One Identity Safeguard for Privileged Sessions 6.1

Remote Desktop Protocol Scenarios

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

SPS Remote Desktop Protocol Scenarios
Updated - August 2019
Version - 6.1

Contents

1

Overview

The aim of the document is to present different working scenarios for One Identity Safeguard for Privileged Sessions (SPS) when RDP monitoring is required and present some best practices for those scenarios. Also, it is intended to demonstrate possible issues with different scenarios. Please note it is only an extract of the official Administration Guide, emphasizing the most important RDP specific topics, so in any case please refer to the official documentation cover this and other topics as well.

NOTE:

This is only an extract of Administration Guide, emphasizing the most common RDP-specific topics.

Glossary

Advanced routing:

The core network device alters the traffic and directs packets to be monitored through SPS (seamless integration: no change required on the computers and servers in the network).

Certificate Revocation List (CRL):

CRL includes a list of the serial numbers of revoked certificates and it must have made publicly available by the PKI service that generates the certificates. Microsoft RDP Client rigorously checks the availability of CRLs.

Gateway authentication:

Gateway authentication requires a secondary logon before the authentication on the remote server, so rules defined on the gateway (in this case SPS) can be evaluated and applied. With gateway authentication it is possible to limit access to specific resources (for example specific sub-channels) to specific local or central groups. It also allows to use usermapping.

Inline transparent mode:

SPS placed directly between the source and destination. This means that the client's and server's gateway is changed to SPS's address.

Man-in-the-Middle (MitM) technologies:

MitM is a required method to be able to decode encrypted traffic. SPS must be placed between the source and the destination of the encrypted traffic, so the client connection attempt to the destination server will be terminated at SPS, decoded, recorded and SPS will establish a second, also encrypted channel to the original destination server. Because this breaks the original encryption chain, some additional measures (for example signing CA) must be applied to avoid warnings.

Non-transparent mode of operation:

User will change the destination host to SPS where some kind of gateway authentication performed (or in some cases not-performed), then SPS will establish the connection to the original destination server.

Proxy:

A system placed between two different zones to allow monitoring the traffic between them. The monitored traffic must be passed through the proxy to allow it to be monitored. SPS is a proxy-based solution.

Public Key Infrastructure (PKI):

A public key infrastructure (PKI) is a set of roles, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Remote Desktop Protocol (RDP):

A proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

One Identity Safeguard for Privileged Sessions (SPS):

One Identity Safeguard for Privileged Sessions is a user monitoring appliance that controls privileged access to remote IT systems, records activities in searchable, movie-like audit trails, and prevents malicious actions.

Singing-CA:

CA certificate installed on SPS to allow generating certificates for TLS layer of different protocols. RDP implementation of SPS also requires TLS layer.

Remote Desktop Gateway (RD Gateway):

Service developed by Microsoft to provide authentication front-end for Remote Desktop Services. One Identity provides an own implementation of RD Gateway (Remote Desktop Gateway) in SPS

Transparent mode of operation:

In transparent mode the user will connect to the original destination server, however the traffic will be passed through the proxy for recording and analysis. From the user perspective there should be no difference between the monitored and not-monitored traffic.

Usermapping:

With usermapping SPS can allow / deny using generic accounts (for example Administrator) based on group membership and can map real users to generic accounts.

x.509-trusted third party:

Certain components of the solution (for example TS-GW TLS layer, Signing-CA) require trusted certificates. It means if the common name parameter of the certificate is different from the DNS name user trying to connect, or the signing CA is not trusted by the client, the connection may fail or generate an error. This is especially true when TS-GW is in use, because the MS RDP client (mstsc) requires a fully trusted third party certificate for this function.

SPS feature comparison

SPS must be part of the target domain, and users can log on to only one domain unless there is a trust relationship between the different domains. For details on using SPS with multiple domains, see Network Level Authentication (NLA) with domain membership.

Transparent RDP

Prerequisites:

To avoid certificate warnings, configure a signing CA that is trusted by the clients for the connection between the client and SPS.

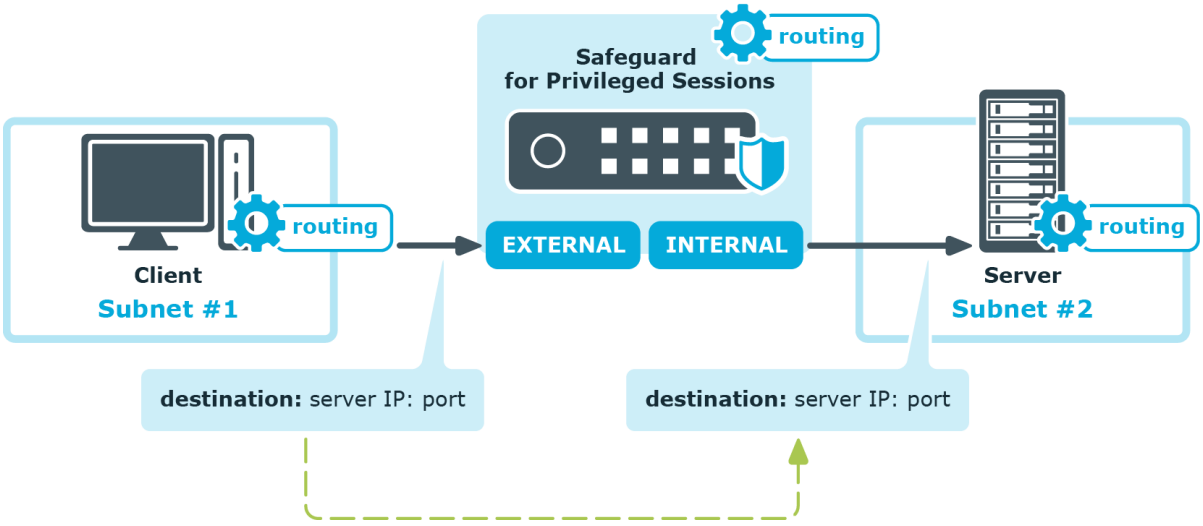
Description:

The One Identity Safeguard for Privileged Sessions connection policies can work in different network models to make it easy to integrate it into an existing network. These

two modes are transparent, and non-transparent modes (for details on modes of operation, see "Modes of operation" in the Administration Guide). The aim is usually the transparent implementation. Although the non-transparent mode can provide some transparency, it is not the best to be used for that purpose.

For the easy-to-deploy and totally transparent solution the transparent mode would be the best. This mode requires integrating SPS in the network level, so all the administrative traffic could pass the box to make it controllable and auditable (for details and illustrations on transparent mode, see "Transparent mode" in the Administration Guide).

Figure 1: SPS in transparent mode



In most cases it is not possible, or not optimal to integrate SPS into the network as in the abovementioned example, because it would require significant changes to the network topology, and SPS could act as a single point of failure. However, it is possible to use SPS in transparent mode transparently without changing the network layout, with a few additional configuration steps in some of the active network devices (firewalls or routers) and the SPS itself.

Disadvantages compared to non-transparent solutions:

- Remote Desktop Gateway (RD Gateway) cannot be used, only out-of-band gateway authentication is possible
- Because of this, user mapping is not possible unless out-of-band gateway authentication is implemented, where the gateway authentication is performed using the web interface of SPS.

2

Typical use-cases

The following use-cases will cover most common scenarios for monitoring RDP connections with SPS. Also the requirements and limitations has been indicated. As a general guideline, implement TLS (with signing CA) or NLA.

Non-transparent RDP + Domain + RD Gateway (Remote Desktop Gateway)

This is one of the most common non-transparent scenarios and the original out-of-the box solution when inline gateway authentication is supported (thanks to the RD Gateway). This is a non-transparent scenario, so users will first connect to SPS, authenticate, then SPS will establish a connection to the original destination server. In case of RDP6 the complete server side authentication also done prior opening Remote Desktop on the server.

Using SPS as a Remote Desktop Gateway (RD Gateway)

With usermapping, you can monitor the real user behind a generic login event (for example Sam Smith logged on as Administrator on Server1.

With usermapping, you can limit which users are allowed to use specific usernames on specific servers.

For details, see Using SPS as a Remote Desktop Gateway.

Prerequisites:

Provide a trusted certificate for Remote Desktop Gateway.

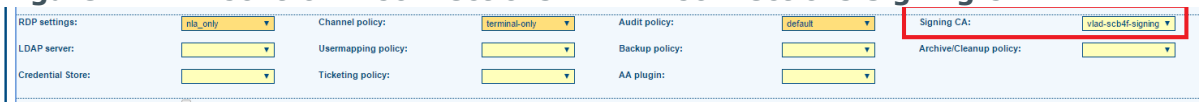
Configure a signing CA trusted by the clients for TLS part of the RDP protocol to avoid receiving a warning about untrusted (self-signed) certificate generated by SPS when the

RDP connection is built. In this case, a trusted certificate will be generated for the RDP connection, however, a warning regarding the CRL accessibility will still be displayed.

NOTE:

It is not required to use a signing CA for the Remote Desktop Gateway TLS connection. You can use the **Use the same certificate for every connection** option.

Figure 2: RDP Control > Connections — RDP Connections Signing CA



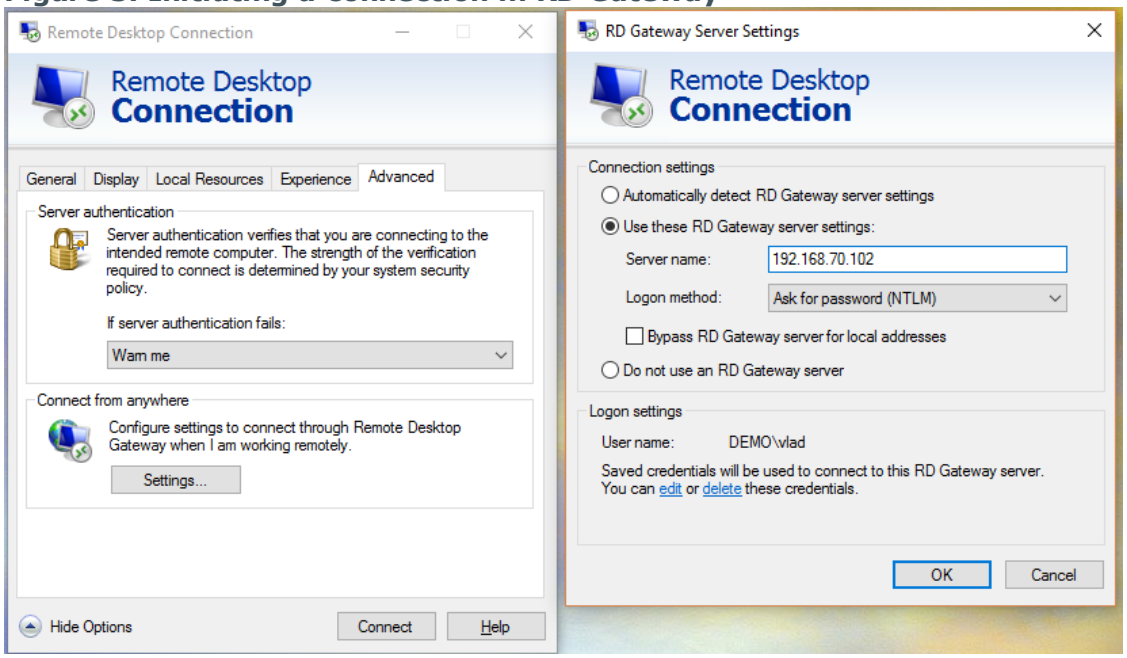
NOTE:

In case of non-NLA, certain Windows settings may interfere with username extraction from the connection. If the **DontDisplayLastUserName** option is enabled on the server, the target username is not visible on the **Search**, **Four Eyes** and **Active Connections** pages. User mapping is also not available.

To use SPS as an RD Gateway

The user initiates a connection to SPS on port 443 and use it as a Remote Desktop Gateway (RD Gateway).

Figure 3: Initiating a connection in RD Gateway



1.
2. If the user authentication is successful:

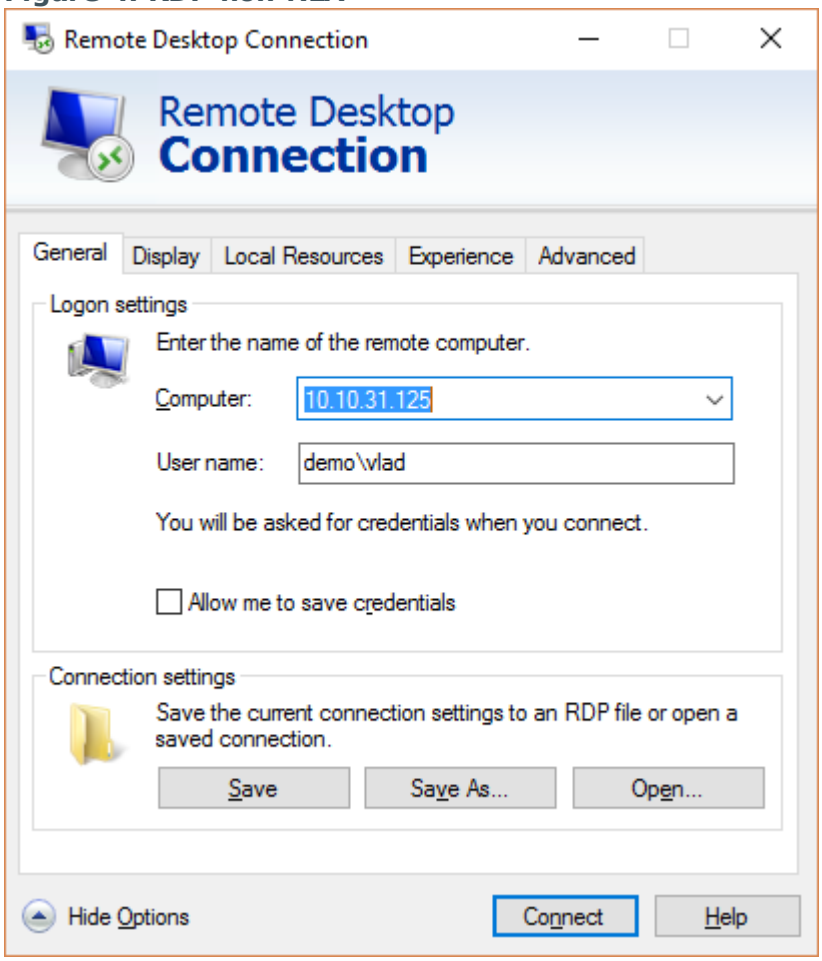
a. SPS evaluates the policies and SPS settings.

b. SPS determines whether to allow the user to use the specified server / username combination.

NOTE:

In case of non-NLA configuration, the target username cannot be used to evaluate channel policies, because it is available too late.

Figure 4: RDP non-NLA



3. In case of positive results, the connection is granted and established.
   - *non-NLA:* the drawing channel is opened and the server-side authentication is performed on the server.
   - *NLA:* the server-side authentication has to be successful first, and the drawing channel is opened only after the successful authentication.

Connecting to a server through SPS using a RD Gateway

For a detailed description of what happens when a client connects a server through SPS using a Remote Desktop Gateway (RD Gateway), and how the different configuration options and policies of SPS affect this process, see Connecting to a server through SPS using a RD Gateway.

Configuring Network Level Authentication without domain membership and inband destination selection

You can authenticate to multiple domains without having trust relationship between them.

Inband destination is available when the target server is not part of the domain or when a local account must be used for logon.

You can use inband destination selection with every RDP version (NLA and non-NLA) without using Remote Desktop Gateway and domain membership.

For details, see Network Level Authentication without domain membership.

Prerequisites:

- The remote server must support NLA.
- Configure a signing CA trusted by the clients for TLS part of the RDP protocol to avoid receiving a warning about untrusted (self-signed) certificate generated by SPS when the RDP connection is built. In this case, a trusted certificate will be generated for the RDP connection, however, a warning regarding the CRL accessibility will still be displayed.
- To implement a Signing CA that is trusted by the clients, every CA certificate of the chain must be placed in the **Trusted Root Certificate Authorities** of the **Local Computer**, otherwise RDP the client will generate two warnings for each connection.
- Configure your RDP clients so SPS can record the username of client uses in the connection. If you do not configure these settings on the clients, SPS will automatically display a login screen for the users to enter their usernames and passwords. Note that although SPS automatically displays a login screen if it cannot determine the username used in the connection, currently you cannot specify the destination address in this login screen, only in your RDP client application.

- *On Windows Vista SP1 and newer platforms (Remote Desktop Protocol 6.1 or newer)*:

  Navigate to **Local Group Policy Editor > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Connection Client** and enable the **Prompt for credentials on the client computer** option in the clients. For details, see the Microsoft Documentation.

- *On Windows Vista and older platforms (Remote Desktop Protocol 6.0 or older)*:

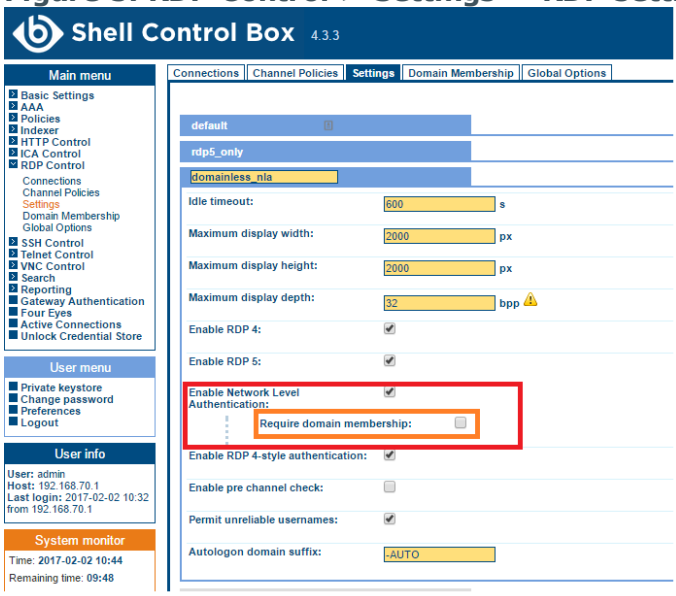
  Configure your RDP clients to save the credentials, or make sure that the **Allow me to save credentials** option is selected in the RDP client.

To configure NLA without domain membership and inband destination selection

Navigate to **RDP Control > Settings** and configure an RDP setting as the following:

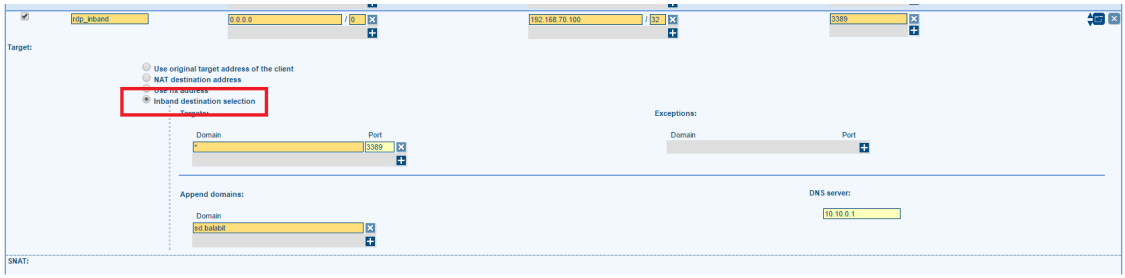
Select **Enable Network Level Authentication**. Deselect **Require domain membership**.

Figure 5: RDP Control > Settings — RDP settings domainless NLA



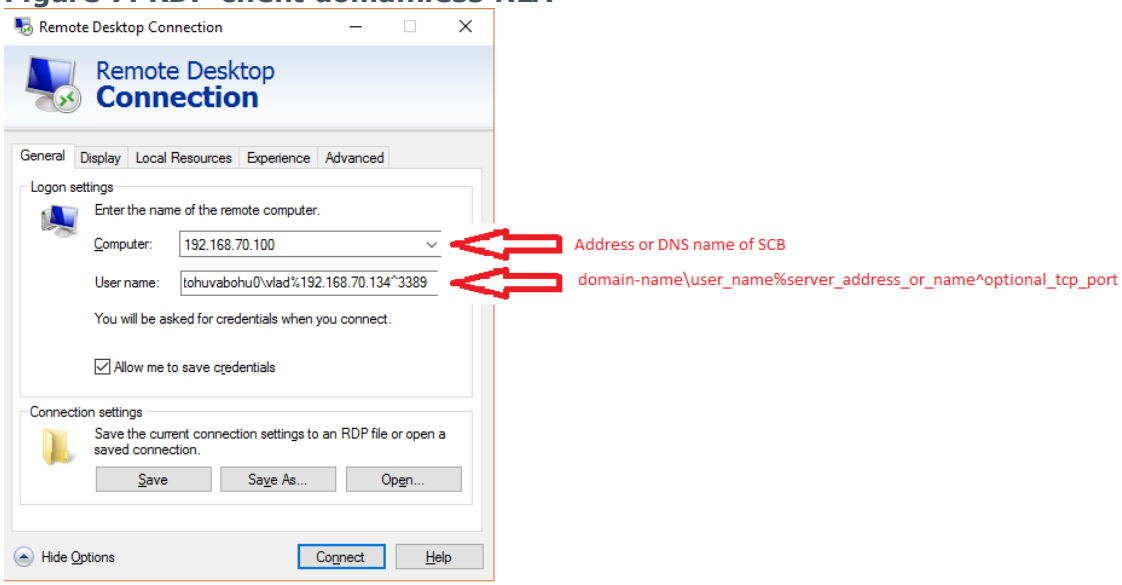
1.
2. Apply this RDP setting to the desired RDP connection policy.
3. For **Target**, select **Inband destination selection**. For details, see Configuring inband destination selection.

Figure 6: RDP Control > Connections — RDP Target Inband destination selection



Configure the RDP client:

Figure 7: RDP client domainless NLA



4.

Configuring RDP with credential store and autologin

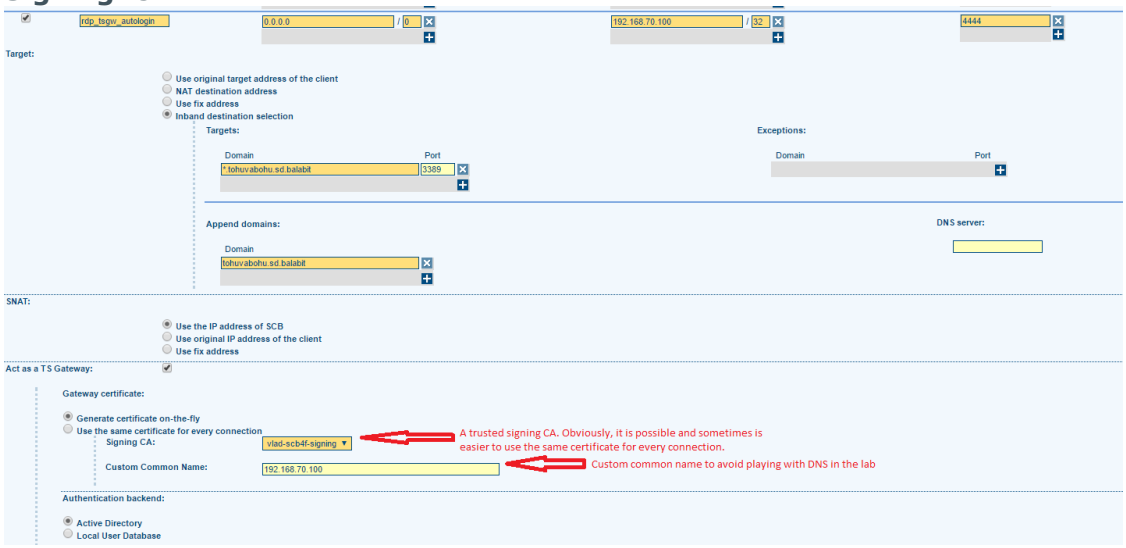
To implement this scenario, you can use either internal or external credential store to provide login information for RDP sessions. You will have to configure some kind of gateway authentication to control who can checkout the credentials from the credential store. It is also advised to use usermapping, because most of the time the gateway username and the target username will be different.

In the following example, you will use the internal credential store.

To configure RDP with credential store and autologin

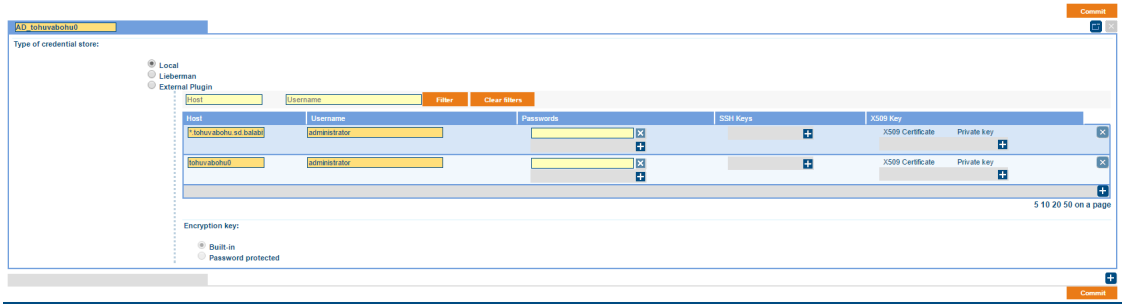
1. Configure the RDP connection policy similarly to the simple Remote Desktop Gateway (RD gateway) scenario. You can use either a fixed certificate, or a certificate that is generated on-the-fly. This example demonstrates the on-the-fly option, where you can specify an alternate common name to avoid DNS modification. In case of fixed certificate, make sure the common name is the same as the user enters in **mstc > Advanced > Settings > Use these RD Gateway server settings > Server name** field.

Figure 8: RDP Control > Connections — Remote Desktop Gateway Signing CA



2. Create a local credential store and inclide all credentials that you want to protect.

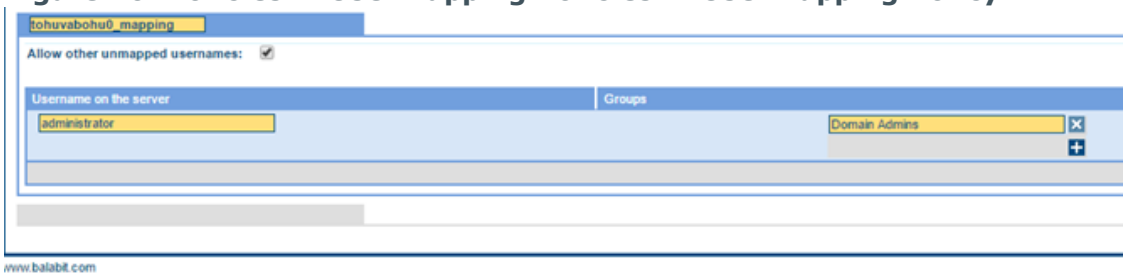
Figure 9: Policies > Credential Stores — Local Credential Store



3. Create a usermapping policy for the desired username to LDAP Group Mapping.

> NOTE:
>
> Usernames in usermapping are case-sensitive, therefore make sure to use the same format in the RDP client, as in SPS.

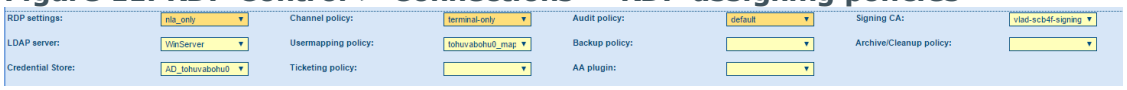
Figure 10: Policies > Usermapping Policies — Usermapping Policy



4. LDAP groups are the same as AD groups most of the time. However, for this feature, navigate to **Policies > LDAP Servers** and configure and LDAP server.

   Assign the policies configured above to the previosuly created RDP connection policy in **RDP Control > Connections**.

Figure 11: RDP Control > Connections — RDP assigning policies

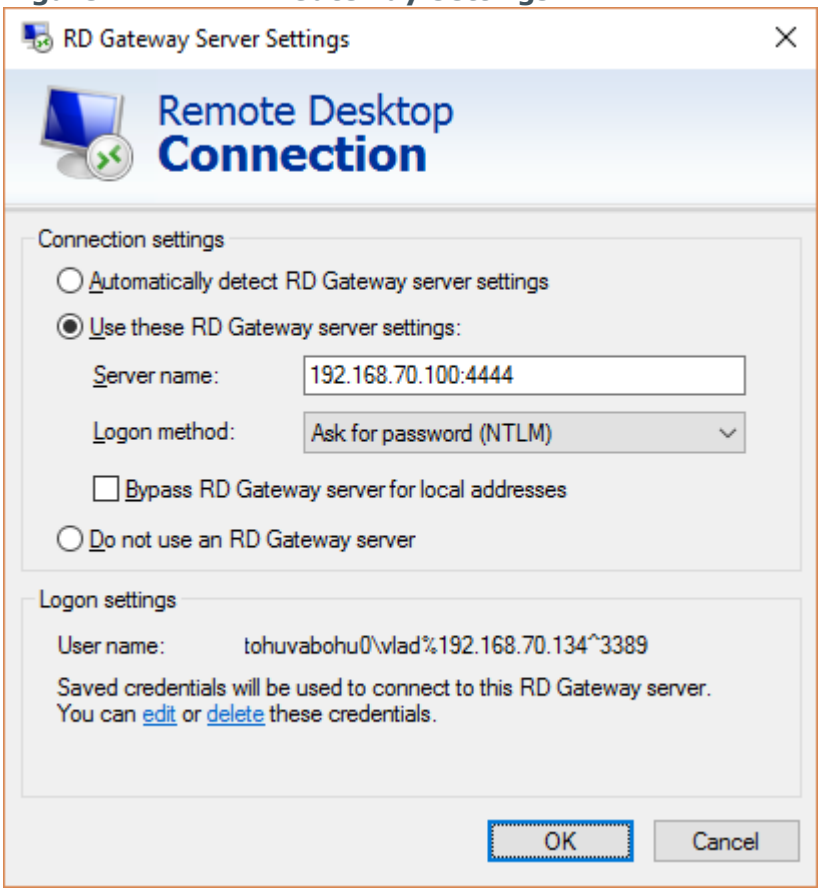


5.

6. Configure the RDP client (mstsc). For details, see Inband destination selection in RDP connections.

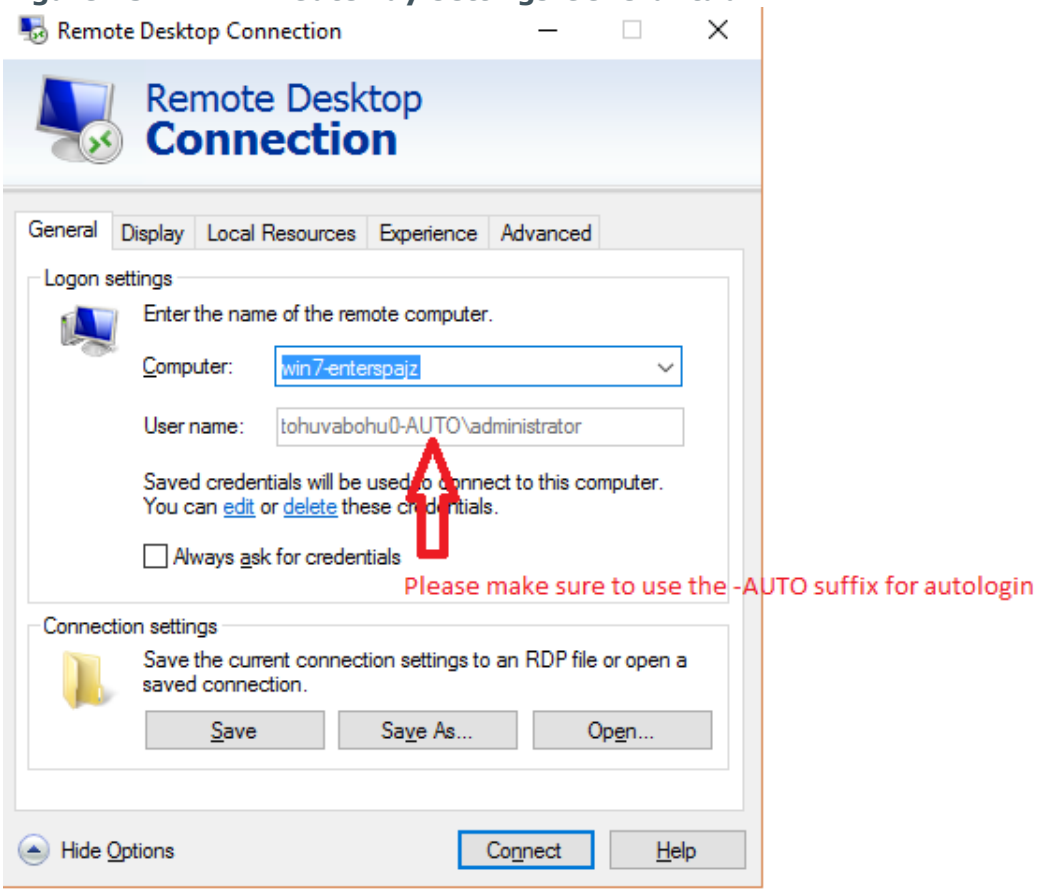
   a. In the RD Gateway, navigate to the **Advanced > Settings** tab, select **Use these RD Gateway server settings** and configure it accordingly.

Figure 12: RDP RD Gateway settings



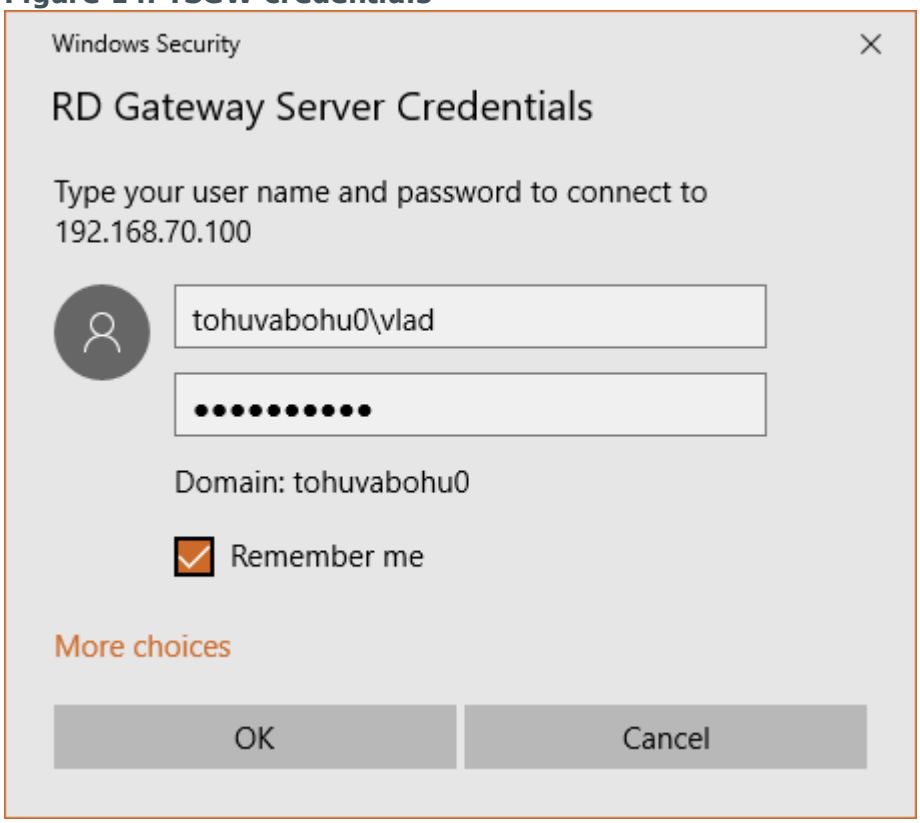
b. On the **General** tab, configure the remote server address and username. Make sure to use the `-AUTO` suffix, this is mandatory for autologin.

Figure 13: RDP RD Gateway settings General tab



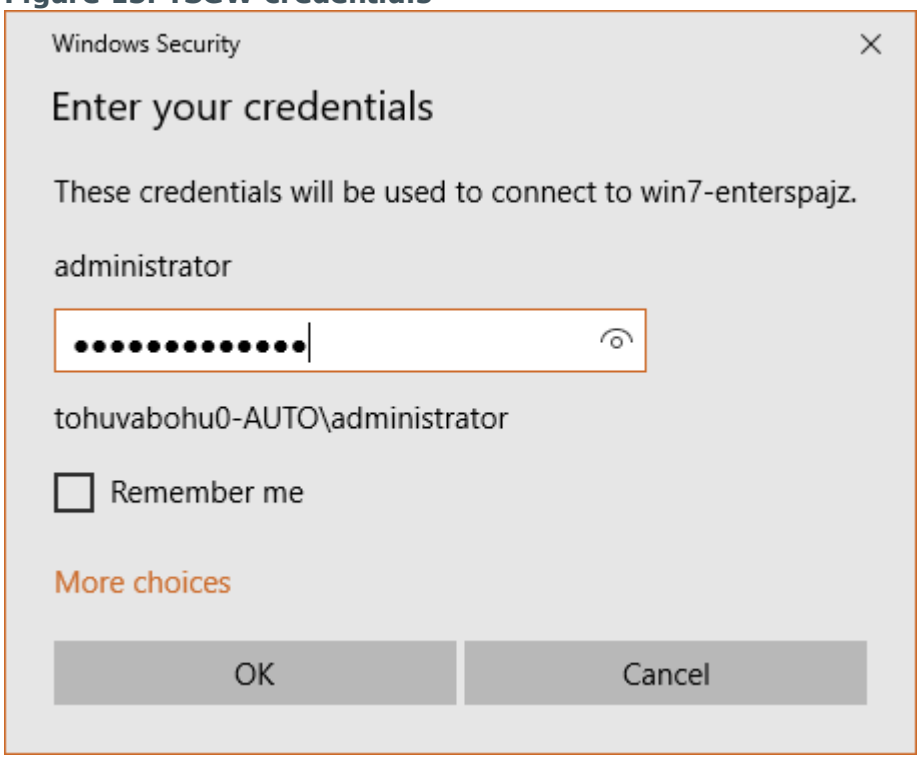
7. Enter the Remote Desktop Gateway credentials.

Figure 14: TSGW credentials



8. Make sure to enter the same username into the password field too.

Figure 15: TSGW credentials

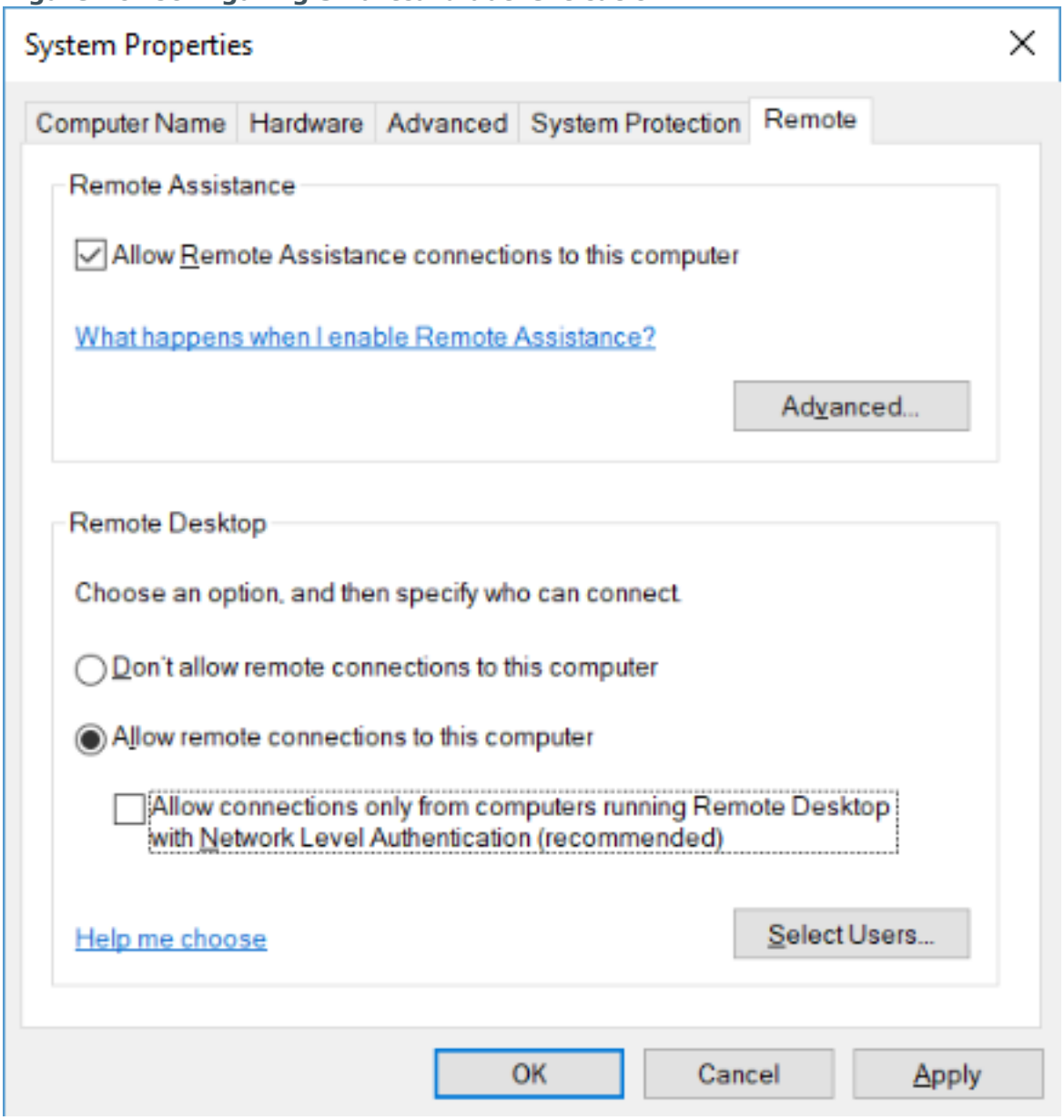


Prerequisites for RDP with Smartcard authentication

In case of Smartcard-based authentication on the server side (SPS to RDP server connection), the follow limitation exists:

This authentication method is only available when RDP5 / TLS is available on the server. For example on Windows Server 2012 and above, the default setting is more restrictive and does not allow the use of Smartcards. Make sure to deselect this option: **Allow connections only from computers running Remote Desktop with Network Level Authentication**.

Figure 16: Configuring Smartcard authentication



Prerequisities:

- Smartcard-based authentication is usually used in a domain environment, so this is not common to be used for standalone Windows servers
- Microsoft Certificate Services or other third party PKI must be available and users must be allowed to use Smartcard for login
- Smartcard supported by Windows operating system and the related tools / libraries

Components that were used in the test system:

- *Domain Controller*: Windows Server 2008r2
- *Certificate Server*: Windows Server 2012r2

  NOTE:

  These two roles (Domain Controller and Certificate Server) cannot reside on the same server

- *Client*: Windows 10
- *Session monitoring*SPS 4F4
- *Smartcard*: YubiKey 4 Nano
- *Guidelines for Windows CA set-up*: YubiKey PIV Deployment Guide
- *Yubikey PIV manager for the certificate request*: YubiKey PIV Manager

3

Troubleshooting

General considerations

Use a layer-to-layer troubleshooting when diagnosing any issue. First, make sure the basic connectivity is working, then move to the next level and continue up to the application layer. Apply the appropriate layer-specific troubleshooting methods.

SPS syslog usually guides you to the proper direction by displaying useful information regarding to the issue you are facing with.

- It is strongly advised to collect SPS syslog at a central location, because it can contain useful information for future troubleshooting purposes.
- SPS syslog can contain sensitive information, therefore make sure to limit access to SPS syslog to the appropriate operational staff.

To increase the protocol level debug, navigate to **RDP Control > Global Options**. Debug level 8 is usually more than enough for diagnostic purposes.

"Domain membership" configuration usually fails because of two reasons:

- Too much time difference between SPS and the Domain Controller (DC). Make sure that the DC and and SPS are synched to a correct NTP source or SPS is synched to DC itself. To do this, navigate to **Basic Settings > Timezone > NTP settings**.
- DNS accessibility / misconfiguration. Make sure your Active Directory DNS services are configured correctly and SPS uses this information (for example DC specified as DNS server in **Basic Settings > Network**).

Consider to limit the allowed channels for specific connection policies. Using some of the RDP channels may lead to security incidents and/or not allowed to be used by some of the security standards. To configure this, navigate to **RDP Control > Channel Policies**.

Smartcard authentication cannot be used when **Enable Network Level Authentication** option is enabled.

Kerberos-based authentication for RDP is currently not supported.

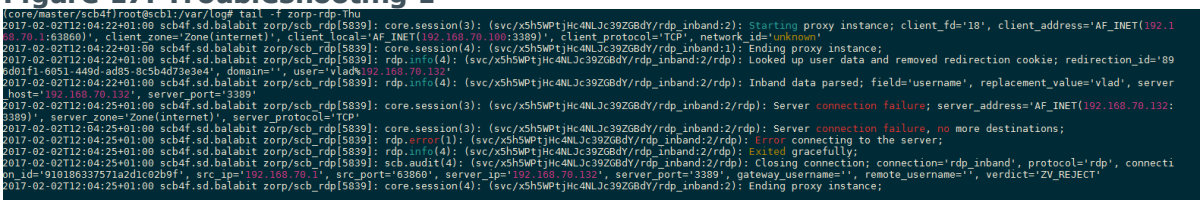
Most common errors and solutions

The following examples may help you to identify the root cause behind a not-working RDP connection

Server is not reachable:

Server is not reachable, either because it is down or network configuration prevents SPS to connect to the server.

Figure 17: Troubleshooting 1



Suggested action: if server can be reached by skipping SPS, verify network configuration

The following is in the log:

In case of domainless NLA the checkbox “Allow me to save credential” is not checked, or local security policy is not modified according to the admin guide.

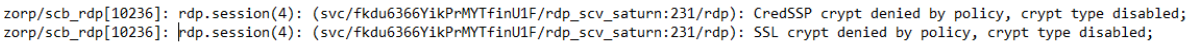
In this case you may see the following in SPS’s RDP log

Figure 18: Troubleshooting 2

Crypt denied:

You may see “Crypt denied” errors in SPS’s RDP log if the server only supports CredSSP (NLA), but the connection policy allows only RDP5

Figure 19: Troubleshooting 3



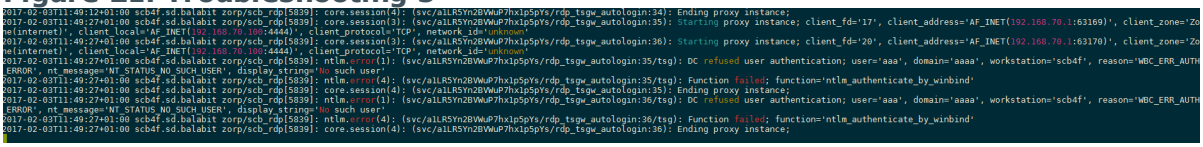
The following is in the log during autologin:

User failed to enter ‘username’ in ‘password’ field, so auto logon cannot be performed

Figure 20: Troubleshooting 4

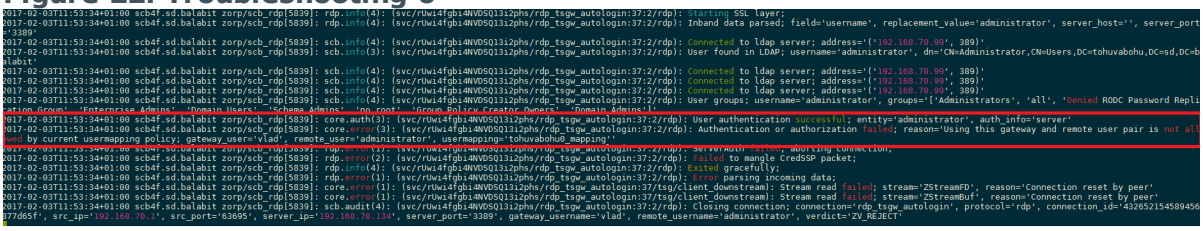
User failed to enter correct credentials for RD Gateway (Terminal Services GW)

Figure 21: Troubleshooting 5



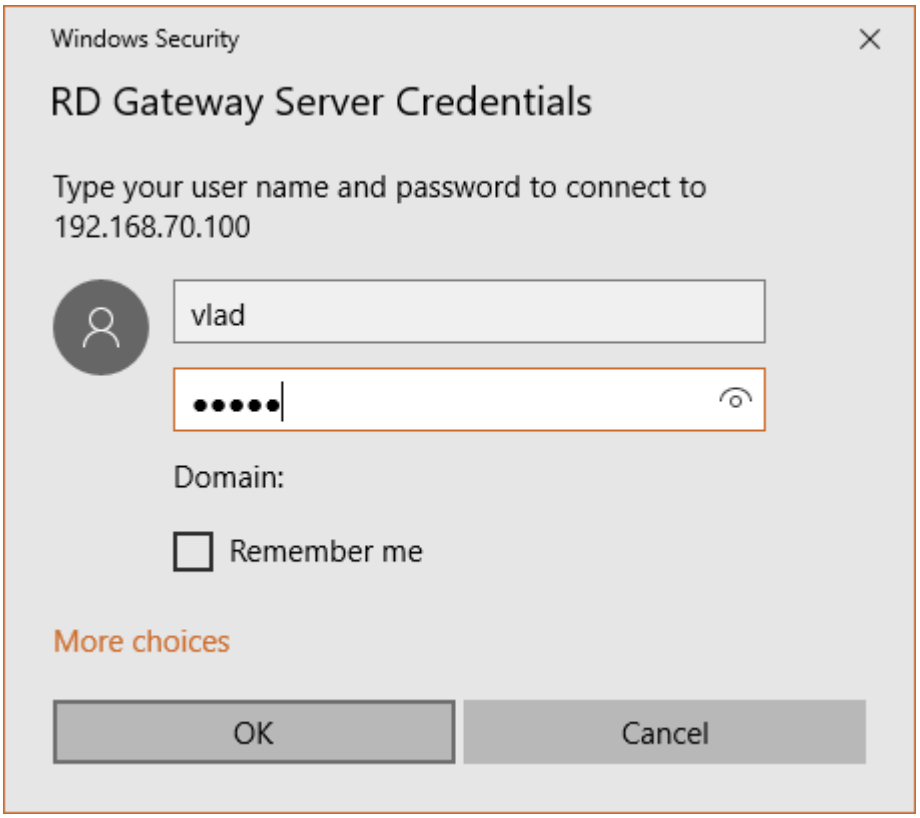
User mapping policy problem. The user is not allowed (based on group membership) to map to the specified remote user

Figure 22: Troubleshooting 6



When user failed to enter domain name into RD Gateway login dialogue (e.g. used only the 'username' part of the credential, mstsc will not try to connect to RD Gateway, so nothing is seen in SPS's log

Figure 23: Troubleshooting 7


Windows Security
RD Gateway Server Credentials
Type your user name and password to connect to 192.168.70.100
vlad
Domain:
Remember me
More choices
OK
Cancel

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product