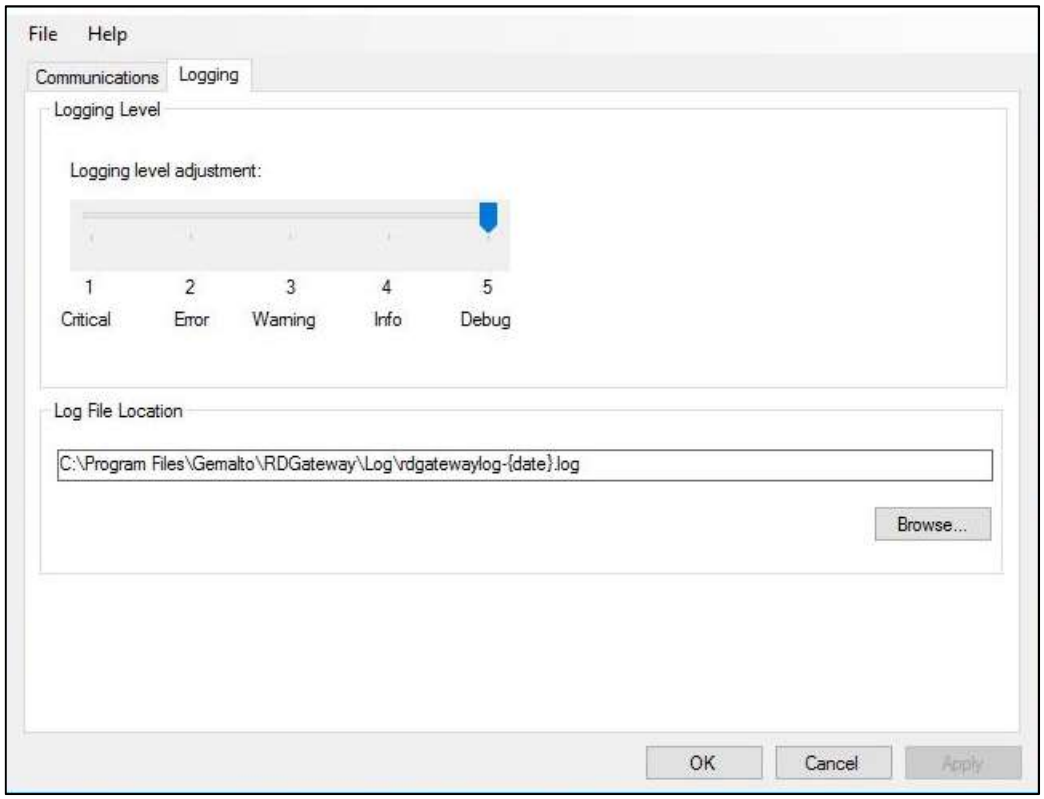
  **NOTE:** The administrator is advised to download a new **Agent.bsidkey** file from the SAS, and update the same (in the agent). To download the **Agent.bsidkey** file, follow the steps:
  1. Login to your SafeNet Authentication Service (SAS) account, and navigate to **COMMS > Authentication Processing**.
  2. Under **Task** list, click **Authentication Agent Settings** link and download the **Agent.bsidkey** file.
  The key file must be kept at a location accessible by all authorized users.

### Server Status Check

This function is used to execute a communication test to verify a connection to the SAS.

## Logging

On the **SafeNet Microsoft RDGateway Manager**, click **Logging** tab.




Complete the following settings, and click **Apply**.

### Logging Level

This setting adjusts the logging level. For log levels 1, 2, and 3, only the initial connection between the agent and the server, and any failed connection attempts are logged.

Drag the pointer on the **Logging level adjustment** scale to the required level:

**1 Critical** - Critical issues

**2 Error** - Critical issues and errors

**3 Warning** – Critical issues, errors, and warnings

**4 Info** – Critical issues, errors, warnings, and information messages.

**5 Debug** - All available information

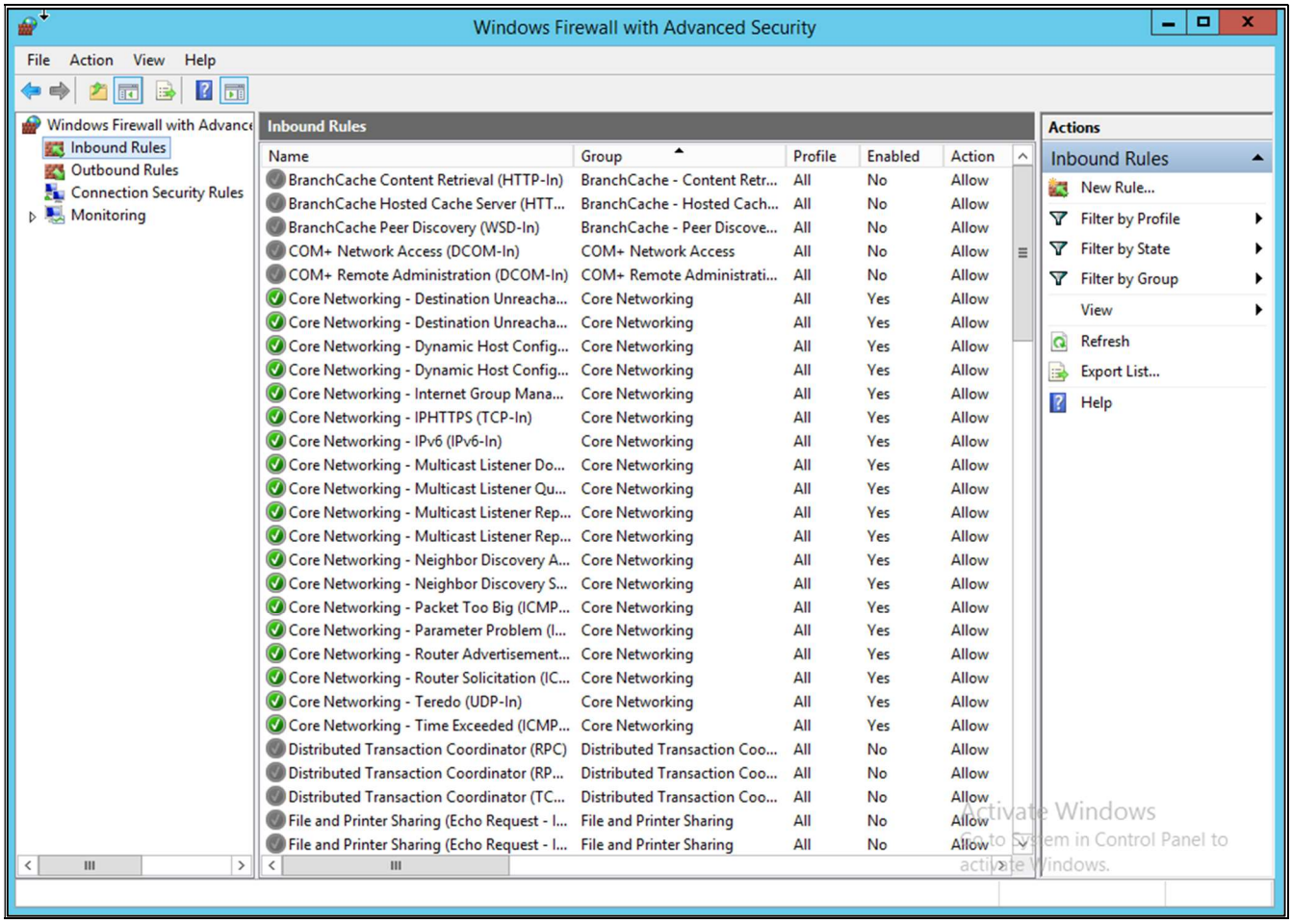
### Log File Location

This setting specifies the location where the log files will be saved. The log files are rotated on a daily basis.

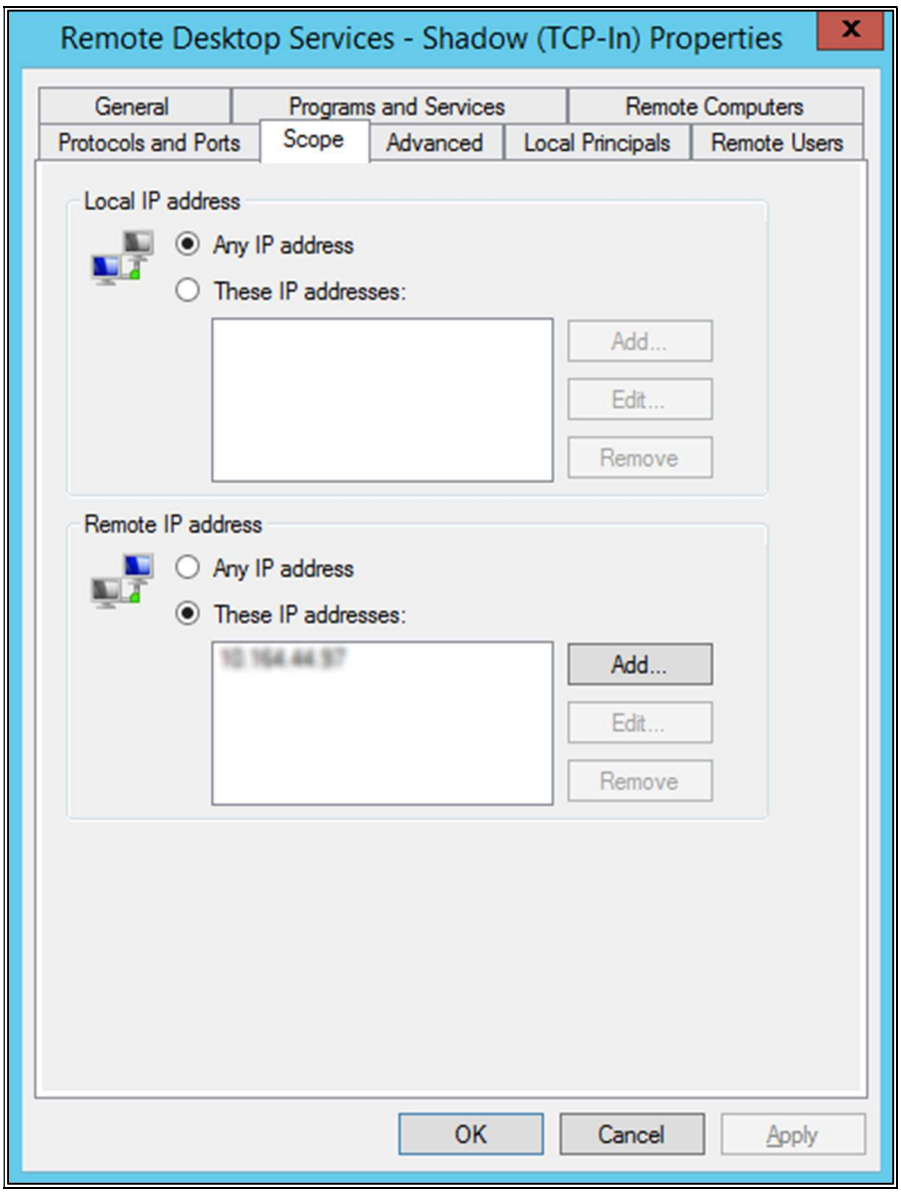
# Blocking Direct Access to Remote Machines

If a client machine can directly access the remote machine (session host), the SafeNet Agent for RD Gateway Agent will not work. To block direct access to the remote machine, complete the following steps:

1. On the remote machine, open **Windows Firewall with Advanced Security**.
2. In the left pane, click **Inbound Rules**.




3. In the middle pane, search for **Remote Desktop Services - Shadow (TCP-In)** and double-click it.
4. On the **Remote Desktop Services - Shadow (TCP-In) Properties** window, click the **Scope** tab.
5. Under **Remote IP address,** select **These IP addresses**.
6. Click **Add** and then add IP address of the RD Gateway server.
7. Click **OK**.




8. Repeat steps **3** to **7** for **Remote Desktop Services – User Mode (TCP-In)** and **Remote Desktop Services – User Mode (UDP-In)**.

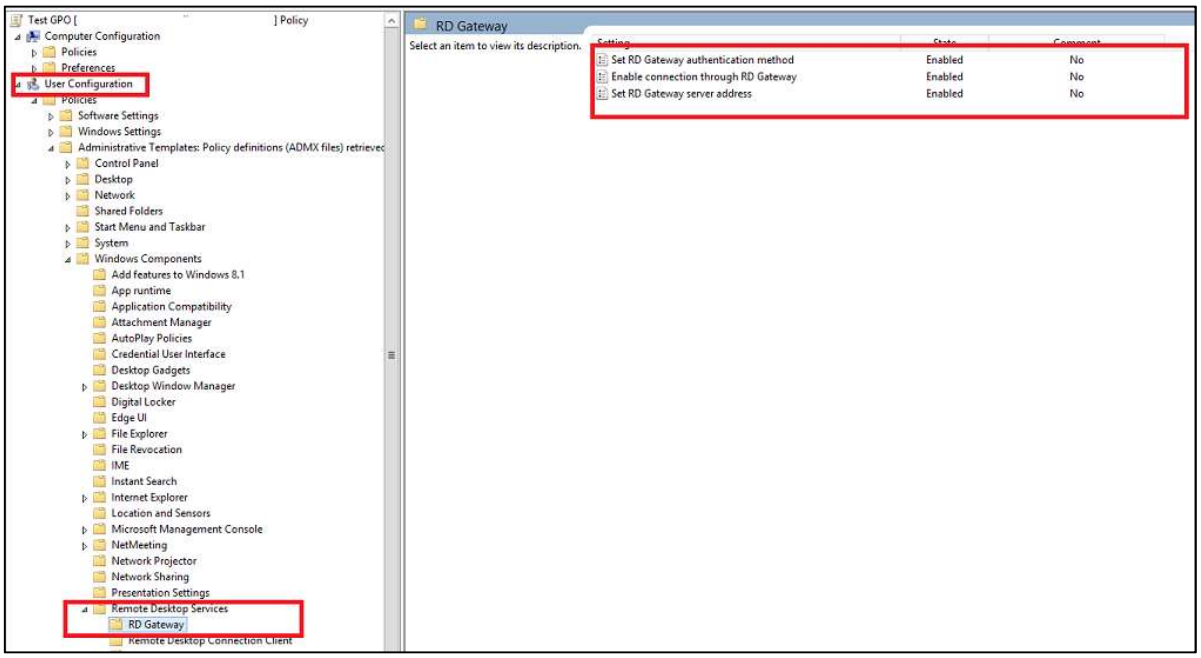
Now, connection to the remote machine can be established only through the RD Gateway server.

# Managing Remote Desktop Services Client Connections

To manage RD Services client connections using the Group Policy, follow the steps:

1. Navigate to **Start** > **Administrative Tools** > **Group Policy Management**.
2. From the left pane, locate the Organizational Unit (OU) you want to edit.
3. Modify an existing Group Policy Object (GPO) for the OU, or create a new one.
4. Right-click the GPO and click **Edit**.

5. Navigate to **User Configuration** > **Policies** > **Administrative Templates: Policy definitions (ADMX files) retrieved from the central store** > **Windows Components** > **Remote Desktop Services** > **RD Gateway**.




   a. Double-click **Enable connection though RD Gateway** option, and perform the following steps:

      i. Click **Enabled**.

      ii. Ensure that the **Allow users to change this setting** check box is not selected.

      iii. Click **OK**.

   b. Double-click **Set RD Gateway server address** option, and perform the following steps:

      i. Click **Enabled**.

      ii. Specify a valid, fully qualified domain name (FQDN) of the RD Gateway server or RD Gateway server farm.

      iii. Ensure that the **Allow users to change this setting** check box is not selected.

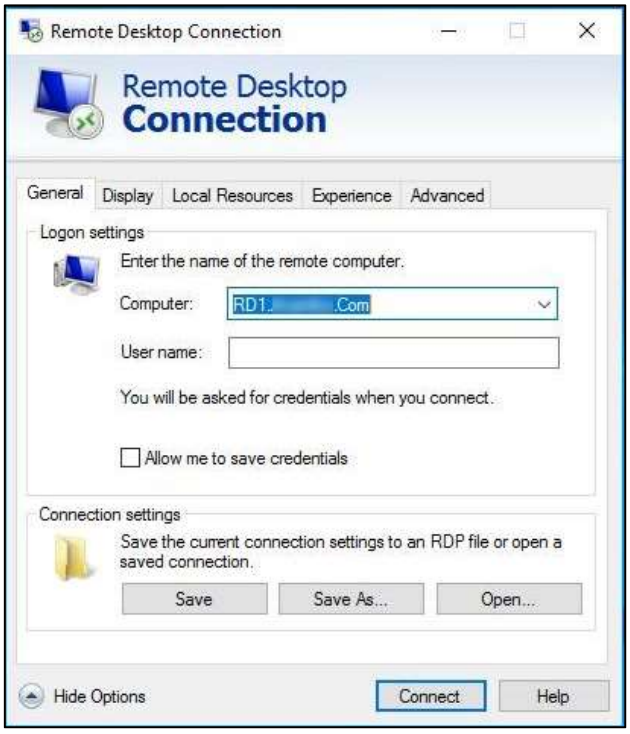
      iv. Click **OK**.

## Remote Desktop Gateway Server Settings

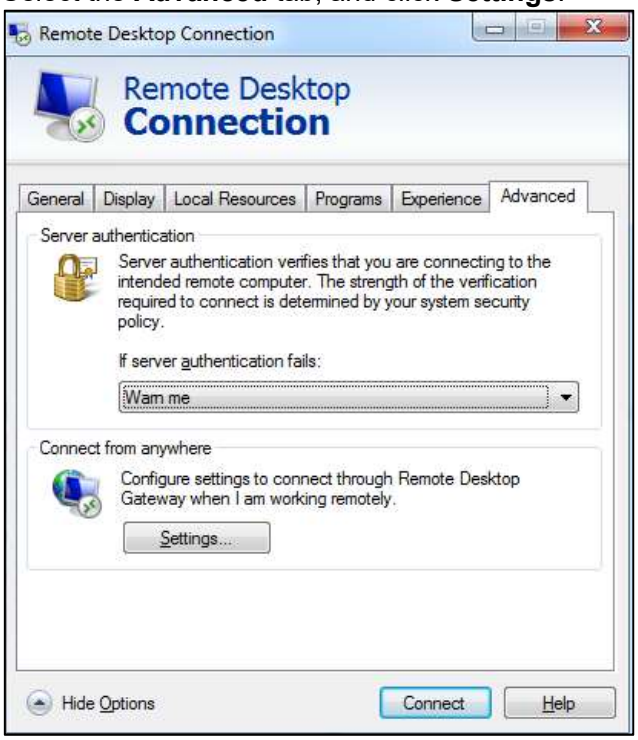
If RD Gateway server settings are not using the address from the Group Policy, the following updates are required to ensure proper functioning of the agent:

1. Open the Remote Desktop Connection from the Start screen.
2. Click **Show Options**, and select the **General** tab.

3. Enter the IP or hostname of the remote client machine in the **Computer** field.




4. Select the **Advanced** tab, and click **Settings**.




5. Perform/ ensure the following actions:

   - Select the **Use these RD Gateway server settings** radio option, and enter the **Server name**.

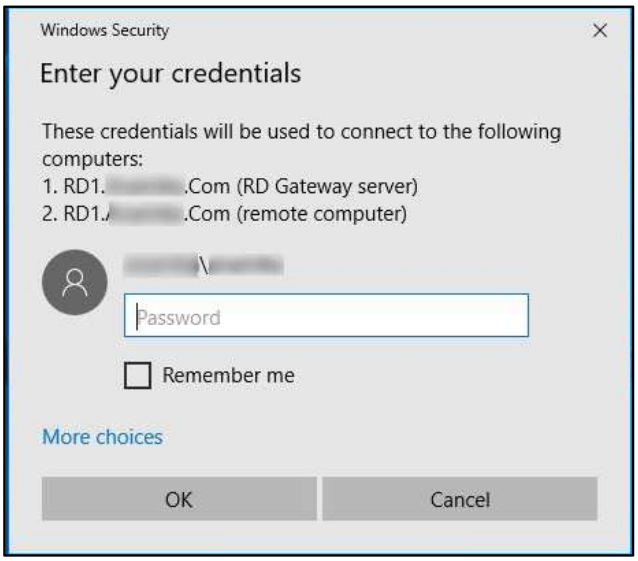
- Ensure that the **Bypass RD Gateway server for local addresses** option is not selected.
- Select the **Use my RD Gateway credentials for the remote computer** check box.


6. Click **OK**.

# CHAPTER 4: Running the Solution

To access any RD resource protected by the **SafeNet Agent for RD Gateway**, follow the steps:

1. Establish an RD connecting using the Microsoft Terminal Services Client.
2. Enter the AD password, and click **OK**.




3. The user will receive a prompt on their MobilePASS+ app (if enrolled), to accept or reject the logon request.
4. On accepting the logon request, the user will be able to access the protected RD resource.

# CHAPTER 5: Troubleshooting

## Creating Installation Log

If you require to create the installation log, execute the installer from the command prompt using the following command:

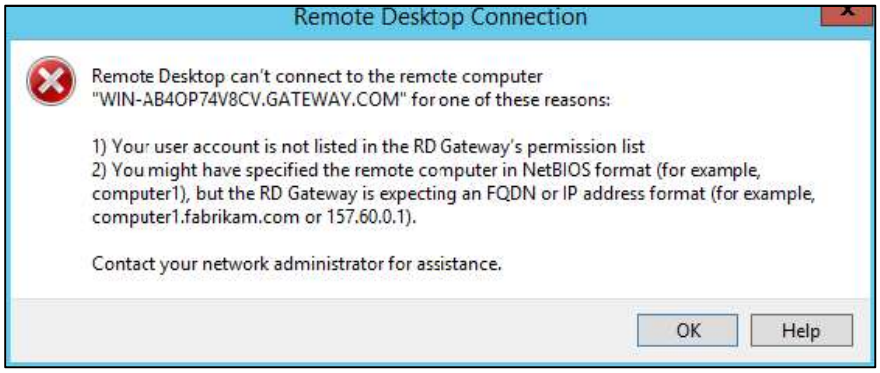
```
SafeNet Agent for Microsoft RDGateway.exe /v"/l*v setup.log"
```

## Resolving Authentication Bypasses

If the SafeNet authentication is not getting invoked consistently, ensure that the **Bypass RD Gateway server for local addresses** option is not selected in your **RD Gateway Server Settings**.

## Error Handling

1. Error Message: The following **Permissions and NetBIOS** error message is encountered while launching the RDP file:



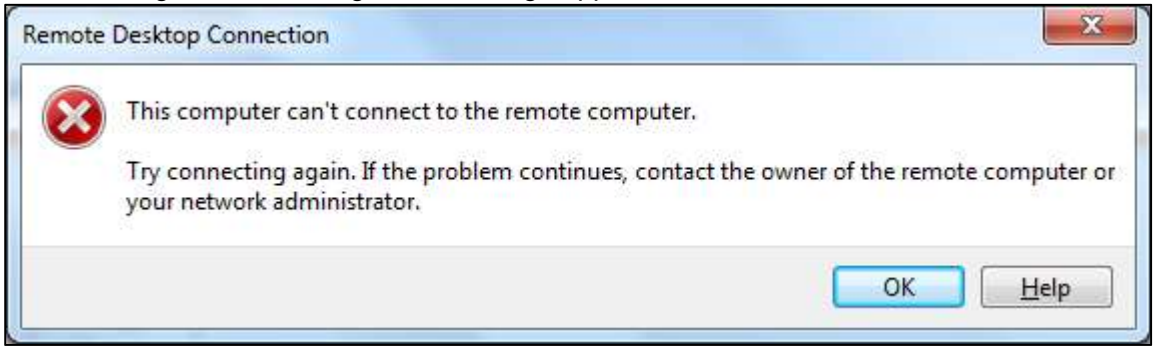

   Solution: Review the Resource Authorization Policy (RAP) and ensure that it is in the right order.

2. Error Message: The following error message appears when the RD Gateway Service is in the **Stopping** or **Stopped** state:

Solution: If the RD Gateway service is in the **Stopped** state, restart the service. If the RD Gateway service is in the **Stopping** state, kill the service and start again. Check if the service is in the **Running** state and try to connect again.

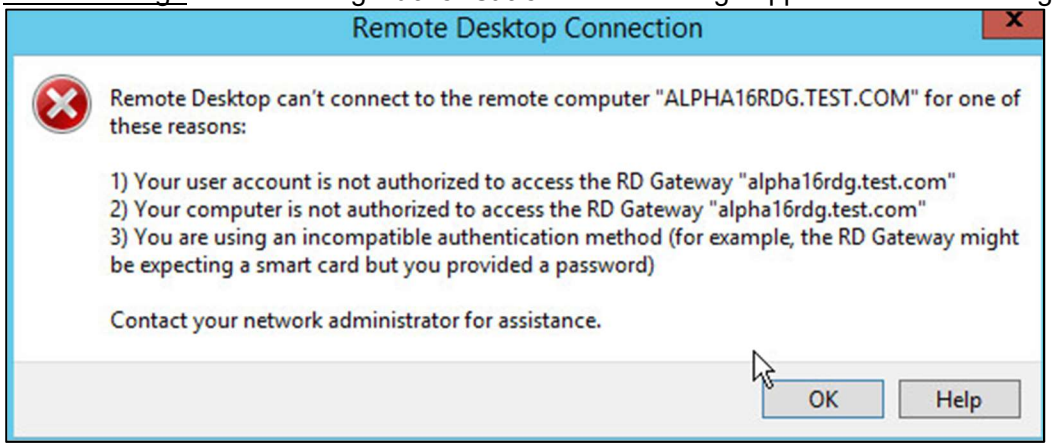
> **NOTE:** If the RD Gateway service takes longer to start, update the settings using the Management Console and ensure that the RD Gateway service is up and running.

3. Error Message: The following error message appears when the Session Host is not reachable.




Solution: The error message indicates that either the machine is switched off, or some network issue exists. Check if the session host machine can be communicated with, ping the machine to verify.

4. Error Message: The following **Authorisation** error message appears while launching the RDP file:




Solution: Review the Resource Authorization Policy (RAP) and ensure that it is in the right order.

5. Error Message: The following error message appears when someone tries to establish a parallel session with a session host, using the same credentials. The last connection remains established. The prior connection shows this error message and the RD connection terminates.