
Installation Guide

Remote Desktop Gateway Plug-in

Version 6.1

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

Copyright © 2018 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

Contents

About NetIQ Corporation	5
About this Book	7
1 Pre-requisites	9
2 Preliminary Configuration	11
Setting DNS for Server Discovery	11
3 Configuring Remote Desktop Gateway Plug-in	13
Configuring Remote Desktop Gateway Plug-in.	14
Configuring Remote Desktop Client	14
Configuring Advanced Authentication Appliance.	15
4 Uninstalling Remote Desktop Gateway Plug-in	17
5 Troubleshooting for Remote Desktop Gateway	19
Debugging Logs for Advanced Authentication	19

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ♦ Identity & Access Governance
- ♦ Access Management
- ♦ Security Management
- ♦ Systems & Application Management
- ♦ Workload Management
- ♦ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

About this Book

This guide describes the pre-requisites and configuration process of the Remote Desktop Gateway integration.

Intended Audience

This book is intended for Advanced Authentication administrators.

About Remote Desktop Gateway Plug-in

Advanced Authentication integrates with Remote Desktop Gateway to enable a secured access of Remote Desktop Gateway by enforcing multi-factor authentication. Users can use the authentication methods such as Smartphone, VoiceCall, and Swisscom methods to confirm their authentication to the Remote Desktop Gateway.

For example: Employees of a company **Digital Airlines** located in London need to access Remote Desktop Gateway located in Amsterdam of the same company from their Remote Desktop client machines. It must be ensured that the Remote Desktop connection with the gateway is secure and users can authenticate with methods such as Smartphone. The Remote Desktop Gateway integration of Advanced Authentication with Remote Desktop helps to achieve this secured connection with multi-factor authentication.

NOTE: Advanced Authentication Remote Desktop Gateway plug-in supports only the out-of-band methods such as VoiceCall, Smartphone, and Swisscom methods.

1 Pre-requisites

Before configuring the Remote Desktop Gateway, ensure that the following pre-requisites are met:

- ♦ Windows Server 2012 R2 or Windows Server 2016 is installed.
- ♦ Microsoft Remote Desktop Gateway role is configured.

2 Preliminary Configuration

This chapter contains sections about the pre-configuration settings on the Remote Desktop Gateway.

Setting DNS for Server Discovery

- 1 Open a DNS Manager. To open the DNS Manager, click **Start**, point to **Administrative Tools**, and click **DNS**.
- 2 Add Host A or AAAA record and PTR record:
 - 2a In the console tree, right-click the forward lookup zone that includes your domain name and click **New Host (A or AAAA)**.
 - 2b Specify a DNS name for the Advanced Authentication Server in **Name**.
 - 2c Specify the IP address for the Advanced Authentication Server in **IP address**. You can specify the address in IP version 4 (IPv4) format (to add a host (A) resource record) or IP version 6 (IPv6) format (to add a host (AAAA) resource record).
 - 2d Select **Create associated pointer (PTR) record** to create an additional pointer (PTR) resource record in a reverse zone for this host, based on the information that you provided in **Name** and **IP address**.
- 3 Add an SRV record:

NOTE: Ensure that the LDAP SRV record exists at DNS server. If the record is not available, you must add it manually.

For best load balancing, you need to perform the following actions only for Advanced Authentication web servers. You need not create the records for Global Master, DB Master, and DB servers.

- 3a For Advanced Authentication servers from a primary Advanced Authentication site (a site with Global Master server):
 - 3a1 In the console tree, locate **Forward Lookup Zones** and right-click on a node with domain name and click **Other New Records**.
 - 3a2 In the **Select a resource record type** list, click **Service Location (SRV)** and then click **Create Record**.
 - 3a3 Click **Service** and then specify **_aav6**.
 - 3a4 Click **Protocol** and then specify **_tcp**.
 - 3a5 Click **Port Number** and then specify **443**.
 - 3a6 In **Host offering this service**, specify the FQDN of the server that is added. For example, `authsrv.mycompany.com`.
 - 3a7 Click **OK**.

3b For Advanced Authentication servers from other Advanced Authentication sites:

- 3b1** In the console tree, locate **Forward Lookup Zones**, switch to a node with domain name then to **_sites** node, right-click on an appropriate site name and click **Other New Records**.
- 3b2** In the **Select a resource record type** list, click **Service Location (SRV)** and then click **Create Record**.
- 3b3** Click **Service** and then specify **_aav6**.
- 3b4** Click **Protocol** and then specify **_tcp**.
- 3b5** Click **Port Number** and then specify **443**.
- 3b6** In **Host offering this service**, specify the FQDN of the server that is added. For example, `authsrv.mycompany.com`.
- 3b7** Click **OK**.

Repeat [Step 2](#) to [Step 3](#) for all the authentication servers. The Priority and Weight values for different servers may vary. For best load balancing, you need to have records only for Advanced Authentication web servers and you do not need to have the records for Global Master, DB Master, and DB servers.

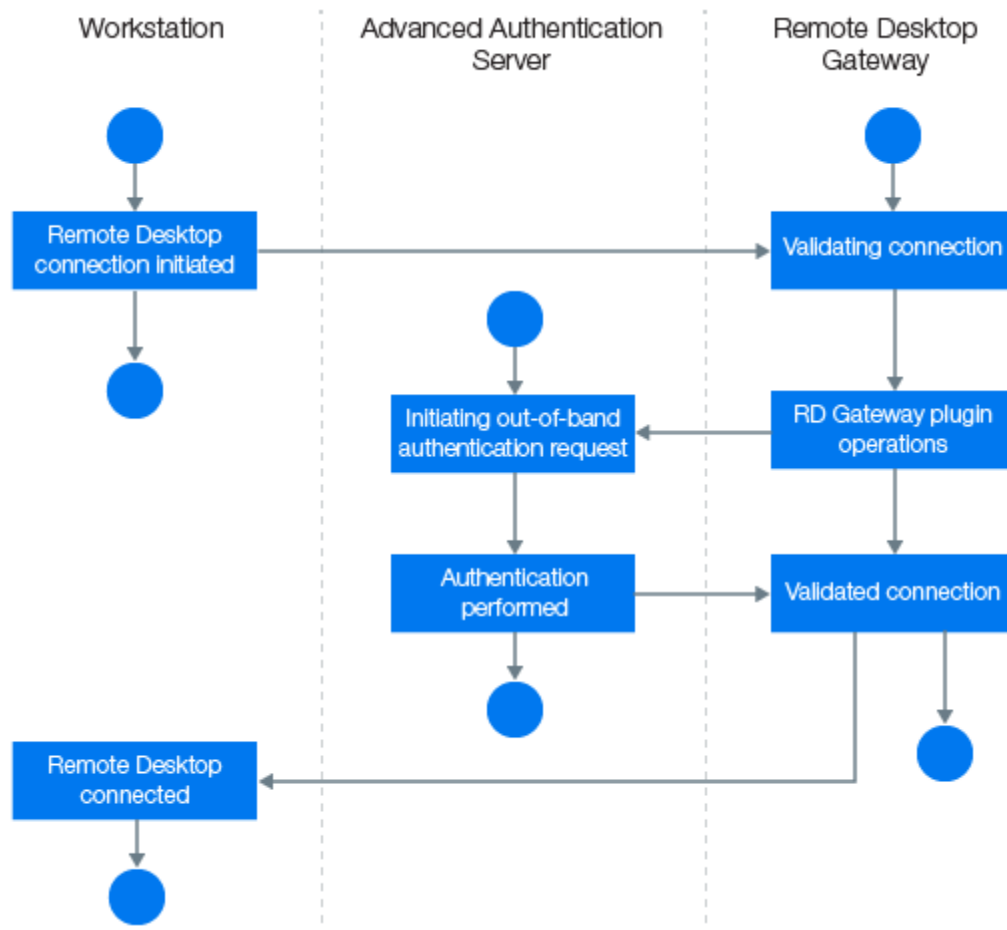
DNS server contains SRV entries `_service._proto.name TTL class SRV priority weight port target`. The following descriptions define the elements present in the DNS server:

- ♦ **Service**: symbolic name of an applicable service.
- ♦ **Proto**: transport protocol of an applicable service. Mostly, TCP or UDP.
- ♦ **Name**: domain name for which this record is valid. It ends with a dot.
- ♦ **TTL**: standard DNS time to live field.
- ♦ **Class**: standard DNS class field (this is always IN).
- ♦ **Priority**: priority of the target host. Lower value indicates that it is more preferable.
- ♦ **Weight**: a relative weight for records with the same priority. Higher value indicates that it is more preferable.
- ♦ **Port**: TCP or UDP port on which the service is located.
- ♦ **Target**: host name of the machine providing the service. It ends with a dot.

3 Configuring Remote Desktop Gateway Plug-in

You can use the Remote Desktop Gateway plug-in to ensure secured access of Remote Desktop connection with multifactor authentication. The plug-in must be installed on Remote Desktop Gateway.

The following diagram illustrates how the Remote Desktop Gateway plug-in works.



This chapter contains the following sections:

- ♦ [“Configuring Remote Desktop Gateway Plug-in” on page 14](#)
- ♦ [“Configuring Remote Desktop Client” on page 14](#)
- ♦ [“Configuring Advanced Authentication Appliance” on page 15](#)

Configuring Remote Desktop Gateway Plug-in

NOTE: Before configuring Remote Desktop Gateway, if you have enabled Multitenancy you must specify a tenant name. This is required because an endpoint can be created in a wrong tenant. For more information on configuring the Multitenancy setting, see “[Configuration Settings for Multitenancy](#)” in the *Advanced Authentication - Windows Client* guide.

- 1 Install `naaf-rdgplugin-x64-release-<version>.msi` on a Remote Desktop Gateway machine.
- 2 If you have enabled Multitenancy, create a file `C:\ProgramData\NetIQ\Windows Client\config.properties`, and add the parameter `tenant_name` with a used tenant name as a value in the configuration file. Otherwise the endpoint might be created in a wrong tenant.
- 3 On a client machine, run `mstsc` and configure the client by performing the steps described in [Configuring Remote Desktop Client](#) section. This establishes a connection between the Remote Desktop Gateway and the Remote Desktop server.

NOTE: When you configure the Remote Desktop Gateway plug-in, the Remote Desktop Connection Authorization Policies (RD CAP) and Resource Authorization Policies (RD RAP) are disabled. These policies cannot be accessed from the Remote Desktop Gateway Manager. Policy settings that are configured prior to the Remote Desktop Gateway integration are overlooked by the Remote Desktop Gateway.

Configuring Remote Desktop Client

- 1 On a client machine, run `mstsc`.
- 2 Click **Show Options** and select **Advanced**.
- 3 Click **Settings** and select **Use these RD Gateway server settings**.
 - 3a Enter the address of RD Gateway in **Server name**. For example: `rdg.test.com`.
 - 3b Deselect **Bypass RD Gateway server for local addresses**.

NOTE: If you select this option, Remote Desktop Gateway is not used when you try to connect from the same subnet.

- 4 Go to the **General** tab and specify the address of remote RDP (Remote Desktop Protocol) server.
- 5 Click **Connect**.
- 6 Specify the domain credentials (for example, `test\administrator` as username) for Remote Desktop Gateway in **RD Gateway Server Credentials**.

A connection is initiated to Remote Desktop through the enrolled authentication method. To configure the methods in Advanced Authentication appliance, see [Configuring Advanced Authentication Appliance](#).
- 7 After you authenticate with the enrolled authentication method, `mstsc` prompts to specify credentials for the remote RDP server. Ensure that a connection has been established between the Remote Desktop Gateway and Remote Desktop server.

Configuring Advanced Authentication Appliance

1 Log into the Advanced Authentication Administrative portal.

2 Create a chain with one of the following methods:

- ♦ Smartphone
- ♦ VoiceCall
- ♦ Swisscom

For more information about how to create chains, see “[Creating a Chain](#)” in *Advanced Authentication - Administration* guide.

3 In the **Events** section, create a Generic event **RDG** event and assign the chain to this event.

4 Enroll the methods in **RDG** for respective users.

4 Uninstalling Remote Desktop Gateway Plug-in

To uninstall the Remote Desktop Gateway plug-in through the Control Panel, perform the following steps:

- 1 In the **Start** menu, select **Control Panel** and then double-click **Programs and Features**.
- 2 Select **NetIQ RDG Plugin** and click **Uninstall**.
- 3 Confirm the uninstallation.
- 4 In the Advanced Authentication Administrative Portal, switch to the **Endpoints** section and remove the endpoint for the Remote Desktop Gateway integration.

NOTE: Endpoint should be removed only if other components such as Logon filter, Windows Client are not installed in Advanced Authentication.

5 Troubleshooting for Remote Desktop Gateway

- ♦ [“Debugging Logs for Advanced Authentication” on page 19](#)

Debugging Logs for Advanced Authentication

To investigate the possible issues you may be asked to collect the debug logs.

1. Run `DiagTool.exe` (the tool must have Microsoft .NET Framework 3.5 installed).
2. Click **Clear All** (if applicable) in the **Debug logs** tab.
3. Click **Enable**.
4. Restart the system.
5. Reproduce your problem.
6. Run `DiagTool.exe`.
7. Click **Save logs** in the **Debug logs** tab.
8. Specify a file name and path. Click **Save** to save the logs.
9. Click **Disable** to disable the logging.
10. Click **Clear All**.

If you don't have the Diagnostic Tool you can perform the actions manually:

1. Create a text file `C:\ProgramData\NetIQ\Logging\config.properties`.
2. Add a string to the file: `logEnabled=True` that ends by a line break.
3. Create a directory: `C:\ProgramData\NetIQ\Logging\Logs\`.
4. Restart the machine.
5. Reproduce your problem.
6. Pack the logs located in `C:\ProgramData\NetIQ\Logging\Logs\` into a zip file.
7. Change `logEnabled=True` to `logEnabled=False` in the folder,
`C:\ProgramData\NetIQ\Logging\config.properties`

With the Diagnostic Tool, you can check the network problems on a workstation, issues in connection between a workstation and DNS Server, and to get a list of the Advanced Authentication Servers that can be discovered. To identify Advanced Authentication server, perform the following steps:

NOTE: As a prerequisite, ensure that `DiagTool.exe` file is available with the following files in the same directory:

- ♦ `DiagTool.exe.config`
 - ♦ `Ionic.Zip.dll`
 - ♦ `JHSoftware.DNSClient.dll`
-

1. Run `DiagTool.exe` (the tool must have Microsoft .NET Framework 3.5 installed).

2. Click **Servers**.
3. In the **Search settings**, specify the domain name in **Domain** to find a list of Advanced Authentication servers in the specified domain.

If you want to find particular server then clear **Use system DNS server** and specify the IP address of the DNS server in **DNS server**.
4. Select **Use v6 DNS lookup** to allow the Diagnostic Tool to find the Advanced Authentication server using **_aav6** records.

If you want to find the Advanced Authentication server using **_aaa** records then clear **Use v6 DNS lookup**.
5. Click **Search**.

NOTE: If you configure IP address of the Advanced Authentication server in the DNS service record, the Diagnostic tool cannot find and retrieve the respective record. Ensure that you configure the DNS service record with Fully Qualified Domain Name (FQDN) to enable the Diagnostic tool to find and retrieve the respective record.
