THALES

SafeNet Agent for Remote Desktop Gateway 2.0.4

INSTALLATION AND CONFIGURATION GUIDE

Document Information

Product Version	2.0.4
Document Part Number	007-000361-001, Rev. E
Release Date	May 2022

Trademarks, Copyrights, and Third-Party Software

Copyright © 2022 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

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**.

Customer Release Notes

The Customer Release Notes (CRN) document provides important information about this release that is not included in other customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release.

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: > Command-line commands and options (Type **dir /p**.) > Button names (Click **Save As**.) > Check box and radio button names (Select the **Print Duplex** check box.) > Window titles (On the **Protect Document** window, click **Yes**.) > Field names (**User Name:** Enter the name of the user.) > Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.)

	> 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] [<optional>] [a | b | c] [<a> | <b> | <c>]	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. 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 }
{ <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.

> **NOTE:** The SafeNet Agent for RD Gateway version 1.0 is not supported in high availability Remote Desktop Services configuration.

The SafeNet Agent for RD Gateway is built on top of Microsoft Pluggable Authentication and Authorization (PAA) framework in combination with an integrated approach to provide uniform user login experience on the Microsoft Remote Desktop Web Portal. The Remote Desktop Gateway Agent comprises of the following four components:

1. **PAA Plugin**: This is built on top of Microsoft PAA framework, and sits and runs on the server which is configured as a Remote Desktop Gateway.

2. **SafeNet RD Gateway Monitor service**: This service monitors the connections established between the client machine and Session Hosts via RD Gateway, and disconnects any session that is invalid.

3. **Remote Desktop Web Update**: Remote Desktop Web Access (RD Web Access), formerly Terminal Services Web Access (TS Web Access), enables users to access Remote Desktop Connections.

   RD Web Access includes Remote Desktop Web Connection, which enables users to connect remotely to the desktop of any computer where they have Remote Desktop access. In order to support strong authentication at RD Gateway, some updates have been incorporated in the RD Web. This part of the solution includes custom login page module, default page module, and inbuilt security modules that together with the other solution components enable strong authentication of the user at RD Gateway.

4. **ActiveX for SafeNet Agent**: A custom Active X component will handle the direct invocation of RDP session from within the Internet Explorer.

   The Pluggable Authentication and Authorization (PAA) framework for RD Gateway provided by Microsoft allows custom authentication and authorization routines to be used with RD Gateway. This can provide custom two-factor authentication and works seamlessly with Remote Desktop Web Access (RD Web Access) or RDP file resource launching.

Agent Features

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

- **Resource Access Duration**: The user is allowed access to a remote resource only for a specific duration, which is set by the administrator.
- **One-time Usage of RDP File**: Once the RDP file is used to access a remote resource, that RDP file cannot be used again unless the administrator permits.
- **Binding an RDP File to an IP Address**: The RDP file can be accessed only from the machine where the RDP file was downloaded. If the RDP file is copied to another machine then the user's session will be forcefully disconnected.
- **Binding a User to an RDP File**: The remote resource can be accessed only from the user login using which the RDP file was downloaded. If any other user tries to access the remote resource, the session will be forcefully disconnected.
- **Support of Native RAP**: The SafeNet Agent for RD Gateway supports native Microsoft authorization.
- **Direct Access Prevention**: The SafeNet Agent for RD Gateway restricts access to users who do not come through RD Web. That is, if the user provides the gateway host directly on the remote desktop connection, the connection is denied.
- **Application Support**: The SafeNet Agent for RDGateway does not support Microsoft Remote Applications and some functionalities may not work.

System Requirements

This guide is applicable to the following:

Operating Systems	• Windows Server 2012 R2 (64-bit) • Windows Server 2016 (64-bit) • Windows Server 2019 (64-bit)
Architecture	64-bit
Web Servers	• IIS 8.5 • IIS 10

Operating System and Web Browsers for ActiveX (Client Machine)	**Operating System**: • Windows 10 **Web Browsers**: • Internet Explorer 11 (supported till June 15, 2022) • Microsoft Edge* * Since, Microsoft will retire Internet Explorer 11 on June 15, 2022, we recommend using Microsoft Edge with Internet Explorer mode. For more details, see Enable IE mode in Edge browser section.

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

> Ensure that users are able to access the remote resource via RD Web access prior to deploying the agent.

> Ensure that the SafeNet Agent for RD Web is installed and configured on the machine which hosts RD Web.

> Administrative rights are required for installation and configuration of the SafeNet Agent for RD Gateway.

> The RD Services (TermService) should not be running on the remote desktop gateway machine unless the operator needs to remotely manage it.

> The 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.

> General purpose SHA1/SHA256 certificate (for RDP file digital signing) and SHA256 certificate (for gateway access token signing) must exist in both the RD Web and RD Gateway machines.

> .NET framework 4.0 (or above) must exist on both the RD Web and RD Gateway machines.

> Ensure that the RDG_CAP_AllUsers policy is enabled.

> Ensure that the user has the 'log on as a service' permission before using the Service Control (SC) command.

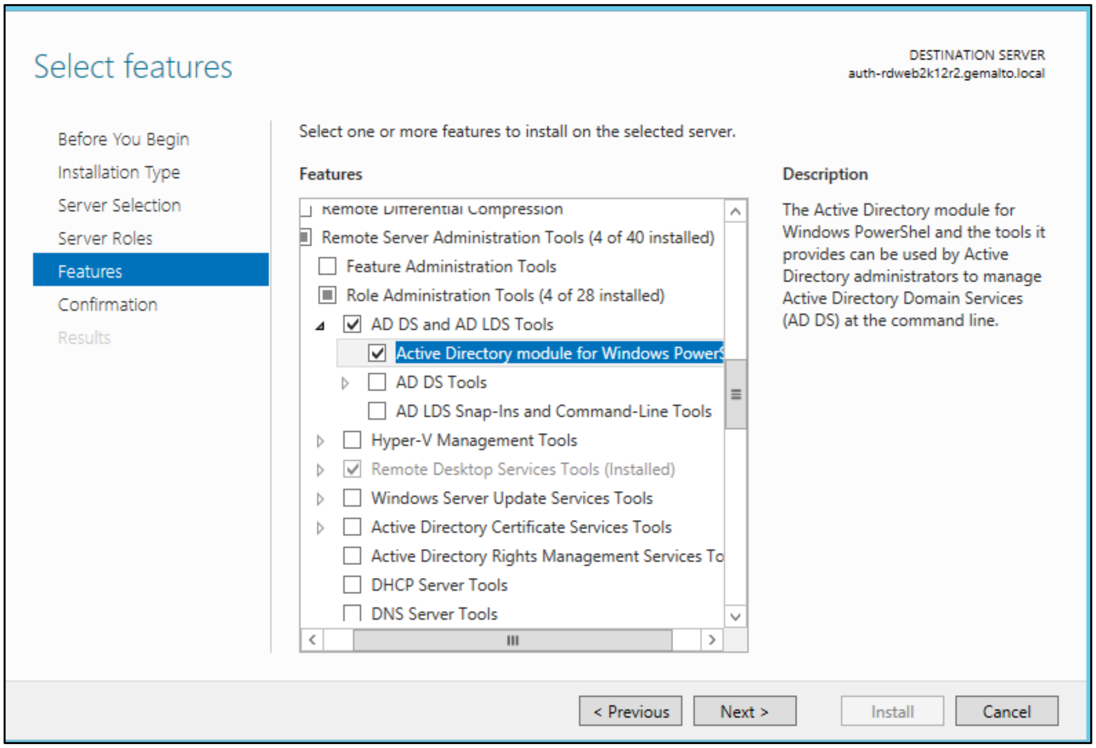
When you configure a service to run under a specific account via Service Properties, Windows automatically grants the account the ‘log on as a service’ permission. Before using the SC command (***sc.exe***) to create the Windows Service (via installer), the administrator has to grant the user the ‘log on as a service’ permission. This setting determines which user accounts can register a process as a service. Running a process as a service avoids the need for human intervention. To configure a user account to have ‘log on as a service’ permission, follow the steps:

Note: The ‘log on as a service’ permission applies only to the local computer and must be granted in the Local Security Policy of the computer.

1. Login to the computer with administrative privileges.
2. Open the administrative tools by selecting **Start** > **Control Panel** > **System and Security** > **Administrative Tools**.
3. Click **Local Security Policy** from the list of file names. The **Local Security Policy** dialog box opens.
4. Expand **Local Policies** by clicking its icon in the left navigation pane. The constituent files list in the right pane.
5. Double-click **User Rights Assignment** from the list.
6. Locate **Log on as a service**, right-click its icon and select **Properties**. The **Log on as a service Properties** dialog box opens.
7. Click **Add User or Group…** to add a new user(s).
8. Search the user(s) using **Select Users, Computers, Service Accounts, or Groups** dialog box, and click **OK**. You can search for multiple users by separating each user name with a semicolon.

Note: Ensure that the user(s) you have added (using the above process) is not listed in the **Deny log on as a service** policy in the Local Security Policy.

> For the agent installer to run successfully, the **Active Directory for Windows PowerShell** feature must be enabled on the Windows Server.



Select features

DESTINATION SERVER
auth-rdweb2k12r2.gemalto.local

Select one or more features to install on the selected server.

Features

- □ Remote Differential Compression
- ▣ Remote Server Administration Tools (4 of 40 installed)
  - □ Feature Administration Tools
  - ▣ Role Administration Tools (4 of 28 installed)
    - ☑ AD DS and AD LDS Tools
      - ☑ Active Directory module for Windows PowerS
      - □ AD DS Tools
      - □ AD LDS Snap-Ins and Command-Line Tools
    - □ Hyper-V Management Tools
    - ☑ Remote Desktop Services Tools (Installed)
    - □ Windows Server Update Services Tools
    - □ Active Directory Certificate Services Tools
    - □ Active Directory Rights Management Services To
    - □ DHCP Server Tools
    - □ DNS Server Tools

Description

The Active Directory module for Windows PowerShel and the tools it provides can be used by Active Directory administrators to manage Active Directory Domain Services (AD DS) at the command line.

Enable the feature by following the steps:

1. Open **Server Manager**.
2. Click **Add roles and features**.
3. Navigate to **Features** tab.
4. Navigate to **Remote Server Administration Tools** > **Role Administration Tools** > **AD DS and AD LDS Tools**.
5. Select the **Active Directory module for Windows PowerShell** checkbox, and click **Next**.
6. Select the **Restart the destination server automatically if required** checkbox, and install the feature.

CHAPTER 2: Installation

Installing the Agent

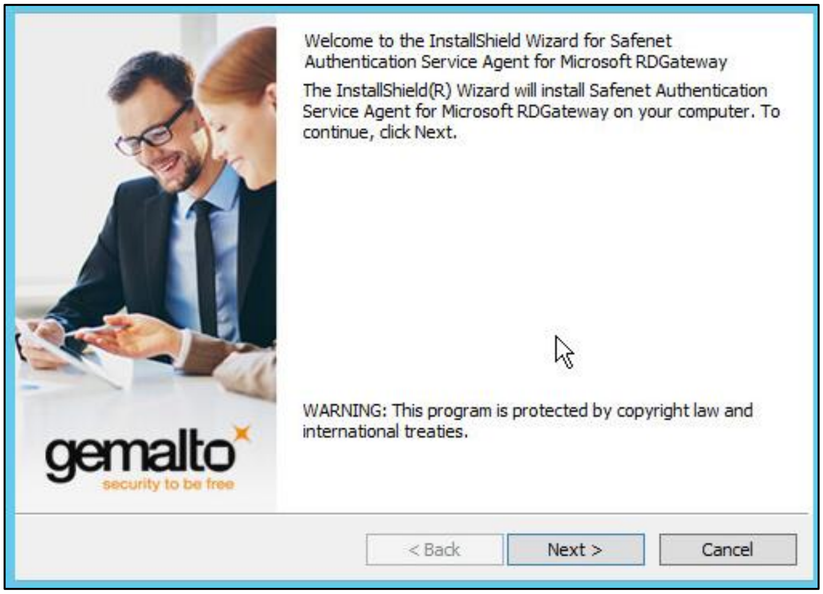
You need to install three components of the SafeNet Agent for RD Gateway—RD Gateway Plugins, RD Gateway Monitor, and RD Web. The RD Gateway Plugins and RD Gateway Monitor components of the agent are to be installed on the computer where you have set up RD Gateway. Similarly, the RD Web component of the agent is to be installed on the computer where you have set up RD Web. For installing all the components, you have only one installer.

> **NOTE:** Installer will always be in the English language, irrespective of the language of the operating system.

1. Run the **Safenet Agent for Microsoft RDGateway** installer.

   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 run successfully. Otherwise, a window will appear requiring you to provide administrator credentials.

2. On the **Welcome to the InstallShield Wizard for SafeNet Authentication Service Agent for Microsoft RDGateway** window, click **Next**.

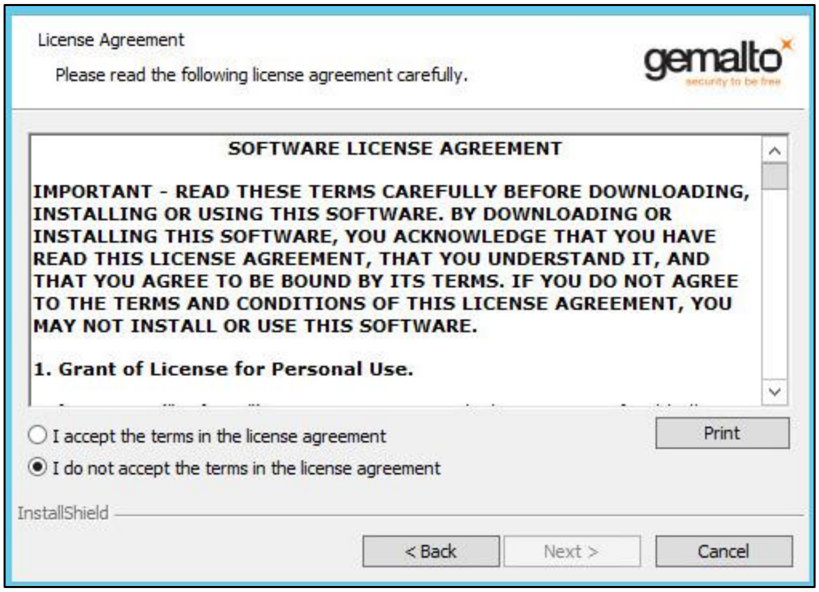


Welcome to the InstallShield Wizard for Safenet Authentication Service Agent for Microsoft RDGateway

The InstallShield(R) Wizard will install Safenet Authentication Service Agent for Microsoft RDGateway on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3. On the **License Agreement** window, read the software license agreement and to proceed, select **I accept the terms in the license agreement** option, and click **Next**.



License Agreement

Please read the following license agreement carefully.

SOFTWARE LICENSE AGREEMENT

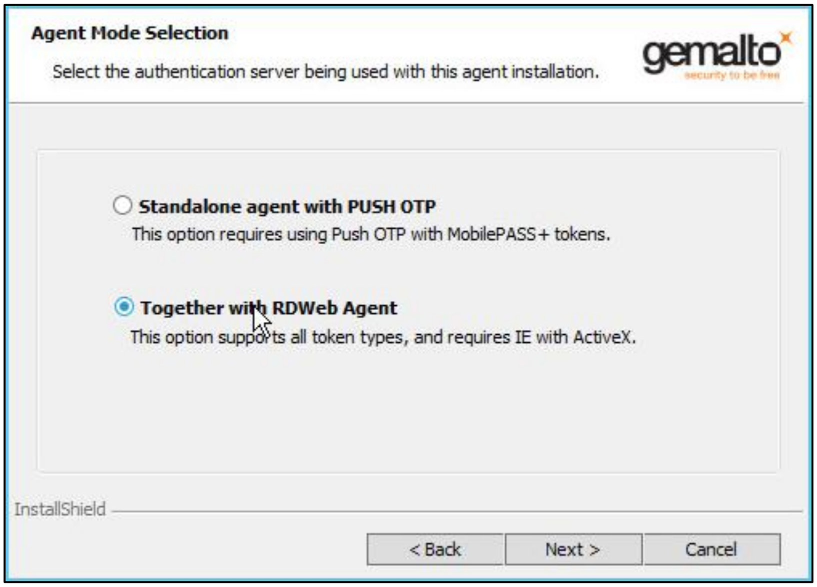
IMPORTANT - READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THIS SOFTWARE. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU MAY NOT INSTALL OR USE THIS SOFTWARE.

1. Grant of License for Personal Use.

○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement

4. On the **Agent Mode Selection** screen, select the **Together with RDWeb Agent** radio option, and click **Next**.



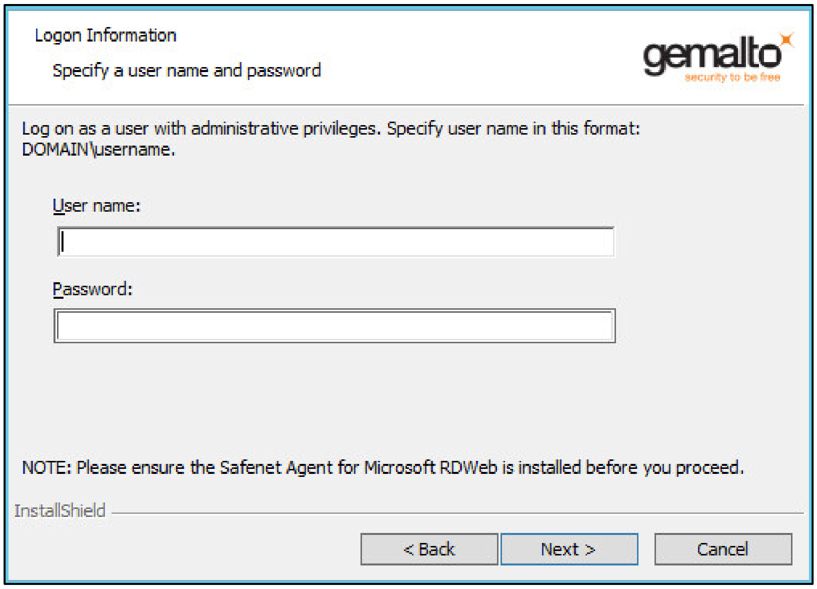
Agent Mode Selection

Select the authentication server being used with this agent installation.

○ **Standalone agent with PUSH OTP**
This option requires using Push OTP with MobilePASS+ tokens.

● **Together with RDWeb Agent**
This option supports all token types, and requires IE with ActiveX.

5. On the **Logon Information** window, enter the credentials of a user with administrator privileges or a user who is a member of the Domain Admin group, and click **Next**.



Logon Information

Specify a user name and password

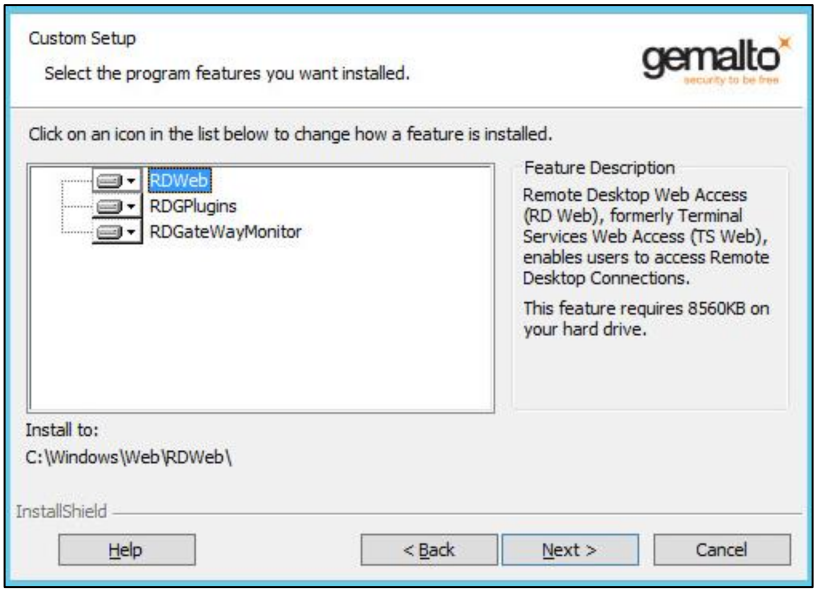
Log on as a user with administrative privileges. Specify user name in this format: DOMAIN\username.

User name:

Password:

NOTE: Please ensure the Safenet Agent for Microsoft RDWeb is installed before you proceed.

6. On the **Custom Setup** window, clear the components that you do not want to install, and click **Next**.
   a. For **RD Gateway**, **RDGatewayMonitor** and **RDGPlugins** features need to be installed.
   b. For **RD Web**, only **RDWeb** feature needs to be installed.



Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- RDWeb
- RDGPlugins
- RDGateWayMonitor

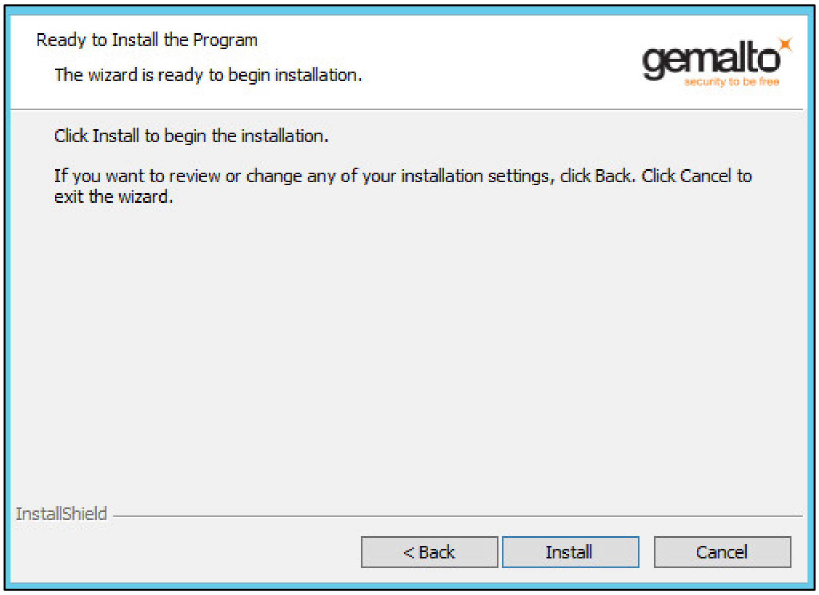
Feature Description

Remote Desktop Web Access (RD Web), formerly Terminal Services Web Access (TS Web), enables users to access Remote Desktop Connections.

This feature requires 8560KB on your hard drive.

Install to:
C:\Windows\Web\RDWeb\

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



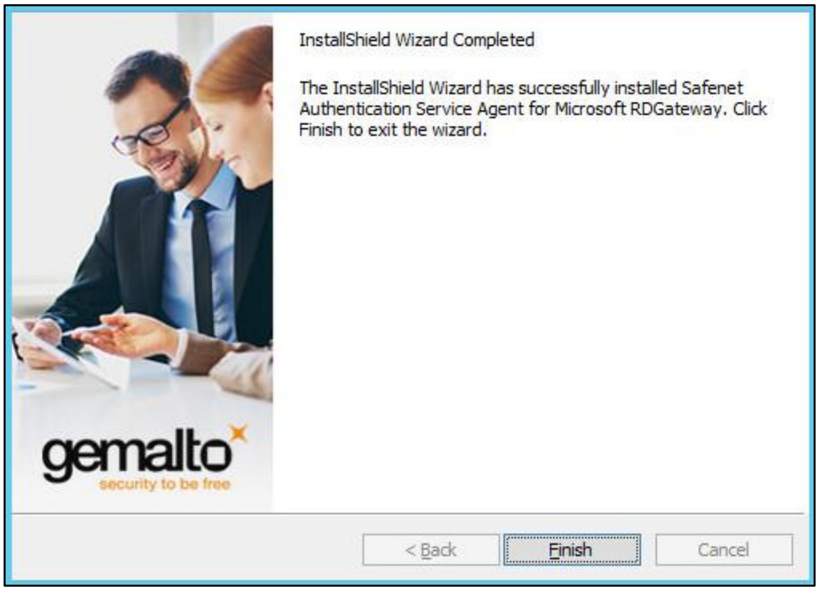
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Safenet Authentication Service Agent for Microsoft RDGateway. Click Finish to exit the 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, **Together with RDWeb** supports upgrade from version 2.0.0 (and above).

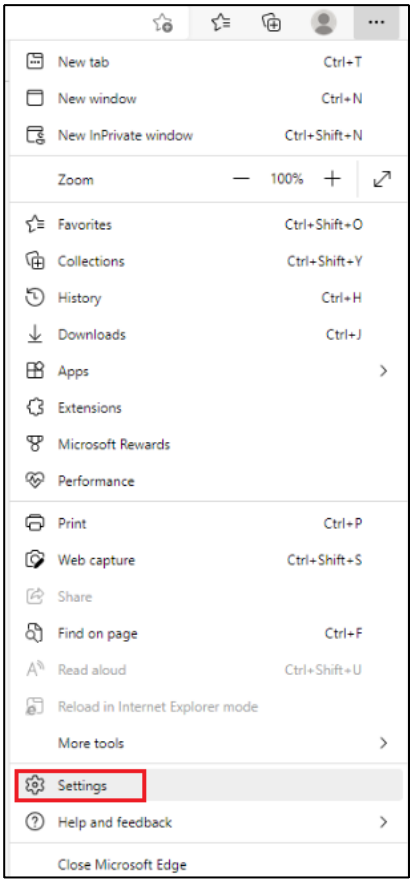
> **NOTE:** Upgrade from earlier versions (v1.0, v1.1.0 and v1.1.1) is not supported.

CHAPTER 3: Configuration

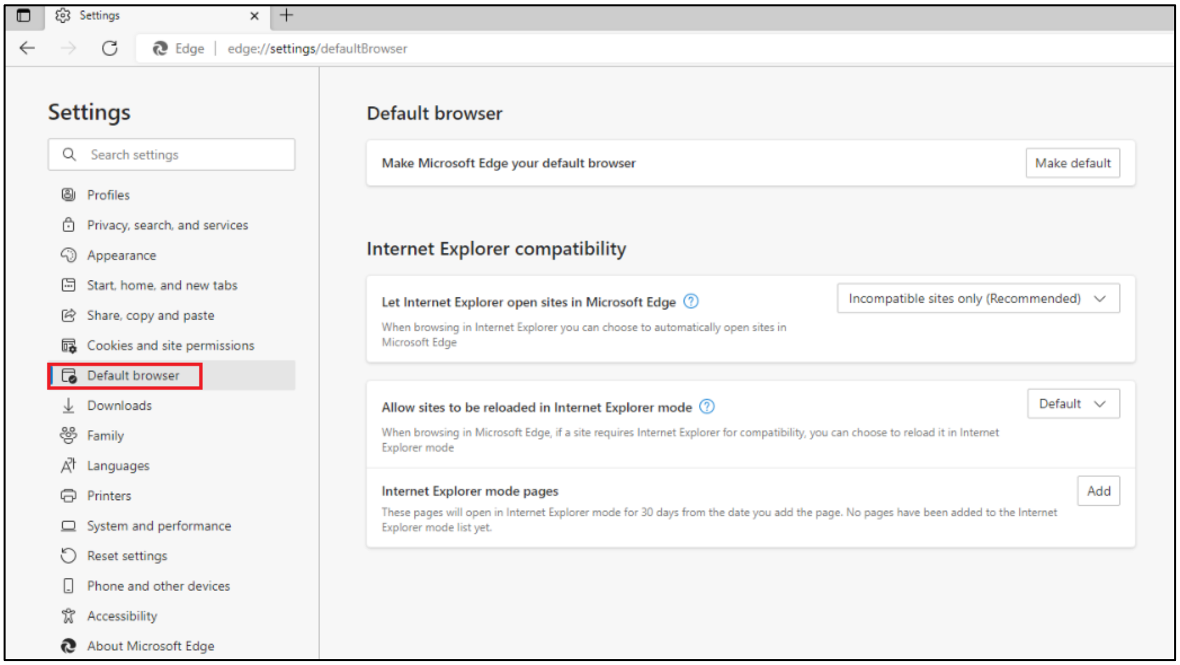
Enable IE mode in Edge browser

Perform the following steps to enable Internet Explorer (IE) mode on Microsoft Edge:

1. Open the Microsoft Edge browser.
2. Click **Options** in the top-right corner of the Edge browser and select **Settings**.



3. In the left pane, under **Settings**, click **Default browser**.



Default browser

Make Microsoft Edge your default browser

Internet Explorer compatibility

Let Internet Explorer open sites in Microsoft Edge: Incompatible sites only (Recommended)

When browsing in Internet Explorer you can choose to automatically open sites in Microsoft Edge

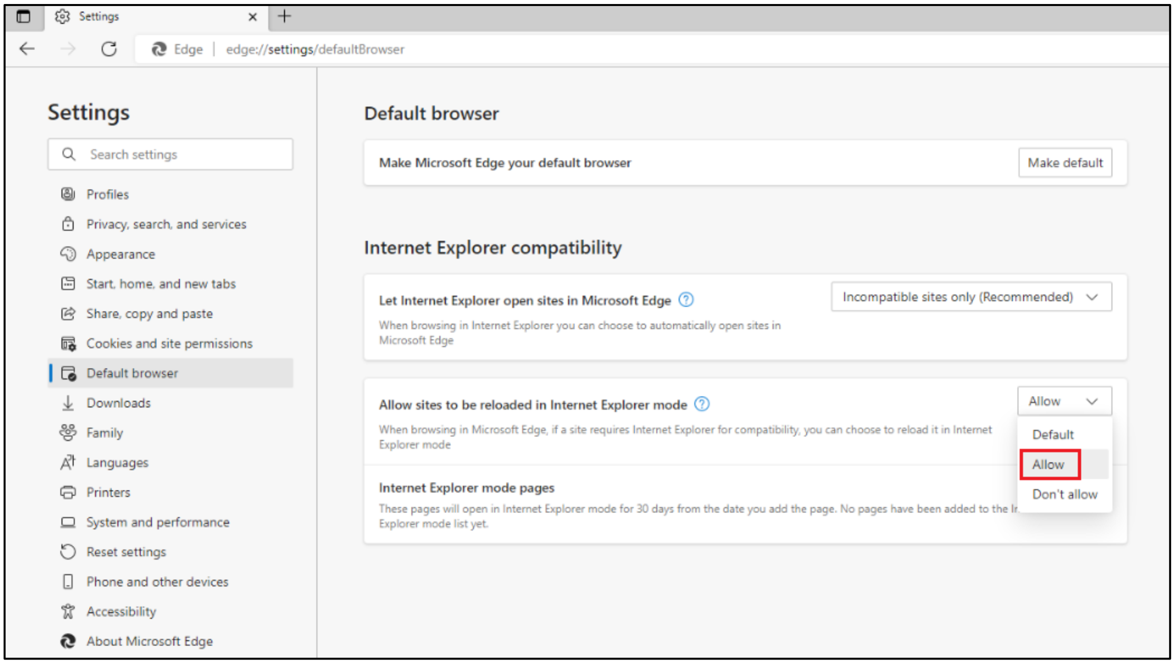
Allow sites to be reloaded in Internet Explorer mode: Default

When browsing in Microsoft Edge, if a site requires Internet Explorer for compatibility, you can choose to reload it in Internet Explorer mode

Internet Explorer mode pages

These pages will open in Internet Explorer mode for 30 days from the date you add the page. No pages have been added to the Internet Explorer mode list yet.

4. Select **Allow** from the **Allow sites to be reloaded in Internet Explorer mode** dropdown.



Default browser

Make Microsoft Edge your default browser

Internet Explorer compatibility

Let Internet Explorer open sites in Microsoft Edge: Incompatible sites only (Recommended)

When browsing in Internet Explorer you can choose to automatically open sites in Microsoft Edge

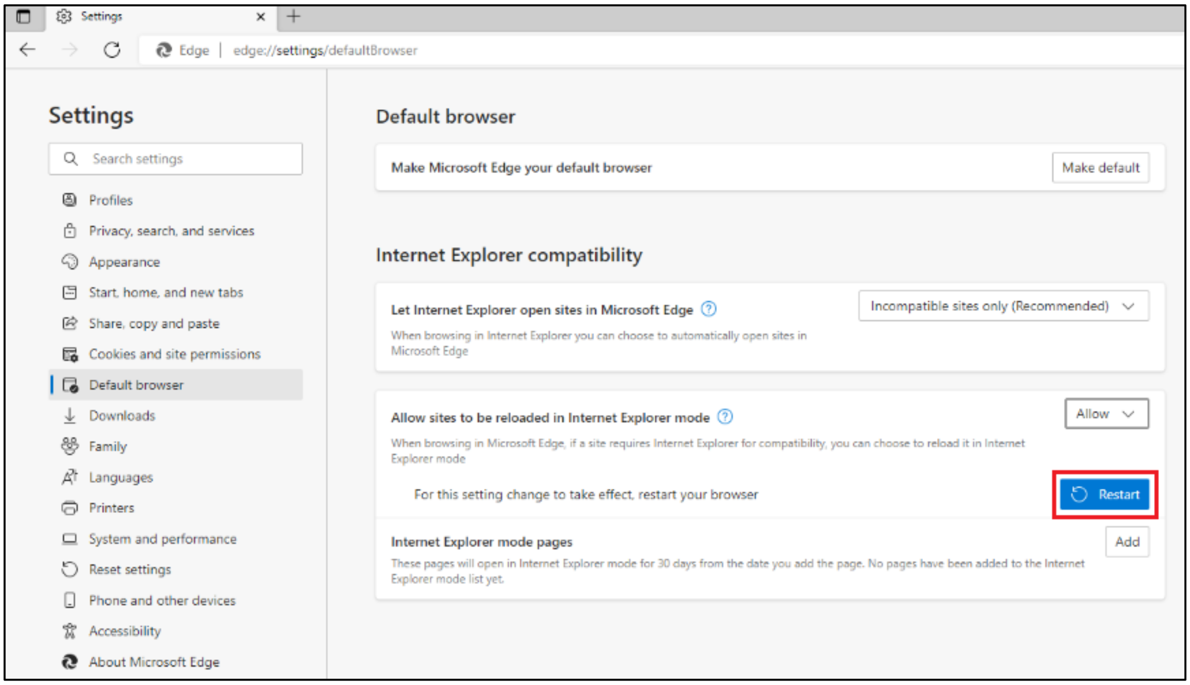
Allow sites to be reloaded in Internet Explorer mode: Allow

When browsing in Microsoft Edge, if a site requires Internet Explorer for compatibility, you can choose to reload it in Internet Explorer mode

Internet Explorer mode pages

These pages will open in Internet Explorer mode for 30 days from the date you add the page. No pages have been added to the In Explorer mode list yet.

5. You will be prompted to restart the browser. Click **Restart**.



Default browser

Make Microsoft Edge your default browser

Internet Explorer compatibility

Let Internet Explorer open sites in Microsoft Edge: Incompatible sites only (Recommended)

When browsing in Internet Explorer you can choose to automatically open sites in Microsoft Edge

Allow sites to be reloaded in Internet Explorer mode: Allow

When browsing in Microsoft Edge, if a site requires Internet Explorer for compatibility, you can choose to reload it in Internet Explorer mode

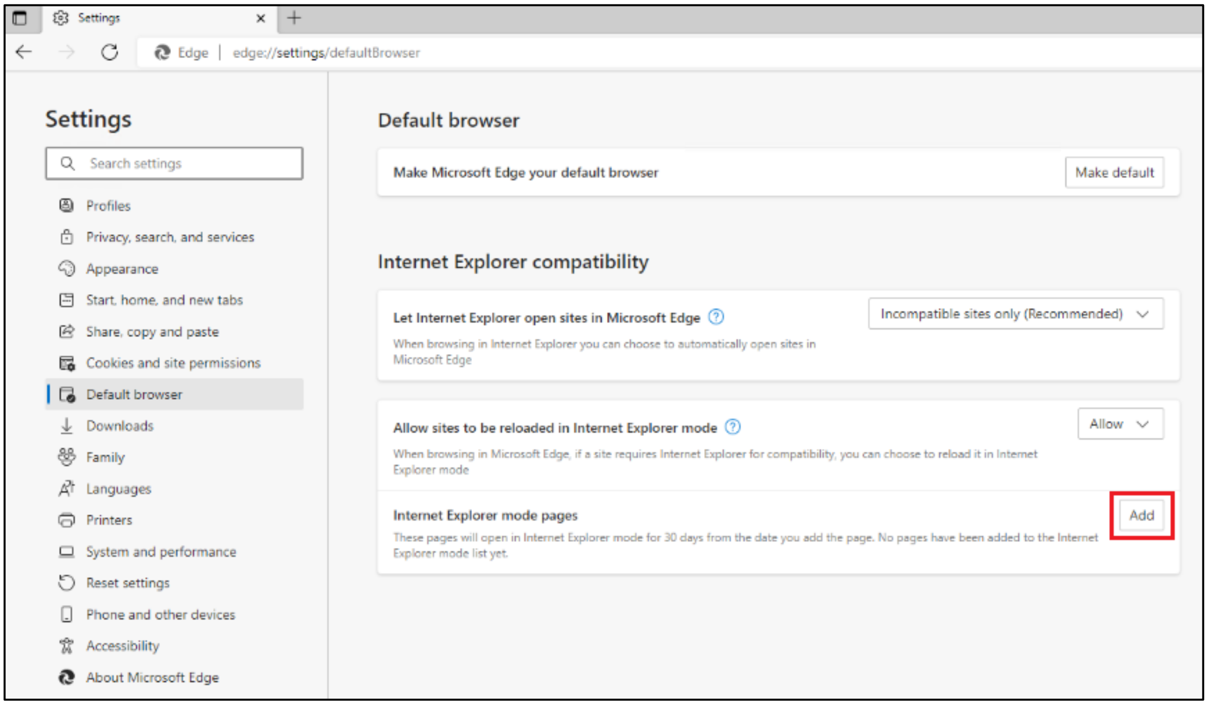
For this setting change to take effect, restart your browser

Internet Explorer mode pages

These pages will open in Internet Explorer mode for 30 days from the date you add the page. No pages have been added to the Internet Explorer mode list yet.

Alternatively, you can restart the Edge browser.

6. Click **Add** next to **Internet Explorer mode pages**.



Default browser

Make Microsoft Edge your default browser

Internet Explorer compatibility

Let Internet Explorer open sites in Microsoft Edge: Incompatible sites only (Recommended)

When browsing in Internet Explorer you can choose to automatically open sites in Microsoft Edge

Allow sites to be reloaded in Internet Explorer mode: Allow

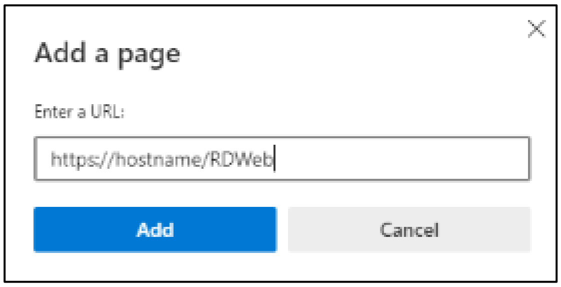
When browsing in Microsoft Edge, if a site requires Internet Explorer for compatibility, you can choose to reload it in Internet Explorer mode

Internet Explorer mode pages

These pages will open in Internet Explorer mode for 30 days from the date you add the page. No pages have been added to the Internet Explorer mode list yet.

Add a page pop-up window will be displayed.

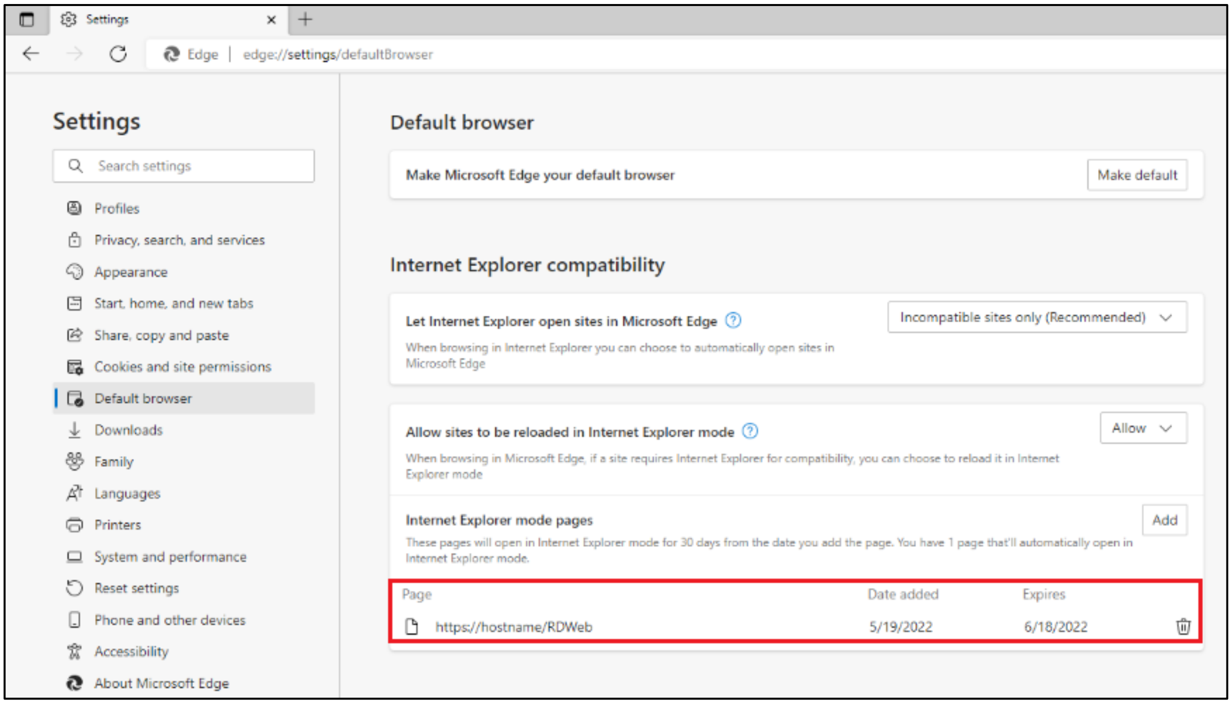
7. In the **Enter a URL** field, enter the RDWeb URL, for example, https://<hostname>/RDWeb. Click **Add.**



Add a page

Enter a URL: https://hostname/RDWeb

The URL will be added to the Page list.



Default browser

Make Microsoft Edge your default browser — Make default

Internet Explorer compatibility

Let Internet Explorer open sites in Microsoft Edge: Incompatible sites only (Recommended)

When browsing in Internet Explorer you can choose to automatically open sites in Microsoft Edge

Allow sites to be reloaded in Internet Explorer mode: Allow

When browsing in Microsoft Edge, if a site requires Internet Explorer for compatibility, you can choose to reload it in Internet Explorer mode

Internet Explorer mode pages — Add

These pages will open in Internet Explorer mode for 30 days from the date you add the page. You have 1 page that'll automatically open in Internet Explorer mode.

Page	Date added	Expires
https://hostname/RDWeb	5/19/2022	6/18/2022

Certificates

The following types of certificates are required:

> **SHA256 signed certificate used for gateway access token signing with a private key** — To be installed at **Local Computer** > **Personal** on RD Web Server.

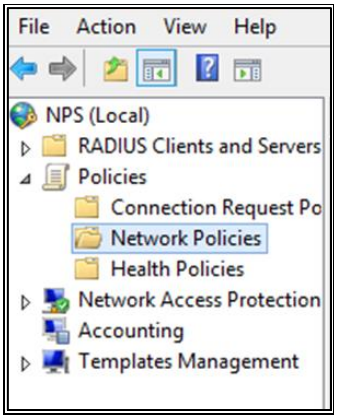
For details on creating certificates for gateway access tokens, refer Appendix C.

> **General purpose SHA1/SHA256 signed certificate, which is capable of digital signing** — To be installed at **Local Computer** > **Personal** on RD Web. The purpose of this certificate is to identify the publisher of the RDP file to the user. It is recommended that the certificate is either generated from a trusted enterprise Certificate Authority (CA) or from any of the commercial certificate authorities. This certificate type (SHA1 or SHA256) should be the same as the one used for your default RD Web setup. It comes with the default RD Web install and helps in identification of the entity, which is distributing the RDP file, in this case, the enterprise itself.

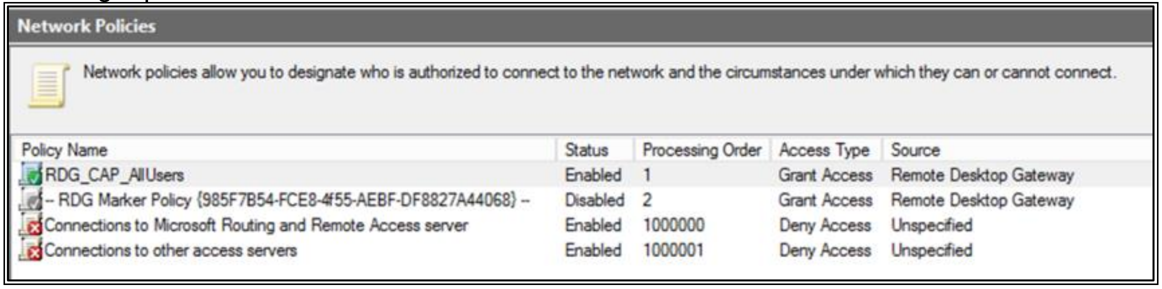
> **NOTE:** If RD Web and RD Gateway are deployed on separate machines, create the SHA256 certificate on the RD Web machine, and then export it without a private key to the RD Gateway machine. The RD Web needs a certificate with the private key, whereas RD Gateway needs only the public key.

Configuring RDG_CAP_AllUsers Network Policy

1. Open the **Network Policy Server** application.
2. In the left pane, click **NPS** > **Policies** > **Network Policies**.



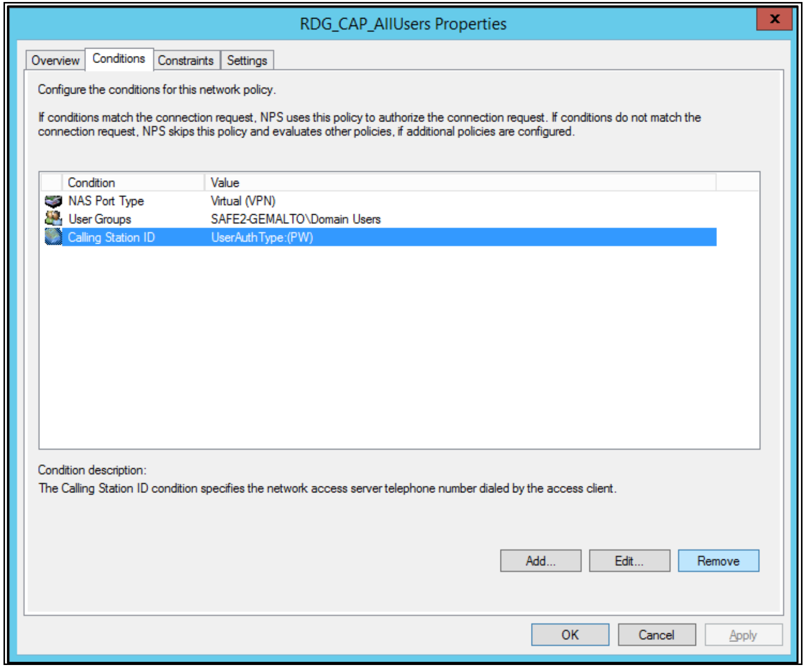
3. In the right pane, double-click **RDG_CAP_AllUsers**.



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
RDG_CAP_AllUsers	Enabled	1	Grant Access	Remote Desktop Gateway
-- RDG Marker Policy {985F7B54-FCE8-4f55-AEBF-DF8827A44068} --	Disabled	2	Grant Access	Remote Desktop Gateway
Connections to Microsoft Routing and Remote Access server	Enabled	1000000	Deny Access	Unspecified
Connections to other access servers	Enabled	1000001	Deny Access	Unspecified

4. On the **RDG_CAP_AllUsers Properties** window, on the **Conditions** tab, select the **Calling Station ID** condition, and then click **Remove**.



Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
NAS Port Type	Virtual (VPN)
User Groups	SAFE2-GEMALTO\Domain Users
Calling Station ID	UserAuthType:(PW)

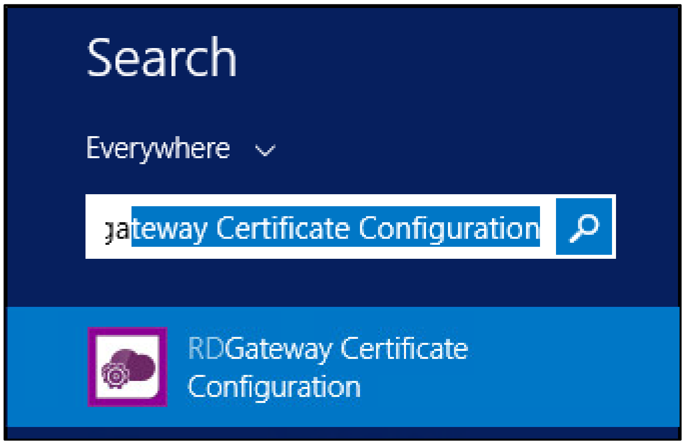
Condition description:
The Calling Station ID condition specifies the network access server telephone number dialed by the access client.

5. Click **OK**.

6. Restart the NPS service.

Updating RD Gateway Configuration with Certificate Info

1. On the computer where you have installed the RD Gateway component of the agent, search for the **RD Gateway Certificate Configuration** application, and click it.


Search
Everywhere
gateway Certificate Configuration
RDGateway Certificate Configuration

> **NOTE:** If you have not logged into the system as an administrator, run the **RD Gateway Certificate Configuration** application as an administrator.

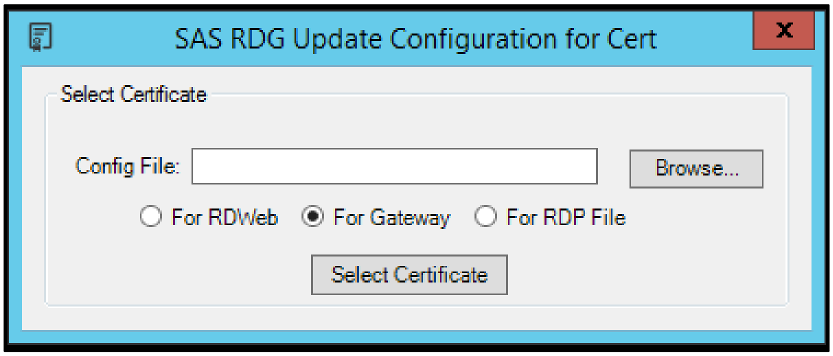
2. On the **SAS RDG Update Configuration for Cert** window, perform the following steps:

   a. Select the **For Gateway** option.

   b. Click **Browse** and select the following file:
   `<SystemDrive>\RDGPlugins\RD GatewayTokenVerification.dll.config`

   > **NOTE: SystemDrive** is a special system-wide environment variable found on Windows NT and its derivatives. Its value is the drive upon which the system directory was placed. In most of the cases, "C:" is the value of this variable.

   c. Click **Select Certificate**.



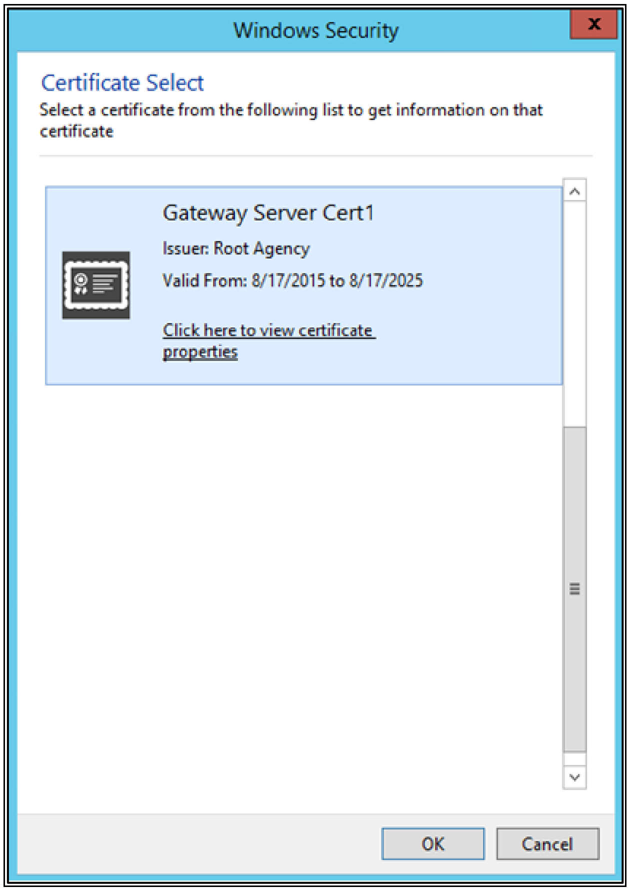
SAS RDG Update Configuration for Cert

Select Certificate

Config File:

○ For RDWeb ● For Gateway ○ For RDP File

3. On the **Windows Security** window, select the SHA256 certificate intended for the gateway access token signing, and click **OK**.



Windows Security

Certificate Select

Select a certificate from the following list to get information on that certificate

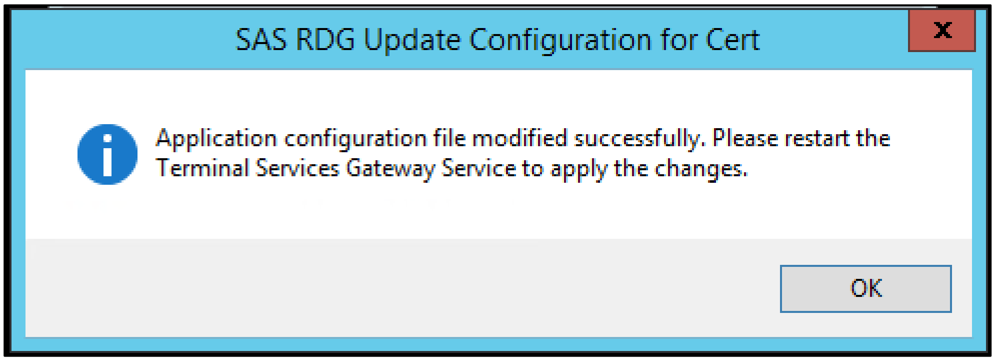
Gateway Server Cert1

Issuer: Root Agency

Valid From: 8/17/2015 to 8/17/2025

Click here to view certificate properties

4. Click **OK**.

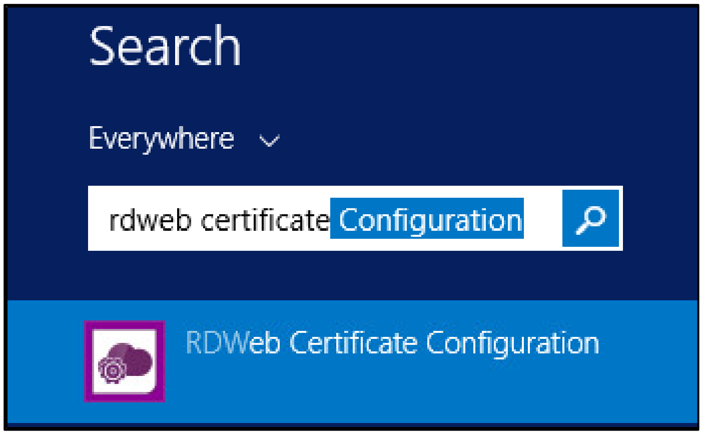


SAS RDG Update Configuration for Cert

Application configuration file modified successfully. Please restart the Terminal Services Gateway Service to apply the changes.

Updating RD Web Configuration with Certificate Info

1. On the computer where you have installed the RD Web component of the agent, search for the **RD Web Certificate Configuration** application, and click it.



rdweb certificate Configuration

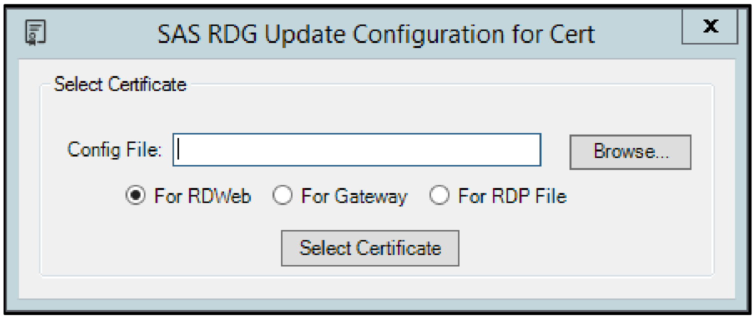
> **NOTE:** If you have not logged into the system as an administrator, run the **RD Gateway Certificate Configuration** application as an administrator.

2. On the **SAS RDG Update Configuration for Cert** window, perform the following steps:

   a. Select the **For RD Web** option.

   b. Click Browse and select the following file:
   `<SystemDrive>\Windows\Web\RD Web\Pages\Web.config`

   c. Click **Select Certificate**.



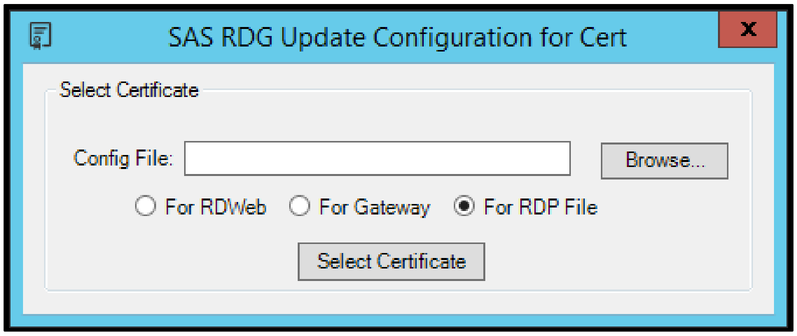
SAS RDG Update Configuration for Cert

Select Certificate

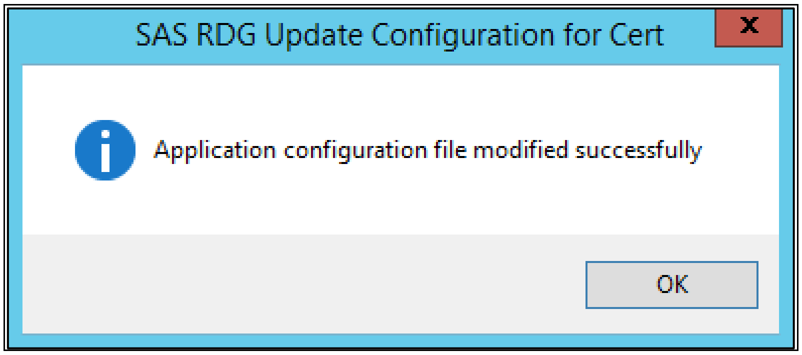
Config File:

● For RDWeb ○ For Gateway ○ For RDP File

3. On the **Windows Security** window, select the SHA256 certificate intended for the gateway access token signing, and click **OK**.
4. On the **SAS RDG Update Configuration for Cert** window, perform the following steps:
   a. Select the **For RDP File** option.
   b. Click Browse and select the following file:
   `<SystemDrive>\Windows\Web\RD Web\Pages\Web.config`
   c. Click **Select Certificate**.



5. On the **Windows Security** window, select the SHA1/SHA256 certificate intended for digitally signing the RDP file, and click **OK**.
6. Click **OK**.



Application configuration file modified successfully

Configuring RD Web Parameters

1. Open the **web.config** file available at the following path:
   `<SystemDrive>\windows\web\RD Web\pages`
2. Edit the following keys with an appropriate value, if required:

Key with no value	Description
<add key="RDPSignPath" value=""/>	Path for the RDPSign utility. By default, the RDPSign utility is available in the system32 folder.
<add key="RDPSignCertHashCode" value=""/>	SHA1/SHA256 certificate hash code used for RDPSign. This is updated when you run the RD Gateway Agent Select Certificate Tool.

Key with no value	Description
<add key="RDPSignAlgo" value=""/>	Signature Algorithm used for RDPSign. This is updated when you run the RD Web Agent Select Certificate Tool.
<add key="RDPTokenTimeout" value=""/>	RDP file validity, in minutes.
<add key="CertThumbPrint" value=""/>	SHA256 certificate for RD gateway access token hash creation. This is updated when you run the RD Gateway Agent Select Certificate Tool.
<add key="DefaultTSGateway" value=""/>	The hostname of the default Terminal Server Gateway.
<add key="PublicModeSessionTimeoutInMinutes" value="" />	The minutes after which the session will timeout, if **This is a public or shared computer** is selected as a security option on the gateway authentication window.
<add key="PrivateModeSessionTimeoutInMiniutes" value="" />	The minutes after which the session will timeout, if **This is a private computer** is selected as a security option on the gateway authentication window.

Example of RD Web parameters in the **web.config** file:

```
<configuration>
.
.
<appSettings>
<add key="RDPSignPath" value="c:\windows\system32" />
<add key="RDPSignCertHashCode"
value="6356cd93eb124ac48bc881a5089c4608702205d5"/>
<add key="RDPSignAlgo" value="sha256RSA"/>
<add key="RDPTokenTimeout" value="60" />
<add key="CertThumbPrint"
value="52c6726c657c15c2a00ea3f4cfd1e89f3785"/>
<add key="RDPFilePath" value="" />
<add key="DefaultTSGateway" value="Gateway.agent.com"/>
<add key="PublicModeSessionTimeoutInMinutes" value="20"
/>
<add key="PrivateModeSessionTimeoutInMiniutes"
value="240" />
</appSettings>
.
.
```

3. Save and close the **web.config** file.

Configuring RD Gateway Plugin Parameters

1. Open the **RD GatewayTokenVerification.config** file available at the following path: `<SystemDrive>\RDGPlugins`
2. Edit the following keys with an appropriate value, if required:

Key with no value	**Description**
<add key="CertThumbPrint" value=""/>	SHA256 certificate for RD gateway access token hash validation. This is updated when you run the RD Gateway Agent Select Certificate Tool.
<add key="MonitorService" value=" "/>	Name of the Gateway Monitor Service to communicate with.
<add key="TokenReplay" value=""/>	Enable or disable gateway access token reuse. To reuse gateway access token, set the value to **false**. Otherwise, set the value to **true**. By default, the value is set to **false**.

Example of RD Gateway parameters in the **RD GatewayTokenVerification.config** file:

```
<configuration>
.
.
<appSettings>
<add key="CertThumbPrint"
value="52C6726c657c15c2a082d30ea3f4cfd1e89f3785"/>
<add key="MonitorService" value="SASRDGMonitor"/>
<add key="TokenReplay" value="true"/>
</appSettings>
.
.
<configuration>
```

3. Save and close the **RD GatewayTokenVerification.config** file.
4. Restart the **RD Gateway** service.

Configuring RD Gateway Monitor Parameters

1. Open the **RD GatewayMonitorservice.exe.config** file available at the following path:
   `<SystemDrive>\RD GatewayMonitor`
2. Edit the following keys with an appropriate value, if required:

Key with no value	Description
<add key="RDPPath" value=""/>	Path for reading *authenticated* and *cancelled* gateway access token queue.
<add key="MonitorInterval" value=""/>	Interval, in seconds, for monitoring active connections.
<add key="Debug" value=" "/>	Enable or disable additional logging.

Example of RD Gateway Monitor parameters in the **RD GatewayMonitorservice.exe.config** file:

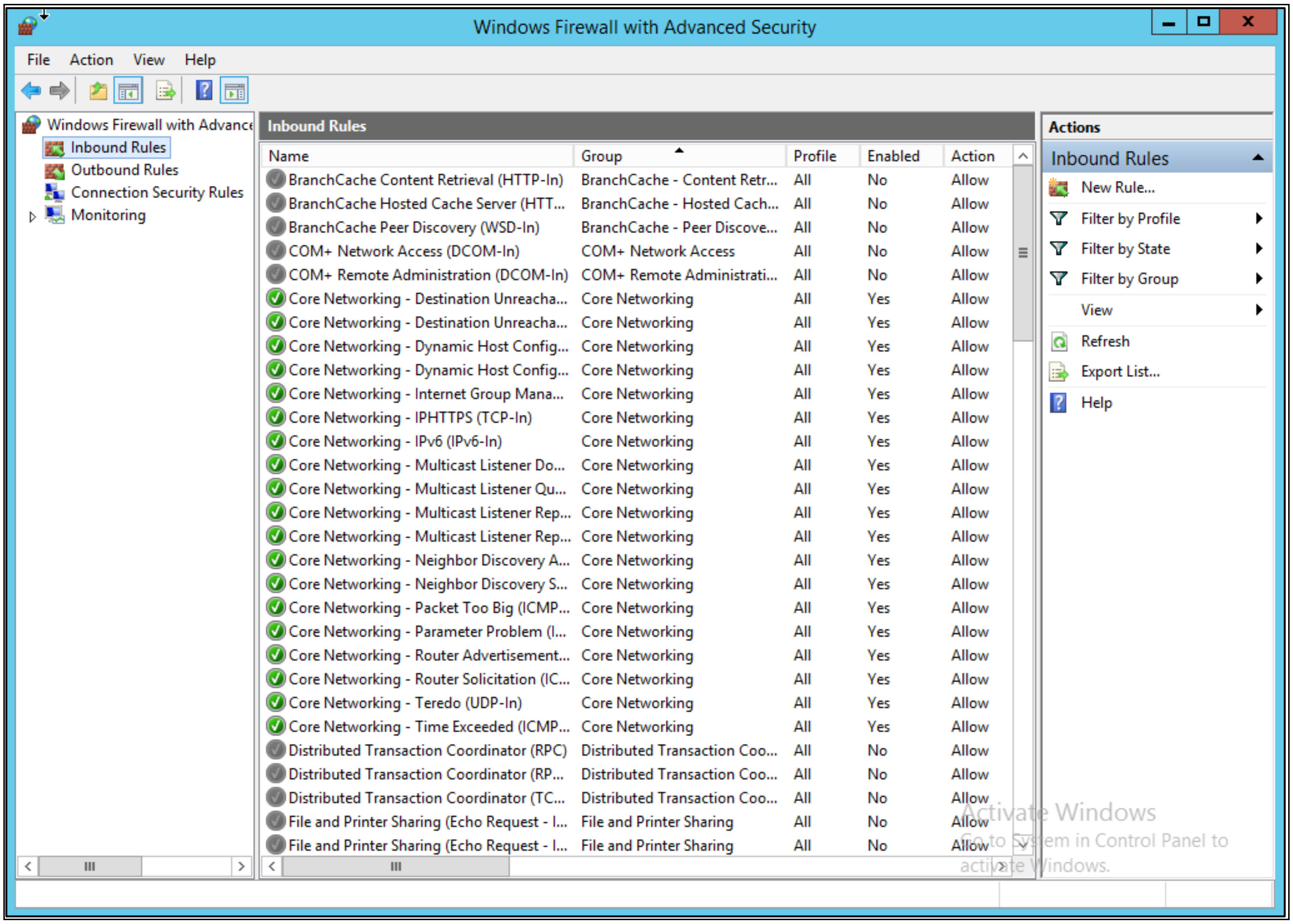
```
<configuration>
.
.
<appSettings>
<add key="RDPPath" value="c:\rdgplugins\rdp"/>
<add key="MonitorInterval" value="5"/>
</appSettings>
.
.
<configuration>
```

3. Save and close the **RD GatewayMonitorservice.exe.config** file.
4. Restart the **SAS RD Gateway Monitor** service.

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:

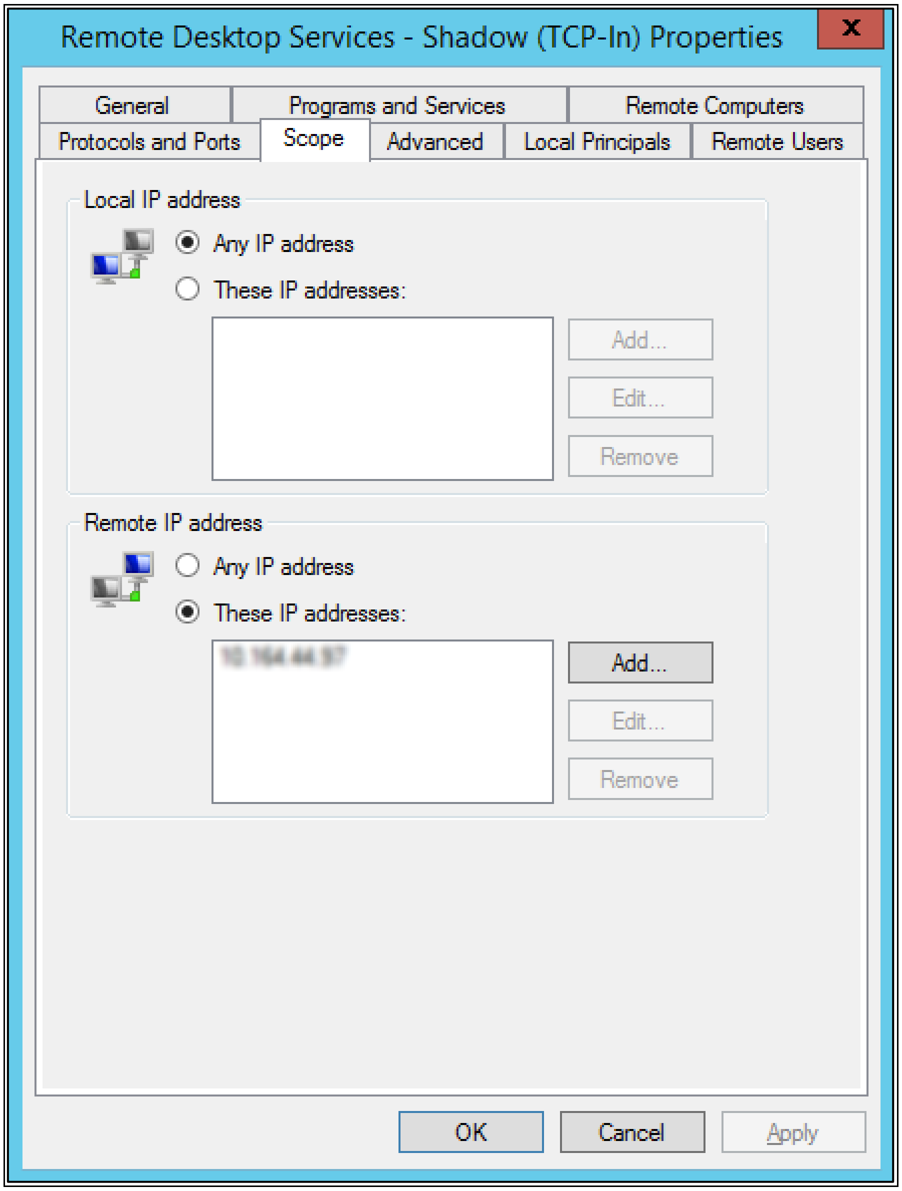
1. On the remote machine, open **Windows Firewall with Advanced Security**.
2. In the left pane, click **Inbound Rules**.



Name	Group	Profile	Enabled	Action
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow
COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati...	All	No	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (RP...	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (TC...	Distributed Transaction Coo...	All	No	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	No	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	No	Allow

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**.



Remote Desktop Services - Shadow (TCP-In) Properties

Local IP address

● Any IP address

○ These IP addresses:

Remote IP address

○ Any IP address

● These IP addresses:

[redacted]

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

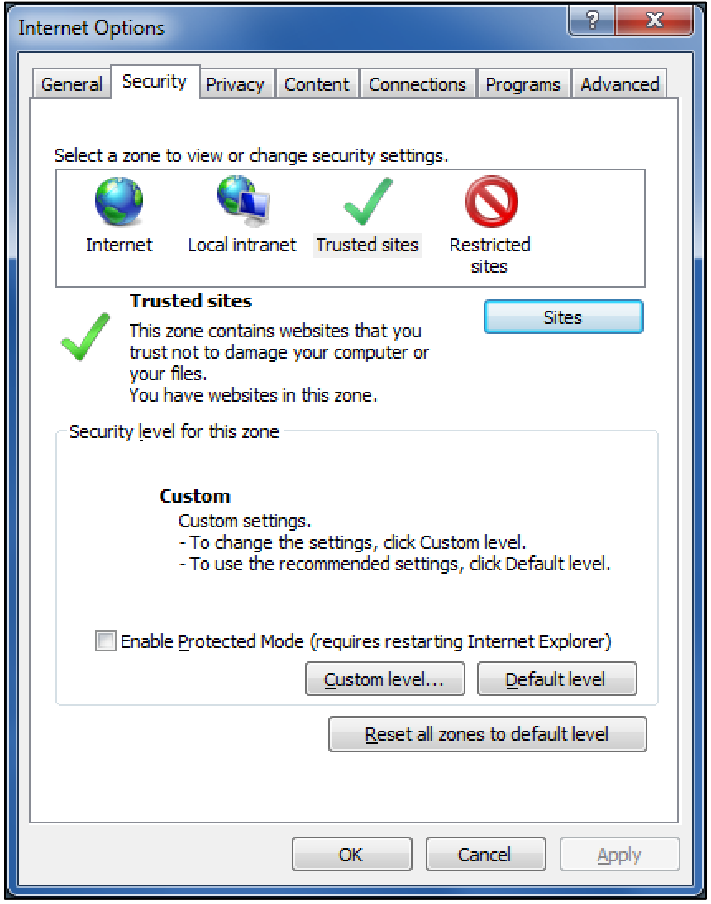
Now, connection to the remote machine can be established only through the RD Gateway server.

Performing Web Browser Settings

The web browser settings to be completed on the client machine are given below.

1. In the Internet Explorer web browser, click **Tools** > **Internet Options**.

2. Click the **Security** tab. Select the **Trusted sites** zone, and click **Sites**.



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

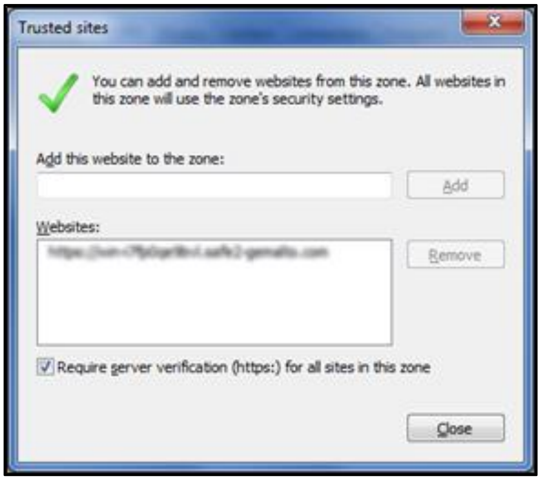
Note: Please make sure that the **Enable Protected Mode…** checkbox is clear.

3. On the **Trusted sites** window, perform these steps:

   a. In the **Add this website to the zone** field, enter the URL of the website that you want to add as a trusted website.

   b. Click **Add**.

   c. Click **Close**.



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:

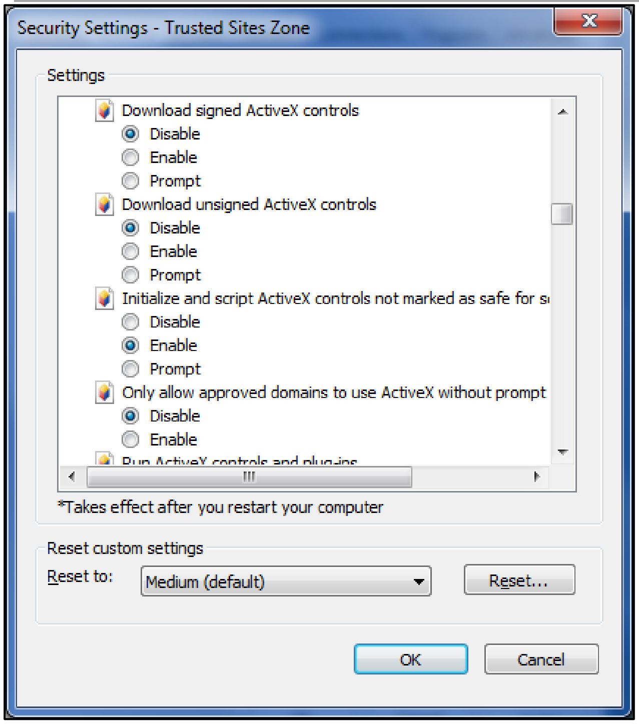
[redacted]

☑ Require server verification (https:) for all sites in this zone

4. On the **Security** tab, click **Custom level**.
5. Under **ActiveX controls and plug-ins**, configure settings as described below. Then, click **OK**.

Download signed ActiveX controls	Disable
Download unsigned ActiveX controls	Disable
Initialize and script ActiveX controls not marked as safe for scripting	Enable

Allow Scriptlets	Prompt
Automatic prompting for ActiveX controls	Enable
Only allow approved domains to use ActiveX without prompt	Enable
Run ActiveX controls and plug-ins	Prompt
Run antimalware software on ActiveX controls	Enable
Script ActiveX controls marked safe for scripting*	Prompt



Security Settings - Trusted Sites Zone

Settings

Download signed ActiveX controls
● Disable
○ Enable
○ Prompt

Download unsigned ActiveX controls
● Disable
○ Enable
○ Prompt

Initialize and script ActiveX controls not marked as safe for s
○ Disable
● Enable
○ Prompt

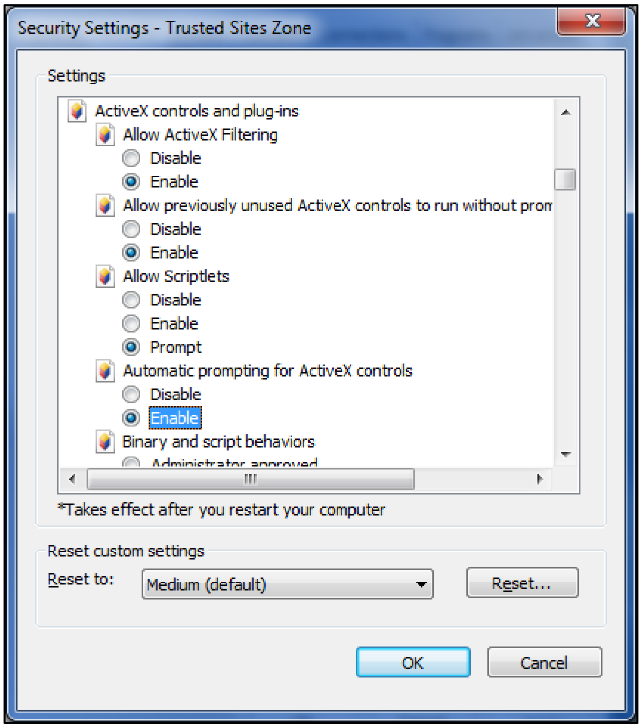
Only allow approved domains to use ActiveX without prompt
● Disable
○ Enable

Run ActiveX controls and plug-ins

*Takes effect after you restart your computer

Reset custom settings

Reset to: Medium (default)



Security Settings - Trusted Sites Zone

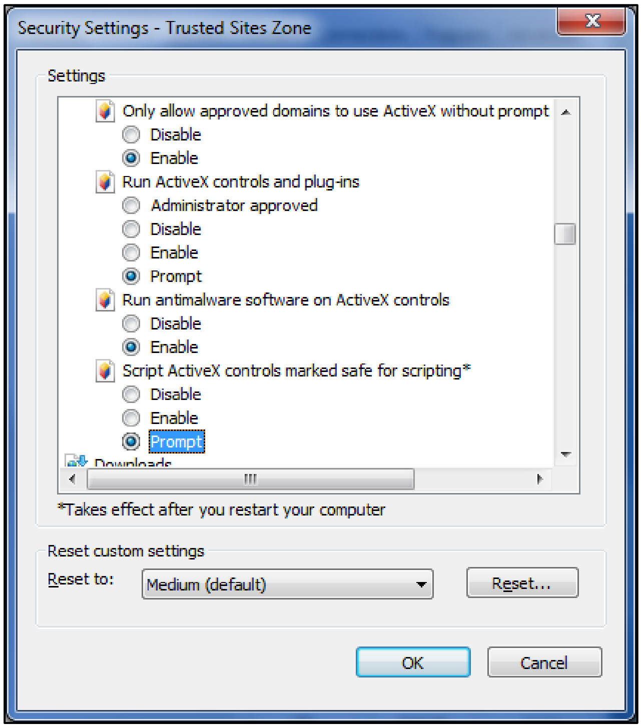
Settings

- ActiveX controls and plug-ins
  - Allow ActiveX Filtering
    - ○ Disable
    - ● Enable
  - Allow previously unused ActiveX controls to run without prom
    - ○ Disable
    - ● Enable
  - Allow Scriptlets
    - ○ Disable
    - ○ Enable
    - ● Prompt
  - Automatic prompting for ActiveX controls
    - ○ Disable
    - ● Enable
  - Binary and script behaviors
    - ○ Administrator approved

*Takes effect after you restart your computer

Reset custom settings

Reset to: Medium (default)



Security Settings - Trusted Sites Zone

Settings

- Only allow approved domains to use ActiveX without prompt
  - ○ Disable
  - ● Enable
- Run ActiveX controls and plug-ins
  - ○ Administrator approved
  - ○ Disable
  - ○ Enable
  - ● Prompt
- Run antimalware software on ActiveX controls
  - ○ Disable
  - ● Enable
- Script ActiveX controls marked safe for scripting*
  - ○ Disable
  - ○ Enable
  - ● Prompt
- Downloads

*Takes effect after you restart your computer

Reset custom settings

Reset to: Medium (default)

RD Gateway ActiveX Control

Installing RD Gateway ActiveX Control Silently

To install the RD Gateway Active X control in silent mode, run the following command as an administrator:

```
ActiveXforSafenetAuthenticationServiceAgent.exe /s /v/qn
```

Uninstalling RD Gateway ActiveX Control Silently

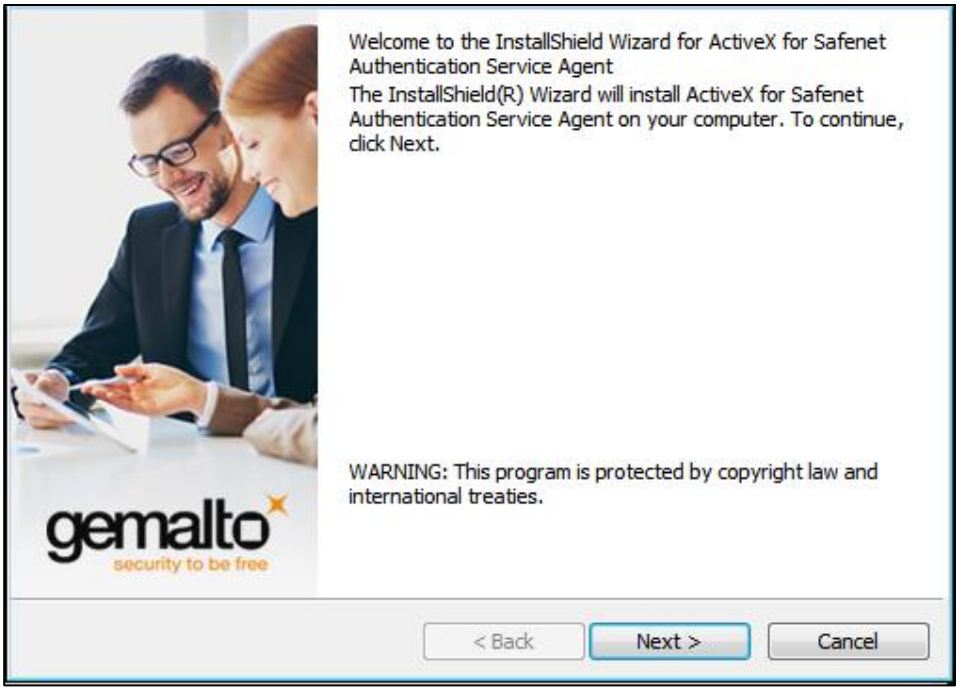
To uninstall the RD Gateway Active X control in silent mode, run the following command as an administrator:

```
ActiveXforSafenetAuthenticationServiceAgent.exe /x /s /v/qn
```

Installing RD Gateway ActiveX Control via Installer

Run the **ActiveX for Safenet Authentication Service Agent** installer. If you have logged into the system as an administrator, the installation process will run successfully.

1. On the **Welcome** window, click **Next**.

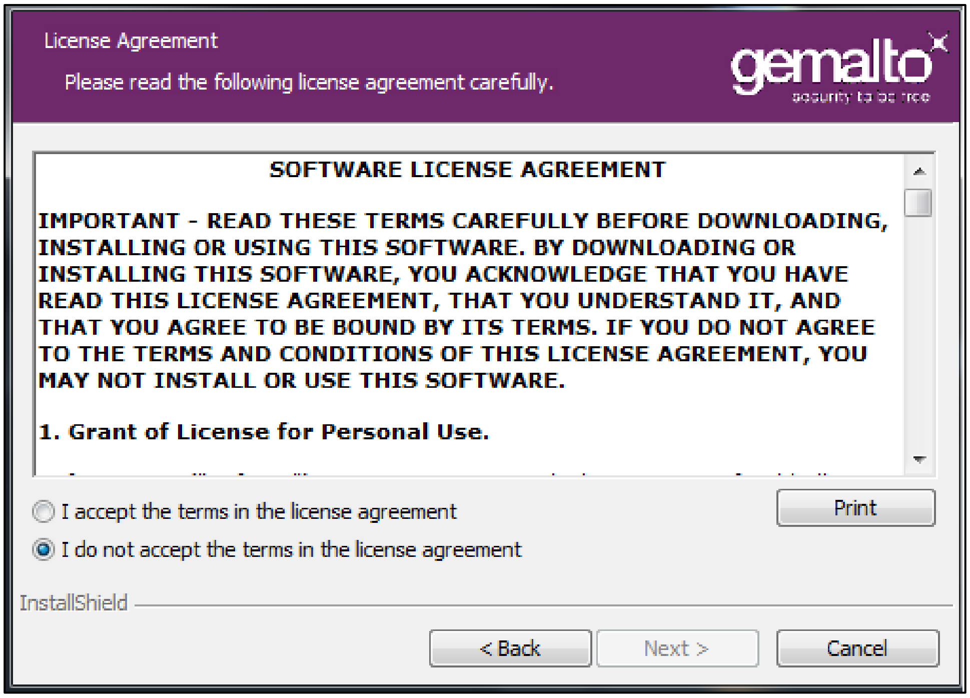


Welcome to the InstallShield Wizard for ActiveX for Safenet Authentication Service Agent

The InstallShield(R) Wizard will install ActiveX for Safenet Authentication Service Agent on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



License Agreement

Please read the following license agreement carefully.

SOFTWARE LICENSE AGREEMENT

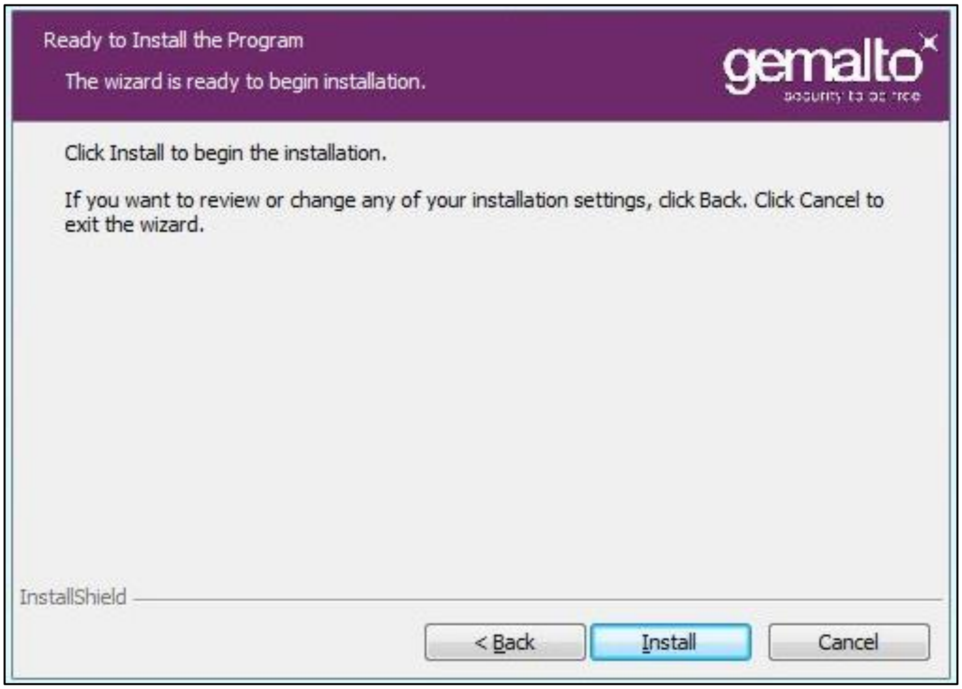
IMPORTANT - READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THIS SOFTWARE. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU MAY NOT INSTALL OR USE THIS SOFTWARE.

1. Grant of License for Personal Use.

○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement

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



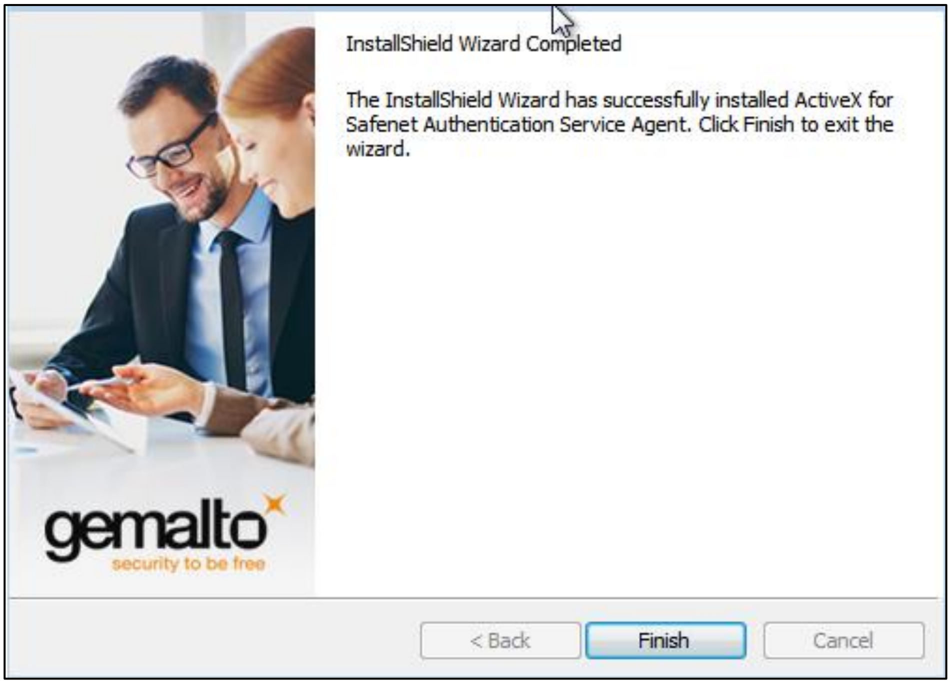
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

4. When the process completes, the **InstallShield Wizard Completed** window opens. Click **Finish** to exit the installation wizard.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed ActiveX for Safenet Authentication Service Agent. Click Finish to exit the wizard.

APPENDIX A: Troubleshooting

Exporting Logs for Troubleshooting

To export logs on RD Gateway, run the following commands on Powershell:

```
(Get-Service "RD GatewayMonitorService").ExecuteCommand(129)
```

```
get-eventlog -newest 1000 -Logname "Application" -Source "RD GatewayMonitorSource"
-ErrorAction SilentlyContinue | Select TimeWritten, Message | Export-csv
.\desktop\RDGateway.csv
```

```
copy c:\RDGPlugins\log.txt and save
```

To export logs on RD Web, run the following command on Powershell:

```
get-eventlog -newest 1000 -Logname "Application" -Source "RD WebAccess" -
ErrorAction SilentlyContinue | Select TimeWritten, Message | Export-csv
.\desktop\RDWeb.csv
```

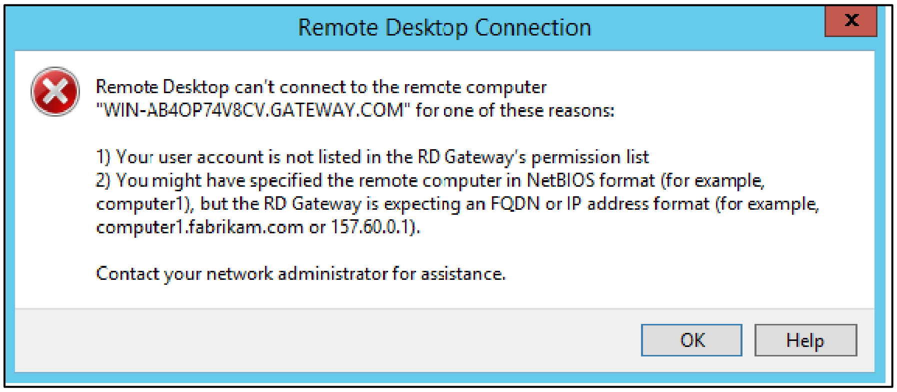
Creating Installation Log

If you require that the installation log is created, run the installer from the command prompt using the following command: `RD Gateway.exe /V"/L* setup.log"`

Error Handling

Permissions and NetBIOS Error

If you encounter the ‘Permissions and NetBIOS’ error while launching the RDP file, review the Resource Authorization Policy (RAP) and ensure that it is in the right order.



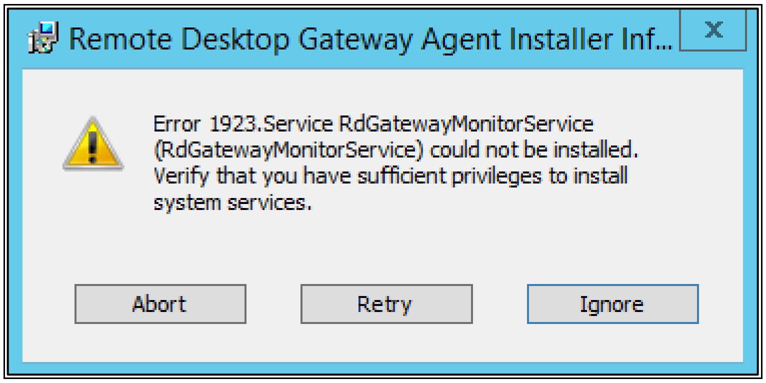
Remote Desktop can't connect to the remote computer "WIN-AB4OP74V8CV.GATEWAY.COM" for one of these reasons:

1) Your user account is not listed in the RD Gateway's permission list
2) You might have specified the remote computer in NetBIOS format (for example, computer1), but the RD Gateway is expecting an FQDN or IP address format (for example, computer1.fabrikam.com or 157.60.0.1).

Contact your network administrator for assistance.

1923 Error

When you have uninstalled the agent and are trying to install it again, you may encounter the 1923 error:



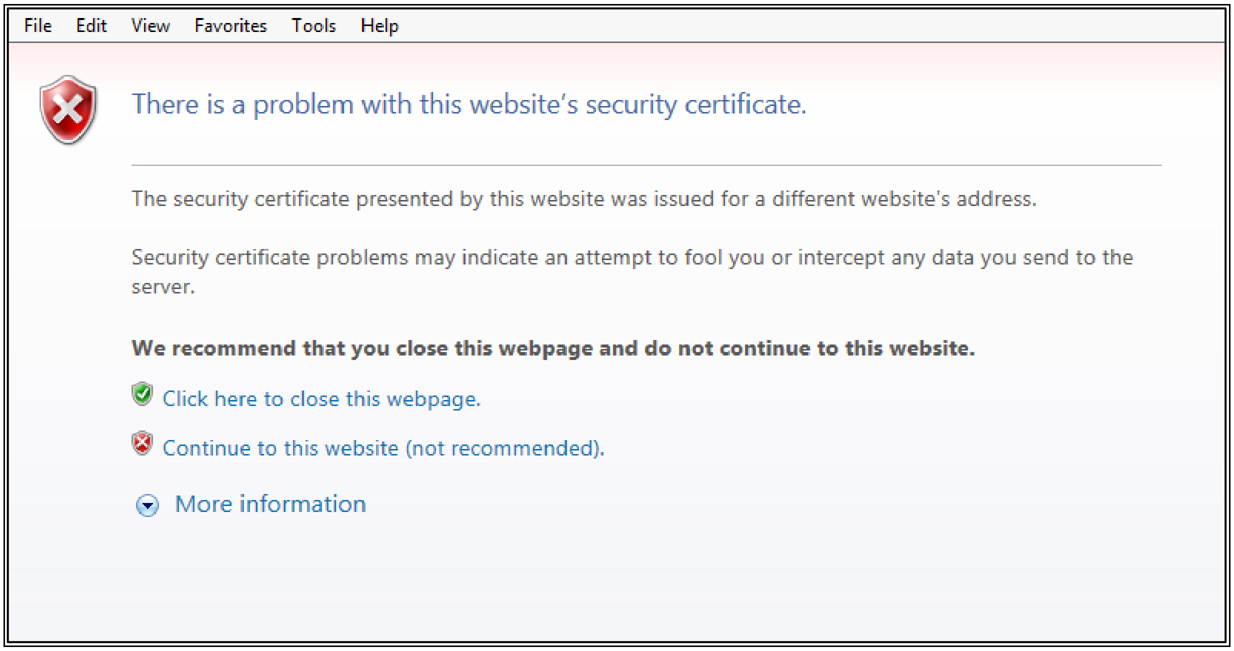
Error 1923.Service RdGatewayMonitorService (RdGatewayMonitorService) could not be installed. Verify that you have sufficient privileges to install system services.

The uninstallation process of the SafeNet Agent for RD Gateway may not remove the RD Gateway Monitor service in several conditions, and change the state of the service to disabled and mark it for deletion.

In this case, log off or restart the system, and then check if the service was removed.

Certificate Error

While connecting to the protected remote computer, you may encounter the error shown in the screen below. This error is shown because the certificate used is not a proper certificate. Replace your certificate with a proper certificate, and then try again.



File Edit View Favorites Tools Help

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

Installation Error

During a few instances, the RD Gateway service (tsgateway) does not stop automatically on installation or uninstallation. In these cases, the user needs to manually stop the service.

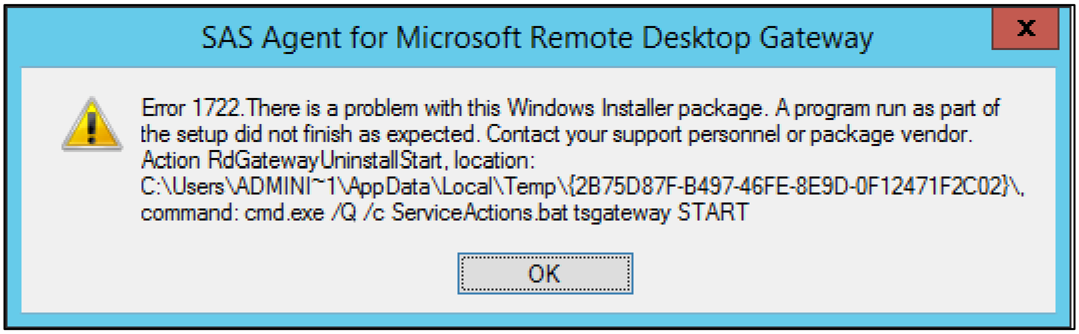
To stop the RD Gateway service, perform the following steps:

1. Open the **Task Manager**.
2. On the **Service** tab, search for the **tsgateway** service, and note down its process ID (PID).
3. On the **Details** tab, search for the process ID.
4. Select the process PID, and click **End Task**.

To verify the status of the RD Gateway service, perform the following steps:

1. Go to **Services Console**.
2. Search for the RD Gateway service. The status should be **Stopped**.

If the user continues with the installation or uninstallation without manually stopping the RD Gateway service, the following error (Error 1722) will appear:

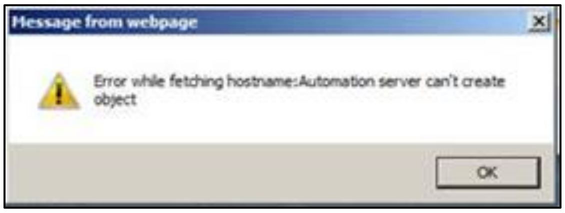


SAS Agent for Microsoft Remote Desktop Gateway

Error 1722.There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected. Contact your support personnel or package vendor. Action RdGatewayUninstallStart, location: C:\Users\ADMINI~1\AppData\Local\Temp\{2B75D87F-B497-46FE-8E9D-0F12471F2C02}\, command: cmd.exe /Q /c ServiceActions.bat tsgateway START

Hostname Fetching Error

On the client machine, while connecting to a remote machine using the agent, you may encounter the following error after the IIS authentication page:

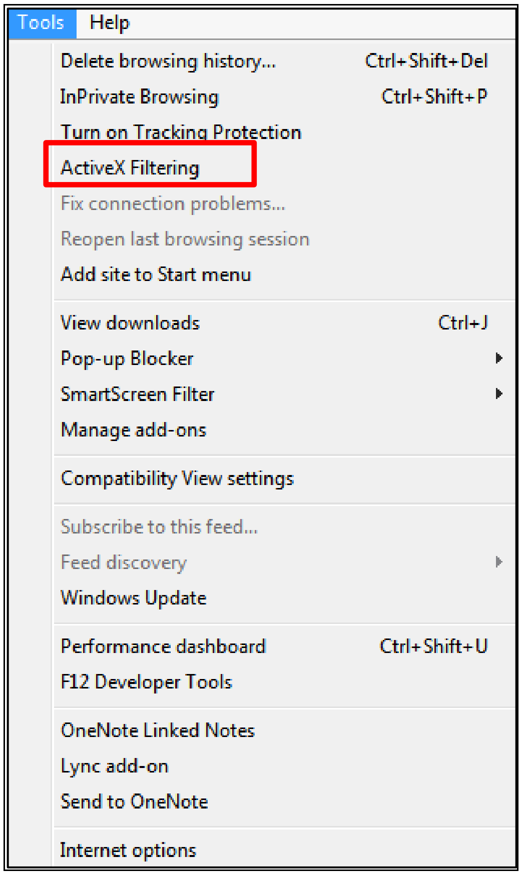


Message from webpage

Error while fetching hostname:Automation server can't create object

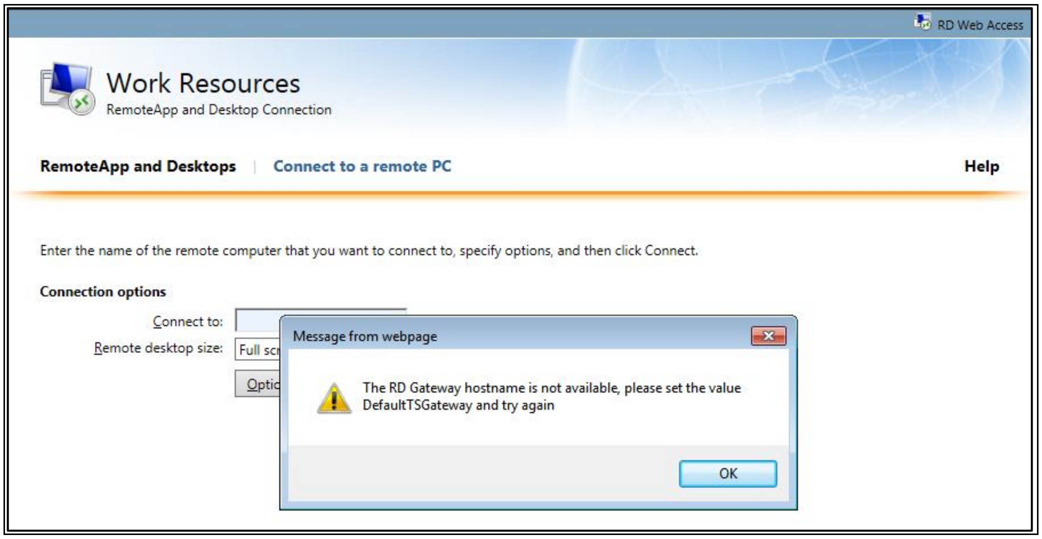
To solve the issue, follow the steps:

1. Perform the Active X settings as illustrated in **Performing Web Browser Settings** on page 32.
2. In Internet Explorer, in the **Tools** menu, ensure that **ActiveX Filtering** is not checked.


Tools
Help
Delete browsing history... Ctrl+Shift+Del
InPrivate Browsing Ctrl+Shift+P
Turn on Tracking Protection
ActiveX Filtering
Fix connection problems...
Reopen last browsing session
Add site to Start menu
View downloads Ctrl+J
Pop-up Blocker
SmartScreen Filter
Manage add-ons
Compatibility View settings
Subscribe to this feed...
Feed discovery
Windows Update
Performance dashboard Ctrl+Shift+U
F12 Developer Tools
OneNote Linked Notes
Lync add-on
Send to OneNote
Internet options

Hostname Unavailability Error

On the **Work Resources** window, when you click on **Connect to a Remote PC**, you may see the following error message:



Enter the name of the remote computer that you want to connect to, specify options, and then click Connect.

The RD Gateway hostname is not available, please set the value DefaultTSGateway and try again

To resolve this issue, refer the **Configuring RD Web Parameters** section, and set the following parameter: *<add key="DefaultTSGateway" value=""/>*

TS Gateway Service Restart Issues

If Remote Desktop Gateway installer reports errors while installation or uninstallation, the RD Gateway service (tsgateway) should be kept in **Stopped** state for subsequent attempts for installation or uninstallation.

The following installation command should be run from the command line:

```
RD Gateway.exe /V"/L* setup.log"
```

The **setup.log** file created should be shared with the support team for troubleshooting.

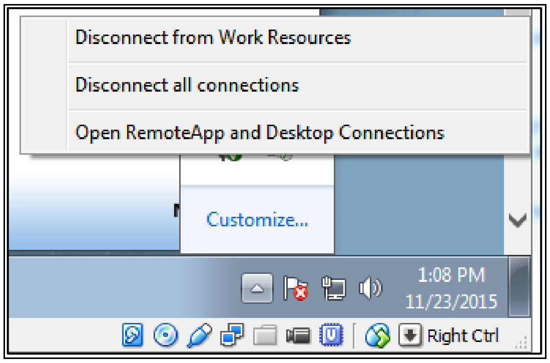
Updating RD Connection Protocol

To update the RD connection protocol to 8.1 (on Windows 7), install the following packages:

- 2830477
- 2574819

Disconnecting Established Connection on RD Web

To fully disconnect an established connection on the client machine, make sure that the remote connection icon at the task bar is not visible. If it is visible, right-click on the icon and select **Disconnect all connections**.


Disconnect from Work Resources
Disconnect all connections
Open RemoteApp and Desktop Connections
Customize...
1:08 PM
11/23/2015
Right Ctrl

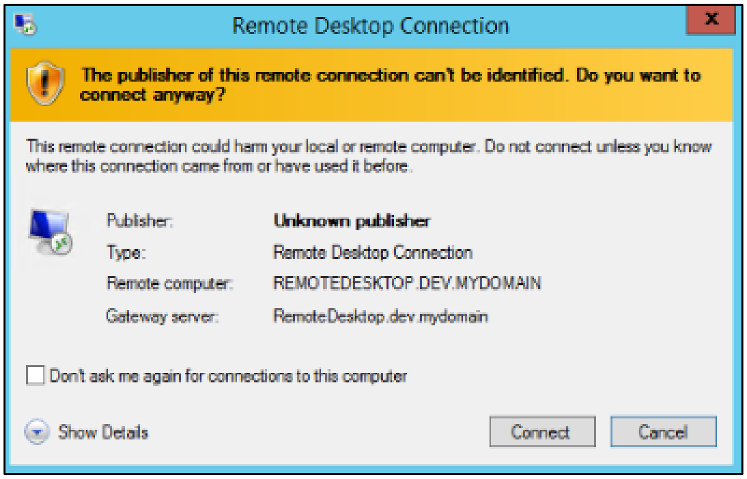
Hostname Resolution

The hostname of the RD Gateway server should be resolvable at the client machine. Ideally, the resolution is done by the DNS server configured on the client machine. Also, in DNS of the corporate network, the entry for the RD Gateway server should already be done. However, if not yet done, it needs to be manually configured in the **hosts** file of the client machine.

This also applies for regular install of the RD Web and the RD Gateway (without the Agent).

Publisher Identity Issues

If a user is prompted with the following publisher identity not recognized screen:



Remote Desktop Connection

The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher: Unknown publisher
Type: Remote Desktop Connection
Remote computer: REMOTEDESKTOP.DEV.MYDOMAIN
Gateway server: RemoteDesktop.dev.mydomain

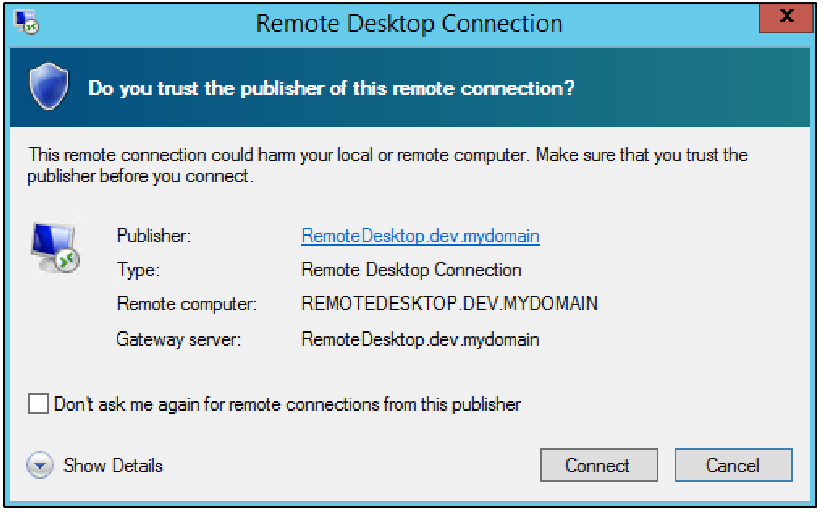
□ Don't ask me again for connections to this computer

The user must perform the following steps:

1. Check if the key ***RDPSignAlgo*** has correct values at: ***<SystemDrive>\windows\web\RDWeb\pages\Web.Config***

2. If the values of the ***RDPSignAlgo*** parameter is not in accordance with the certificate algorithm of the default RD Web setup, upload the correct certificate in the configuration update section.

3. Once all the values are correct, the user will be prompted with the following screen:



Remote Desktop Connection

Do you trust the publisher of this remote connection?

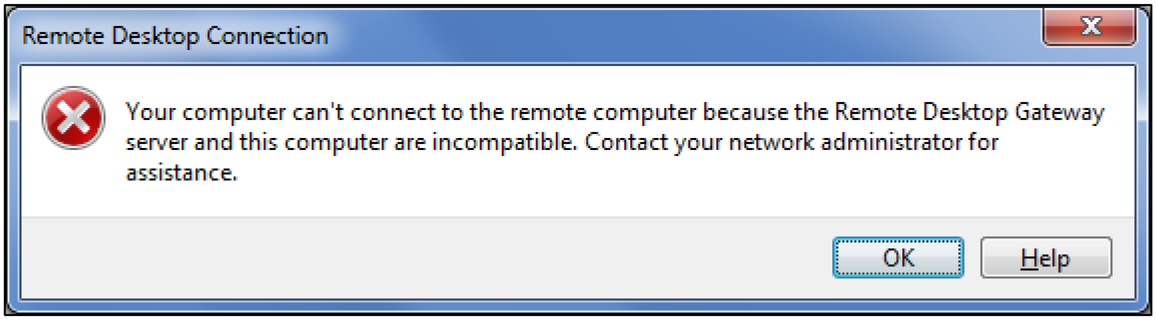
This remote connection could harm your local or remote computer. Make sure that you trust the publisher before you connect.

Publisher: RemoteDesktop.dev.mydomain
Type: Remote Desktop Connection
Remote computer: REMOTEDESKTOP.DEV.MYDOMAIN
Gateway server: RemoteDesktop.dev.mydomain

□ Don't ask me again for remote connections from this publisher

APPENDIX B: Error Codes and Messages

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



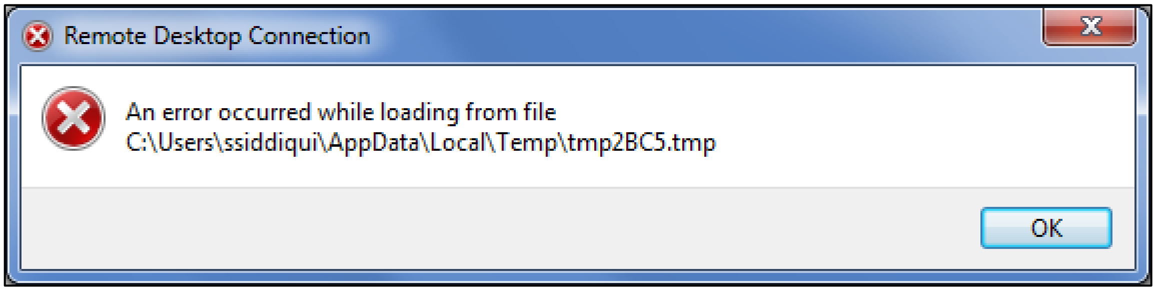
Remote Desktop Connection

Your computer can't connect to the remote computer because the Remote Desktop Gateway server and this computer are incompatible. Contact your network administrator for assistance.

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.

The following error message appears when the user is on the IIS Resource page and IIS Stops working:



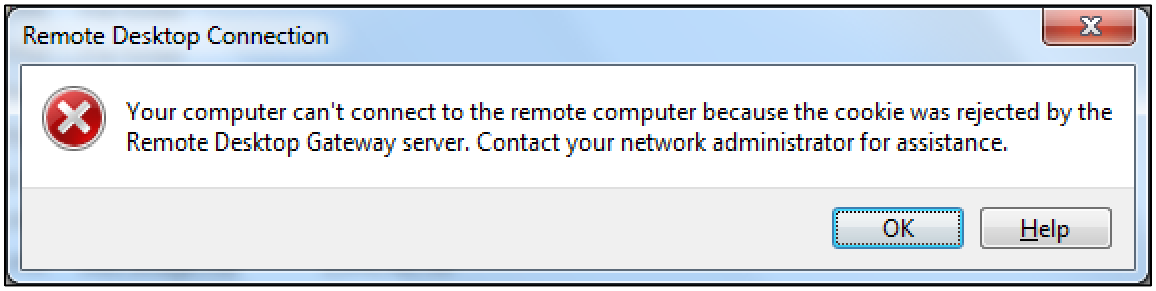
Remote Desktop Connection

An error occurred while loading from file C:\Users\ssiddiqui\AppData\Local\Temp\tmp2BC5.tmp

Start IIS. Check if the Remote Desktop Gateway service is up (start if it is stopped) and try to connect again.

The following error message appears when:

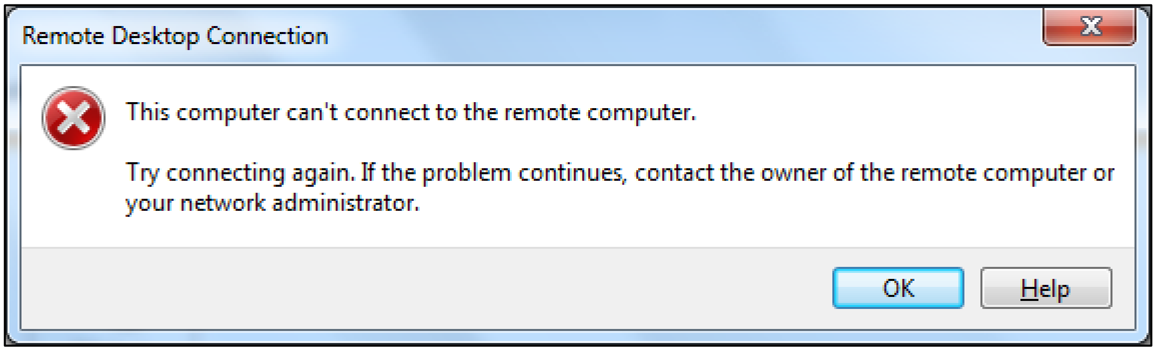
- An RDP file is downloaded by a user on a machine, and that file is used with the same user credentials on a different machine.
- Timeout for a token occurs.



Remote Desktop Connection

Your computer can't connect to the remote computer because the cookie was rejected by the Remote Desktop Gateway server. Contact your network administrator for assistance.

The following error message appears when the Session Host is not reachable. Either the machine is switched off, or some network issue exists:



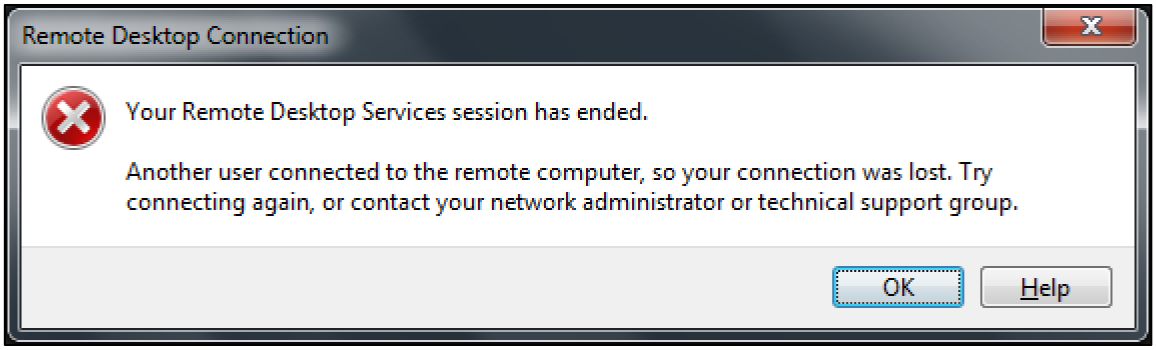
Remote Desktop Connection

This computer can't connect to the remote computer.

Try connecting again. If the problem continues, contact the owner of the remote computer or your network administrator.

Check if the session host machine could be successfully pinged.

The following error message appears when a parallel session is tried to establish 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.



Remote Desktop Connection

Your Remote Desktop Services session has ended.

Another user connected to the remote computer, so your connection was lost. Try connecting again, or contact your network administrator or technical support group.

APPENDIX C: Creating Certificates for Gateway Access Tokens

Creating Certificates Using *makecert* Command

If you want to generate a certificate on your own using the Command Line Interface (CLI), use the following command:

```
makecert [basic | extended options] [outputCertificateFile]
```

Example of the **makecert** command:

```
makecert -pe -n "CN=Gateway Server Cert" -b 08/17/2015 -e 08/17/2025 -ss My -sr
LocalMachine -sky exchange -sy 24 -a sha256
```

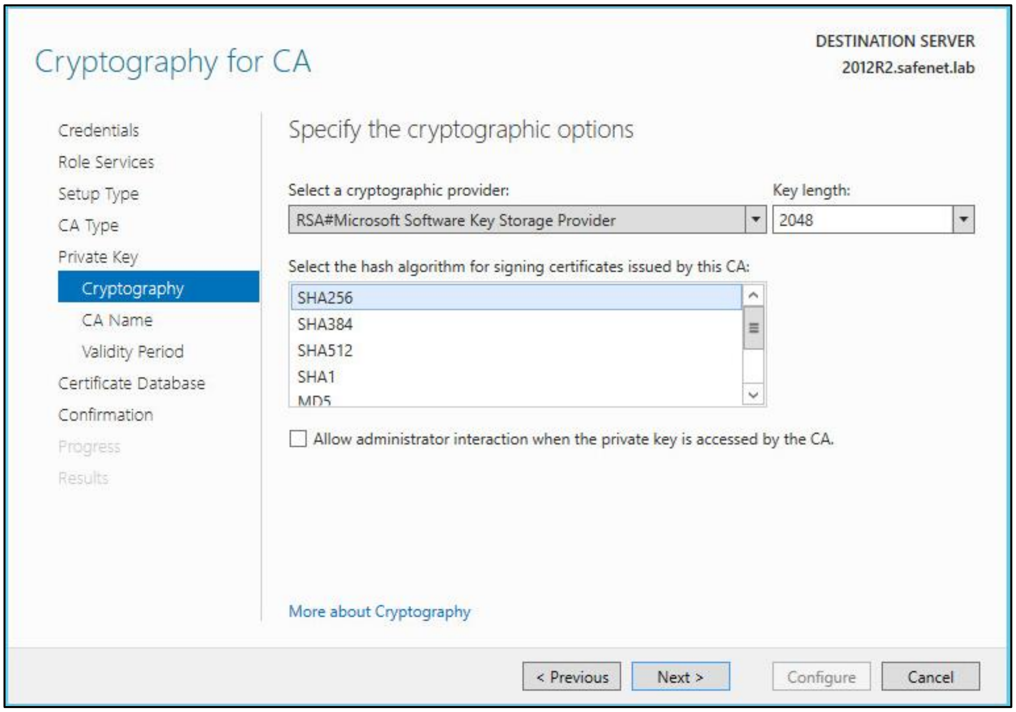
> **NOTE:** MakeCert is available as part of the Windows SDK, which you can download from here.

The table below contains the list of options used in the above command:

Command Option	Description
-pe	Mark generated private key as exportable
-ss <store>	Subject's certificate store name that stores the output certificate
-sr <location>	Subject's certificate store location <CurrentUser | LocalMachine>. Default value used is **CurrentUser**.
-n <X509name>	Certificate subject X500 name (for example, CN=Fred Dews)
-a <algorithm>	The signature's digest algorithm, which should be **SHA256**.
-sy <type>	Subject's CryptoAPI provider's type
-sky <keytype>	Specifies the subject's key type, which must be a signature, an exchange, or an integer that represents a provider type. Here, pass 1 for an exchange key.
-b <mm/dd/yyyy>	Start of the validity period; default value used is now
-e <mm/dd/yyyy>	End of validity period; defaults value used is 2039

Creating Certificates Using Enterprise Certificate Authority

Ensure that the Microsoft Enterprise Certificate Authority is set up. Also, while configuring AD CS, ensure that the SHA256 algorithm is specified as a cryptographic provider for signing certificates.


Cryptography for CA

DESTINATION SERVER
2012R2.safenet.lab

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

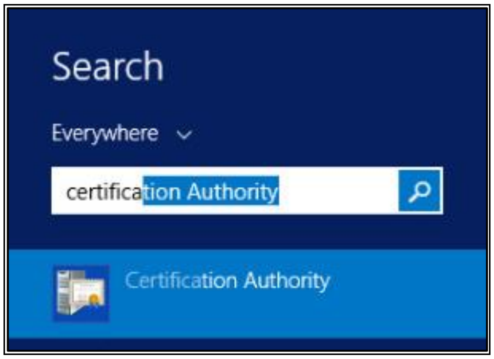
Select the hash algorithm for signing certificates issued by this CA: SHA256

□ Allow administrator interaction when the private key is accessed by the CA.

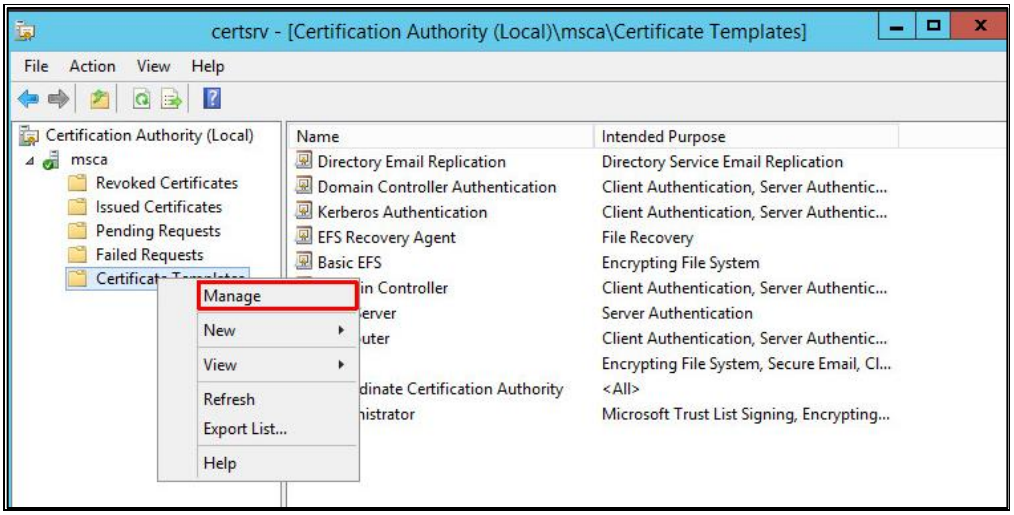
NOTE: If you have RD Gateway and RD Web installed on separate machines, perform the steps:
1. On the RD Web machine, create a certificate using a certificate template.
2. On the RD Web machine, export this new certificate (without a private key).
3. On the RD Gateway machine, import this certificate.
The subsections below discuss **creating a certificate template** and **creating a certificate using a template**.

Creating Certificate Template for SHA256 Certificates

1. Search for the **Certificate Authority** application, and click it.

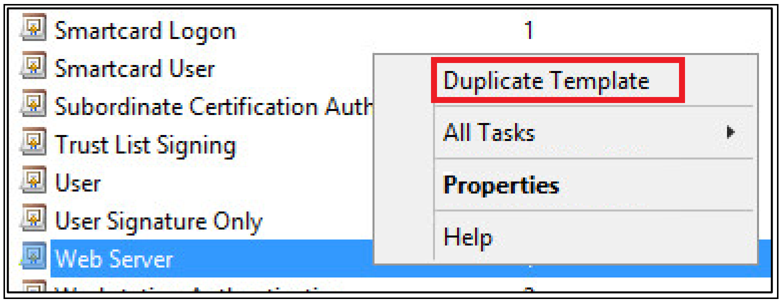

certification Authority

2. On the **Certification Authority Management Console** window, in the left pane, right-click **Certificate Templates**, and then select **Manage**.

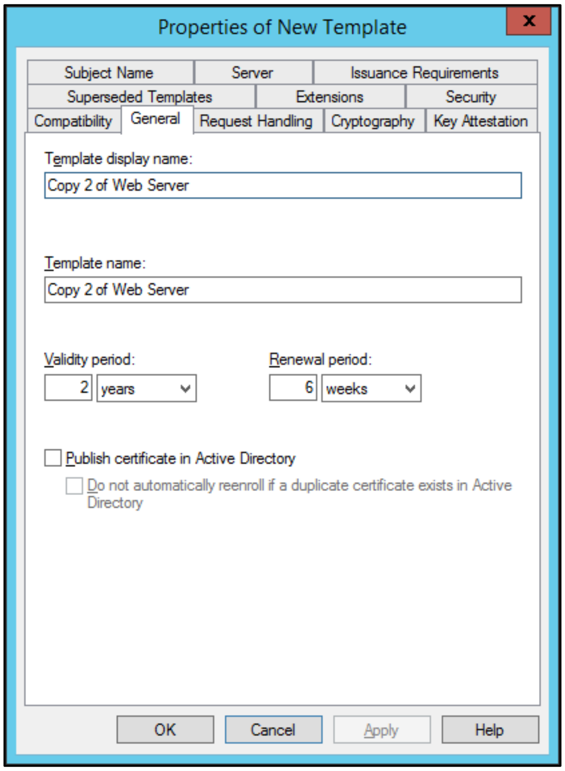


Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
in Controller	Client Authentication, Server Authentic...
erver	Server Authentication
uter	Client Authentication, Server Authentic...
	Encrypting File System, Secure Email, Cl...
dinate Certification Authority	<All>
istrator	Microsoft Trust List Signing, Encrypting...

3. Scroll down to the **Web Server** certificate template, right-click it, and select **Duplicate Template**.



4. On the **Properties of New Template** window, on the **General** tab, enter the **Template display name** and **Template name**.



Properties of New Template

Template display name: Copy 2 of Web Server

Template name: Copy 2 of Web Server

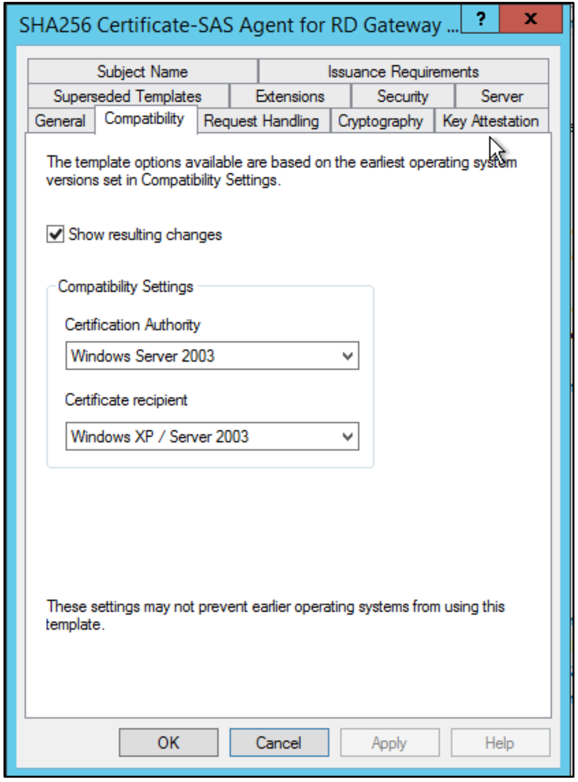
Validity period: 2 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

5. On the **Compatibility** tab, specify the applicable compatibility settings.



SHA256 Certificate-SAS Agent for RD Gateway ...

The template options available are based on the earliest operating system versions set in Compatibility Settings.

☑ Show resulting changes

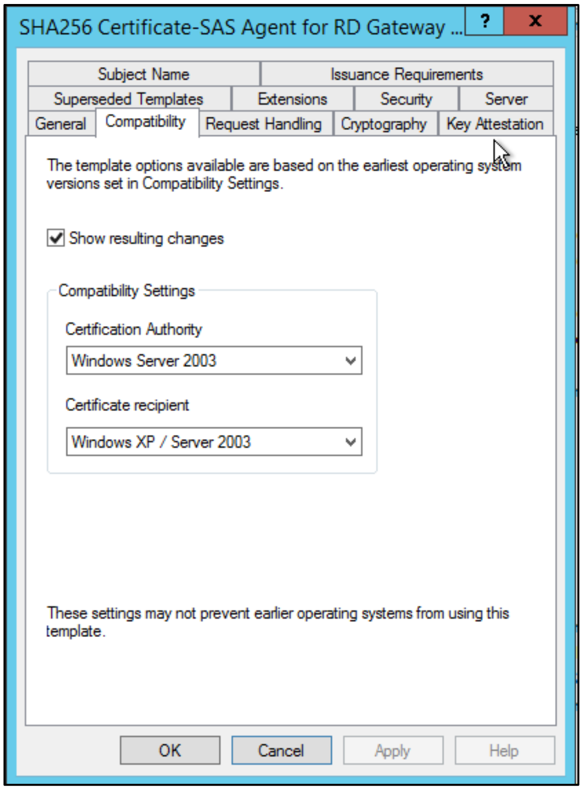
Compatibility Settings

Certification Authority: Windows Server 2003

Certificate recipient: Windows XP / Server 2003

These settings may not prevent earlier operating systems from using this template.

6. On the **Compatibility** tab, specify the applicable compatibility settings.



The template options available are based on the earliest operating system versions set in Compatibility Settings.

☑ Show resulting changes

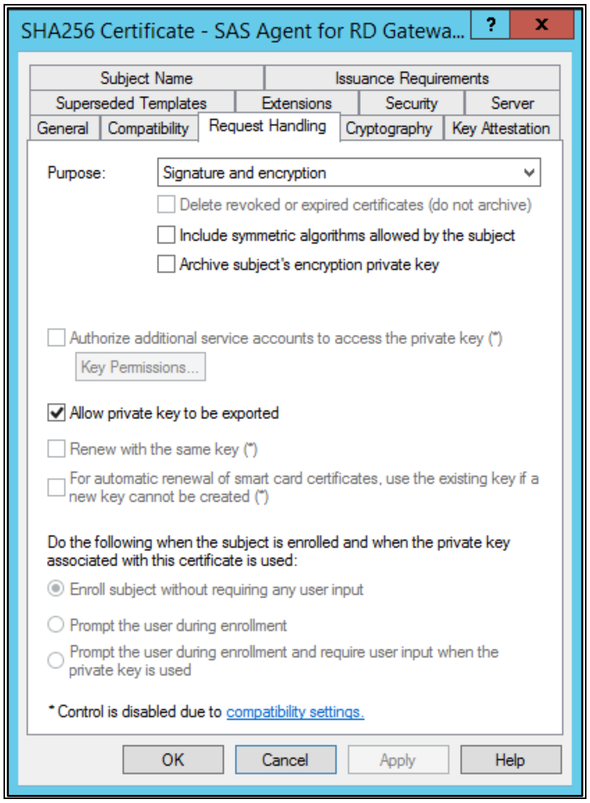
Compatibility Settings

Certification Authority: Windows Server 2003

Certificate recipient: Windows XP / Server 2003

These settings may not prevent earlier operating systems from using this template.

7. On the **Request Handling** tab, select **Allow private key to be exported** if the certificate is to be deployed to multiple servers.



Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Authorize additional service accounts to access the private key (*)

☑ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

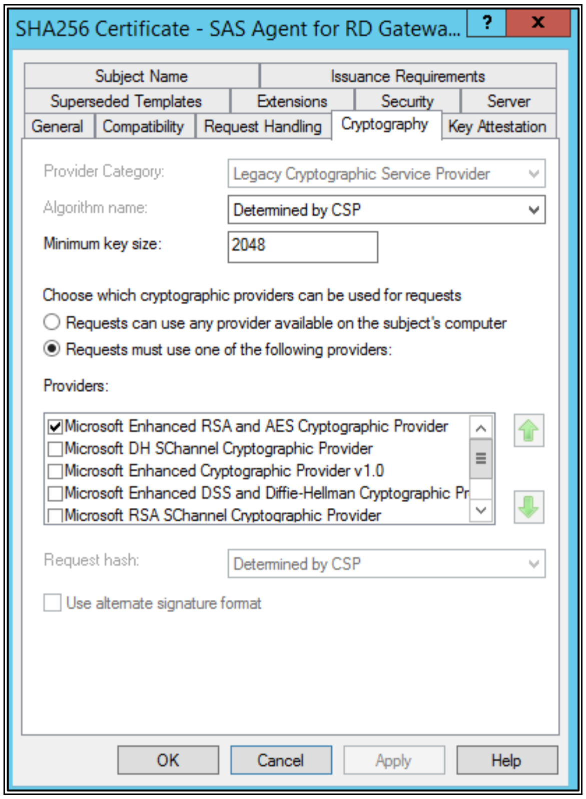
● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.

8. On the **Cryptography** tab, select **Requests must use one of the following providers**. Then, in the list of providers, select only **Microsoft Enhanced RSA and AES Cryptographic Provider**.



Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

○ Requests can use any provider available on the subject's computer

● Requests must use one of the following providers:

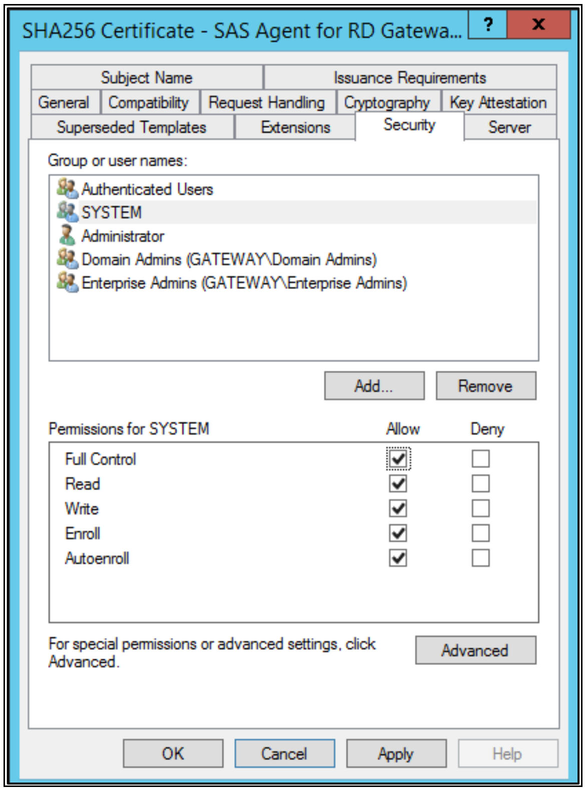
Providers:

☑ Microsoft Enhanced RSA and AES Cryptographic Provider
☐ Microsoft DH SChannel Cryptographic Provider
☐ Microsoft Enhanced Cryptographic Provider v1.0
☐ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr
☐ Microsoft RSA SChannel Cryptographic Provider

Request hash: Determined by CSP

☐ Use alternate signature format

9. On the **Security** tab, add **SYSTEM** as a user. Then, provide **Enroll** permission to the SYSTEM user.



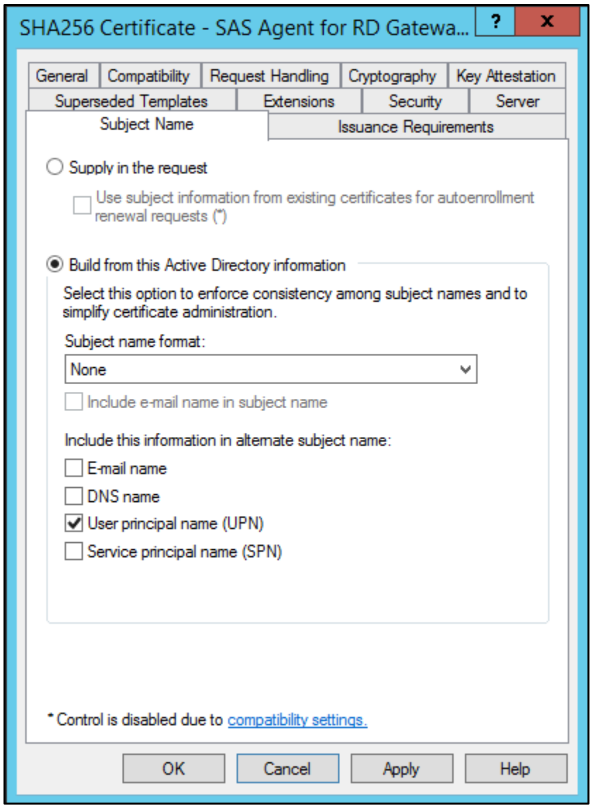
Group or user names:

Authenticated Users
SYSTEM
Administrator
Domain Admins (GATEWAY\Domain Admins)
Enterprise Admins (GATEWAY\Enterprise Admins)

Permissions for SYSTEM	Allow	Deny
Full Control	☑	☐
Read	☑	☐
Write	☑	☐
Enroll	☑	☐
Autoenroll	☑	☐

For special permissions or advanced settings, click Advanced.

10. On the **Subject Name** tab, select **Build from this Active Directory information**.


SHA256 Certificate - SAS Agent for RD Gatewa...

○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

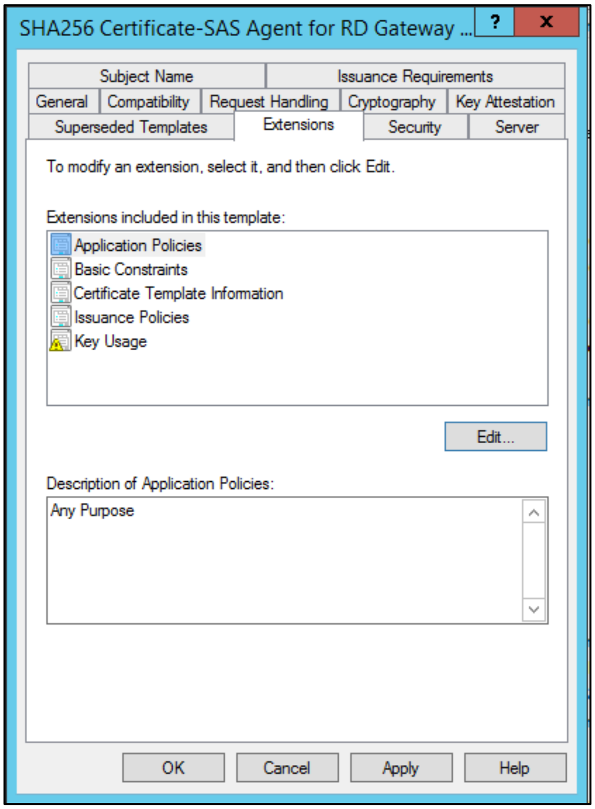
□ DNS name

☑ User principal name (UPN)

□ Service principal name (SPN)

* Control is disabled due to compatibility settings.

11. On the **Extensions** tab, select the **Application Policies** extension, and then click **Edit**.


SHA256 Certificate-SAS Agent for RD Gateway ...

To modify an extension, select it, and then click Edit.

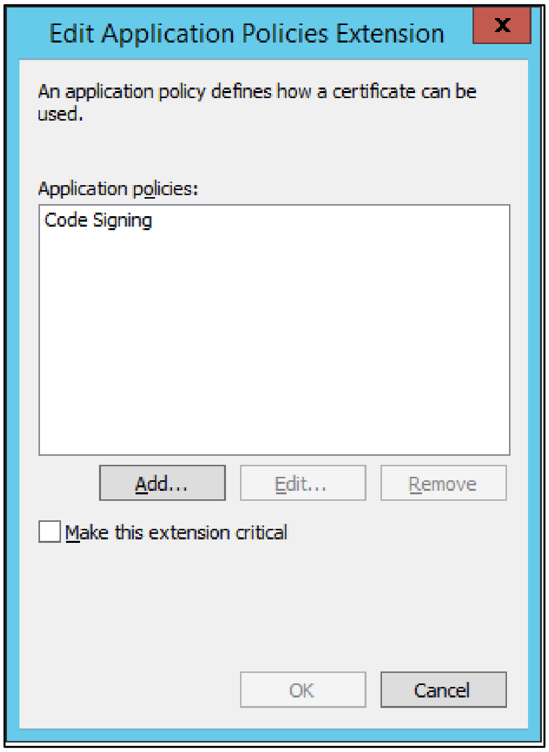
Extensions included in this template:

Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage

Description of Application Policies:

Any Purpose

12. On the **Edit Application Policies Extension** window, add **Code Signing** as an application policy, and then click **OK**.



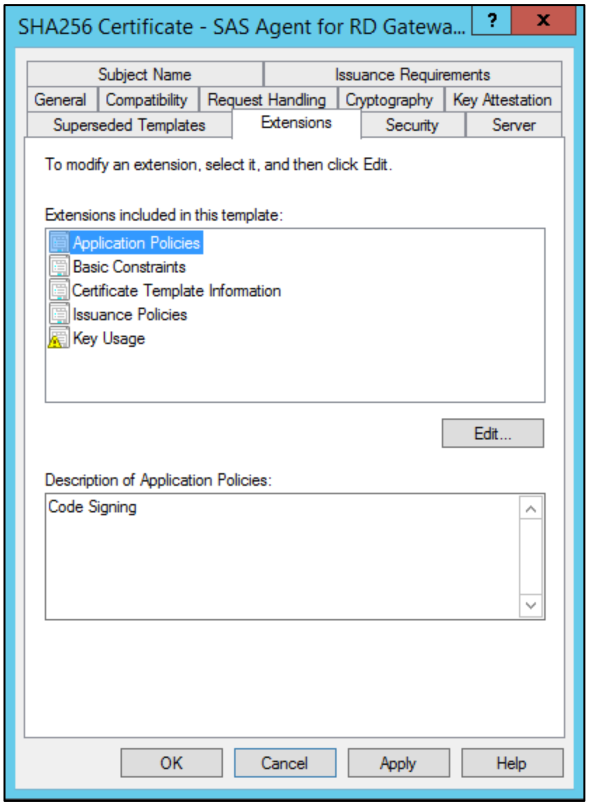
Edit Application Policies Extension

An application policy defines how a certificate can be used.

Application policies:

Code Signing

13. On the **Extensions** tab, under **Description of Application Policies**, **Code Signing** is added. Remove all other application policies. Then, click **OK**.



SHA256 Certificate - SAS Agent for RD Gatewa...

To modify an extension, select it, and then click Edit.

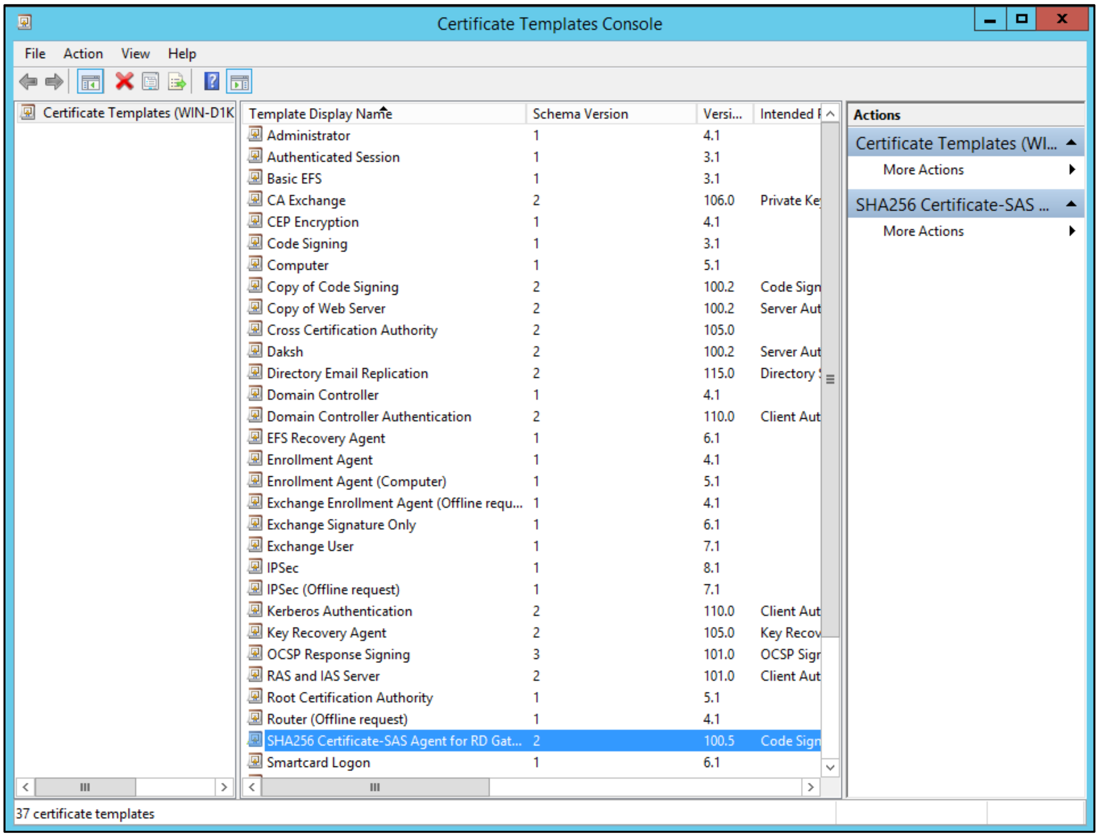
Extensions included in this template:

Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage

Description of Application Policies:

Code Signing

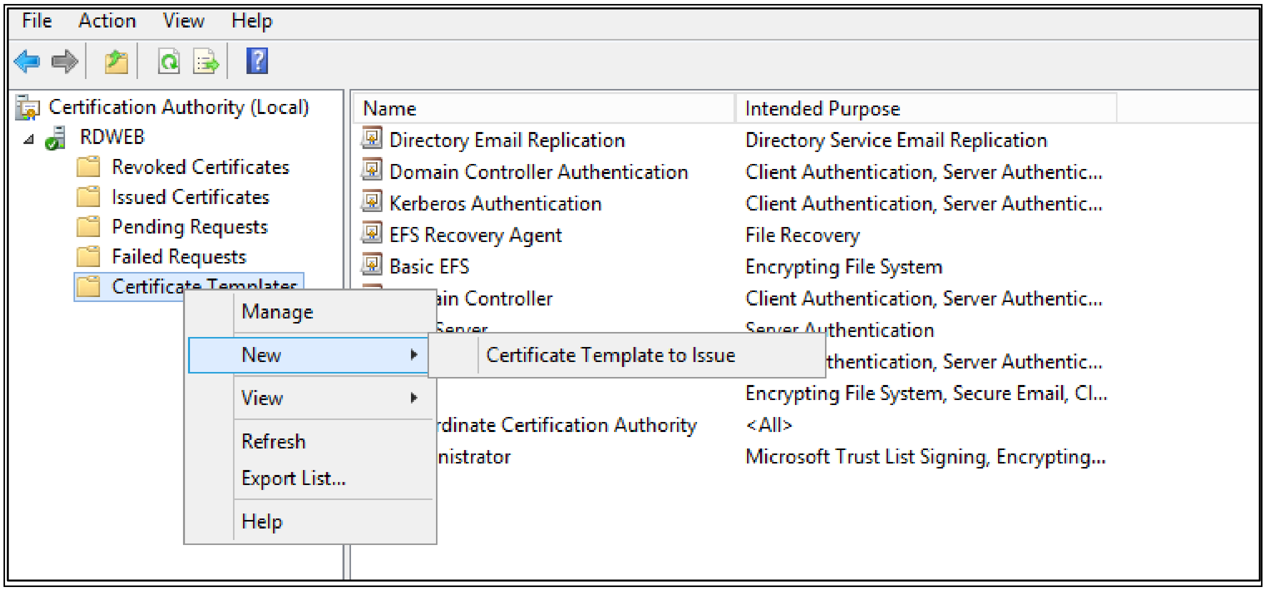
14. The newly created template, **SHA256 Certificate - SAS Agent for RD Gateway**, is now available in the list of certificate templates.


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-D1K
Actions
Certificate Templates (WI...
More Actions
SHA256 Certificate-SAS ...
More Actions

Template Display Name	Schema Version	Versi...	Intended F
Administrator	1	4.1	
Authenticated Session	1	3.1	
Basic EFS	1	3.1	
CA Exchange	2	106.0	Private Ke
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Copy of Code Signing	2	100.2	Code Sign
Copy of Web Server	2	100.2	Server Aut
Cross Certification Authority	2	105.0	
Daksh	2	100.2	Server Aut
Directory Email Replication	2	115.0	Directory S
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Aut
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Client Aut
Key Recovery Agent	2	105.0	Key Recov
OCSP Response Signing	3	101.0	OCSP Sigr
RAS and IAS Server	2	101.0	Client Aut
Root Certification Authority	1	5.1	
Router (Offline request)	1	4.1	
SHA256 Certificate-SAS Agent for RD Gat...	2	100.5	Code Sign
Smartcard Logon	1	6.1	

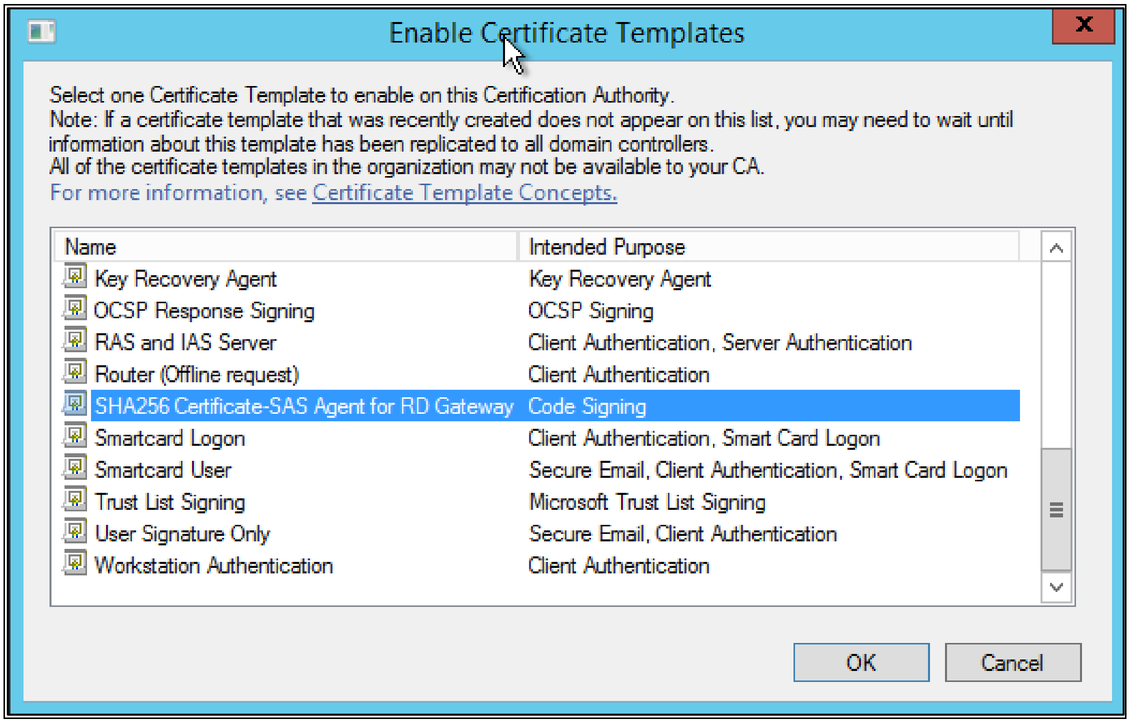
37 certificate templates

15. On the **Certification Authority Management Console** window, in the left pane, expand **RD WEB**, right-click **Certificate Templates**, and then click **New** > **Certificate Template to Issue**.



Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
ain Controller	Client Authentication, Server Authentic...
Server	Server Authentication
	thentication, Server Authentic...
	Encrypting File System, Secure Email, Cl...
rdinate Certification Authority	<All>
nistrator	Microsoft Trust List Signing, Encrypting...

16. On the **Enable Certificate Templates** window, select your certificate template, and click **OK**.

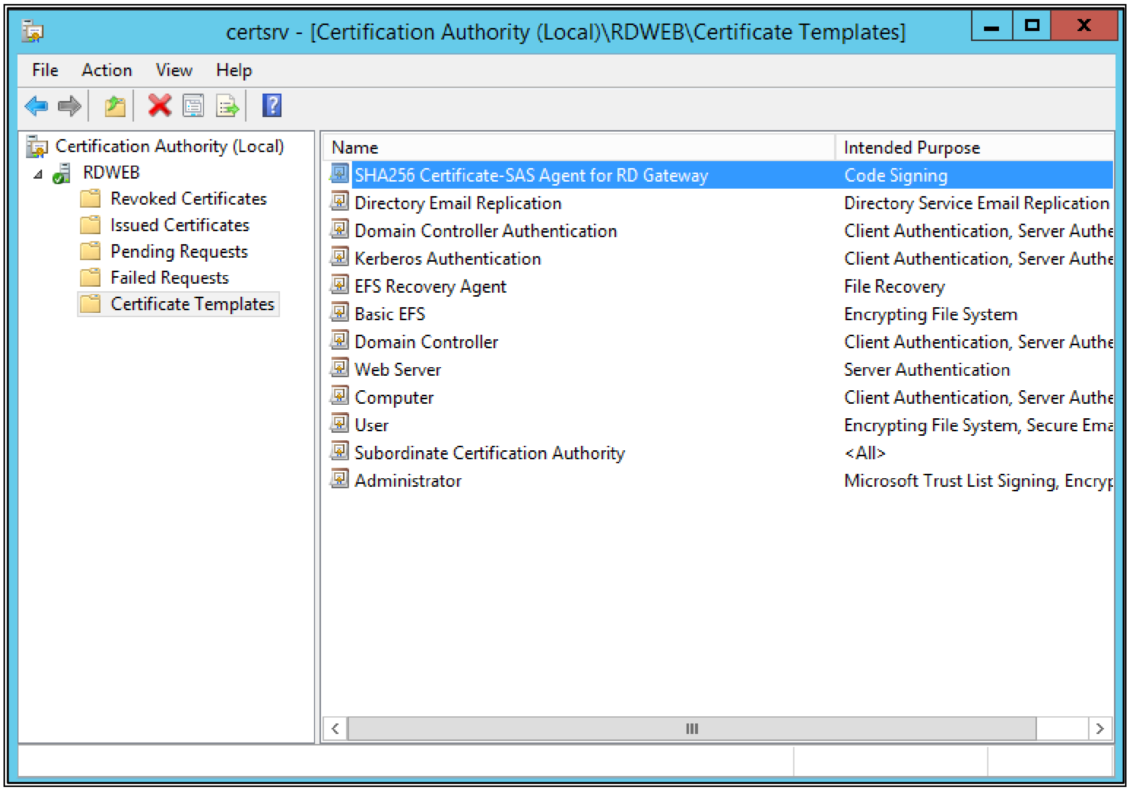


Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
SHA256 Certificate-SAS Agent for RD Gateway	Code Signing
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication
Workstation Authentication	Client Authentication

17. The certificate template you selected is added to the list certificate templates. Close this window.



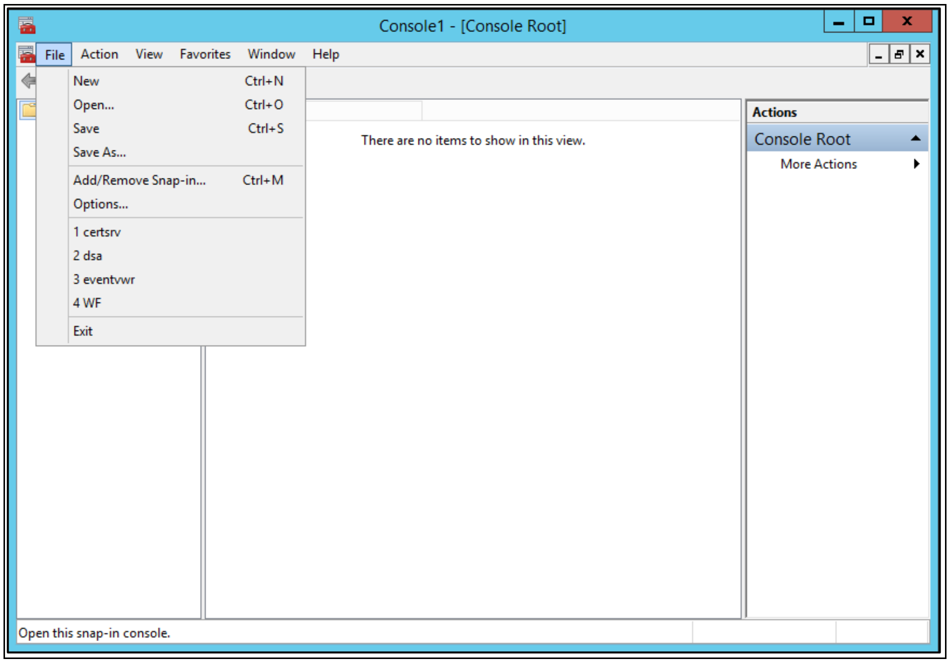
certsrv - [Certification Authority (Local)\RDWEB\Certificate Templates]

- Certification Authority (Local)
  - RDWEB
    - Revoked Certificates
    - Issued Certificates
    - Pending Requests
    - Failed Requests
    - Certificate Templates

Name	Intended Purpose
SHA256 Certificate-SAS Agent for RD Gateway	Code Signing
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authe
Kerberos Authentication	Client Authentication, Server Authe
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authe
Web Server	Server Authentication
Computer	Client Authentication, Server Authe
User	Encrypting File System, Secure Ema
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encryp

Creating SHA256 Certificate Using Certificate Template

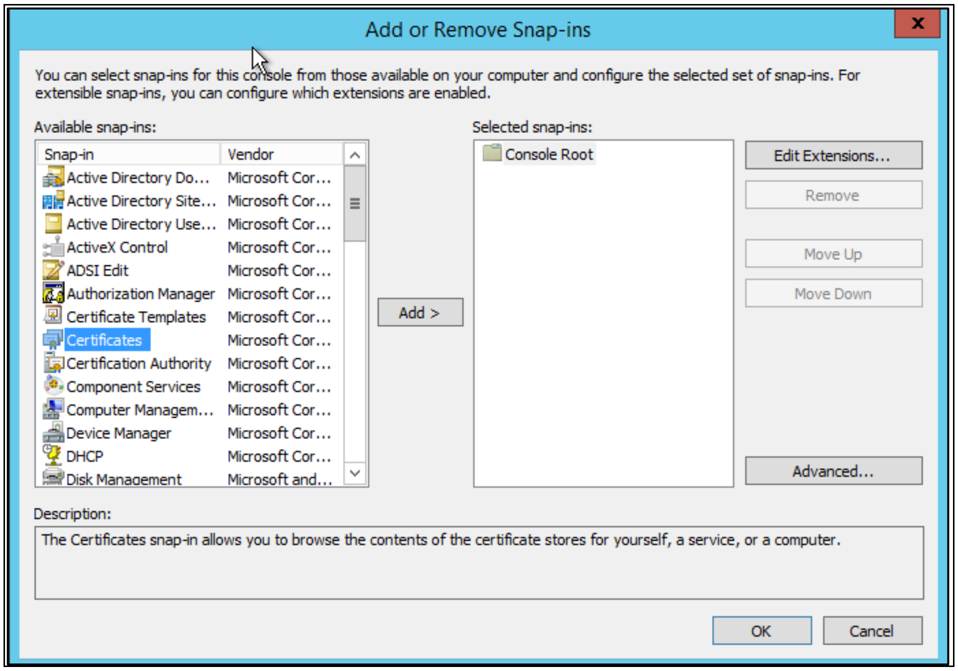
1. Open the **Microsoft Management Console**.
2. From the **File** menu, select **Add/Remove Snap-in**.



There are no items to show in this view.

Open this snap-in console.

3. On the **Add or Remove Snap-ins** window, in the **Available snap-ins** list, select **Certificates**, and click **Add >**.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
DHCP	Microsoft Cor...
Disk Management	Microsoft and...

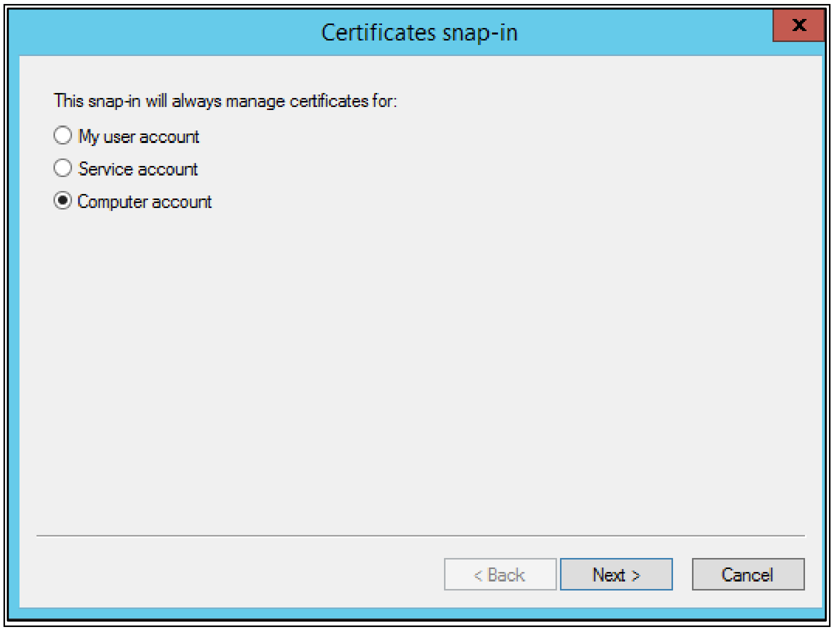
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. On the **Certificates snap-in** window, select **Computer account**, and then click **Next**.



Certificates snap-in

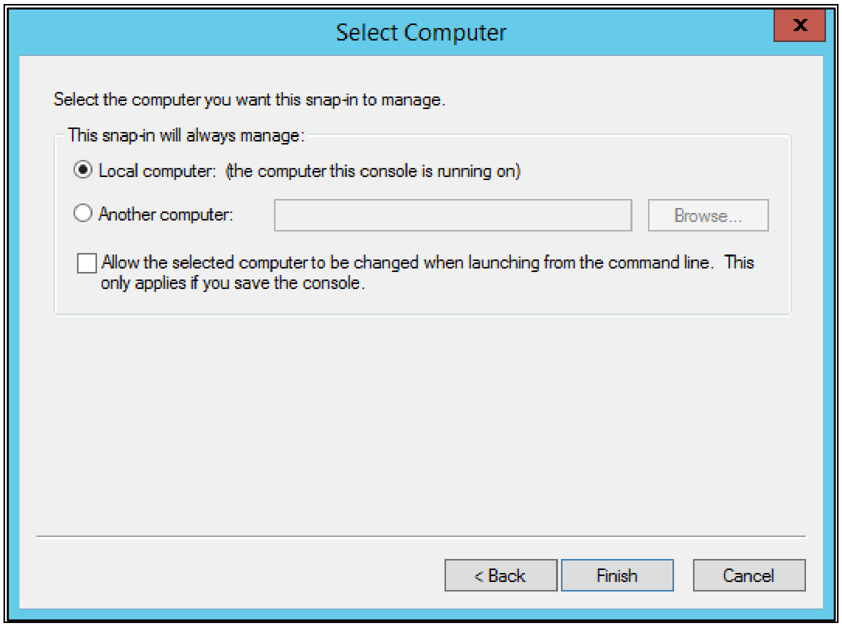
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

5. On the **Select Computer** window, click **Finish**.



Select Computer

Select the computer you want this snap-in to manage.

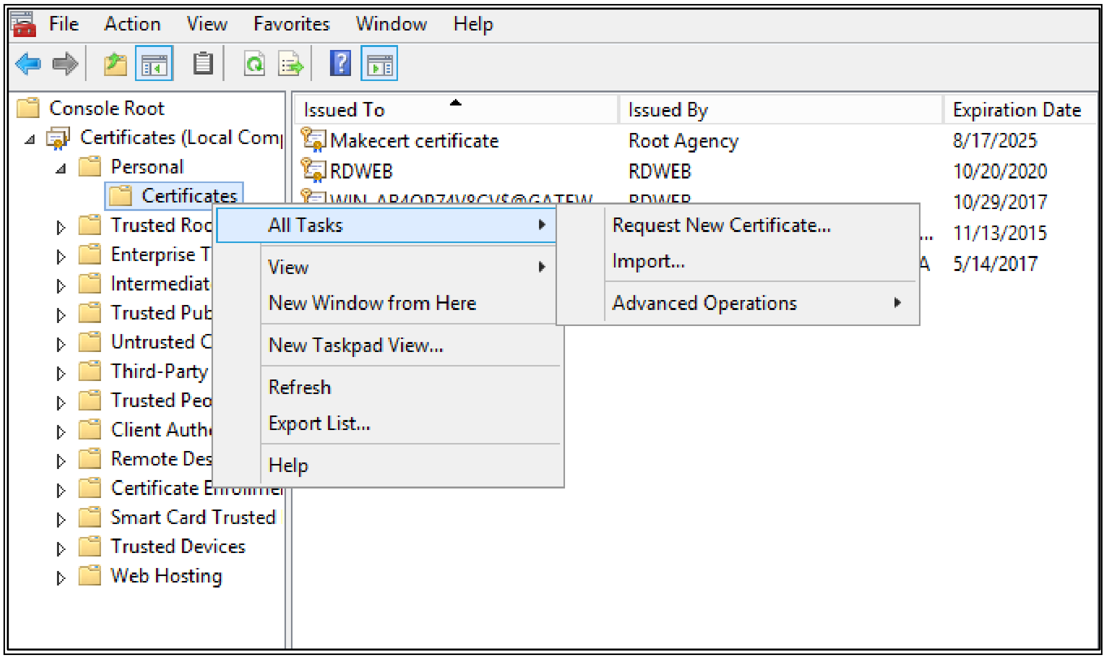
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

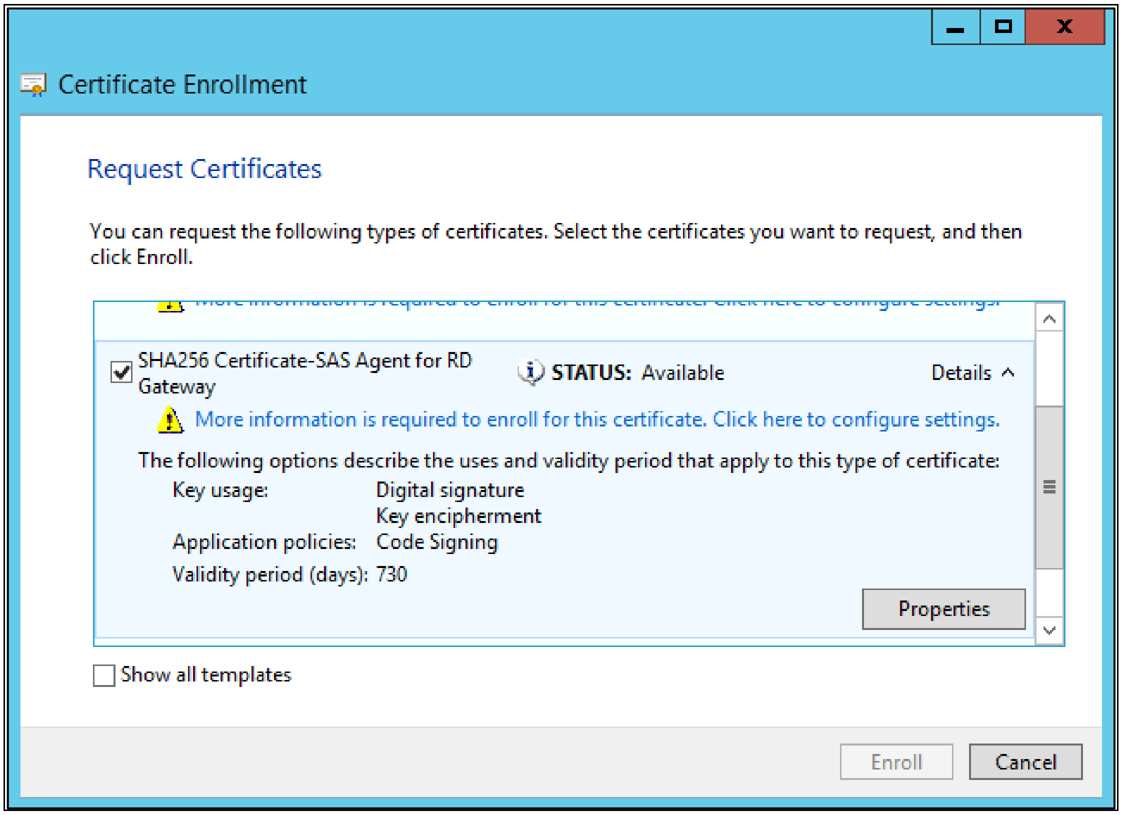
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

6. On the **Console Root** window, expand **Console Root** > **Certificates** > **Personal**. Then, right-click **Certificates** and click **All Tasks** > **Request New Certificate**.



Issued To	Issued By	Expiration Date
Makecert certificate	Root Agency	8/17/2025
RDWEB	RDWEB	10/20/2020
WIN-AR4QP74V8CVS@GATEW	RDWEB	10/29/2017
	...	11/13/2015
	A	5/14/2017

7. On the **Certificate Enrollment** window, select your certificate template, and click **Enroll**.


Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

More information is required to enroll for this certificate. Click here to configure settings.

☑ SHA256 Certificate-SAS Agent for RD Gateway **STATUS:** Available

More information is required to enroll for this certificate. Click here to configure settings.

The following options describe the uses and validity period that apply to this type of certificate:

Key usage:	Digital signature Key encipherment
Application policies:	Code Signing
Validity period (days):	730

□ Show all templates